דוח מבקר המדינה | סייבר ומערכות מידע | התשפ"ג-2022

משרד התחבורה והבטיחות בדרכים

הגנת הסייבר במגזר התחבורה

הגנת הסייבר במגזר התחבורה

רקע

משרד התחבורה והבטיחות בדרכים ממונה על קביעת המדיניות בענף התחבורה וכן על שירותי מערכות התחבורה בים, באוויר וביבשה. מגזר התחבורה כולל גופים מסוגים שונים - ממשלתיים, ציבוריים ופרטיים, הפועלים במגוון תחומים: התחבורה הימית, התחבורה היבשתית, התחבורה האווירית, התחבורה הציבורית, התשתיות התחבורתיות והתחבורה החכמה.

בשנים האחרונות קיימת עלייה חדה במספרם ובחומרתם של אירועי סייבר המשבשים את פעילותם התקינה של ארגונים בארץ ובעולם. בתחום התחבורה קיימים סיכונים רבים שעלולים להתממש כתוצאה מפגיעות במרחב הסייבר: פגיעה בתשתיות התחבורה ובאמצעי תחבורה המוניים שעשויה לגרום לפגיעה בחיי אדם, להפסקת תהליכי ייצור, לנזק כלכלי כבד, לדלף מידע אישי, לפגיעה במוניטין של הארגון הנפגע ובמקרים מסוימים אף להשלכות פוטנציאליות במישור הביטחוני.

החלטת ממשלה 2443 משנת 2015 הטילה על משרדי הממשלה, ובכללם משרד התחבורה, לקדם את הטיפול בהיערכות לאיומי סייבר במגזר שבו הם פועלים. במסגרת זו הוקם אגף הסייבר במשרד התחבורה שמנחה את הגופים במגזר, למעט גופים שמוגדרים כתשתיות מדינה קריטיות (תמ"ק) שמונחים ישירות על ידי מערך הסייבר.

מאסדרים מגזריים יכולים לחייב גופים שמונחים על ידם לעמוד בדרישות סייבר בכמה אופנים: חוקים, תקנות, התניית מתן רישיון בעמידה בדרישות סייבר, מתן הנחיות והכללת דרישות סייבר במסגרת ההתקשרויות. משרד התחבורה הנחה את הגופים במגזר לעמוד בדרישות הסייבר שנכללו במסגרת המדיניות להגנת הסייבר.

להלן תרשים המתאר את תחומי הפעילות במגזר התחבורה:

נתוני מפתח

28,000	4 מתוך 5	6 מתוך 30	7 שנים
מספר הגופים הפועלים במגזר התחבורה, לרבות בתחום הרכב הפרטי, התשתיות, התחבורה הציבורית, התעופה והים	דירוג האיום על הפרטיות שקבעה הרשות להגנת הפרטיות בנוגע לתחום התחבורה	20% מהגופים שמוגדרים כתשתיות מדינה קריטיות ומחזיקים במערכות ממוחשבות חיוניות שייכים למגזר התחבורה	משך העיכוב בחקיקת חוק הסייבר, שטרם הושלם, ביחס לנדרש בהחלטת ממשלה 2444 משנת 2015

36 מיליארד ש"ח	6.3 מיליון ש"ח	21 מתוך 35	0%
תקציב הפיתוח של משרד התחבורה לשנת 2022	התקציב שאושר לאגף הסייבר מתוך סך הדרישות שהגיש בסך 30 מיליון ש"ח (21%) נכון לדצמבר 2021	60% מהגופים שמתוכננים להתחבר למרכז ניטור אירועי אבטחת מידע מגזרי (SOC) לא חוברו אליו עד מועד סיום הביקורת	שיעור הגופים שביצעו מבדקי חֲדִירוּת לאיתור פרצות אבטחה במערכות בתחום התחבורה בשנים 2019 - 2021 (0 מתוך 8 גופים שנבדקו בביקורת)

פעולות הביקורת

בחודשים מרץ 2021 עד אפריל 2022 בדק משרד מבקר המדינה את הגנת הסייבר במגזר התחבורה. הביקורת נעשתה במשרד התחבורה - באגף הסייבר ובמחלקת הייעוץ המשפטי; במערך הסייבר הלאומי במשרד ראש הממשלה - באגף להכוונה מגזרית וביחידה להנחיית גופי תמ"ק (אגף תמ"ק); וברשות להגנת הפרטיות במשרד המשפטים. בדיקות השלמה נעשו בכמה חברות ממשלתיות, וביחידות הגנת הסייבר המגזריות במשרד האנרגיה, במשרד להגנת הסביבה, במשרד התקשורת ובמשרד הבריאות.

במסגרת הביקורת, משרד מבקר המדינה ביצע בשיתוף עירייה א' מהלך חדשני - מבדק חדירה במערכות בתחום התחבורה שלה כדי לבחון היבטים בהגנת הסייבר.

כמו כן המשרד הפיץ בקרב עשר עיריות ושתי חברות ממשלתיות שאלון הבודק את היבטי הגנת הסייבר בנוגע למערכות בתחום התחבורה כדי לבחון את הנושאים ברמה המערכתית.

הדוח שבנדון הומצא לראש הממשלה ביום 31/7/22 והוטל עליו חיסיון עד לדיון בוועדת המשנה של הוועדה לענייני ביקורת המדינה. מתוקף הסמכות הנתונה למבקר המדינה בסעיף 17(ג) לחוק מבקר המדינה, התשי"ח-1958 [נוסח משולב], ובשים לב לנימוקי הממשלה, לאחר היוועצות עם הגופים האמונים על אבטחת המידע הביטחוני ובתיאום עם יו"ר הכנסת, משלא התכנסה ועדת המשנה האמורה, הוחלט לפרסם דוח זה תוך הטלת חיסיון על חלקים ממנו. חלקים אלה לא יונחו על שולחן הכנסת ולא יפורסמו.

ממצאי דוח הביקורת והמלצותיו נכונים למועד המצאתו האמור לעיל.

תמונת המצב העולה מן הביקורת

- **אסדרה ברמת חקיקה ראשית** - נכון למועד סיום הביקורת באפריל 2022, לא הושלמה חקיקת חוק הסייבר, וזאת יותר משבע שנים ממועד החלטת הממשלה 2444, וכן אסדרת תחום הסייבר לא הושלמה במסגרת עבודת הצוות הבין-משרדי שהוקם באוגוסט 2021. נוכח זאת כל מאסדר, נדרש לפעול באופן עצמאי ולבצע תיקונים בחוקים ובתקנות שלו כדי ליישם את דרישות הסייבר במגזר שלו, בכלל זה משרד התחבורה.

- **הכנסת דרישות סייבר לתקנות ולחוקים במגזר התחבורה** - במשך יותר משבע שנים לא השלים משרד התחבורה את עבודת המטה לבחינת התיקונים והשינויים הנדרשים לאסדרה בתחומי פעילותו למימוש אפקטיבי של האחריות להגנת הסייבר במגזר. משרד התחבורה בחר להמתין לאסדרה במסגרת חוק הסייבר, למעט בתחום הרכב האוטונומי שהוא נושא אחד מיני רבים, זאת שעה שעלו עיכובים בחקיקתו. במצב זה חסרים למשרד התחבורה כלים לאכוף על הגופים במגזר (בהם מפעילי תחבורה ציבורית, נמלי ים וחברות תעופה) את דרישות הסייבר שקבע במסגרת המדיניות להגנת הסייבר במגזר.

- **הכנסת דרישות סייבר להתקשרויות עם מפעילים בתחום התחבורה** - משרד התחבורה החל בספטמבר 2021 בהכנסת נספחי סייבר מחייבים בהתקשרויות חדשות בתחומי התשתיות היבשתיות, אולם עדיין ישנם תחומים בהם המשרד אינו מחייב לכלול דרישות סייבר בהתקשרויות חדשות. יודגש כי בתחומי פעילותו של המשרד חלק מההסכמים נחתמים לתקופה ארוכה, כאשר בהסכמים שנחתמו בעבר אין דרישות סייבר. למשל: נמלים - זיכיון ל-25 שנים; הפעלת אשכולות תחבורה ציבורית - 10 שנים. עוד עלה כי למשרד אין מיפוי מרוכז של ההתקשרויות הקיימות לרבות מועד סיומן, וממילא אין בידו רישום אם קיימות בחוזים אלה דרישות סייבר. נוכח זאת קיים סיכון שגם ההתקשרויות שצפויות להסתיים בשנים הקרובות יוארכו, מבלי שיתווספו להן דרישות סייבר במסגרת הארכתן וחידושן.

- **ביקורות לבחינת מצב הגנת הסייבר בגופי תחבורה גדולים שביצע משרד התחבורה** - בשנת 2021 ביצע משרד התחבורה ביקורות כדי לבחון את מידת עמידת חלק

מהגופים בדרישות הסייבר שפרסם במסגרת המדיניות להגנת הסייבר במגזר. הביקורות בוצעו על חברות בתחומים שונים ובהן חברות תחבורה ציבורית, חברות תשתיות כבישים, ונמלי ים. בביקורות נמצאו שורה של ליקויים רוחביים המחייבים טיפול מערכתי, אך המשרד לא ביצע מעקב אחר תיקון הליקויים שמצא בביקורות אלו.

משאבי אגף הסייבר - משאבי כוח האדם והתקציב הדרושים לטובת מימוש אחריות של משרד התחבורה בתחום הסייבר במגזר אינם מספיקים (למשל: באגף מועסקים שלושה עובדים במקום חמישה, ואושרו לו 6.3 מיליון ש"ח (21%) מהתקציב שהאגף ביקש לצורך מימוש תפקידו), כך שהוא אינו יכול לתת מענה לחלק מהאיומים הניצבים בפניו. בשל היעדר המשאבים נמצאו משימות של אגף הסייבר שלא בוצעו, ובהן: בניית יכולת התערבות באירועי סייבר; פעילויות להעלאת החוסן במגזר; הרחבת הביקורות בגופי המגזר; וליווי הגופים בתיקון ליקויים חמורים.

גיבוש תמונת מצב מגזרית - משרד התחבורה אחראי לקדם את הטיפול בהיערכות לאיומי הסייבר של כל המגזר, אולם הוא מתקשה במילוי תפקידו מהסיבות האלו: המשרד אינו רואה את התמונה המגזרית כולה על תתי-המגזרים שבה (למשל תחום התחבורה האווירית וגופי התמ"ק שמנחה מערך הסייבר); הוא אינו רואה את מפת הסיכונים ואת הפערים הקיימים בכל גוף; והוא אינו מקבל מידע חיוני מהגופים על פעילויות שהם עצמם ביצעו, כמו מבדקי חדירות, תוכניות עבודה לתיקון הליקויים, דיווח על אירועי סייבר ותחקירים עליהם שביצע הגוף. כמו כן נמצאו פערים במספר אירועי הסייבר שדווחו למאסדרים השונים.

מרכז לניטור אירועי אבטחת מידע (SOC מגזרי) - 21 מתוך 35 מהגופים שמתוכננים להיות מחוברים ל-SOC המגזרי שהקים משרד התחבורה לא חוברו אליו עד מועד סיום הביקורת ולא נקבעה תוכנית עבודה מפורטת לחיבור ולמבצוע של כלל הגופים. כן עלה כי ההתקשרות הנוכחית של משרד התחבורה עם רש"ת בנוגע להפעלת ה-SOC נחתמה לשנה אחת בלבד ואינה נותנת מענה מלא לארגונים גדולים.

שיתוף מידע - נמצא כי שיתוף המידע בתחום הסייבר בין גופים דומים (כמו למשל נמלי הים ומערכות בתחום התחבורה) הוא חלקי. כן נמצא כי לא קיימת תבנית לצורך פרסום מכרזים בתחום הסייבר לשימוש הגופים במגזר.

הנחיית מערכות בתחום התחבורה - מערכת תחבורה עירונית אחראית על התחבורה בתחום השיפוט של העיר שבה היא פועלת. בסקר שערך משרד מבקר המדינה בעשר עיריות ובשתי חברות עלו פערים מהותיים בין מצב הגנת הסייבר של המערכות לבין דרישות הסייבר של משרד התחבורה. כן עלה כי כל המערכות בתחום התחבורה (למעט המערכות המופעלות על ידי חברות התשתית ועירייה א') אינן מונחות על ידי משרד הפנים או משרד התחבורה, אף שיש כאלו שפגיעה בהן עשויה לגרום לפגיעה כלכלית ניכרת ואף לפגיעה בחיי אדם.

מבדקי חדירה וסקרי סיכונים על מערכות בתחום התחבורה - מתוצאות שאלון בנושא הגנת הסייבר, שהועבר לגופים המחזיקים מערכות בתחום התחבורה העירונית והבין עירונית, עלה כי בשנים 2019 - 2021 אף אחד מהגופים שנבדקו לא ביצע מבדקי חדירה, וכי 75% מהגופים שנבדקו לא ביצעו סקרי סיכונים.

התאוששות עסקית, סביבת בדיקות וניטור - מתוצאות שאלון בנושא הגנת הסייבר על מערכות בתחום התחבורה עלה כי בשנים 2019 - 2021 בחלק מהגופים שנבדקו לא קיימת תוכנית להתאוששות עסקית להתמודדות עם אירועי אסון ובהם אירועי סייבר. כן נמצא כי בחלק גדול מהגופים שנבדקו אין סביבת בדיקות שבה נבדקים עדכוני תוכנה ואבטחה קודם התקנתם. כן נמצא כי בחלק גדול מהגופים שנבדקו אין חיבור למערכת בקרה מסוימת.

מבדק חדירה במערכות בתחום התחבורה בעירייה א' - במסגרת מבדק החדירה שבוצע כחלק מהביקורת, נבדקו כל הנושאים האלה ובחלקם נמצאו ליקויים: ניהול משתמשים והרשאות; תיעוד וניטור; בקרת גישה לרשת; הגנת עמדות ושרתים; סגמנטציה ובקרת זרימה; עדכניות התוכנה ואבטחת הגישה לרשת התקשורת.

משרד מבקר המדינה מציין לחיוב את שיתוף הפעולה מצד עירייה א' בכל שלבי מבדק החדירה: החל בתכנונו, דרך ביצועו, תהליך הצגת הממצאים, הנכונות לשפר את התהליכים הקיימים, וכלה בטיפול בחלק מהליקויים שנמצאו בזמן קצר ביותר.

משרד מבקר המדינה מציין לחיוב את הפעילות שביצע משרד התחבורה בתחום הרכב האוטונומי, לרבות תיקון החוק, פרסום הנוהל והקמת מרכז הניסויים בבאר שבע. עם זאת, משרד התחבורה טרם החל בביצוע ביקורות בתחום זה. במהלך הביקורת חל שיפור בכמה תחומים שבהם פועל אגף הסייבר במשרד התחבורה, ובהם הקמת SOC מגזרי, פרסום מדיניות וביצוע ביקורות בחלק מהגופים המונחים לבחינת עמידת הגופים בה.

עיקרי המלצות הביקורת

על מערך הסייבר להשלים את התהליך הנדרש לצורך חקיקת חוק הסייבר. נושא זה רלוונטי לכלל המגזרים, לכן מוצע כי מערך הסייבר יפעל יחד עם הצוות הבין-משרדי להשלמת בחינת אסדרת תחום הסייבר וידון גם בצורך בהכנסת אסדרה רוחבית שתיתן מענה לכלל המגזרים בתחום הסייבר.

מומלץ כי משרד התחבורה ייזום תיקון לחוקים ולתקנות ויגדיר סדר עדיפות להתחלת הפעילות בתחום תוך מתן עדיפות לתחומים שבהם מוקמים פרויקטים חדשים רחבי היקף ותחומים שבהם יש סיכוני סייבר רבים ומצב ההגנה הנוכחי של הגופים אינו מספק להם מענה הולם. כמו כן מוצע כי משרד התחבורה יבחן את האפשרות לעדכן את הזיכיונות, הרישיונות וההתקשרויות הקיימות ולהוסיף להן דרישות מתחום הגנת הסייבר, בפרט לאלו שמסתיימות בקרוב.

מומלץ כי משרד התחבורה, בשיתוף מערך הסייבר והרשות להגנת הפרטיות, יבחן כיצד ניתן להעביר את המידע הרלוונטי ביניהם, לצורך הפקת לקחים מאירועים, נקיטת פעולות להעלאת החוסן של הגופים במגזר וטיוב ההנחיות.

- מומלץ כי משרד התחבורה יבחן את האפשרויות העומדות לפניו להפעלת SOC בצורה קבועה. עוד מומלץ למשרד התחבורה לבחון כיצד לנטר בצורה אפקטיבית גופים גדולים. נוכח העובדה שייקח זמן לחבר את כל הגופים ל-SOC, מוצע למשרד התחבורה לתעדף את הטיפול בגופים שאינם מנוטרים כלל.

- מומלץ כי מערך הסייבר ואגפי הסייבר המגזריים, ובהם אגף הסייבר במשרד התחבורה, יעלו צרכים משותפים בתחום הסייבר לצורך הכנת תבניות שיוכלו לשמש את כלל הגופים במגזר - בין היתר בתחומים האלו: גיוס יועצים; רכש כלים; רכש שירותי התערבות באירועים; הקמה ותפעול של SOC.

- נוכח הממצאים שעלו מהשאלון וממבדק החדירה בנושא הגנת הסייבר במערכות בתחום התחבורה, מומלץ כי משרד הפנים ומשרד התחבורה בשיתוף מערך הסייבר יפעלו יחד להסדרת תחומי האחריות ביניהם ולקביעת נהלים מתאימים כך שנושא הגנת הסייבר במערכות בתחום התחבורה ברשויות המקומיות יקבל את המענה האסדרתי ההולם. זאת על מנת שגורם מנחה יבצע פיקוח ובקרה על תיקון הליקויים ועל הגנת המערכות מפני תקיפות סייבר.

- נוכח הממצאים שעלו מהשאלון, על הגופים שנבדקו לקיים הערכת מצב ולקבוע תוכנית עבודה לתיקון הליקויים. מומלץ כי כלל הרשויות שבהן מותקנות מערכות בתחום התחבורה, יבדקו את מערכותיהן באמצעות סקרי סיכונים ומבדקי חדירה ויפעלו לתקן את הממצאים שבתחומן.

- מומלץ כי עירייה א' תפעל לתקן את הליקויים שעלו במבדק החדירה במערכת בתחום התחבורה.

סוגי הגופים במגזר התחבורה והמאסדרים שלהם בתחום הגנת הסייבר

התחום	מערך הסייבר - אגף תמ"ק	אגף הסייבר במשרד התחבורה
רכבות	רכבת ישראל; נת"ע - הרכבת הקלה בגוש דן	הרכבת הקלה בירושלים; הרכבת הקלה בחיפה - נצרת
תעופה	רשות שדות התעופה; חברות תעופה (שוטף)	חברות תעופה (זמן אמת)
נמלי ים	נמל חיפה; נמל אשדוד; חברת נמלי ישראל	נמל המפרץ; נמל הדרום; נמל אילת
תחבורה ציבורית		חברות אוטובוסים
מרכזי ניהול תנועה		ירושלים; תל אביב; חיפה

הרשות להגנת הפרטיות - הגנת מידע אישי

מצב ההגנה בתחומים שנבדקו במסגרת שאלון על מערכות בתחום התחבורה

תחום	השאלה	שיעור הגופים שבהם נמצא הליקוי
כללי	כתיבת דרישות בתחום הסייבר או אבטחת המידע במכרז לבחירת הספקים	שיעור גבוה
	קיום פורום לשיתוף ידע עם מערכות אחרות בתחום התחבורה	שיעור בינוני
ממשל תאגידי	ביצוע מבדקי חֲדירות לאיתור פרצות אבטחה	שיעור גבוה
	ביצוע סקרי סיכונים	שיעור גבוה
	קיום תוכנית להתאוששות עסקית	שיעור בינוני
	מינוי ועדת היגוי סייבר	שיעור בינוני
	מינוי בעלי תפקידים שאחראים להגנת הסייבר ולאבטחת המידע	שיעור נמוך
	קיום שרתי גיבוי	שיעור נמוך
ארכיטקטורה וטכנולוגיה	קיום סביבת בדיקות, שבה נבדקים היבטי סייבר	שיעור גבוה
	חיבור למערכת אבטחת מידע א'	שיעור גבוה
	חיבור למערכת אבטחת מידע ב'	שיעור גבוה
	התקנת עדכוני אבטחת מידע	שיעור בינוני
	קיום אנטי-וירוס	שיעור נמוך
	מערכות הפעלה ישנות	שיעור נמוך
	קיום חומת אש	שיעור נמוך
תיעוד וניטור	חיבור למרכז בקרה	שיעור גבוה
	קבלת התראה אוטומטית בנושא מסוים	שיעור נמוך
	שמירת לוגים	שיעור נמוך
ניהול משתמשים והרשאות	נושא א' בתחום ניהול המשתמשים וההרשאות	שיעור גבוה
	נוהל להסרת משתמשים	שיעור בינוני
	מנגנון בקרה מסוים	שיעור נמוך
גישה מרחוק	נוהל עבודה לגישה מרחוק של ספקי המערכת	שיעור בינוני
	הקלטה או שמירה של לוג של פעילות הספק בעת החיבור מרחוק	שיעור נמוך

שיעור גבוה | שיעור בינוני | שיעור נמוך

סיכום

תשתיות התחבורה נועדו להבטיח את הבטיחות והיעילות של התחבורה הימית, התחבורה האווירית והתחבורה היבשתית עבור כל משתמשי הדרך. ככל שתשתית מסוימת חיונית יותר לחיי היום-יום של התושבים, כך היא מושכת יותר את התוקפים, וככל שהיא תלויה יותר בממד הסייבר, כך היא פגיעה יותר לתקיפות שעשויות לגרום לשיבושים בתפקודה התקין ואף להשבתתה המלאה, לפגיעה כלכלית ניכרת ולפגיעה בחיי אדם.

ממצאי דוח זה משקפים בעיה מבנית ותפקודית יסודית בכל הנוגע להיערכות של מדינת ישראל לאיומי הסייבר במגזר התחבורה. במהלך הביקורת חל שיפור בכמה תחומים שבהם פועל אגף הסייבר במשרד התחבורה, ובהם: הקמת SOC מגזרי לקבלת תמונת מצב ענפית מלאה, שתאפשר זיהוי מכנה משותף בעת תקיפה וכן תאפשר התרעה מפני חשיפה אפשרית לגופים דומים, שתסייע להם להיערך ולהתגונן; פרסום מדיניות וביצוע ביקורות בחלק מהגופים המונחים לבחינת עמידת הגופים בה; קידום אסדרת תחום הרכב האוטונומי, לרבות תיקון החוק, פרסום נוהל והקמת מרכז הניסויים בבאר שבע. עם זאת עדיין קיימות כמה בעיות יסודיות:

חסרה הסדרת תחומי האחריות והסמכות של מערך הסייבר ומשרד התחבורה בכל הנוגע לגופים שאינם תשתית מדינה קריטיות (תמ"ק); משרד התחבורה אחראי לפעילויות המגזר אולם אין בידיו תמונה מלאה של מצב ההגנה של הגופים בו; היעדר הלימה בין האיומים והמענים להם במגזר כולו לבין המשאבים של משרד התחבורה; היעדר דרישות סייבר בהתקשרויות בחלק ניכר מהפעילויות במגזר והיעדר הקצאת המשאבים הנדרשים לכך על ידי הגופים.

הבעיה התפקודית והמבנית שהועלתה בדוח זה אפשר כי היא רלוונטית למגזרים גדולים נוספים, ולכן טיפול מערכתי בנושאים אלו עשוי לשפר את מוכנות המשק והמגזרים הגדולים הפועלים בו להתמודד עם אירועי סייבר.

במסגרת ביקורת זו בוצע מבדק חדירה על ידי צוות הביקורת במערכות בתחום התחבורה בעירייה א'. חשיבותה של פעולה חדשנית זו, שיושמה לראשונה בדוח ביקורת של משרד מבקר המדינה, הינה בכך שהיא מאפשרת להעריך את מוכנותו האמיתית של הגוף לעמוד בפני התקפות סייבר, באמצעות שימוש בכלים החושפים חולשות אבטחה בסביבת העבודה התפעולית של הגוף ולסייע בכך באופן מעשי וממשי לשיפור רמת ההגנה של הגופים המבוקרים.

על משרד התחבורה ועל מערך הסייבר לוודא כי תשתיות התחבורה, ובפרט התשתיות הקריטיות, מבצעות הערכת סיכונים באופן שוטף ומשפרות את מידת עמידתן בפני מתקפות סייבר אפשריות.

הגנת הסייבר במגזר התחבורה

מבוא

משרד התחבורה והבטיחות בדרכים (להלן - משרד התחבורה) ממונה על קביעת המדיניות בענף התחבורה וכן על שירותי מערכות התחבורה בים, באוויר וביבשה. המשרד אחראי לתכנון, פיתוח והסדרה של תשתיות ומערכות תחבורתיות תוך שמירה על הבטיחות שלהן. בשנת 2022 תקציב פיתוח התחבורה הוא כ-36 מיליארד ש"ח.

מגזר התחבורה הוא מגזר-על הכולל גופים מסוגים שונים - ממשלתיים, ציבוריים ופרטיים, הפועלים במגוון תחומים: התחבורה הימית, התחבורה היבשתית, התחבורה האווירית, התחבורה הציבורית, התשתיות התחבורתיות והתחבורה החכמה (להלן - הגופים). כמו כן חלק מהגופים מוגדרים כתשתיות מדינה קריטיות (להלן - גופי תמ"ק) ובהם רכבת ישראל בע"מ (להלן - רכבת ישראל) וחלק מנמלי הים: חברת נמל אשדוד בע"מ (להלן - נמל אשדוד) וחברת נמל חיפה בע"מ (להלן - נמל חיפה). במשרד התחבורה פועלות כמה רשויות האחראיות לתחומי פעילות שונים, ובהן רשות התעופה האזרחית (להלן - רת"א); רשות הספנות והנמלים והרשות הארצית לתחבורה ציבורית.

תרשים 1: **תחומי הפעילות במגזר התחבורה**

על פי נתוני משרד התחבורה, בעיבוד משרד מבקר המדינה.

במגזר התחבורה פועלים אלפי גופים בתחומים השונים. להלן הפירוט:

תרשים 2: **מספר הגופים הפועלים במגזר התחבורה**

תחום פעילות	רכב	תשתיות	תחבורה ציבורית	תעופה	ספנות ונמלים
מספר גופים	28000~	13	21	4	11
גופים לדוגמא	יבואני רכב מכוני רישוי מוסכים חברות ליסינג	נתיבי ישראל חוצה ישראל מנהרות הכרמל הנתיב המהיר נתיבי היובל	אגד דן מטרופולין סופרבוס קוים	אל על ישראייר ארקיע קאל	חברת נמלי ישראל נמל מספנות ישראל נמל חיפה נמל אשדוד נמל אילת

על פי נתוני משרד התחבורה, בעיבוד משרד מבקר המדינה.

מרחב הסייבר, הכולל מחשוב, תקשורת מחשבים ומערכות מידע ממוחשבות, הוא חלק אינטגרלי ממרקם החיים שלנו. אנו משתמשים במרחב הסייבר כמעט בכל שירות ציבורי ופרטי שאנו צורכים וכך גם בשירותי התחבורה. התלות הגוברת במרחב הסייבר מביאה עימה חדשנות טכנולוגית ופיתוחים לאדם ולסביבתו. לצד היתרונות שמאפשרות המערכות הממוחשבות, הן יצרו גם איום חדש העשוי להשפיע על הרציפות התפקודית הארגונית, על השלמות והאמינות של התהליכים העסקיים המתרחשים בארגון ואף לפגוע בסודיות המידע המוחזק בארגון. ככל שהטכנולוגיה מתקדמת ומתפתחת, כך גדלה מידת החשיפה לאיום זה.

איום סייבר הוא צירוף של כוונות ויכולות לתקיפה במרחב הסייבר שטרם התממש. אירוע סייבר הוא התרחשות אשר מעידה על פגיעה אפשרית בפעילותה התקינה של מערכת מחשוב, שקיים יסוד להניח כי היא נובעת מפעילות מכוונת במרחב הסייבר. אירועים אלו מבוססים על ניצול פגיעות או חולשה של הארגון, העלול לפגוע בו ברמות חומרה שונות.

בשנים האחרונות קיימת עלייה חדה במספרם ובחומרתם של אירועי סייבר המשבשים את פעילותם התקינה של ארגונים בארץ ובעולם. כך לדוגמה, בשנת 2020 חלה עלייה של 50% באירועי הסייבר שדווחו למרכז המבצעי של מערך הסייבר הלאומי (להלן - מערך הסייבר), ביחס לשנה שקדמה לה[1]. אירועי סייבר ואבטחת מידע עלולים להיגרם בשוגג או במזיד, על ידי גורם פנימי או חיצוני, ולגרום לפגיעה ניכרת ברציפות התפקודית והעסקית של הארגון, ובמקרים מסוימים אף לגרום לסיכון חיי אדם ולפגיעה בשירות חיוני המאפשר את חופש התנועה. חוסנו של ארגון, עמידותו בפני אירועי סייבר ויכולתו להתמודד איתם, תוך שמירה על רציפות תפקודית, נגזרים מרמת ההיערכות להגנה בסייבר המיושמת בעת שגרה.

1 מתוך סיכום שנת 2020 של מערך הסייבר.

בתחום התחבורה קיימים סיכונים רבים שעלולים להתממש כתוצאה מפגיעות במרחב הסייבר: פגיעה בתשתיות התחבורה ובאמצעי תחבורה המוניים שעשויה לגרום לפגיעה בחיי אדם, להפסקת תהליכי ייצור, לנזק כלכלי כבד, לדלף מידע אישי, לפגיעה במוניטין של הארגון הנפגע ובמקרים מסוימים אף להשלכות פוטנציאליות במישור הבטחוני. בשנים האחרונות מוקמים במגזר התחבורה פרויקטים רבי משאבים, כמו פרויקט הרכבת הקלה במטרופולין תל אביב והקמת נמלי הים החדשים, שבהם נדרשת התייחסות להיבטים של הגנת הסייבר. להלן הסיכונים העיקריים הנשקפים למגזר התחבורה:

תרשים 3: **מפת הסיכונים הנשקפים למגזר התחבורה**

- פגיעה בחיי אדם או בבריאותו (תאונות, שינוע חומרים מסוכנים)
- פגיעה בשירות חיוני לציבור המאפשר את חופש התנועה
- גרימת נזק כלכלי ניכר למדינה
- פגיעה בפרטיות - פריצה למידע אישי, פגיעה כלכלית ופגיעה במוניטין של הארגון
- פגיעה באמון הציבור
- פגיעה בסדר הציבורי

בשנים האחרונות התרחשו בעולם כמה אירועי סייבר שהסבו נזקים ניכרים בתחום התחבורה. להלן כמה דוגמאות:

לוח 1: **דוגמאות לאירועי סייבר, בשנים האחרונות, בתחום התחבורה בעולם**

התאריך	האירוע	הנזק
ינואר 2022	מתקפת סייבר השביתה חלקית את מערכות המחשוב של חברה העוסקת בהפעלת מסוף מטענים ומחסנים בתחום הסחר הימי בישראל למשך עשרה ימים.	נזק כלכלי ניכר
אוקטובר 2021	קבוצת האקרים איראנית תקפה שרתי חברת אחסון אתרים ישראלית. בעקבות התקיפה הושבתו, בין היתר, שני אתרי חברות המפעילות קווי אוטובוסים לתחבורה ציבורית בארץ.	פגיעה בשירות חיוני לציבור
יולי 2021	מתקפת סייבר על מערך הרכבות באיראן גרמה לעיכובים ולביטולים של מאות קווי רכבת.	פגיעה בשירות חיוני לציבור
מאי 2021	פריצה למחשביה של חברת תעופה בהודו חשפה פרטים אישיים של 4.5 מיליון נוסעים, ובכלל זה שמות, תאריכי לידה, פרטי יצירת קשר ומידע לגבי דרכונים, פרטי מועדון הנוסע המתמיד ופרטי כרטיסי אשראי.	פגיעה בפרטיות - דלף מידע אישי
יולי 2017	מתקפת סייבר מסוג נוזקת כופר שבוצעה נגד חברת ספנות בין-לאומית גרמה נזקים הנאמדים ב-200 עד 300 מיליון דולר.	נזק כלכלי ניכר

פעולות הביקורת

בחודשים מרץ 2021 עד אפריל 2022 בדק משרד מבקר המדינה את הגנת הסייבר במגזר התחבורה. הביקורת נעשתה במשרד התחבורה - באגף הסייבר (להלן - אגף הסייבר) ובמחלקת הייעוץ המשפטי; במערך הסייבר הלאומי במשרד ראש הממשלה - באגף להכוונה מגזרית וביחידה להנחיית גופי תמ"ק (להלן - אגף תמ"ק); וברשות להגנת הפרטיות במשרד המשפטים. בדיקות השלמה נעשו בכמה חברות ממשלתיות, וביחידות הגנת הסייבר המגזריות במשרד האנרגיה, במשרד להגנת הסביבה, במשרד התקשורת ובמשרד הבריאות.

במסגרת הביקורת, משרד מבקר המדינה ביצע בשיתוף עירייה א' מהלך חדשני - מבדק חדירה במערכת בתחום התחבורה שלה כדי לבחון היבטים בהגנת הסייבר. כמו כן המשרד הפיץ לעשר עיריות ולשתי חברות ממשלתיות שאלון הבודק את היבטי הגנת הסייבר בנוגע למערכות בתחום התחבורה כדי לבחון את הנושאים ברמה המערכתית.

הדוח שבנדון הומצא לראש הממשלה ביום 31/7/22 והוטל עליו חיסיון עד לדיון בוועדת המשנה של הוועדה לענייני ביקורת המדינה. מתוקף הסמכות הנתונה למבקר המדינה בסעיף 17(ג) לחוק מבקר המדינה, התשי"ח-1958 [נוסח משולב] ובשים לב לנימוקי הממשלה, לאחר היוועצות עם הגופים האמונים על אבטחת המידע הביטחוני ובתיאום עם יו"ר הכנסת, משלא התכנסה ועדת המשנה האמורה, הוחלט לפרסם דוח זה תוך הטלת חיסיון על חלקים ממנו. חלקים אלה לא יונחו על שולחן הכנסת ולא יפורסמו.

ממצאי דוח הביקורת והמלצותיו נכונים למועד המצאתו האמור לעיל.

אסדרת תחום הגנת הסייבר

אופן האסדרה בתחום הגנת הסייבר בכלל ובמגזר התחבורה בפרט נקבע במסגרת שורה של חוקים והחלטות ממשלה שהתקבלו משנת 2002. להלן תרשים המתאר את החוקים ואת החלטות הממשלה המרכזיות שהתקבלו בתחום זה ואת הנושאים העיקריים שנכללו בהם:

תרשים 4: **אבני הדרך המרכזיות בתחום אסדרת הגנת הסייבר**

2002
החלטה ב/84

- החלטה מסדירה את התבחינים להגדרת גוף תמ"ק - גוף עם מערכות מחשוב חיוניות שהפגיעה בהן עלולה לגרום לנזק פיזי או כלכלי משמעותי מאוד, לפגיעה בחיי אדם או לפגיעה באספקת שירות ציבורי. כמו כן ההחלטה מסדירה את אופן ההכנסה של גוף חדש לתוספת של החוק להסדרת הביטחון ואת אופן ההסרה של גוף קיים.

2005
החוק להסדרת הביטחון בגופים ציבוריים

- החוק המקורי משנת 1998 עסק בנושאי ביטחון פיזי. בשנת 2005 תוקן החוק וטיפל לראשונה גם באבטחת מערכות ממוחשבות חיוניות, ובמסגרתו הוגדרו גופים אזרחיים כגופי תמ"ק, ואלו הונחו ישירות באמצעות שירות הביטחון הכללי.

2011
החלטת ממשלה 3611

- הוחלט על הקמת המטה הקיברנטי הלאומי במשרד ראש הממשלה, ועליו הוטל לקדם היערכות לאומית להגנת הסייבר ובכלל זה לגבש תפיסת הגנה לאומית במרחב הסייבר.

2015
החלטת ממשלה 2443

- ההחלטה הטילה על המנכ"לים של משרדי הממשלה שבמסגרתם מופעלות סמכויות אסדרה כלפי גופים או פעילויות החשופים לאיומי סייבר, לקדם את הטיפול בהיערכות לאיומי סייבר במסגרת המגזר שבו הם פועלים.
- בהחלטה הוגדר הייעוד של יחידות הסייבר המגזריות במשרדי הממשלה.
- בעקבות ההחלטה, בשנת 2015 הוקם במשרד התחבורה אגף הסייבר, אשר אחראי להנחיית כל גופי התחבורה למעט גופי תמ"ק.

2015
החלטת ממשלה 2444

- הוחלט להקים רשות לאומית להגנת הסייבר (כיום - מערך הסייבר) שבין תפקידיה לבנות ולחזק את החוסן של כלל המשק בסייבר באמצעות היערכות, כשירות ואסדרה.
- נקבע כי על המערך ועל הלשכה המשפטית במשרד ראש הממשלה בשיתוף משרד המשפטים להכין תזכיר חוק הגנת הסייבר ולהביאו לאישור ראש הממשלה בתוך חצי שנה מיום קבלת ההחלטה.

2016
תיקון החוק להסדרת הביטחון בגופים ציבוריים

- הועברה האחריות לטיפול בגופי תמ"ק, בהיבטי אבטחת מערכות ממוחשבות חיוניות, של מרבית הגופים האזרחיים מאחריות שירות הביטחון הכללי לאחריות מערך הסייבר. האחריות על גופי התקשורת נותרה בשירות הביטחון הכללי.
- עם השנים הוגדרו בתוספת החמישית לחוק ששה גופים במגזר התחבורה: רכבת ישראל, רשות שדות התעופה, נמל אשדוד, נמל חיפה, נתיבי תחבורה עירוניים (נת"ע) וחברת נמלי ישראל (חנ"י).

המאסדרים בתחום

היחידה להנחיית גופי תמ"ק במערך הסייבר: בשנת 2016, במסגרת מימוש החלטות הממשלה בדבר גורם לאומי בתחום הגנת הסייבר, עודכן החוק להסדרת הביטחון בגופים ציבוריים, התשנ"ח-1998 (להלן - החוק להסדרת הביטחון), והאחריות להנחיית מרבית גופי התמ"ק הועברה משירות הביטחון הכללי (השב"כ) למערך הסייבר הלאומי[2]. בהתאם לכך מנחה אגף תמ"ק במערך הסייבר הלאומי את גופי התמ"ק המופיעים בתוספת החמישית לחוק. נכון לחודש אפריל 2022 בתוספת זו מנויים 29 סעיפים ובהם 30 גופים, שישה מהם (20%) שייכים למגזר התחבורה: רכבת ישראל, רשות שדות התעופה (להלן - רש"ת), נמל אשדוד, נמל חיפה, חברת נתיבי תחבורה עירוניים (להלן - נת"ע) וחברת נמלי ישראל (להלן - חנ"י).

אגף תמ"ק מנחה באופן ישיר את גופי התמ"ק, והוא אחראי ללוות את הגוף באופן שוטף ולסייע לו בפעולות האלו: בניית תוכנית העבודה השנתית בתחום הגנת הסייבר ומעקב אחר ביצועה; ויישום תורת ההגנה הייעודית לגופי תמ"ק ופיקוח על אופן יישומה באמצעות ביצוע ביקורות ובהן בדיקות חדירה. כמו כן אגף תמ"ק מלווה את גוף התמ"ק ומסייע לו כשיש חשש לאירוע סייבר.

2 גופי התקשורת נותרו באחריות השב"כ. רשימת הגופים והאחריות עליהם מוגדרת בחוק להסדרת הביטחון בגופים ציבוריים, התשמ"ח-1998.

היחידה להכוונת גופים מגזריים במערך הסייבר: בהחלטת הממשלה 2443 מפברואר 2015 (להלן - החלטה 2443) נקבעה תפיסת אסדרה לאומית שמטרתה העלאה שיטתית ורציפה של רמת ההגנה במרחב הסייבר הכולל במדינה (המרחב האזרחי והמרחב הביטחוני). במסגרת ההחלטה הוקם במערך הסייבר האגף להכוונה מגזרית שאחראי להנחיה מקצועית ישירה של יחידות הסייבר המגזריות במשרדי הממשלה, ואלו אחראיות להכוונה ולהנחיה של כל הגופים הכפופים לסמכויות האסדרה של אותו המשרד. כך שלמעשה, מערך הסייבר מנחה בעקיפין את כלל הגופים שאינם מוגדרים כתמ"ק וכפופים לסמכויות אסדרה באמצעות אגפי הסייבר המגזריים.

היחידות המגזריות להכוונת הסייבר: החלטה 2443 הגדירה את תפקידי יחידות הסייבר המגזריות כמפורט להלן:

1. הכוונה והנחיה בהיבטי הגנת הסייבר לרבות הגדרת המדיניות ודרישות האסדרה, ליווי מקצועי שוטף ומענה לפניות מקצועיות בהתאם למאפיינים של הגופים אשר ביחס אליהם מתבצעת הפעילות. בנושאים שחל עליהם החוק להסדרת הביטחון ובנושאים שחל עליהם חוק הגנת הפרטיות התשמ"א-1981[3] תתבצע ההנחיה בתיאום עם הגורם המוסמך לפי חוקים אלו, אם הדבר יידרש.

2. בקרת ביצוע הדרישות המקצועיות בהתאם לאסדרה וברמה המקצועית הנדרשת לרבות הכרת הפערים והצורך בהתאמות.

3. בנייה והפעלה של תהליכי שיתוף מידע פנימיים וחיצוניים בתוך המגזר לרבות דיווח על אירועים, איומים, חולשות, פוגענים ונוזקות למרכז הארצי לניהול אירועי סייבר (CERT לאומי) וכן הגדרת הנהלים ושיטות הדיווח בין הגופים במגזר.

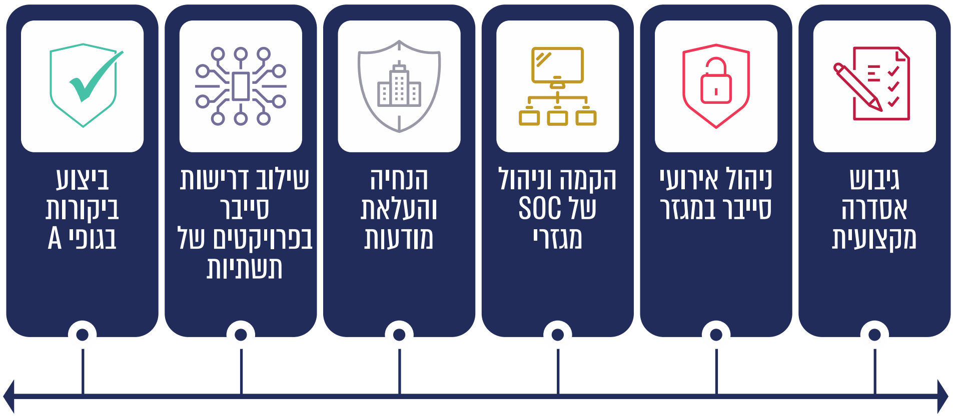
4. ייזום ומימוש של פעילות רוחבית לרבות הקמת תשתיות והפעלת מנגנונים שתכליתם שיפור הגנת הסייבר במגזר.

החלטת ממשלה 2443 הגדירה גם את היקף כוח האדם והתקציב של יחידות הסייבר המגזריות במשרדי הממשלה בהתאם לנזק הפוטנציאלי שצפוי להיגרם כתוצאה מפגיעה במערכות הממוחשבות של הגופים במגזר ובהתאם לקטגוריות האלה: גדול, בינוני וקטן.

בעקבות החלטה 2443 הוקם בשנת 2015 במשרד התחבורה אגף הסייבר. להלן תרשים המסכם את המשימות העיקריות שלו בשנת 2021:

3 בחוק מוגדר "רשם מאגרי המידע", מכוחו ניתנו תפקידים לרשות להגנת הפרטיות בעניין מאגרי המידע.

תרשים 5: **המשימות העיקריות של אגף הסייבר, 2021**



על פי נתוני משרד התחבורה, בעיבוד משרד מבקר המדינה.

הרשות להגנת הפרטיות: הרשות להגנת הפרטיות אחראית על הפיקוח על מילוי הוראות חוק הגנת הפרטיות, והתקנות שהותקנו מכוחו ובהן תקנות הגנת הפרטיות (אבטחת מידע) התשע"ז-2017 (להלן - תקנות אבטחת מידע). בידי הרשות סמכויות אכיפה פליליות וסמכויות אכיפה מינהליות.

במקרים שבהם הרשות להגנת הפרטיות סבורה כי מחזיק מאגר מידע או בעל מאגר מידע הפרו את הוראות החוק או את הוראות התקנות או לא מילאו אחר דרישות שהוצגו לו, היא יכולה להתלות את תוקפו של רישום המאגר לתקופה מסוימת או אף לבטל את רישומו של מאגר המידע בפנקס מאגרי המידע[4]. מאגר שרישומו הותלה הוא מאגר שחל איסור לנהל אותו או להחזיק בו[5]. המשמעות המעשית של הפסקת השימוש במאגר עשויה להיות הפסקת הפעילות העסקית של הגוף או פגיעה בו. סמכות זו מסייעת לרשות לממש את תפקידה ולהבטיח שהגוף יתקן מהר את הנדרש תיקון.

הרשות להגנת הפרטיות מקיימת מדי שנה בשנה סקרי סיכונים במטרה למקד את פעילותה בשנה הבאה במוקדים שבהם הסיכון גבוה ולבנות את תוכנית העבודה באופן שיממש את ייעודה ואת יכולת השפעתה בצורה המיטבית. לקראת השנים 2020 - 2021 קבעה הרשות כי סיכוני הפרטיות בעולם התחבורה מציבים את התחום כאחד מהתחומים שבהם יש להתמקד על בסיס הדירוג הבא: איום - 4 מתוך 5; יכולת התמודדות ואכיפה - 4 מתוך 5; סיכון ממשי - 4 מתוך 5. כן מפרסמת הרשות להגנת הפרטיות מדריכים ומסמכי מדיניות: בשנת 2020 פרסמה הרשות מדריך בנושא "הגנת הפרטיות בגופי תחבורה בסביבה דיגיטלית"; וביולי 2021 פרסמה הרשות מסמך מדיניות בנושא "היבטי פרטיות ביישומונים לתשלום ותיקוף שימוש בשירותי תחבורה ציבורית".

4 חוק הגנת הפרטיות, תשמ"א 1981, סעיף 10(ו).

5 לפי סעיף 10(ב2) לחוק הגנת הפרטיות, זולת אם בית המשפט קבע אחרת.

כלים לאכיפת דרישות סייבר במגזר התחבורה

מאסדרים מגזריים יכולים לחייב גופים שמונחים על ידם לעמוד בדרישות סייבר בכמה אופנים: חוקים, תקנות, התניית מתן רישיון בעמידה בדרישות סייבר, מתן הנחיות והכללת דרישות סייבר במסגרת ההתקשרויות. להלן פירוט הכלים לאכיפת דרישות הסייבר ואופן השימוש של משרד התחבורה בכל כלי על הגופים במגזר:

אסדרה ברמת חקיקה ראשית והשלכות אי-השלמת חקיקת "חוק הסייבר"

בהתאם להחלטת הממשלה 2444 מפברואר 2015, תזכיר חוק הגנת הסייבר היה אמור להיות מובא לאישור ראש הממשלה בתוך כחצי שנה ממועד ההחלטה - באוגוסט 2015, אך הוא הופץ ביוני 2018. בתזכיר נכלל פרק בנושא "אסדרה לאומית בתחום הגנת הסייבר" שבו נקבע, בין היתר, כי רשות מאסדרת שמוסמכת להעניק לארגון היתר או רישיון לפעילות לפי דין, רשאית להתנות את מתן הרישיון או את חידושו בקיום הוראות הנוגעות לתחום הסייבר.

לאחר שמערך הסייבר פרסם את תזכיר חוק הסייבר הוא קיבל הערות מגופים שונים, ובהם מחלקת הייעוץ המשפטי במשרד התחבורה, וקיים דיונים רבים הנוגעים בעיקר לעניין הגדרת הסמכויות והאיזונים הנדרשים. בשנת 2021 הפיץ מערך הסייבר טיוטה נוספת לחוק הסייבר[6], וזאת כהוראת שעה עד לחקיקת חוק הסייבר המלא, אשר נועדה להקנות לו סמכויות לתת הוראות או לפנות לבית המשפט במקרה של סיכון משמעותי להגנת הסייבר. הוראת שעה זו לא עסקה ביחידות הסייבר המגזריות ובסמכויות הרשויות המאסדרות.

יצוין כי באוגוסט 2021 התקבלה החלטת ממשלה 219 בנושא בחינת האסדרה בתחום הסייבר[7]. לפי ההחלטה, יוקם צוות בין-משרדי בראשות משרד ראש הממשלה שיגיש בתוך 180 יום את המלצותיו בנוגע להתאמות הנדרשות להיערכות של מרחב הסייבר האזרחי לאיומי הסייבר לנוכח השינויים באופי ובהיקף של תקיפות הסייבר בשנים האחרונות.

בביקורת עלה כי הצוות שהוקם בעקבות החלטה 219 התכנס לראשונה בפברואר 2022. מסדר הדיונים של הצוות עלה כי הוא דן, בין היתר, בהצגת מאפייני הסיכון של המגזרים השונים במשק, הצגת הסמכויות הקיימות בידי המגזרים בתחום הסייבר והפערים למול המצב הרצוי, וכמו כן בגיבוש חלופות אסדרה. לפי לוח הזמנים המעודכן שקבע, הוא היה צפוי להגיש את המלצותיו עד יוני 2022, אולם נכון ליולי 2022 הוא לא התכנס שנית בתקופה שבין פברואר 2022 ליולי 2022.

---

6 טיוטת חוק הגנת הסייבר ומערך הסייבר הלאומי (סמכויות לצורך חיזוק הגנת הסייבר) (הוראת שעה), התשפ"א-2021.

7 החלטת הממשלה 219, "בחינת רגולציה חכמה בסייבר וכללים והסמכות למתן הנחיות בזמן תקיפת סייבר שעודנה בעיצומה תוך שקילת שיקולים כלכליים" (1.8.21). בהחלטה מובאים העקרונות שלפיהם על חברי הצוות לנהוג בבואם להמליץ על יצירת אסדרה נפרדת לגופים שאינם מנויים בתוספות הרביעית והחמישית לחוק להסדרת הביטחון בגופים ציבוריים, ובכלל זה קביעת הכללים והסמכויות למתן הנחיות הנוגעות להיערכות למתקפת סייבר, או על יצירת כללים וסמכויות למתן הנחיות לעניין תקיפת סייבר שעודנה בעיצומה.

משרד ראש הממשלה מסר בתשובתו מיולי 2022 כי החלטת הממשלה מספר 219 הקימה והתוותה את אופן עבודתו של צוות בין-משרדי לבחינת האסדרה בתחום הסייבר, והגדירה את סוגיות הליבה שבהן אמור הצוות לדון. המשרד הוסיף כי בשל חילופי בעלי תפקידים במערך הסייבר ובמשרד ראש הממשלה במהלך החודשים האחרונים התעכבה עבודת הצוות, ובחודש הקרוב משרד ראש הממשלה יפעל לחידוש דיוני הצוות.

נכון למועד סיום הביקורת, באפריל 2022, לא הושלמה חקיקת חוק הסייבר, וזאת יותר משבע שנים ממועד החלטת הממשלה 2444, וכן אסדרת תחום הסייבר לא הושלמה במסגרת עבודת הצוות הבין-משרדי שהוקם באוגוסט 2021. נוכח זאת כל מאסדר, נדרש לפעול באופן עצמאי ולבצע תיקונים בחוקים ובתקנות שלו כדי ליישם את דרישות הסייבר במגזר שלו, בכלל זה משרד התחבורה (שלא ביצע זאת, כפי שיפורט בהמשך).

על מערך הסייבר להשלים את התהליך הנדרש לצורך חקיקת חוק הסייבר. נושא זה רלוונטי לכלל המגזרים, לכן מוצע כי מערך הסייבר יפעל יחד עם הצוות הבין-משרדי להשלמת בחינת אסדרת תחום הסייבר וידון גם בצורך בהכנסת אסדרה רוחבית שתיתן מענה לכלל המגזרים בתחום הסייבר.

אסדרה ברמת מגזר התחבורה

החלטה 2443 הטילה על משרד התחבורה ומשרדים נוספים לבצע, בתיאום עם מערך הסייבר[8], עבודת מטה שתוגש לראש הממשלה, הבוחנת את התיקונים והשינויים הנדרשים מהבחינה המשפטית למימוש אפקטיבי של האחריות על הגנת הסייבר במגזר.

הרעיון העומד בבסיס החלטה 2443 הוא שהמשרד המאסדר את מכלול הפעילות במגזר הוא המתאים ביותר להסדיר גם את הטיפול בסיכונים הנוגעים למערכות הממוחשבות של הגופים. עם זאת, יחידות הסייבר המגזריות מבססות את פעילות ההנחיה שלהן על סמכויות האסדרה הקיימות בכל משרד ומשרד, אשר מטבען שונות בכל אחד מהמשרדים ומשפיעות גם על אפשרויות ההנחיה, הבקרה, הפיקוח והאכיפה של יחידות אלו.

במצב זה, שבו חקיקת חוק הסייבר לא הושלמה, נתקל משרד התחבורה בקשיים באכיפת דרישות הסייבר, כפי שיפורט בהמשך. יצוין כי משרד האנרגיה[9], המשרד להגנת הסביבה[10]

8 בהחלטה 2443 צוינה היחידה בשם "המטה הקיברנטי הלאומי". בשנת 2017, החליטה הממשלה במסגרת החלטה 3270 לאחד את המטה והרשות הלאומית להגנת הסייבר שהיו קיימות באותה עת, ולקרוא ליחידה החדשה "מערך הסייבר הלאומי".

9 "אמות מידה לרמה, לטיב ולאיכות השירות שנותן ספק שירות חיוני", לפי חוק משק החשמל, התשנ"ו- 1996. באמת מידה 210 ג' 3 נקבע כי יצרן חשמל המקים מתקנים בעלי הספק מותקן מצרפי העולה על 20 מגוואט שלהם מרכז בקרה משותף, יחוייב לעמוד בהנחיות הגנת סייבר כפי שיינתנו על ידי קצין הביטחון במשרד האנרגיה.

10 "תנאים נוספים לעניין ניהול סיכוני סייבר" - התניות נוספות על מתן היתר רעלים, מתוקף סמכות לפי סעיף 3 לחוק החומרים המסוכנים, התשנ"ג-1993.

ומשרד התקשורת[11] פתרו את הנושא באמצעות התניית מתן הרישיונות בעמידה בדרישות הגנת הסייבר על הגופים העיקריים הפועלים במגזרים אלו.

מערך הסייבר מסר בתשובתו מיוני 2022 כי הסמכות להעניק רשיונות כוללת גם סמכות לתת הנחיות לעניין הגנת הסייבר, ומשכך ניתן לראות כי גם משרדים אחרים פועלים בנושא על אף היעדר חוק סייבר ייעודי.

משרד התחבורה מסר למשרד מבקר המדינה ביולי 2021 כי משנת 2018 הוא מסר הערות רבות לתזכיר חוק הסייבר, אולם עד היום הוא לא קיבל את תגובת מערך הסייבר. במשרד הוסיפו כי הם סבורים שאין טעם בכפל אסדרה (כלומר טיפול בנושא במסגרת חוק הסייבר לכשיחוקק ובד בבד טיפול בחוקים נוספים הנוגעים לתחום התחבורה בלבד). עוד מסר המשרד כי נכון יהיה לגבש חוק מתכלל שיבטיח עקביות באסדרה ובפיקוח, וכי לדעתו תיקון חקיקה ספציפי (במגזר התחבורה) חלף תיקון חקיקה כללי (במסגרת חוק הסייבר) עלול להחטיא את העיקר.

יצוין כי בנושא הרכב האוטונומי, שהוא נושא חדשני, בחר משרד התחבורה לעגן את דרישות הסייבר באמצעות חקיקה[12].

ממסמכים שהעביר משרד התחבורה למשרד מבקר המדינה באפריל 2021 עולה כי משרד התחבורה מיפה את הפעילות המאוסדרת במגזר באמצעות אוסף של עשרות חוקים ותקנות. בין תחומים אלו ניתן למנות את רישוי מפעילי התחבורה הציבורית, הפעילות בתחום רשות הספנות והנמלים, הפעילות בתחום התעופה, הפעילות בתחום ההיסעים וההובלה והפעילות בתחום שירותי הרכב. יצוין כי רישוי בתחום התחבורה ניתן בחלק מהמקרים לתקופת זמן ארוכה. למשל: בתחום הנמלים הרישוי להפעלת נמלים הוא ל-25 שנים, והרישוי להפעלת תחבורה ציבורית הוא ל-10 שנים. כמו כן תהליך שינוי תקנות וחקיקה הוא תהליך מורכב שבו שותפים גורמים רבים, ולכן הוא עשוי להימשך כמה חודשים ואף כמה שנים.

עולה כי במשך יותר משבע שנים לא השלים משרד התחבורה את עבודת המטה אשר היה צריך להגיש לראש הממשלה בהתאם להחלטה 2443, לבחינת התיקונים והשינויים הנדרשים לאסדרה בתחומי פעילותו למימוש אפקטיבי של האחריות להגנת הסייבר במגזר. משרד התחבורה בחר להמתין לאסדרה במסגרת חוק הסייבר, למעט בתחום הרכב האוטונומי שהוא נושא אחד מיני רבים, זאת שעה שעלו עיכובים בחקיקתו.

משרד התחבורה החל בפעולות לעגן בחוק (בתחום הרכב האוטונומי) את נושא הסייבר ועליו להמשיך ולפעול לקדם חוקים ותקנות שנמצאים בתחום אחריותו, לצורך מימוש אפקטיבי של האחריות להגנת הסייבר במגזר.

11 במאי 2022 עדכן משרד התקשורת את הרישיונות למתן שירותי תקשורת על ידי הספקים כך שיכללו דרישות הנוגעות להגנת הסייבר.

12 ס' 16יד לפקודת התעבורה [נוסח חדש], התשכ"ב-1961. במרץ 2022 תוקנה פקודת התעבורה כדי להסדיר, בין היתר, את הגנת הסייבר על הפעלה ניסיונית של רכב אוטונומי (עצמאי) ללא נהג.

אסדרה במסגרת הכנסת דרישות סייבר להתקשרויות עם מפעילים בתחום התחבורה

דרישות סייבר יכולות להיות מוטמעות במסגרת חוקים ותקנות שחלים על כל הגופים הכפופים להם או במסגרת התקשרויות עם ספקים. בוועדת היגוי בנושא סייבר שהתקיימה בדצמבר 2020 בראשות מנכ"ל משרד התחבורה דאז נדונו תחומי פעילות שבהם יש פער בין דרישות הסייבר הרצויות לאלו הקיימות בהתקשרות מול ספקי השירות של המשרד. להלן הפירוט:

1. **מכרזי הפעלה של תחבורה ציבורית:** מרבית המכרזים שפורסמו בעבר לא כללו את כלל דרישות הסייבר. עם זאת במכרזי ההפעלה החדשים פרסם אגף הסייבר נספח סייבר. נוכח זאת הנחה מנכ"ל המשרד דאז כי יש לפעול לעדכון הדרישות הקיימות בנספח הסייבר גם במכרזים הישנים ולקדם את השיח עם החברות שזכו במכרזים כדי לנסות ולשלב בהם את הדרישות הנוספות.

2. **תחום הים:** מנהלת אגף הסייבר דיווחה כי היא אינה מכסה את תחום הים מפאת מחסור במשאבים. נוכח זאת הנחה מנכ"ל המשרד לייצר נספחי סייבר עבור חברות הנמל.

במצב הנוכחי שבו חלק מההתקשרויות הקיימות אינן מכילות דרישות סייבר, למשרד התחבורה חסרים כלים רגולטוריים שיאפשרו לו לחזק את הגנת הסייבר. להלן כמה דוגמאות: בתחום התחבורה הציבורית - המשרד לא הוסיף אפשרות להוסיף תנאים ברישיונות למפעילים (הניתנים לעשר שנים) בנושאי מדיניות הגנת סייבר; לגבי תחום הים (בגופים שאינם תמ"ק) - המשרד לא דרש מגופים אלה לגבש נוהל בקרת גישה וניהול חשבונות משתמשים, ולגבש נוהל שימוש בשירותי ענן. בפברואר ומרץ 2022 מסר משרד התחבורה כי לגבי תחומי הרכבה, הרכבות והנמלים - נושאים אלו עדיין מצויים בטיפול מקצועי ולא הושלמו.

במרץ 2022 מסר משרד התחבורה למשרד מבקר המדינה כי נספחי סייבר הוכנו והחל בספטמבר 2021 הם משולבים בהתקשרויות חדשות בתחומי התשתיות היבשתיות[13]. כך למשל ציין משרד התחבורה בתשובתו מיולי 2022 כי בכל המכרזים החדשים להפעלת אשכולות תחבורה ציבורית, ובהסכם ההפעלה החדש המתגבש עם רכבת ישראל, כלולות דרישות סייבר מחמירות.

גם מסקר סיכונים[14] שביצע אגף הביקורת הפנימית במשרד התחבורה בחודשים אוקטובר 2017 עד יוני 2018 נמצא כי לאגף הסייבר במשרד התחבורה אין סמכות חוקית להנחות בנושא את הגופים במגזר, וכי אין לו סמכות אכיפה על כלל הגופים לבצע מהלכים לעמידה בהנחיות. בסקר זה נמצאו בתחום הסייבר 22 סיכונים - כולם ברמת החומרה הגבוהה ביותר.

בדיון ועדת היגוי סייבר במשרד התחבורה שהתקיים באוקטובר 2021 נידון נושא מקור הסמכות והפעילות המשפטית הנדרשת לאסדרת תחום הסייבר במגזר. לצורך "ייצור מקור סמכות

13 נוהל עבודה להטמעת דרישות סייבר בפרויקטים תשתיתיים, תאריך עדכון ספטמבר 2021. הנוהל חל לדוגמה בסלילת כבישים חדשים או מסילות רכבת חדשות המבוצעים באמצעות חברות הביצוע של המשרד.

14 "סקר סיכונים למיפוי נושאים לביקורת באגף ביטחון, חירום וסייבר במשרד התחבורה."

לקביעת דרישות מחייבות בתחום הגנת הסייבר בתחבורה" הנחתה מנכ"לית המשרד את הלשכה המשפטית לפעול בחמש דרכי פעולה:

1. בעדיפות ראשונה ינוצלו כלים קיימים המאפשרים להעמיד דרישות מחייבות בתחום הסייבר, תוך וידוא כי יש יכולת לאכוף אותן.
2. בתחומים שבהם לא ניתן לקבוע דרישות מחייבות בתחום הגנת הסייבר תוצג תוכנית פעולה הכוללת תיקוני חקיקה נדרשים ותיעדוף מדורג לטיפול בהם.
3. ייבחן כיצד ניתן להחיל דרישות על גופים אשר קיבלו רישיונות בלי להמתין שנים עד למועד חידושם, תוך בחינה אם ניתן לשייך את תחום הסייבר לתחום הבטיחות שבו ניתן לקבוע דרישות באופן מיידי לנוכח סיכונים חדשים.
4. ייבחנו מודלים של משרדים מקבילים כמו משרדי האנרגיה, הגנת הסביבה והתקשורת, כדי להיעזר בידע ובניסיון שצברו לביצוע פעולות דומות.
5. תיבחן אפשרות לתיקון חקיקה ראשית אחודה שתספק מענה לכלל המגזרים בתחבורה (התחבורה הימית, האווירית והיבשתית) במקום לתקן כל חוק בנפרד.

עוד הנחתה מנכ"לית משרד התחבורה בדיון זה כי יש לוודא שבכל מכרז חדש מופיע פרק העוסק בדרישות סייבר ברמה מספקת ובבקרה והכוונה של אגף הסייבר במשרד.

משרד התחבורה החל בספטמבר 2021 בהכנסת נספחי סייבר מחייבים בהתקשרויות חדשות בתחומי התשתיות היבשתיות, אולם עדיין ישנם תחומים בהם המשרד אינו מחייב לכלול דרישות סייבר בהתקשרויות חדשות. יודגש כי בתחומי פעילותו של המשרד חלק מההסכמים נחתמים לתקופה ארוכה, כאשר בהסכמים שנחתמו בעבר אין דרישות סייבר. למשל: הפעלת נמלים - זיכיון ל-25 שנים; הפעלת אשכולות תחבורה ציבורית - 10 שנים. עוד עלה כי למשרד אין מיפוי מרוכז של ההתקשרויות הקיימות לרבות מועד סיומן, וממילא אין בידו רישום אם קיימות בחוזים אלה דרישות סייבר. נוכח זאת קיים סיכון שגם ההתקשרויות שצפויות להסתיים בשנים הקרובות יוארכו, מבלי שיתווספו להן דרישות סייבר במסגרת הארכתן וחידושן.

במצב האמור אין למשרד התחבורה סמכות חוקית או חוזית על חלק מהגופים במגזר בנושא הגנת הסייבר, דבר המשפיע על מידת יכולתו של אגף הסייבר במשרד התחבורה לממש את אחריותו ולהעלות את רמת הגנת הסייבר. כמו כן יכולת משרד התחבורה להכניס דרישות סייבר חדשות ברישיונות שכבר ניתנו למפעילים, אף שהרישוי תקף לשנים ארוכות, היא מצומצמת.

מערך הסייבר מסר בתשובתו ביוני 2022 כי יש מקום לבחון את נושא שינוי הרישיונות באמצע תקופתם עם מחלקת ייעוץ וחקיקה במשרד המשפטים, מאחר שמדובר במעין חוזה יחס שאמור להתאים את עצמו לנסיבות משתנות על מנת למנוע מגבלות פורמליות שיגרמו להפקרת נושא הנמלים למשל ל- 25 שנים.

מוצע כי משרד התחבורה יבחן את התיקונים הנדרשים מבחינה משפטית, תוך השלמת מיפוי ההתקשרויות הקיימות של המשרד, כדי לממש בצורה אפקטיבית את אחריותו לטיפול בסיכוני הסייבר במגזר. עוד מומלץ כי המשרד יפעל להטמיע דרישות סייבר במסגרת כל הליך רישוי או חידוש של רישוי שנעשה מול מפעיל. במסגרת זו יש לתת את הדעת על האיומים המתגברים בתחום הסייבר מחד ועל חלון הזמן להכנסת דרישות להגנת סייבר ברישיונות שאמורים להינתן בשנים הקרובות מאידך. בהתאם להנחיית מנכ"לית המשרד, מומלץ כי המשרד יבחן אם ניתן להחיל דרישות על גופים אשר קיבלו רישיונות מבלי להמתין שנים עד למועד חידושם, תוך בחינה אם ניתן לשייך את תחום הסייבר לתחום הבטיחות בו ניתן לקבוע דרישות באופן מיידי לאור סיכונים חדשים.

פרסום מדיניות הגנת הסייבר במגזר התחבורה לצורך אסדרת התחום

רקע

בינואר 2021 פרסם אגף הסייבר במשרד התחבורה מסמך מדיניות להגנת הסייבר במגזר (להלן - המדיניות), במעמד של הוראת מנכ"ל מחייבת. לפי המדיניות, גופי התחבורה שעליהם היא חלה מחויבים לנהוג בהתאם לעקרונות המובאים בה, ובהתאם לנהלים, תקנים והנחיות שיפרטו את העקרונות האלה ויופצו מפעם לפעם על ידי אגף הסייבר או הרשויות המאסדרות הכפופות למשרד. במכתב הנלווה למסמך המדיניות צוין כי לגופים תינתן תקופת התארגנות של שנתיים להטמעת כל עקרונות המדיניות ובקרות התקן שבו בחר הגוף לעמוד (ISO 27001 או תורת ההגנה בסייבר לארגון 2.0 של מערך הסייבר), ובפרק זמן זה יפעל המשרד לצורך עיגון המדיניות בכלי האסדרה.

למדיניות שתי מטרות: הראשונה - להגדיר לגופים את קווי היסוד להגנה על נכסי הסייבר של הארגון כדי לצמצם את הסיכונים לפגיעה בסודיות, בשלמות ובזמינות של נכסים אלה, ולהבטיח רציפות תפקודית של הארגון עצמו ושל מגזר התחבורה בכללותו. המטרה השנייה - להגדיר את ממשקי העבודה וערוצי העדכון והדיווח בין הגופים לבין אגף הסייבר במשרד התחבורה.

במדיניות נקבע כי הגופים יסווגו לשלוש רמות דירוג: A, B, C בהתאם לחומרת הפגיעה האפשרית באינטרס חיוני למדינה כתוצאה מתקיפת סייבר נגדם ובהתאם לחומרת חשיפתם לתקיפה. דירוג זה יתבצע על פי שיטה ותבחינים שקבע מערך הסייבר. ואלה תבחיני הנזק אשר לפיהם מתבצע תהליך דירוג הגופים: הפגיעה בחיי אדם, הנזק הכלכלי, החיוניות לציבור, הפגיעה באמון הציבור, הקריטיות בחירום (תמיכה ביעדי שירות לאומיים), קיומן של חלופות במגזר, ההחזקה בנכסי מידע חיוניים למדינה והבחינה אם הגוף מספק למדינה נכסי סייבר תשתיתיים.

המדיניות חלה על גופים המפוקחים על ידי משרד התחבורה, לרבות זכייני הפעלה של תשתיות שירותי תחבורה, המדורגים ברמה A או B, וכן על החברות הממשלתיות המשמשות זרועות ביצוע

של המשרד. עבור גופים בדירוג C המדיניות משמשת המלצה בלבד. המדיניות אינה חלה על גופי תמ"ק ועל גופים בתחום התעופה האזרחית, המונחים על ידי מערך הסייבר בשיתוף רת"א[15].

להלן סיווג הגופים במגזר התחבורה נכון לחודש פברואר 2022:

תרשים 6: **סיווג הגופים במגזר התחבורה נכון לחודש פברואר 2022**

סיווג	A	B	C	פרויקטים	ללא סמכות רגולטורית	תמ"ק
תשתיות	2 גופים	3 גופים	5 גופים	6 גופים		
תח"צ	7 גופים	5 גופים	6 גופים			
רכבות	1 גוף		2 גופים	1 גוף		3 גופים
ספנות ונמלים	4 גופים		7 גופים			5 גופים
תעופה				1 גוף	4 גופים	1 גוף
ניהול תנועה	3 גופים		2 גופים			

על פי נתוני משרד התחבורה, בעיבוד משרד מבקר המדינה. חלק מהגופים המופיעים בטבלה כתמ"ק עדיין לא מוגדרים בתוספת החמישית לחוק הסדרת הביטחון בגופים ציבוריים, אך מונחים בפועל על ידי מערך הסייבר כגופי תמ"ק.

מערך הסייבר מסר בתשובתו מיוני 2022 כי בשנת 2021 התקבלה החלטה במערך שקביעת הגופים הרגישים תיעשה על ידי המאסדרים, על פי תבחינים של המשרד הרלוונטי ובהתייחס לערכיות הארגון במגזר והרציפות התפקודית, ולא לפי אמות המידה שנקבעו על ידי המערך.

15 בינואר 2022 פורסמה "מדיניות לאומית להגנת סייבר בתעופה אזרחית", בהמשך להחלטה 4814. במדיניות נקבע כי נוסף על מערך הסייבר ורת"א, האחראים לפעילות השוטפת בתחום הסייבר במגזר התעופה, משרד התחבורה יבטיח את אספקת שירותי ה-SOC עבור גופים תעופתיים.

מוצע כי משרד התחבורה יבחן את סיווג הגופים ואת התבחינים לקביעתם לאור ההנחיה המעודכנת של מערך הסייבר המגדירה כי המאסדר הוא הקובע את סיווג הגופים על פי תבחיני המשרד, וכן יעדכן את המדיניות בהתאם.

הפעולות לאכיפת המדיניות

לאחר הפצת טיוטת המדיניות בחודש אוקטובר 2020 נתקל משרד התחבורה בקשיים לאכוף את המדיניות בין היתר מאחר שיישומה מצריך הקצאת תקציב מצד הגופים, שאותו משרד התחבורה אינו מעניק להם בצורה ישירה. להלן דוגמאות:

1. מפעילה א' בתחום התשתיות השיבה למשרד התחבורה על טיוטת המדיניות כי להבנתה בהחלטה 2443 אין כדי לייצר מקור סמכות על פעילות חברה פרטית מאחר שפעילות החברה מוסדרת בכללים ובתנאים המפורטים בתנאי המכרז שפרסמה המדינה.

2. מפעילה ב' בתחום התשתיות, הפועלת באמצעות חוזה מול חברה ממשלתית ג', השיבה למשרד התחבורה על טיוטת המדיניות כי "הפורמט בו אנו מונחים הוגדר כהנחיה וולונטרית ותחת הגדרה זו אנו מתנהלים בשיתוף פעולה שנים מספר, הנחיה חדשה זו משמעותית ונרחבת מהנחיות שהיו בעבר, מבקש לקבל הנחייה זו מבעל החוזה שלי, קרי חברה ממשלתית ג'".

קשיים בהטמעת המדיניות עלו גם מצד גופים המשמשים זרועות ביצוע של המשרד. כך למשל, במכתב מחודש מרץ 2021 הודיעה חברה ז', שסווגה כגוף A במועד הפצת טיוטת המדיניות, למשרד התחבורה כי היא נערכת להטמיע את המדיניות במהלך השנתיים הקרובות, אך מציינת כי קיימים פערים שונים ומשמעותיים בדגש על המשאבים והתקציבים הייעודיים שיש להקצות לנושא ושבלעדיהם לא תוכל לממש אותה. יצוין עוד כי בתשובת חברה ז' למשרד מבקר המדינה מיוני 2022 היא ציינה כי היא פועלת להטמיע את המדיניות שפרסם משרד התחבורה, והיא הגדירה תקציבים ייעודיים למימושה. חברה ז' הוסיפה כי תידרש לכך הקצאת משאבים תקציביים כדי שתתאפשר עמידה מלאה במדיניות.

משרד התחבורה מסר למשרד מבקר המדינה ביולי 2021 כי כל זמן שאין למשרד מקור אסדרתי (סמכות חוקית) לקבוע הנחיות בנושא, הרי שהמדיניות שהופצה אינה מחייבת והיא בגדר המלצה בלבד.

יצוין כי משרד התחבורה עצמו ציין במדיניות כי "המשרד יטמיע את החובה להגנת הסייבר בכלים הרגולטוריים והחוזיים העומדים לרשותו מתוקף החוקים המסדירים את סמכויותיו".

בביקורת עלה כי במצב האסדרה החוקית הנוכחי אין בידי משרד התחבורה כלים להטמיע את המדיניות שקבע ולממש את אחריותו על הגנת הסייבר במגזר התחבורה.

מפעילה א' ומפעילה ב' מסרו בתשובותיהן מיוני 2022 כי כל דרישה נוספת מעבר לתנאי הרישיון תחייב הוראת שינוי וכיסוי העלות הכספית בהתאם.

במהלך שנת 2021 (שנה וחצי לפני המועד הסופי ליישום המדיניות) ביצע אגף הסייבר במשרד התחבורה ביקורות בחלק מגופי A כדי לבחון את מצב הגנת הסייבר שלהם ואת מידת יישום המדיניות החדשה שפרסם. להלן תרשים הממחיש את הסיכונים הפוטנציאליים בגופי תחבורה כתוצאה מאי-עמידה בדרישות המדיניות, ודוגמאות לגופים (שחלקם בעלי רישוי לתקופה ארוכה) שבהם נמצאו הסיכונים במסגרת הביקורות:

תרשים 7: **סיכוני הגנת הסייבר כתוצאה מאי-עמידה בדרישות המדיניות**

בביקורת עלו פערים ביכולת משרד התחבורה לעדכן דרישות סייבר בהתקשרויות ארוכות טווח ולכן בהיעדר כלים רגולטוריים, אין למשרד סמכות להנחות גוף פרטי ללא הסדר חוזי - כך שהמשרד צפוי להתקל בקשיים ביכולת להנחות את הגופים במגזר ולפקח על אופן יישום הנחיותיו. עוד נמצאו פערים בין דרישות הסייבר שהוגדרו במדיניות ובין היכולת ליישמן בחלק מהגופים, בטווח הזמן שנקבע ליישומה ופערים בתחום מוגנות הסייבר בגופי A בהתאם לביקורות שביצע אגף הסייבר משנת 2021.

מוצע כי משרד התחבורה ייזום תיקון לחוקים ולתקנות ויגדיר סדר עדיפות להתחלת הפעילות בתחום תוך מתן עדיפות לתחומים שבהם מוקמים פרויקטים חדשים רחבי היקף; ותחומים שבהם יש סיכוני סייבר רבים ומצב ההגנה הנוכחי של הגופים אינו מספק להם מענה הולם. פעילות זו תעלה בקנה אחד עם פעילות חלק מיחידות הסייבר המגזריות האחרות שהחלו להפעיל את הרישוי רק בחלק מהתחומים בהתאם לניהול סיכונים שביצעו. כמו כן מוצע כי משרד התחבורה יבחן את האפשרות לעדכן את הזיכיונות, הרישיונות וההתקשרויות הקיימות ולהוסיף להן דרישות מתחום הגנת הסייבר, בפרט לאלו שמסתיימות בקרוב.

משרד התחבורה מסר בתשובתו ביולי 2022 כי בגופים שבהם הוסדרה הסמכות של משרד התחבורה, ובהם מפעילות תחבורה ציבורית וחברות הביצוע, מועברים חומרים, ממצאים, בדיקות, סיכומים ועוד. בהיעדר חובה חוקית, אין למשרד סמכות להנחות גוף פרטי ללא הסדר חוזי. משרד התחבורה הוסיף כי הוא מקדם חוק סייבר בתחבורה, שיחיל חובת הנחיה ודיווח על כל דרישות הסייבר של המשרד, של כל הגופים המקבלים רישיון או זיכיון ממנו. אך עד לחקיקת חוק הסייבר בתחבורה המשרד מכניס דרישות סייבר להתקשרויות חדשות עם מפעילים בתחום התחבורה. כך, למשל, בכל המכרזים החדשים להפעלת אשכולות תחבורה ציבורית, ובהסכם ההפעלה החדש המתגבש עם רכבת ישראל, כלולות דרישות סייבר מחמירות. במקביל, המשרד מקיים הליך מול זכיינים קיימים, חלקם משתפים פעולה מרצון. משרד התחבורה הוסיף כי בדיון שהתקיים עם מערך הסייבר, תמך המערך בביצוע "תיקוני חקיקה שיאפשרו (למשרד התחבורה) לבצע בקרה ואכיפה של רמת האבטחה הנדרשת".

תקציב ותקנים

החלטת הממשלה 2443 כללה הנחיות בנושא תקינת כח האדם הנדרשת מהיחידה להנחיית הסייבר המגזרי: במשרד שהוגדר כמשרד "גדול" - למשל משרד התחבורה - נקבע כי נדרשים חמישה עובדים לפי החלוקה הזאת: מנהל, שני עובדים בתחום ההכוונה ושני עובדים בתחום הבקרה.

עוד נקבע בהחלטה כי איוש התפקידים יבוצע באמצעות תקני כוח אדם ועובדים ממיקור חוץ למשרדי הממשלה. בשנתיים הראשונות התקציב לאיוש התפקידים יתבסס על מקורות מערך הסייבר בסכום שלא יסתכם ביותר מ-500,000 ש"ח בשנה לתפקיד, ובשלוש השנים שלאחר מכן מחצית מהתקציב תהיה ממקורות המערך ומחציתו ממקורות המשרד הממשלתי הרלוונטי, והמערך ישתתף בתקציב עד לתקרה של 500,000 ש"ח בשנה ליועץ. כן נקבע כי המערך יבחן חמש שנים לאחר קבלת ההחלטה את מנגנון האיוש והתקצוב של התפקידים - קרי בפברואר 2020.

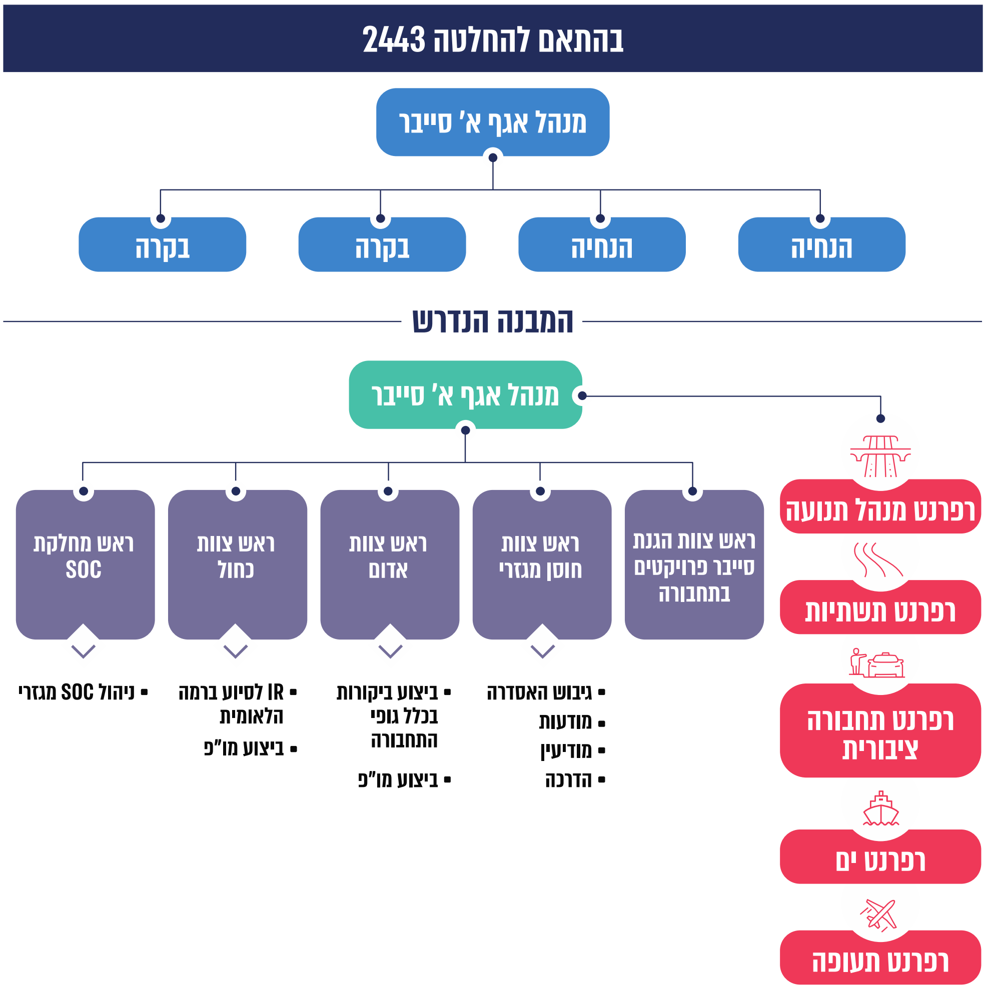
באוקטובר 2020 דיווחה מנהלת אגף הסייבר במשרד התחבורה לראש מחלקת הכוונת המשק במערך הסייבר כי עד כה מילאה היחידה רק חלק ממשימותיה, וזאת לנוכח פער בניהול ופער בכוח אדם שמיומן לביצוע הבקרה ולעמידה בדרישות האסדרתיות. מנהלת האגף הוסיפה כי האיום האיראני במרחב הסייבר ומשבר הקורונה מייצרים אתגר גדול אף יותר בהגנה על מגזר התחבורה, וביקשה גיבוי ממערך הסייבר להצעתה להוספת שני יועצים: האחד בתחום ההנחיה והשני בתחום הבקרה; לדבריה מצב זה אינו מיטבי, אך הוא יאפשר לצאת לשטח ולייצר תמונת מצב לאומית.

בדיון ועדת היגוי סייבר במשרד התחבורה שהתקיים בנובמבר 2020 בראשות מנכ"ל המשרד דווח כי המשרד לא ביצע עד כה ביקורות בגופים בהיבטי סייבר, וכי בתחום התחבורה הימית לא מבוצעת פעילות סייבר. מנהלת אגף הסייבר עדכנה כי משאבי כוח האדם המצומצמים אינם מצויים בהלימה להחלטת הממשלה 2443, וכי אגף הסייבר מבקש שהנהלת המשרד תתעדף את פעילותו - הכוונת פרויקטי תחבורה או יציאה לביקורות של הגופים בשטח.

עוד הוצג בדיון כי המבנה המיטבי של אגף הסייבר המגזרי צריך להיות רחב בהרבה מהקיים ולכלול בעלי תפקידים שיעסקו בביצוע ביקורות בכלל גופי התחבורה ובמחקר ופיתוח (מו"פ); צוותי התערבות באירועי סייבר ברמה הלאומית; צוותי ניהול SOC[16] מגזרי ועוד. להלן בתרשים פירוט המבנה הנדרש של אגף הסייבר, לפי אגף הסייבר במשרד התחבורה, למול המבנה שנקבע בהחלטת הממשלה:

16 Security Operation Center.

תרשים 8: **המבנה שנקבע בהחלטת הממשלה למול המבנה הנדרש**



על פי נתוני משרד התחבורה, בעיבוד משרד מבקר המדינה.

בדיון בחודש דצמבר 2020 בין מערך הסייבר למשרד התחבורה ציין המערך כי אגף הסייבר במשרד התחבורה הוא אגף חסר במשאבים באופן שאינו מאפשר לו להתמודד באופן נאות עם הצורך המבצעי ועם מספר הפרויקטים העצום במגזר.

בהמשך לדיון זה, בדצמבר 2020 שלחה שרת התחבורה דאז מכתב לשר האוצר דאז בנושא "פערים ביטחוניים להגנת הסייבר של תשתיות תחבורה בים, באוויר וביבשה". במכתב זה הבהירה השרה כי לפי עבודת המטה שבוצעה במשרדה נדרש תקצוב של 30 מיליון ש"ח כדי לאפשר למשרד לממש את אחריותו, וכי כל הפניות למשרד האוצר בעניין זה סורבו. השרה טענה עוד כי גם הצעות להסיט תקציב בתוך המשרד נענו בשלילה, וביקשה מהשר כי "יורה באופן מיידי לפקידי אגף התקציבים להקצות סך של 30 מיליון ש"ח **שיאפשרו למשרד**

התחבורה לממש תוכנית מיידית להגנת סייבר של תשתית התחבורה הלאומית בים, באוויר וביבשה, או לחילופין הסטת תקציב משרדי לצמצום פערים אלו" (ההדגשה במקור).

בעקבות המכתב לעיל התקיים בחודש ינואר 2021 דיון בהשתתפות נציגי משרד התחבורה, אגף התקציבים במשרד האוצר ומערך הסייבר, שאותו סיכם מנכ"ל משרד התחבורה באומרו כי נושא הסייבר הודגש והונח במרכז סדר היום, וכי הוא קורא לעזרה לנוכח הפערים שהצטברו והכוננות שבה נמצא המשרד, והוסיף כי במצב דברים זה המשרד אינו יכול לממש את אחריותו.

בדיון טען משרד התחבורה כי אין בידיו התקנים והתקציב הדרושים להקמה ולהפעלה של הגנת סייבר על מגזר התחבורה, והציג דרישות בפני נציגי אגף התקציבים המסתכמות ב-30 מיליון ש"ח לצורך משאבי כוח האדם, היכולות האופרטיביות, ריכוז תמונת המצב בזמן אמת, המערכות הטכנולוגיות והכלים להעלאת הכשירות והמודעות. נציגי משרד התחבורה הוסיפו כי מאז החלטת הממשלה 2443 שהתקבלה בשנת 2015 (אשר קבעה תקן של חמישה עובדים ליחידה מגזרית במשרד "גדול") ועד מועד הדיון משאבי היחידה המגזרית מסתכמים ב-1 מיליון ש"ח ומגלמים שני עובדים במיקור חוץ בלבד. הודגש כי הסכום המבוקש הוא קטן ונדרש לפצות על הזנחה של כמה שנים, וכי בהשוואה להיקף הנזק אשר עשוי להיגרם, סכום זה בטל בשישים.

נציגי מערך הסייבר ציינו כי משרדי ממשלה מקבילים כדוגמת משרד האנרגיה ומשרד הבריאות מעסיקים ביחידת הסייבר המגזרית[17] מספר דו-ספרתי של בעלי תפקיד מקצועיים, וכי ליחידות אלו יכולות של ניטור המגזר והמשרד. עוד הוסיפו כי נדרש לפתח יכולת סייבר חזקה במגזר, אשר תוכל לתת מענה מקצועי בעת ההיערכות לקראת תקיפה ובזמן אירוע סייבר. זאת לנוכח העובדה כי מערך הסייבר מחזיק בצוותים בהיקף מצומצם, ובמצב חירום ייעשה תיעדוף ותידרש עצמאות מגזרית.

יצוין כי בניגוד למשרד התחבורה, משרדים אחרים נקטו גישות שונות לצורך הסדרת תקני כוח האדם והתקציב. כך למשל, במשרד האנרגיה עוסקים כ-30 עובדים בתחום הגנת הסייבר במגזר - מספר המאפשר ביצוע פעולות הנחיה, בקרה וניטור בגופים (הלאומיים והפרטיים) ורמת מעורבות מעמיקה בשטח. משרד התחבורה אף שונה באופן התקצוב והתקינה, ביחס למגזרים אחרים, בשל כך שתקציב יחידת הסייבר המגזרית אינה בבסיס התקציב[18], דבר המשפיע על יכולתו לממש את אחריותו. כך לדוגמה, במשרד האנרגיה תקציב היחידה הוא חלק מהתקציב הקבוע של המשרד, עובדה המאפשרת תכנון רב-שנתי של המשימות.

באוגוסט 2021 שלח ראש מחלקת (רמ"ח) הכוונת המשק במערך הסייבר הלאומי מכתב למנהלת אגף הסייבר במשרד התחבורה, ובו ביקש לפעול בהקדם כדי לאייש את התפקידים באגף בהתאם למבנה שהציע המשרד עצמו, וזאת לנוכח העובדה שבמשך שנים לא אוישו התפקידים - דבר שצמצם מאוד את יכולות היחידה למלא את תפקידה באופן מיטבי.

---

17 משרד הבריאות ציין בתשובתו מיוני 2022 כי הוא מעסיק מספר דו-ספרתי של בעלי תפקיד מקצועיים עבור הגנת המשרד והמגזר יחד.

18 בבסיס התקציב מופיעה פעולות באחת מרמות הפירוט של תקציב המדינה (סעיף, תחום, תוכנית או תקנה) שקרוב לוודאי שתתוקצב גם בשנים הבאות. אפשר לתקצב פעולות גם שלא במסגרת זו (למשל באמצעות שימוש בסעיפים כלליים, רזרבות וכד'), אך במקרה כזה קיימת אי ודאות בדבר המשכיות התקציב ופגיעה אפשרית בתקציב העתידי.

בספטמבר 2021 אישרה ועדת המכרזים של משרד התחבורה גיוס של ארבעה עובדים במיקור חוץ לאגף הסייבר של המשרד: שני עובדים לתפקידי הנחיה ושני עובדים לתפקידי בקרה.

יצוין כי מעורבות אגף הסייבר במשרד התחבורה נדרשת במיוחד בפרויקטים חדשים, מתוך הבנה כי זול יותר לשלב את דרישות הגנת הסייבר בשלבי תכנון הפרויקט מלהכניסן בשלבים מאוחרים שבהם יידרשו שינויים והתאמות (תפיסת Security by Design), וכי למשרד התחבורה פרויקטים רבים בשלבי תכנון, כפי שיפורט בפרק "הגנת הסייבר בפרויקטים חדשים".

בנובמבר 2021 אושר בכנסת תקציב המדינה לשנים 2021 - 2022. בתקציב משרד התחבורה נכללו 70 מיליון ש"ח בסעיף תקציבי אחד עבור הנושאים האלה: הגנת הסייבר במגזר, טכוגרף ועלייה לענן, ללא חלוקה פנימית בין הנושאים.

בדצמבר 2021 התקיימה במשרד התחבורה ועדת היגוי סייבר ובה הוצג שנית כי התקציב הנדרש להגנת הסייבר בשנים 2021 - 2022 הוא 30 מיליון ש"ח, אך בפועל הוקצו לנושא 6.3 מיליון ש"ח. לפי המשרד, אלה הנושאים הצפויים להיפגע בהיעדר תקציב, בין היתר: כוח אדם, יכולת אופרטיבית, כשירות ואחיזה בתמונת מצב רחבה.

במועד סיום הביקורת, באפריל 2022, מנה אגף הסייבר במשרד התחבורה שלושה עובדים במשרה מלאה: מנהלת אגף שמונתה בשנת 2019, ושני עובדים במיקור חוץ - רמ"ח פרויקטים וחדשנות ורמ"ח חוסן. תפקיד רמ"ח SOC לא מאויש בשלב זה מאחר שלא נמצאו במכרז מתמודדים מתאימים.

בביקורת עלה כי לאגף הסייבר במשרד התחבורה אין תקציב בסיס קבוע אלא תקציב שמתעדכן מדי שנה בשנה. במצב זה האגף אינו יכול לבצע תכנון רב-שנתי של המשימות בהתאם לתקציב, לכן אין וודאות להמשך תקציבי. כן נמצא כי למול התקציב הנדרש המוערך ב-30 מיליון ש"ח, בשנים 2021 עד 2022 הוקצו לנושא כ-6.3 מיליון ש"ח.

בשנים 2015 עד 2022 פעל אגף הסייבר במשרד התחבורה באיוש חסר בהשוואה למספר התקנים שנדרש בהחלטה 2443, והועסקו בו רק שלושה מתוך חמישה (60%) עובדים. עוד עלה כי מערך הסייבר לא פיקח על יישום ההחלטה ולא התריע על אי-יישומה לפני גורם כלשהו. במצב זה אין בידי משרד התחבורה משאבי כוח האדם והתקציב הדרושים לטובת מימוש אחריותו והוא אינו יכול לתת מענה לחלק מהאיומים הניצבים בפני מגזר התחבורה.

משרד התחבורה מסר בתשובתו ביולי 2022 כי הוא טרם קיבל מהאוצר את המשאבים והתקנים בטענה שהחלטת הממשלה 2443 אינה בתוקף, כיוון שטרם הושלמה עבודת המטה, וכי הוגדרו מדרגות של מימון משותף עם מערך הסייבר, כאשר מנגנון המימון המשותף נדרש להיות מוחלף בעבודת תקינה של נציבות שירות המדינה ותקצוב מתאים.

נציבות שירות המדינה מסרה בתשובתה מיולי 2022 כי למשרד התחבורה קיימת משרת מיישם הגנת סייבר א' המאוישת מתחילת שנת 2022, וככל שידרשו משרות נוספות בתחום זה, הנושא ייבחן ויטופל ע"י גורמי המקצוע בנציבות שירות המדינה.

מוצע כי משרד התחבורה ומערך הסייבר יבחנו את התקציב ואת הלימת תקינת כוח האדם המוקצת למול המשימות שעומדות לפתחו של אגף הסייבר ולצורך מתן מענה לאיומי הסייבר הניצבים בפני מגזר התחבורה.

חשיבה מחודשת על החלטה 2443

בחלוף שש שנים מהחלטה 2443, בשנת 2021, החל מערך הסייבר בתהליך חשיבה מחודשת על ההחלטה. החשיבה הייתה בין היתר בנוגע ל"מודל המגזרים" שנקבע - מתן אחריות בנושא הגנת הסייבר למשרדי הממשלה המשמשים מאסדרים בתחומם. התהליך הותנע מכמה סיבות: הזמן שחלף מההחלטה והלקחים שנלמדו בתהליך יישומה במשרדים שונים; תובנות שעלו מתהליך קידום הוראת השעה הנוגעת למתן סמכויות אופרטיביות למערך הסייבר כלפי ארגונים "סרבנים"; ושינויים ארגונים ותפקודיים במכלול הרלוונטי במערך הסייבר.

בדיונים עלו כמה נושאים ובהם: השונות בין המגזרים השונים אשר אינה מאפשרת מודל אחיד לכולם; קשב נמוך לנושא מצד מנכ"לי המשרדים; חלוקת האחריות בין המערך ליחידות הסייבר המגזריות ומערכת היחסים ביניהם.

במרץ 2022 מסר מערך הסייבר למשרד מבקר המדינה כי תהליך החשיבה המחודשת על החלטה 2443 טרם הסתיים, בין היתר עקב כניסת ראש מערך חדש לתפקידו.

בשנת 2021 קיים מערך הסייבר כמה דיונים בעניין "מודל המגזרים", אולם עד מועד סיום הביקורת באפריל 2022 לא הסתיים התהליך, כך שהתשתית הנורמטיבית לפעילותן של יחידות הסייבר המגזריות (החלטה 2443), מספקת מענה חסר הטעון עדכון.

מומלץ כי מערך הסייבר ישלים את תהליך החשיבה המחודשת על החלטה 2443 כדי לתת מענה לאיומי הסייבר הקיימים ברמה הלאומית, תוך מתן כלים ליחידות הסייבר המגזריות או באמצעות מודל אחר שיימצא לנכון. במסגרת זו מומלץ כי תבוצע חשיבה גם על נושא תקצוב יחידות אלו.

בהחלטה 2443 נקבע, בין היתר, כי לצורך שיפור רמת הגנת הסייבר של המשרד יש להקצות תקציב ייעודי להגנת הסייבר בשיעור של 8% מהשיעור של כלל תקציב המחשוב של המשרד.

החלטה 2443 הגדירה את התקציב הנדרש להגנת המערכות הפנים-משרדיות; היא לא הגדירה את התקציב הנדרש לביצוע משימות יחידות הסייבר המגזריות (האחראיות להנחות גורמים הכפופים למשרד). מומלץ כי מערך הסייבר, במסגרת החשיבה המחודשת על ההחלטה, ייתן דעתו גם על סוגיה זו.

מערך הסייבר מסר בתשובתו מיוני 2022 כי עם כניסת ראש המערך הנוכחי לתפקידו בפברואר 2022 החלה בחינת חקיקת העבר, תוך ביצוע חשיבה מחודשת לגבי חקיקת ההמשך, וכחלק מהחלטת הממשלה 219 הוקם צוות מנכ"לים בין-משרדי אשר בוחן את כלל רגולציית הסייבר הממשלתית. המערך הוסיף כי אבן דרך מרכזית היא בחינת מצב ההגנה במגזרים ודרכי השיפור שלה.

מוצע שמערך הסייבר יעלה את נושא תקצוב היחידות המגזריות לדיון במסגרת פעילות הצוות הבין משרדי, שנכון למועד סיום הביקורת, אפריל 2022, לא השלים את עבודתו.

ההגנה על גופי תמ"ק

הגדרת גופי תמ"ק במגזר התחבורה

חלק מהגופים הפועלים במגזר התחבורה מוגדרים כגופי תמ"ק: רכבת ישראל, רש"ת, נמל אשדוד, נמל חיפה, נת"ע וחנ"י. אגף תמ"ק במערך הסייבר מנחה באופן ישיר את גופי התמ"ק והוא אחראי ללוות את הגוף באופן שוטף ולסייע לו בפעולות האלה: בניית תוכנית העבודה השנתית בתחום הגנת הסייבר ומעקב אחר ביצועה; יישום תורת ההגנה שנכתבה באופן ייעודי לגופי תמ"ק; ופיקוח על אופן יישומה באמצעות ביצוע ביקורות ובהן בדיקות חוסן. כמו כן אגף תמ"ק במערך הסייבר מלווה את גוף התמ"ק ומסייע לו כשיש חשש לאירוע סייבר. מחומרים שהועברו למשרד מבקר המדינה עולה כי אירועי סייבר קרו בשנים האחרונות גם בגופי תמ"ק.

כיום, כדי להגדיר גוף כתמ"ק, נדרש להוסיפו לתוספת החמישית בחוק להסדרת הביטחון. תהליך זה עלול להימשך לעיתים כמה שנים. כך לדוגמה, מערך הסייבר המליץ להגדיר את חברה כ"ה בתחום הספנות והנמלים כגוף תמ"ק בנובמבר 2018, אך רק באפריל 2022 הושלם תהליך זה.

כדי לזרז את תהליכי ההכרה בגופים כתמ"ק החליטה הממשלה[19] באוגוסט 2021 על הקמת צוות בין-משרדי שבין היתר יבצע בחינה של אסדרה חכמה בסייבר, ובמסגרתה נקבע בין היתר כי יש לבחון "את המנגנון הקיים להמלצה בנוגע לשינוי הגופים המנויים בתוספת החמישית לחוק להסדרת הביטחון בגופים ציבוריים". לצורך כך ניתנו 180 ימים לצוות שעליו הוטלה הבחינה כאמור.

נמצא כי בחינת המנגנון הקיים הנוגע להגדרת גופי התמ"ק לא הושלמה בהתאם להחלטת הממשלה מאוגוסט 2021, ולפיכך לא עודכן המנגנון המורכב שבו נעשה שימוש, הכולל צורך בשינוי חקיקה עבור כל גוף לגביו הוחלט כי נדרש להגדירו כתמ"ק.

העיכובים בהגדרת גופי תמ"ק עלולים להביא לסיכונים בנושאים שטרם מטופלים וכן לניצול משאבים לא יעיל. למשל: בגופים חדשים שטרם נכנסו לחוק - היעדר היכולת לדרוש מהעובדים בגופים לעבור תהליכי מהימנות וסיווג בטחוני; בגופים שטרם הוסרו מהחוק - בזבוז משאבים עקב הנחיה צמודה של הגופים שאינה נדרשת יותר.

משרד התחבורה מסר בתשובתו מיולי 2022 כי המתודולוגיה להכרה בגוף כתמ"ק אינה אחידה. כך למשל, לעיתים ההגדרה היא על זכיין (מפעיל), ולעיתים על חברה ממשלתית מבצעת. על

19 החלטת הממשלה 219, "בחינת רגולציה חכמה בסייבר וכללים והסמכות למתן הנחיות בזמן תקיפת סייבר שעודנה בעיצומה תוך שקילת שיקולים כלכליים" (1.8.21).

כן, המשרד פנה למערך הסייבר בבקשה לקיים דיון על המתודולוגיה, נוכח השינויים בענף התחבורה והקמת אגף הסייבר במשרד.

מערך הסייבר מסר בתשובתו כי נכון ליולי 2022 כל הגופים אשר צריכים להיות תמ"ק הוגדרו במסגרת התוספת החמישית לחוק הסדרת הביטחון. עוד הוסיף המערך כי נושא שינוי המנגנון להגדרת גופים כתמ"ק ייבחן במסגרת הצוות הבין-משרדי שהוקם בעקבות החלטת ממשלה 219.

על מערך הסייבר והצוות הבין משרדי לפעול להשלמת בחינת שינוי המנגנון להגדרת גופי תמ"ק בהקדם.

תמונת המצב המגזרית

שגרות הניהול

מערך הסייבר עובד מול היחידה המגזרית במשרד התחבורה בעבודה שוטפת הכוללת בין היתר אישור תוכניות עבודה, פגישות עיתיות, ליווי פרויקטים וסיורים בארגונים.

בנובמבר 2020 פרסמה היחידה להנחיה מגזרית במערך הסייבר הנחיה המפרטת את שגרות הניהול המצופות מיחידות הסייבר המגזריות במשרדים (להלן - שגרות הניהול). הנחיה זו נכנסה לתוקף ב-1.12.20. שגרות הניהול נועדו בעיקר לאפשר ליחידות הסייבר המגזריות לנהל מעקב אחר הנושאים הניהוליים והמבצעיים שבאחריותן וכן לאפשר למערך הסייבר לקבל תמונת מצב עדכנית באמצעות דיווחים. לפי ההנחיה, מערך הסייבר מבקש לקבל דיווחים חודשיים, רבעוניים, חציוניים ושנתיים על אירועי אבטחת מידע ועל פעילות היחידה במגזר התחבורה בנוגע לנושאים האלו: פעילויות הנחיה, מודעות לאיומי סייבר, ביקורות וסקרים בגופי המגזר; תהליכי חקיקה ותיקון תקנות; אתגרים וניהול סיכונים במגזר וההתמודדות איתם; תרגילים ואימונים; פעילויות טכנולוגיות; פרויקטים חדשים שבכוונת המגזר להוביל; ופרויקטים בתחום שרשרת האספקה במגזר. עוד מונחות יחידות הסייבר המגזריות לבצע שורת משימות מחזוריות: תכנון תוכנית עבודה על בסיס ניהול סיכונים, עדכון מסמכי מדיניות אבטחה, כתיבת נהלים ועדכונם ועוד.

מערך הסייבר מסר בתשובתו מיוני 2022 כי אופן העבודה מול היחידה המגזרית בהיבטי שגרת הניהול יעלה במסגרת החשיבה המחודשת שמתקיימת לאור השינוי הארגוני במערך.

עוד פרסם מערך הסייבר בספטמבר 2020 מסמך ליחידות הגנת הסייבר המגזריות המכיל את הפעילויות העיקריות שעל היחידות לשלב בתוכניות העבודה שלהן בשנת 2021 (להלן - עוגנים לתכנון תוכנית העבודה).

כמו כן הוגדר בהנחיה כי עד סוף יולי בכל שנה קלנדרית על ראש היחידה המגזרית (במשרד התחבורה - מנהלת אגף הסייבר) להעביר למנחה המגזרי במערך הסייבר דוח המסכם את פעילות היחידה בחציון א'. הדוח יתמקד בנושאים האלו: הישגי ההגנה המשמעותיים במגזר; תקציר התכנון מול הביצוע של תוכנית העבודה לחציון א'; מספר אירועי הסייבר שחווה המגזר בחציון א' ומאפייניהם; הלקחים המרכזיים שעלו בביקורות שביצעה היחידה המגזרית; האתגרים

או ניהול הסיכונים במגזר וההתמודדות עימם; סטטוס הנושאים והפערים המרכזיים הדורשים את מעורבות מערך הסייבר; סטטוס הכשירות היחידתי; היעדים והמשימות המתוכננים לחציון ב'.

בדצמבר 2020, כחודש לאחר פרסום שגרות הניהול, פנתה מנהלת אגף הסייבר במשרד התחבורה למנחה המגזרי ומסרה כי המסמך כולל משימות ודרישות רבות מהיחידה, אך עקב המשאבים החסרים אין לאגף יכולת לבצע חלק משמעותי מהדרישות במסמך.

מסקירת תוכניות העבודה של אגף הסייבר במגזר התחבורה, כפי שהועברו למערך הסייבר, עולה כי משימות מסוימות שתוכננו לשנים 2019 עד 2020 לא בוצעו עקב מחסור במשאבים, כך לדוגמה משימת "הקמת SOC תחבורה בבאר שבע" שתוכננה לשנת 2019, החלה בשלב ה"מבצוע" שלה במועד סיום הביקורת באפריל 2022 (ראו פירוט בפרק "הקמת SOC עבור מגזר התחבורה").

בוועדת ההיגוי בנושא סייבר במגזר התחבורה שהתקיימה בדצמבר 2021 דווח כי יש משימות הנגזרות מדרישות מערך הסייבר בדבר עוגנים לתכנון תוכנית העבודה שלא בוצעו עקב היעדר תקציב. בין משימות אלו: יכולת התערבות לאומית - כלומר התקשרות מיידית לצוות IR (צוות התערבות לניהול משברים) לסיוע בעת אירוע בעל השפעות לאומיות; העלאת החוסן במגזר - הבאה לידי ביטוי באמצעות גיבוש אסדרה מחייבת, הרחבת ביקורות סייבר לגופי B, ליווי הגופים בטיפול שלהם בליקויים חמורים, ליווי פרויקטים והעלאת מודעות לאיומי סייבר באמצעות הכשרות, תרגילים וכנסים.

בביקורת עלה כי אגף הסייבר לא מסר ליחידה להכוונה מגזרית במערך הסייבר דיווחים חודשיים, רבעוניים, חצי-שנתיים וכן דיווח שנתי על שנת 2021, כנדרש בשגרת הניהול שלה. עוד נמצאו משימות של אגף הסייבר שלא בוצעו עקב היעדר משאבים - ביניהן: בניית יכולת התערבות לאומית באירועי סייבר; פעילויות להעלאת החוסן במגזר; הרחבת הביקורות לגופי B; ליווי הגופים בתיקון ליקויים חמורים; ליווי פרויקטים; והעלאת מודעות לאיומי הסייבר.

נוכח אי ביצוע חלק ניכר מהמשימות שנדרשו באגף הסייבר, מוצע שמערך הסייבר ומשרד התחבורה יפעלו להכנת תוכנית עבודה בהתאם למשאבים הקיימים ויפעלו לבקרה עליה ולמימושה.

לצורך ביצוע תפקידיו למול רמת האיומים במגזר, נדרש האגף לכמה יכולות בסיסיות, שחלקן חסרות. להלן כמה דוגמאות:

1. **אי-יכולת התערבות באירועים בזמן אמת ואי דיווח מצד הגופים:** לאגף הסייבר אין כיום צוות התערבות היכול לסייע לגופים שהוא מנחה בקרות אירוע. נמצא כי הגופים אינם מדווחים לאגף הסייבר על כלל האירועים שהם חווים, וכי האגף אינו מבצע תחקירים על אירועים שקרו כדי להעביר תובנות לכלל הגופים במגזר.

2. **אי-קבלת חומרים מהגופים במגזר שהכרחיים להבנת מצב הגנת הסייבר שלהם:** אגף הסייבר אינו משתתף בוועדות היגוי בנושא סייבר שפועלות בגופים במגזר. כמו כן האגף אינו מקבל מהגופים במגזר חומרים על פעולות שהגופים עצמם ביצעו בתחום הגנת הסייבר כמו סיכומי דיוני ועדות ההיגוי להגנת הסייבר, תוכניות העבודה בנושא הגנת הסייבר ונתוני הביצוע שלהן, הסיכונים שעימם מתמודד הגוף, הפרויקטים החדשים שהגוף מקים, תוצאות מבדקי החדירה והתוכניות לטיפול בממצאים שעלו. יצוין כי לרוב חומרים אלו מסווגים היות שהם מצביעים על חולשות ופערים שקיימים בגופים. יצוין כי בגופי A משרד התחבורה עשה

ביקורות כדי לבחון את מידת עמידתם בדרישות המדיניות; ראו פירוט בנושא בפרק "הממצאים שעלו בביקורות שביצע משרד התחבורה".

3. **אי קיום תשתית מסוימת.**

4. **חוסר בכלים מקצועיים:** לאגף הסייבר אין כלים הדרושים לו לצורך מילוי תפקידו, לדוגמה רישיונות עבור שימוש בכלים להגנת הסייבר או גישה לתקנים מקצועיים ומקובלים בתחום, הכרוכה בדרך כלל בתשלום לגוף המנפיק אותם.

בביקורת עלה כי אגף הסייבר אינו מקבל מידע חיוני מהגופים על פעילויות שהם עצמם ביצעו כמו סיכומי ועדות היגוי להגנת הסייבר, סקרי סיכונים, תוצאות מבדקי חדירה ודיווח על אירועי סייבר - הנדרשים לאגף הסייבר כדי לייצר תמונה מערכתית של מצב ההגנה בסייבר של מגזר התחבורה, ולצורך עמידה בשגרות הניהול הנדרשות ממנו. עוד נמצא כי האגף אינו מבצע ביקורות בכל הגופים לצורך בחינת מצב הגנת הסייבר בהם ולא עוקב אחר אופן תיקון הליקויים בביקורות שכבר ביצע - זאת עקב היעדר משאבים התואמים את מספר המשימות המוטלות על יחידת הסייבר המגזרית.

עוד עלה כי אגף הסייבר במשרד התחבורה לא הצטייד ביכולות מתאימות כנגד רמת האיומים במגזר. מומלץ כי אגף הסייבר במשרד התחבורה יצטייד בכלים וביכולות מתאימות של עובדיו כנגד רמת האיומים על המגזר.

משרד התחבורה מסר בתשובתו מיולי 2022 כי בהיעדר חובה חוקית, אין לו סמכות להנחות גוף פרטי ללא הסדר חוזי, וכי הוא מקדם חוק סייבר בתחבורה, שיחיל חובת הנחיה ודיווח על כל דרישות הסייבר של המשרד, של כל הגופים המקבלים רישיון או זיכיון ממנו.

☆

מומלץ כי משרד התחבורה יפעל בשני נתיבים: קידום ההסדרה החוקית שתתן מענה לכלל ההתקשרויות ומתן מענה לפערים הקיימים בהסדרה החוזית הקיימת למול הגופים במגזר.

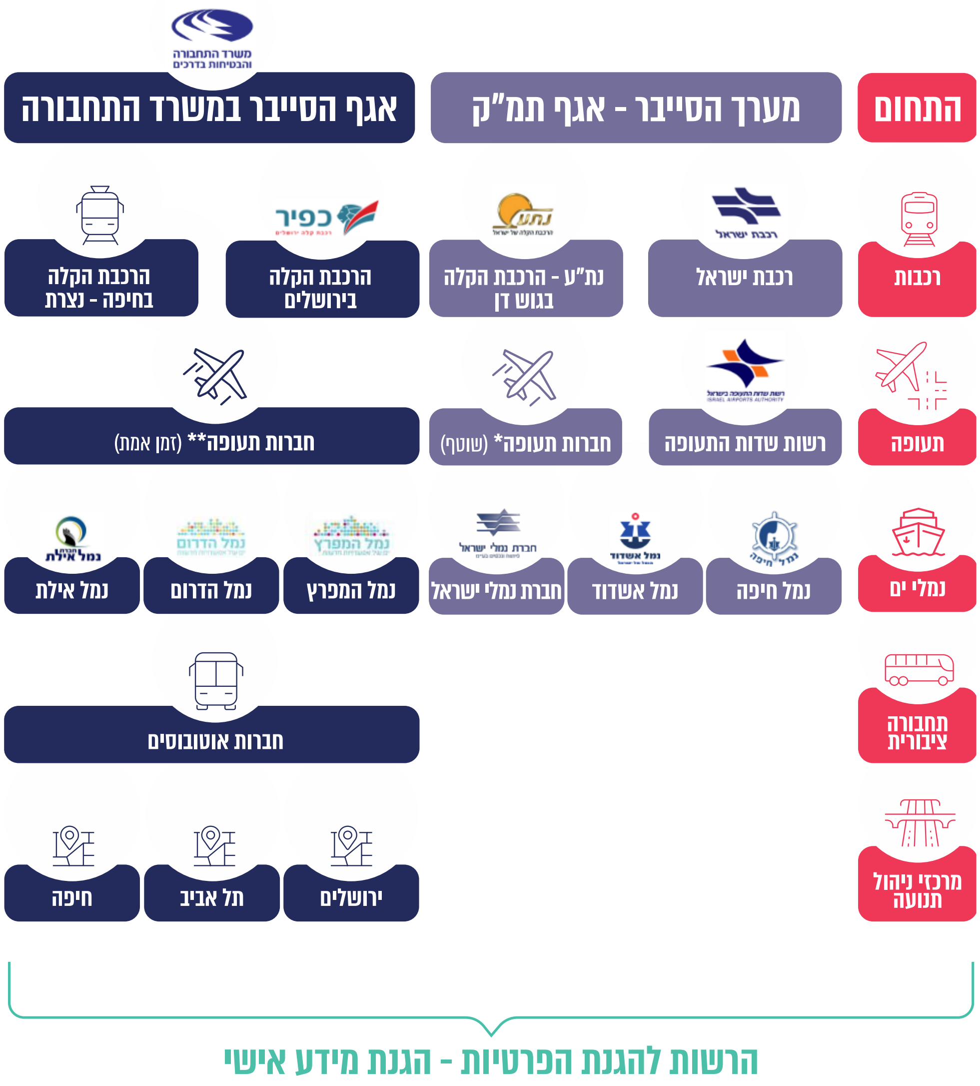
גיבוש תמונת מצב מגזרית אחודה בתחום הסייבר בידי משרד התחבורה

לפי החלטת הממשלה 2443, אחד מתפקידי יחידות הסייבר המגזריות במשרדי הממשלה (ובהן אגף הסייבר במשרד התחבורה) הוא בנייה והפעלה של תהליכי שיתוף מידע פנימיים וחיצוניים בתוך המגזר, לרבות דיווח על אירועים, איומים, חולשות, פוגענים ונוזקות למרכז הממשלתי לסיוע בהתמודדות עם איומי סייבר וכן הגדרה של נהלים ושיטות דיווח בין הגופים במגזר. עוד לפי ההחלטה תפקיד היחידה הוא ייזום ומימוש של פעילות רוחבית, לרבות הקמת תשתיות והפעלת מנגנונים שתכליתם שיפור הגנת הסייבר במגזר.

יוזכר כי גם שגרות הניהול מבהירות כי אלו נועדו, בין היתר, כדי לאפשר למערך הסייבר הלאומי לקבל תמונת מצב עדכנית באמצעות דיווחים.

להלן תרשים המתאר את תחומי הפעילות של המאסדרים בתחום ומציג כי בכל תחום (רכבות, תעופה, נמלי ים) פועלים כמה מאסדרים שאחראים להנחיית גופים שונים:

תרשים 9: **סוגי הגופים במגזר התחבורה והמאסדרים שלהם בתחום הגנת הסייבר**



* לפי המדיניות הלאומית להגנת הסייבר בתעופה אזרחית, פעילות שוטפת תהיה באחריות מערך הסייבר בגופי תמ"ק ובאחריות רת"א בגופים שאינם תמ"ק.

** לפי המדיניות הלאומית להגנת הסייבר בתעופה אזרחית, פעילות זמן אמת (ניטור באמצעות SOC) תהיה באחריות משרד התחבורה, תוך קיום ממשקים עם רת"א ועם מערך הסייבר.

מהתרשים עולה כי במצב הנוכחי למשרד התחבורה, שעליו הוטל בהחלטת הממשלה 2443 לקדם את הטיפול בהיערכות לאיומי סייבר במגזר, אין את התמונה המגזרית כולה של מצב הגנת הסייבר נוכח העובדה שאינו מודע לנעשה בחלק מגופי התחבורה (בגופי התמ"ק ובחברות התעופה שמנחה מערך הסייבר) ונוכח היעדר הסמכות של האגף לקבל את המידע מהגופים. עוד עולה מהתרשים כי בחלק מתחומי הפעילות, כמו התחבורה הציבורית והתחבורה הימית, לא פועל מאסדר אחד שרואה את התמונה המלאה והעדכנית בתת-המגזר. למשל: בתחבורה הימית, את חלק מהנמלים מנחה מערך הסייבר ואת חלקם מנחה אגף הסייבר במשרד התחבורה.

מערך הסייבר מסר בתשובתו מיוני 2022 כי במסגרת השינוי הארגוני במערך, עבודת התמ"ק והמגזרים ישולבו באופן שלראש הפעילות במערך הסייבר תהיה תמונה רחבה על כל מגזר, וכך גם במגזר התחבורה.

עוד עלה כי אגף הסייבר במשרד התחבורה ואגף תמ"ק במערך הסייבר לא נפגשים בקביעות כדי לקבל תמונת מצב האחד מהשני, ולכן עלול להיווצר חוסר סינכרון בפעילותם.

מערך הסייבר מסר בתשובתו מיוני 2022 כי אין מנגנון לקבלת תמונת מצב בין משרד התחבורה לאגף תמ"ק. המערך הוסיף כי במסגרת השינוי הארגוני ייקבעו נהלים ותהליכי עבודה משולבים בין אגף תמ"ק ואגף הסייבר במגזר התחבורה.

מוצע כי מערך הסייבר ומשרד התחבורה יקבעו נהלי דיווח ביניהם בכל הנוגע לגופי התמ"ק המונחים על ידי המערך ויפעלו לממשם, כדי שלמשרד התחבורה תהיה תמונה כוללת של מצב הגנת הסייבר גם בגופי התמ"ק. מומלץ כי נהלים אלו יתייחסו, בין השאר, לנושאים הבאים: שיתוף מידע; דיווחים שוטפים; חולשות ואירועים; נוהל טיפול באירוע; נוהל סגירת חולשה; הערכות מצב עיתיות; תיאום תוכניות עבודה וביקורות; ודיווח על תוצאות אירועים, תחקורים ולקחים.

בחלק מהגופים במגזר התחבורה קיימים מאגרי מידע המכילים מידע פרטי ובו מעל 100,000 רשומות, ולכן הם מוגדרים כמאגרי מידע שבהם נדרשת רמת אבטחה גבוהה לפי תקנות אבטחת מידע. בעל מאגר מידע שחלה עליו רמת אבטחה בינונית או גבוהה מחויב להודיע לרשות להגנת הפרטיות באופן מיידי על אירוע אבטחה חמור (כהגדרתו בתקנות), וכן לדווח לרשות על הצעדים שנקט בעקבות האירוע.

מערך הסייבר מסר בתשובתו ביוני 2022 כי כל אירוע בגופי התחבורה מרוכז במרכז הניטור של מערך הסייבר הלאומי. המערך הוסיף כי מבוצע עדכון מצד המנחה המגזרי במערך ליחידת הסייבר המגזרית, וכי מבוצע עדכון בין מרכזי הניטור של המשרדים לזה של המערך.

משרד מבקר המדינה בדק את הדיווחים שנמסרו על אירועי סייבר וההגנה על הפרטיות בתקופה שבין ינואר 2019 עד יוני 2021 לגופים הבאים: משרד התחבורה, מערך הסייבר והרשות להגנת הפרטיות. בבדיקה נמצא כי התרחשו 21 אירועים, וכל אירוע דווח למאסדר אחד (13 - למערך הסייבר, 4 - לאגף הסייבר במשרד התחבורה, 4 - לרשות להגנת הפרטיות).

עוד נמצא בבדיקה כי דיווחים על אירועים שבהם הייתה השפעה אפשרית על פרטיות משתמשים, אשר נמסרו למשרד התחבורה לא דווחו לרשות להגנת הפרטיות - או להפך. להלן דוגמאות לדיווחים שנמצאו רק בידי הרשות להגנת הפרטיות ולא הועברו למשרד התחבורה:

1. אירוע בו נתגלתה חולשה באתרים של שתי חברות פרטיות המספקות שירות לתהליך רישום לקורסי תיקון נהיגה של משרד התחבורה. חולשה זו אפשרה, ללא צורך בהזדהות, גישה לנתוני הנרשמים ובהם: שם, דוא"ל, תאריך מבחן, מיקום בו התבצע המבחן, סטאטוס הצלחה, האם בוצע תשלום וסכום התשלום.

2. שני אירועים שקשורים בספקי משנה של חברה לתחבורה ציבורית: באירוע הראשון נתגלתה פרצה במנגנון הפקת החשבוניות של החברה אשר אפשרה לצפות ולהוריד חשבוניות שנשלחו ללקוחותיה ללא צורך במנגנון זיהוי כלשהו; באירוע השני התגלתה תקלה באתר האינטרנט שאפשרה גישה למסמכים אשר כללו מידע על חלק ממבקשי זכאות לקבלת תעריף לאזרחים ותיקים, לרבות צילומי תעודות זהות, ותעודת אזרח ותיק.

בביקורת עלה כי קיימים שלושה גורמים בתחום הגנת הסייבר והגנת הפרטיות שאליהם מדווחים אירועי הגנת הסייבר במגזר התחבורה, וכי אין גורם אחד שמחזיק בתמונה הרוחבית של כלל האירועים, אף לא משרד התחבורה שאחראי לפי החלטה 2443 לטפל באירועים אלו. כך למשל: אירועים המתרחשים בגופי תמ"ק מטופלים בידי אגף תמ"ק במערך הסייבר ללא העברת תחקירים ליחידת להכוונת מגזרים במערך הסייבר, לאגף הסייבר במשרד התחבורה, לרשות להגנת הפרטיות (אם נדרש) או לגופים הדומים לגוף שבו התרחש האירוע. כך לדוגמה, בבדיקת משרד מבקר המדינה נמצא כי בתקופה שבין ינואר 2019 עד יוני 2021 דווחו 21 אירועים, וכל אירוע דווח לגורם אחר (13 - למערך הסייבר, 4 - לאגף הסייבר, 4 - לרשות להגנת הפרטיות). עוד נמצא כי אירוע שהתרחש בנמל כ' בפברואר 2020 דווח רק למערך הסייבר ולא לאגף הסייבר במגזר התחבורה או לנמלים אחרים.

עוד עלה כי משרד התחבורה אינו מקבל מהרשות להגנת הפרטיות וממערך הסייבר דיווחים על אירועי סייבר שהתרחשו בגופי המגזר, דבר שמקשה על המשרד ליצור תמונת מצב בזמן אמת, תוך שיתוף הידע עם גופי המגזר שלהם הוא עשוי להיות חיוני.

מומלץ כי משרד התחבורה, בשיתוף מערך הסייבר והרשות להגנת הפרטיות, יבחן כיצד ניתן להעביר את המידע הרלוונטי ביניהם, לצורך הפקת לקחים מאירועים, נקיטת פעולות להעלאת החוסן של הגופים במגזר וטיוב ההנחיות.

☆

משרד התחבורה אחראי לקדם את הטיפול בהיערכות לאיומי הסייבר של כל מגזר התחבורה אולם הוא מתקשה במילוי תפקידו מהסיבות האלו: המשרד אינו רואה את התמונה המגזרית כולה על תתי-המגזרים שבה (למשל תחום התחבורה האווירית וגופי התמ"ק שמנחה מערך הסייבר); הוא אינו רואה את מפת הסיכונים ואת הפערים הקיימים בכל גוף; והוא אינו מקבל מידע חיוני מהגופים כמו מבדקי חוסן, תוכניות עבודה לתיקון הליקויים, דיווח על אירועי סייבר ותחקירים עליהם שביצע הגוף.

מוצע כי משרד התחבורה יסדיר ויפעל לאסוף נתונים מהגופים ומיתר המאסדרים בתחום הסייבר כדי לייצר תמונת מצב מגזרית, למשל באמצעות פגישות סטטוס עיתיות עם הרשות להגנת הפרטיות ועם מערך הסייבר שמנחה את גופי התמ"ק במגזר; קבלת מסמכים עיקריים מהגופים וקבלת דיווח על אירועי סייבר. כן מוצע כי מערך הסייבר ומשרד התחבורה האחראים להנחיית הגופים במגזר יגבשו בסיס נהלי ליישום שגרת הניהול השוטפת שיתייחס, בין השאר, לנושאים הבאים: שיתוף מידע; דיווחים שוטפים; הערכות מצב עיתיות; תיאום תוכניות עבודה וביקורות; ודיווח על תוצאות אירועים, תחקורים ולקחים. עם השלמת איסוף המידע, מוצע כי משרד התחבורה יממש את תפקידו כאחראי על הגנת הסייבר של כל המגזר וינחה בהתאם למידע שירוכז על ידו את כלל המגזר באופן שוטף.

הרשות להגנת הפרטיות מסרה בתשובתה מיוני 2022 כי בנובמבר 2021 נערכה פגישה בין ממלא מקום ראש הרשות להגנת הפרטיות לבין מנכ"לית משרד התחבורה, ובה עלה לדיון בין היתר נושא אבטחת המידע והגנת הפרטיות במגזר התחבורה. במהלך הישיבה סוכם כי משרד התחבורה יגבש רשימת נושאים המשלבים היבטי פרטיות, ויוקם צוות חשיבה ומשימה לגבי פרויקטים וממשקים עתידיים. עם כניסתו לתפקיד של ראש הרשות הנוכחי, הוא צפוי לקיים פגישה נוספת עם מנכ"לית משרד התחבורה, בין היתר כדי לדון ברשימת הנושאים האמורה.

הקמת SOC עבור מגזר התחבורה

מרכז שליטה ובקרה לאיומי סייבר (להלן - SOC) הוא פתרון מקובל לאיגום ולניטור של אירועים בתחום הסייבר. תפקידו של ה-SOC הוא לסייע לארגון לזהות פרצות, אירועים חריגים, ניסיונות לתקיפות סייבר, לתחקר אותם ולהגיב עליהם בזמן אמת. הזיהוי נעשה באמצעות איסוף מידע בנוגע לתהליכים, אירועים, איומים, חולשות, פוגענים ונוזקות הקשורים למערכות המידע ולמערכות הטכנולוגיות והתפעוליות של הארגון; עיבוד המידע; זיהוי אנומליות; והקפצת התראות למערכת השליטה והבקרה. במרכז מועסקים מומחי סייבר שמתחקרים את ההתראות ואת המידע שמתקבל ובמידת הצורך מפעילים צוותי תגובה לטיפול באירוע.

תהליך הקמת SOC הוא תהליך מורכב הכולל בין היתר את תתי-התהליכים האלה: אפיון צרכים; הגדרות המערכות הנדרשות לניטור; הגדרת חוקים לניטור; ביצוע התקשרות לקבלת מרכז השליטה כשירות מנוהל (אפשרות) או הקמה עצמית; טיוב החוקים במערכת; פיתוח, בדיקות ויישום. פתרון הקמת SOC יכול להתבצע באמצעות כוח האדם של הארגון או באמצעות מיקור חוץ.

כדי לשפר את יכולות ההגנה בסייבר קיימת אפשרות לחבר כמה מערכות של ארגונים למרכז שליטה ובקרה מערכתי (מגזרי או ממשלתי). מרכז זה אחראי לרכז את אירועי הסייבר המתרחשים בגופים הכפופים לו וממקורות מידע נוספים כמו גופי מודיעין; לתכלל את הדיווחים לתמונת מצב מערכתית; ולהתריע לפני כל הגופים הרלוונטיים על תקיפות שמתרחשות באותו מגזר. קיימים שלושה סוגי SOC: ברמת הארגון - ניטור אירועי סייבר, הצגת תמונת מצב, הצגת מידע פרטני; ברמת המגזר - איגום מידע מעובד הכולל אירועי סייבר שמתרחשים במגזר מסוים; וברמת המדינה - איגום מידע מעובד הכולל אירועי סייבר שמתרחשים בכלל המגזרים.

קיימות שתי חלופות נפוצות לאופן ההקמה וההפעלה של SOC:

1. **הפעלה עצמית של הארגון:** בשיטה זו נדרש צוות מיומן ומשאבים טכנולוגיים גדולים. כמו כן יש להביא בחשבון זמן הקמה ארוך יחסית של כמה חודשים. היתרון המרכזי בשיטת הפעלה זו הוא ההיכרות הצמודה עם מערכות הארגון והאיומים שאיתם הוא מתמודד.

2. **שירותי MSSP[20] מנוהלים:** שירות הניתן כמיקור חוץ מטעם חברות המתמחות בכך. ארגונים מסוימים מעדיפים הפעלה בצורה כזו עקב הצורך בכוח אדם מומחה, בצוותי תגובה לאירועים ובזמינות במשך 24 שעות שבעה ימים בשבוע. בדרך זו לעיתים ניתנות ללקוח שירותים נוספים בתחומי הגנת הסייבר, כגון מבדקי חדירה תקופתיים ובנייה ותחזוקה של מדיניות ונוהלי עבודה.

המדיניות שפרסם משרד התחבורה קובעת כי המשרד יקים SOC שירכז את תמונת המצב של כלל הגופים במגזר התחבורה, לרבות גופי תמ"ק. ה-SOC יאפשר זיהוי פעילויות חריגות בסייבר, הן ברמת הגוף הבודד והן ברמה המגזרית, ויסייע לגופים בהתמודדות עם אירועי סייבר. עוד נקבע כי ה-SOC יהנה מגישה למידע ומודיעין ברמה הלאומית, נוסף על מודיעין ייעודי בתחום התחבורה, וכי כלל הגופים במגזר יידרשו להתחבר אליו.

בשנת 2019 פרסם מערך הסייבר נוהל המגדיר את עבודת יחידות הסייבר המגזריות להגנת הסייבר מול מערך הסייבר[21]. בנוהל הוגדר כי באחריות ממונה הגנת הסייבר המגזרית לפעול להקמת SOC.

יצוין כי משרדי ממשלה אחדים, כדוגמת משרד האנרגיה ומשרד הבריאות, מפעילים SOC רחב המנטר את פעילות המשרד ואת המגזר.

בחודשים מאי עד יולי 2020 בוצעה בדיקה מקדמית (פיילוט) של הפעלת SOC במגזר התחבורה באמצעות רש"ת, שבה השתתפו ארבעה גופים מתחומים שונים ובהם אחד המוגדר כתמ"ק. יצוין כי לכל הגופים למעט אחד מהם לא היה ניטור עצמאי במועד ביצוע הבדיקה המקדמית.

ביולי 2020 דיווחה רש"ת לאגף הסייבר במשרד התחבורה על סיכום הפיילוט. מהסיכום עולה כי במהלך הפיילוט טופלו התראות ואירועים בשיתוף פעולה עם גופי התחבורה שחוברו ל-SOC; נבנתה תשתית לחיבור מהיר של גופי התחבורה השונים (כשבוע ימים לחיבור של כל גוף ל-SOC); נבנתה מערכת שמציגה תמונת מצב סייבר אחודה של גופי התחבורה המחוברים ל- SOC לטובת משרד התחבורה; ונבנה ותורגל מנגנון המאפשר טיפול מהיר באירועים מול גופי התחבורה שחוברו ל SOC- באופן ישיר. במכתבה הדגישה רש"ת כי היא יצאה לפיילוט מתוך הבנה משותפת שעם סיום מוצלח שלה יתחיל תהליך של חיבור כלל גופי התחבורה לשירות ה-SOC במתכונת של שירות מנוהל; כי נדרשת החלטה של המשרד לגבי המשכיות התהליך, קרי המשך ניטור הגופים במתכונת שירות מנוהל; וכי רש"ת ערוכה לספק את השירות לגופי התחבורה באופן מיידי.

מסיכום הפיילוט שבוצע באחד הגופים שהתחברו (חברה ז') עלה כי חיבור ל-SOC חדש הוא תהליך מורכב מאוד המצריך עבודת ניהול, טיוב והתאמה רבה הן מצד ספק ה-MSSP והן מצד הגוף המתחבר אשר נמשכת זמן רב. צוין כי קשה לאמוד בפיילוט של חודשיים את היכולות

20 Managed Security Service Provider.

21 "נוהל אב להגדרת מסגרת אחריות משרדי הממשלה ויחידות הסייבר המגזריות למול אגף הכוונת ואסדרת המשק במערך הסייבר הלאומי בהיבטי הגנת מגזרי המשק למול איומי סייבר", גרסה 1.0 (20.05.19).

הכלליות של השירות הניתן מכיון שלא נבחנו כלל היכולות, ולא בוצע תרגיל תקיפה במטרה לבחון את אופן הזיהוי והדיווח של האנליסטים. עם זאת, חברה ז' הביעה שביעות רצון גבוהה מהפיילוט וציינה לחיוב כמה היבטים ובהם: האפשרות לשיתוף ידע מגזרי; התקשרות מול גורם MSSP עם ידע בעולמות ה-IT וה-OT[22] (אף שעולמות ה-OT לא נבחנו בפיילוט); צוות תגובה לתחקור אירועים; חיסכון בעלויות - הפחתת תקורת הניהול של מחלקת אבטחת המידע; ביצוע פעולות יזומות; וקבלת דוח שבועי המסכם את ההתראות. עם זאת צוינו גם כמה חסרונות ובהם העובדה שהידע והחוקה[23] לא נשמרים בגוף המתחבר.

בדצמבר 2020 שלח מנהל רת"א מכתב למנהלת אגף הסייבר במשרד התחבורה ובו נימוקים להתקשרות עם רש"ת כספק יחיד לשירותי SOC במגזר התעופה. במכתבו פירט מנהל רת"א כי מקומה המרכזי של רש"ת בתוך המערכת התעופתית הישראלית מקנה לה היכרות עם הגופים השונים והרבים המרכיבים את המערכת הזו, שעימם נבנו מנגנוני תיאום ושיתוף פעולה וממשקים טכנולוגיים רבים. עוד פירט כי במהלך הקיץ האחרון התבצע פיילוט מוצלח, שבמסגרתו חוברה, בין היתר, גם חברת תעופה אזרחית ל-SOC של רש"ת, ומידע משמעותי וערכי עבור חברת התעופה הצליח להתקבל ולתרום תרומה ניכרת בהיבט של הגנת סייבר עבור חברת תעופה זו.

בדיון שהתקיים בחודש ינואר 2021 בהשתתפות משרד התחבורה ונציגי אגף התקציבים במשרד האוצר ומערך הסייבר ציינה סמנכ"לית מדיניות במערך הסייבר כי כיום אין בידי המדינה תמונת מצב של מגזר התחבורה, ובכלל זה של גופי תמ"ק כמו נמלים, רכבות וגופים בתחום התעופה, וכי תפיסת העולם של מערך הסייבר היא שנדרש לייצר תמונה אחודה של מגזר התחבורה - משרד, מגזר ותמ"ק, כדי לאפשר לכל מקבלי ההחלטות, ובכלל זה ראש הממשלה, לרכז תמונת מצב עדכנית בזמן משבר או בעת חירום. עוד בדיון תיאר רמ"ח הנחיה במערך הסייבר את הצורך ביכולת עצמאית במשרד התחבורה, זאת בשל המומחיות המקצועית הנדרשת וההיכרות המעמיקה עם סוגי הכלים השונים ועם האלמנטים בתחום הבטיחות שעליהם המשרד מופקד, העשויים להיפגע כתוצאה מהתקפה במימד הסייבר.

ביולי 2021 פנה ראש מערך הסייבר אל שרת התחבורה וביקש, בין היתר, את השלמת הטיפול המשותף ב-SOC.

בדיון שהתקיים באוקטובר 2021 בנושא הגנת הסייבר במגזר התחבורה בראשות מנכ"לית משרד התחבורה הודגש כי פרויקט ה-SOC מתועדף גבוה על ידי השרה, וכי המשרד נדרש לפעול כדי להחזיק תמונת מצב בזמן אמת של גופי התחבורה במגזר, אשר כיום אינה בהישג יד של אף גורם ברמה הלאומית. בדיון צוין כי החלופה שבחר המשרד להקמת ה-SOC היא באמצעות רש"ת, וכי המנכ"לית מבקשת לפעול כדי לחנוך את ה-SOC עד סוף 2021 תוך טיפול בהיבטים המשפטיים (רש"ת כספק יחיד או הסכם שותפות של המשרד ורש"ת), התקציביים והמכרזיים.

בנובמבר 2021 אישרה ועדת המכרזים במשרד התחבורה התקשרות בפטור ממכרז עם רש"ת לצורך הקמה ותפעול של SOC לשישה חודשים עם אפשרות להארכה של שישה חודשים נוספים בהיקף כספי כולל של כ-4 מיליון ש"ח לשנה, בהתאם לפרוטוקול מיום 24.11.2021. במסגרת

22 OT - Operational Technology - מערכות המשמשות לתפעול, שליטה ובקרה. עם התפתחות הטכנולוגיה והקישוריות הארגונית לרשת האינטרנט, החלו ארגונים ומפעלים לשלב טכנולוגיות IT-Information Technology מודרניות במערכות OT ולעיתים אף לקשרן ישירות לרשת. התפתחות טכנולוגית זו חושפת את סביבת ה-OT - המערכות התפעוליות, לסיכונים ולאיומים שבעבר לא היו קיימים - איומי הסייבר.

23 אוסף ההגדרות והחוקים שבעזרתה מסווגות התראות על פעילות חשודה.

החוזה נקבע כי התמורה שתשולם לרש"ת תהיה תלויה בין היתר בהיקף המידע המועבר מכל גוף המחובר ל-SOC, לפי שלוש מדרגות שנקבעו לשם כך: עד EPS 1,000[24] , EPS 3,000 - 1,000, ויותר מ-EPS 3,000.

בדצמבר 2021 החלה רש"ת בהפעלת SOC עבור מגזר התחבורה. ביולי 2022 מסר משרד התחבורה למשרד מבקר המדינה כי עד כה חוברו ל-SOC 14 מתוך 35 גופים, מהם חמישה נמצאים בסטטוס "מבצעי", ותשעה מחוברים אך טרם "מבצעיים". להלן תרשים המתאר את סטטוס חיבור הגופים ל-SOC המגזרי, תחום הפעילות של הגוף והסיווג שלו (A,B,C):

תרשים 10: **סטטוס חיבור הגופים ל-SOC של מגזר התחבורה**

	ניטור מלא		צפייה בלבד	
1	גוף A	גוף A	תמ"ק	גוף B
2	גוף B	גוף C	תמ"ק	גוף B
3	גוף בהנחייה **משולבת***	גוף A	גוף A	גוף C
4	גוף בהנחייה **משולבת***	גוף B	גוף A	גוף C
5	גוף A	גוף B	גוף A	גוף C
6	גוף בהנחייה **משולבת***	גוף B	גוף B	תמ"ק
7	גוף A	גוף B	גוף A	תמ"ק
8	גוף A	משרד ממשלתי	גוף בהנחייה **משולבת***	תמ"ק
9			גוף A	גוף A
10			גוף A	

מבצעי ■ מחובר ■ ממתין לחיבור ■ לא הותנע ■

נכון ליולי 2022, על פי נתוני משרד התחבורה, בעיבוד משרד מבקר המדינה.

* לפי המדיניות הלאומית להגנת הסייבר בתעופה אזרחית, פעילות זמן אמת (ניטור באמצעות SOC) תהיה באחריות משרד התחבורה, תוך קיום ממשקים עם רת"א ועם מערך הסייבר.

עוד מסר משרד התחבורה למשרד מבקר המדינה בפברואר 2022 כי עקב תקציב מוגבל, הוקצו לארגונים מאוד גדולים (שלושה לפי הערכת משרד התחבורה) אמצעים שלא הספיקו לניטור כל הרכיבים החשובים בכל ארגון.

כמו כן נמצאו מספר חסמים עיקריים שמונעים את החיבור ל-SOC, בהם היעדר מיפוי נכסים עצמאי של הארגון הנדרש כהיערכות מקדימה לתהליך החיבור ל-SOC; זמינות גורמים טכניים

24 Events Per Second - אירועים לשנייה - מדד המתאר את נפח המידע המועבר מהגוף אל ה-SOC.

רלוונטיים בגוף המתחבר; והיעדר מוטיבציה מצד הגופים המתחברים. יצוין כי משרד התחבורה מציע את החיבור ל-SOC ללא עלות מצד הגופים אף שהוא משלם בעבורה.

בביקורת עלה כי לא נקבעה תוכנית עבודה מפורטת לחיבור ול"מיבצוע" של כלל הגופים ל-SOC, אף שההתקשרות מול רש"ת מתוכננת להסתיים לאחר כשנה (בדצמבר 2022) ואף שנכון ליולי 2022 מחוברים ל-SOC פחות ממחצית מהגופים (14 מתוך 35), מהם חמישה בלבד בסטטוס "מבצעי", 9 מחוברים אך לא "מבצעיים", 18 בסטטוס "ממתינים לחיבור", ושלושה בסטטוס "לא הותנע". עוד עלה כי ההתקשרות הנוכחית עם רש"ת אינה נותנת מענה מלא לארגונים גדולים.

מוצע כי משרד התחבורה יקבע לוח זמנים מפורט לחיבור כלל הגופים ולהפיכת חיבור זה ל"מבצעי". בנוסף מוצע כי המשרד ימפה את החסמים לחיבור ל-SOC של גופים שהוגדרו "ממתין לחיבור" או "לא הותנע" ויפעל לשחרור החסמים.

במועד סיום הביקורת, באפריל 2022, החל משרד התחבורה להקים SOC מגזרי זמני ולחבר אליו גופים בהדרגה - מהלך חשוב ומורכב שעשוי לתרום רבות למשרד בנוגע לקבלת תמונת מצב על הגנת הסייבר בגופים המנחים על ידו. נוכח טווח הזמן של כשנה שאושר להפעלת ה-SOC ברש"ת ומשך הזמן הדרוש לביצוע התקשרות מורכבת להקמת SOC, מומלץ כי משרד התחבורה יבחן, עוד במהלך תקופת ההתקשרות עם רש"ת, את האפשרויות העומדות לפניו להפעלת SOC בצורה קבועה. כן מומלץ למשרד התחבורה לבחון כיצד לנטר בצורה אפקטיבית גופים גדולים. נוכח העובדה שייקח זמן לחבר את כל הגופים ל-SOC, מוצע למשרד התחבורה לתעדף את הטיפול בגופים שונים ובגופים שאינם מנוטרים כלל.

חברה ז' מסרה בתשובתה ביוני 2022 כי מספר חודשים לאחר סיום הפיילוט התנתקה החברה מה-SOC שאליו היתה מחוברת והתחברה ל-SOC המגזרי, אשר להבנתה היה אמור להיות מבצעי לחלוטין ולספק כיסוי התראתי מלא לאירועי סייבר המאותרים במערכות החברה, זאת נוסף על סיוע ראשוני במקרה של אירוע. בפועל, לדעת חברה ז', ה-SOC המגזרי היה רחוק מלתת את המענה הנדרש לצורכי החברה - הן בנושא הגילוי וההתראה והן בנושא החקירה והתגובה, כאשר רמתו היתה נמוכה הן מהרמה שהתקבלה בפיילוט והן מזו של ה-SOC הקודם שהפעילה החברה. לפיכך, לאחר התייעצות עם משרד התחבורה, החברה הפסיקה להשתמש ב-SOC המגזרי לצורכי ניטור וקבלת התראות. לבקשת משרד התחבורה, חברה ז' נשארה מחוברת ל-SOC במטרה לאפשר למשרד לקבל תמונת מצב מגזרית (דשבורד). במקביל, חברה ז' התחברה ל-SOC אחר באופן פרטני, ומאז היא מקבלת את שירותי הניטור וההתראות מ- SOC זה.

משרד התחבורה מסר בתשובתו הנוספת מיולי 2022 כי הוא דוחה את טענות חברה ז'. המשרד ציין כי חברה ז' השתתפה בפיילוט והביעה שביעות רצון, ותוכננה להתחבר ל-SOC כגוף לצפייה בלבד ולא בחיבור מלא, אך עברה לניטור מלא עקב פער זמנים בהתקשרות עם חברה פרטית שתספק לה את השירות על מנת שיישמר לה רצף הניטור. המשרד הוסיף כי חברה ז' מנוטרת כיום על ידי ה- SOC המגזרי ובמקביל על ידי ספק פרטי, וכי השירות ב-SOC משתפר בעקביות, עם קבלת תמונת מצב ענפית ברורה וטיוב החיבורים וכוח האדם. המשרד הוסיף כי תהליך הפיכת גוף ל"מבצעי" דורש זמן וכי לאחר השלמת חיבור של גוף, מוזרמת תמונה מלאה על אודותיו ומצויה בידי המשרד.

מוצע שמשרד התחבורה יבחן בשיתוף חברה ז' את הסיבות לכך שה-SOC המגזרי לא סיפק עבור חברה ז' מענה הולם, ויבצע את הפעולות הנדרשות לתיקון.

הגנת הסייבר בפרויקטים חדשים

משרד התחבורה אחראי מטעם הממשלה להקמה ולניהול של התשתית התחבורתית במדינה, ומתוקף אחריות זו הוא יוזם ומבצע פרויקטים תחבורתיים שונים, אשר חלקם נשענים על תשתית טכנולוגית הפגיעה מטבעה לאיומי סייבר. עלות פרויקטים אלה מתוקצבת במיליארדי ש"ח מדי שנה. כך לדוגמה, ביצוע התקציב של סעיף "פיתוח תחבורה"[25] הסתכם בשנת 2019 בכ-25 מיליארד ש"ח ובשנת 2020 בכ-30 מיליארד ש"ח.

העלאת המודעות לחשיבות הטמעת הגנת הסייבר והקצאת משאבים לטובת יישומה בפועל, החל בשלב הייזום, דרך כל שלבי הקמת הפרויקט וכלה בהפעלתו השוטפת, חיוניות כדי למזער את פגיעותה של התשתית לאיומים המתעצמים.

המדיניות מגדירה כי חברות התשתית המבצעות פרויקטים תשתיתיים עבור המשרד, הכוללים מערכות ורכיבים טכנולוגיים, נושאות באחריות להגנת הסייבר של הפרויקט בכל שלביו, תוך ליווי ובקרה של אגף הסייבר. פרויקטים שיסווגו כתמ"ק יונחו על ידי מערך הסייבר הלאומי.

בספטמבר 2021 פרסם משרד התחבורה "נוהל עבודה להטמעת דרישות סייבר בפרויקטים תשתיתיים". בנוהל נקבע כי אגף הסייבר אחראי על הנחיה מקצועית ובקרה על הטמעת דרישות הגנת סייבר בפרויקטים. הנוהל גם מגדיר עקרונות כלליים להגנת הסייבר, לרבות תקצוב הנושא, איוש תפקיד של יועץ סייבר וקיום פגישות בקרה תקופתיות בהשתתפות הגורמים הרלוונטיים מטעם חברת התשתית המבצעת ואגף הסייבר.

לפי הנוהל, בתקצוב פרויקט יש להקצות משאבים לצורך הטמעת דרישות הגנת הסייבר בכל שלבי הפרויקט. בפרויקטים זכייניים התקצוב יכלול גם את ההפעלה השוטפת בהתאם לאומדן הבא:

1. יועץ לתכנון וביצוע - 60 שעות עבודה חודשיות, 300 ש"ח לשעה לכל אורך חיי הפרויקט.
2. השקעה במערכות הגנה - 10% מתקציב הטכנולוגיות.
3. תפעול שוטף - 8% מתקציב ה-IT, ובכלל זה: כוח אדם, רישיונות ושירותים בתשלום (ייעוץ, מבדקי חדירה, סקרי סיכונים, מודעות עובדים, SOC, צוותי התערבות וכדומה).

למשרד התחבורה פרויקטים רבים בשלבי תכנון בלבד או בשלבי ביצוע מוקדמים, ובהם: הרכבת הקלה חיפה-נצרת (רק"ל נופית); רכבל ירושלים; הקו הירוק והקו הכחול ברכבת הקלה בירושלים; הקו הירוק והקו הסגול ברכבת הקלה בגוש דן; ומערך המטרו בגוש דן. להלן תרשים המפרט כמה מהפרויקטים החדשים המתוכננים בשנים הקרובות:

25 סעיף תקציבי מס' 79 הכולל את תתי-הסעיפים האלה: תחבורה ציבורית; כבישים; בטיחות בדרכים; תמיכות בתחבורה; פיתוח אחר.

תרשים 11: **פרויקטים חדשים במגזר התחבורה**

המקור: משרד התחבורה, בעיבוד משרד מבקר המדינה.

בשנת 2017, במסגרת ההיערכות להקמת שני הנמלים החדשים, נערך דיון בהשתתפות נציגי משרד התחבורה, רשות הסייבר הלאומית (כיום - מערך הסייבר), חנ"י ונציגי הזכיינים המפעילים. בדיון זה הועלה הצורך בליווי הנמלים מבחינת היבטי הסייבר כבר בשלבים המוקדמים להקמתם מפאת המאפיינים הייחודיים שלהם. בסיכום הדיון נכתב כי "על בסיס החלטת ממשלה 2443 מיום 15.2.15, ההכוונה המקצועית בתחום הגנת הסייבר תהיה בהתאם לסמכות הרגולציה המופעלת על ידי משרד התחבורה. בהקשר האמור, הרשות הלאומית להגנת הסייבר תשמש כגורם מקצועי, אשר ינחה את משרד התחבורה בעניין זה".

בעניין נמלי הים החדשים, בפברואר 2020 שלחה מנהלת אגף הסייבר מכתב אל מנהל רשות הספנות והנמלים ובו ציינה כי בימים אלה נמצא המשרד בעיצומו של תהליך תכנון טכנולוגי במסגרת הקמת הנמלים החדשים. עוד צוין כי בשונה מהנמלים הקיימים, החדשים יהיו נמלים מודרניים שתפעולם יושתת על מערכות טכנולוגיות ממוחשבות לתפעול ואוטומציה, דבר המקנה יתר חשיבות לתכנון וליישום מדיניות, נהלים ואמצעי הגנה יעילים ומתקדמים להגנה מפני איומי הסייבר, וכי כל נמל כנכס אסטרטגי של מדינת ישראל, נדרש בהנחיה להתמודדות נגד איום הסייבר. במכתבה סקרה את הסיכונים האפשריים העומדים בפני הנמלים ואת פוטנציאל הנזק בהם - פגיעה בחיי אדם ובבריאות הציבור, וגרימת נזק כלכלי. מנהלת אגף הסייבר סיכמה את מכתבה בכך שבשלב הנוכחי, אין ביכולתה לפעול מול הנמלים החדשים ללא סמכות ואחריות.

כאמור בדיון ועדת היגוי סייבר במשרד התחבורה שהתקיים בנובמבר 2020 בראשות מנכ"ל המשרד דווח כי המשרד לא ביצע עד כה ביקורות בגופים בהיבטי סייבר, וכי בתחום התחבורה הימית לא מבוצעת פעילות סייבר.

משרד התחבורה מסר בתשובתו ביולי 2022 כי בעקבות הפנייה שלו לרשות הספנות והנמלים (שבוצעה כאמור בפברואר 2020) הובהר שקיימת למשרד סמכות מלאה באמצעות החוק להסדרת הביטחון[26] למתן הוראות לנמלים בענייני סייבר במסגרת כתבי ההסמכה של התאגידים המוסמכים בנמלים. בהתאם לכך הוסדרה הפעילות אל מול המפעילים השונים בנמל, ומאז ביצע המשרד ביקורות בנמלים והוסכם בין הצדדים על תוכנית עבודה, המנוהלת בשיתוף פעולה. המשרד הוסיף כי ממועד פרסום נוהל "עבודה להטמעת דרישות סייבר בפרויקטים תשתיתיים" בספטמבר 2021, כל פרויקט שעומד בתבחינים שהוגדרו עובר ליווי והכוונה של אגף הסייבר. לגבי הנמלים החדשים,

26 תיקון מס' 10 לחוק להסדרת הביטחון משנת 2019.

בשל התשתית המשפטית של הקמת הנמלים והפעלתם לא חלו לגביהם הוראות החוק להסדרת הביטחון בגופים ציבוריים. יחד עם זאת הדגשים לעניין סייבר ניתנו לנמלים החדשים על ידי המשרד כבר בהליך ההקמה, וקודם לאמצע שנת 2021, וזאת באמצעות גורם אחר על בסיס ההסכם מול מקימי הנמלים. כשהועברו התשתיות אל מפעילי המסופים תוקן החוק בהתאמה והחלה עבודת הפיקוח בנושא הסייבר ישירות מולם.

נמצא כי בשנים 2017 עד 2020 לא היה ברור מי המאסדר האחראי להנחיית הנמלים החדשים, והנמלים לא הונחו באופן סדור שהולם את הסיכונים בנוגע להיערכותם להתמודדות עם איומי סייבר, זאת עד שנת 2020 שבה הובהר למשרד התחבורה שקיימת לו סמכות מלאה. בהמשך לכך, בספטמבר 2021 פרסם המשרד נוהל עבודה להטמעת דרישות סייבר בפרויקטים תשתיתיים וביצע ביקורות בשני הנמלים החדשים באוקטובר ובנובמבר 2021, כאשר אחת מהביקורות בוצעה בסמוך להפעלת הנמל והועלו בה פערים שיש לתקן כתנאי להפעלת הנמל.

מומלץ כי משרד התחבורה יהיה מעורב בהיבטי הסייבר בפרויקטים חדשים עוד בשלבי התכנון, שכן בהתאם לתפיסת Security by Design זול יותר לשלב את דרישות הגנת הסייבר בשלבי תכנון הפרויקט מלהכניסן בשלבים מאוחרים שבהם יידרשו שינויים והתאמות, ויעקוב אחר יישום הדרישות בטרם מתן רישיון ההפעלה.

הרכב האוטונומי

בשנים האחרונות מתקדם בכל העולם פיתוחו של רכב אוטונומי, דהיינו רכב שמסוגל לנווט ולנסוע ללא התערבות פעילה של נהג אנושי באמצעות מערכת נהיגה עצמאית המשלבת רכיבי חומרה ותוכנה שמאפשרים לה שליטה על הרכב.

מדינת ישראל מצויה בחזית הפיתוח בתחום, וכיום יש כמה חברות, ישראליות וזרות, המבצעות בישראל ניסויים המדמים נסיעות של רכב אוטונומי. בניסויים אלו מערכת הנהיגה העצמאית מסיעה את הרכב אך יושב בו נהג בטיחות שתפקידו להשתלט על הרכב במקרה חירום. מלבד נהג הבטיחות לא מעורבים בניסויים נוסעים אחרים, והם אינם בעלי אופי מסחרי (כלומר, אין הסעות בתשלום).

הפעלת התחבורה האוטונומית מעוררת אתגרים וסיכונים בתחומים שונים הנוגעים להגנת הסייבר והפרטיות, ובהם: סיכונים לפגיעה בחיי המשתמשים או משתמשי הדרך הסמוכים לרכבים האוטונומים, באמצעות שיבוש מערכות הרכב בעת נסיעה באמצעות תקיפות במרחב הסייבר; וסיכונים לפגיעה בפרטיות באמצעות מידע הנאסף על ידי החיישנים והמצלמות הרבים המותקנים ברכבים אלו, האוספים מידע על המשתמשים ויתר משתמשי הדרך הסמוכים.

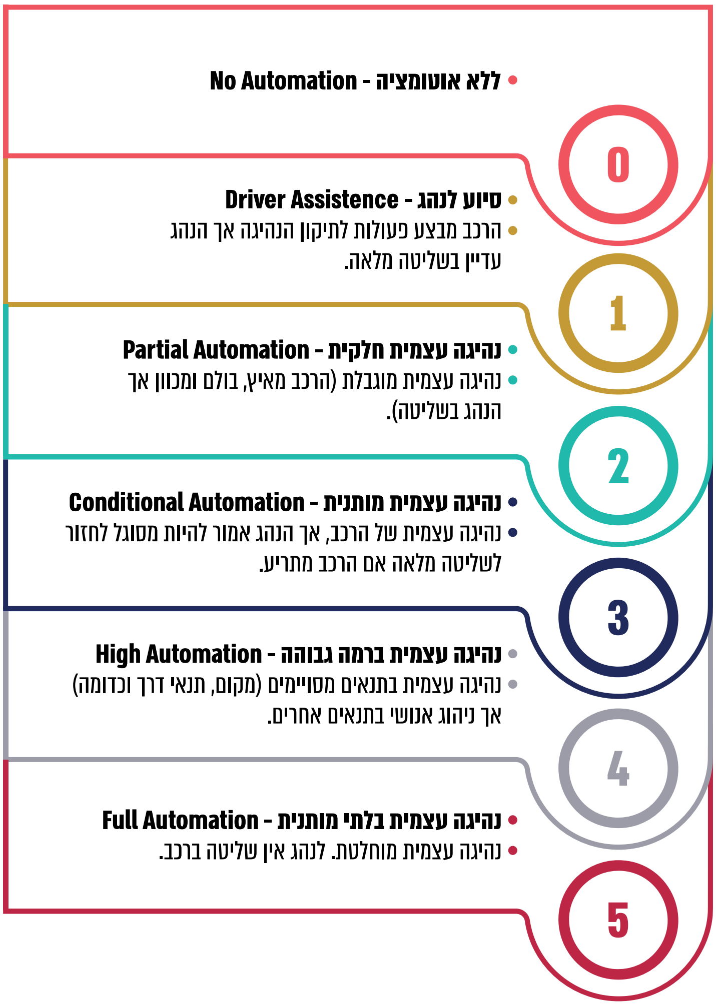
במרץ 2022 נחקק חוק לתיקון פקודת התעבורה[27] במטרה לאפשר נסיעה של רכבים אוטונומים בכבישי ישראל. החוק, שהוכן בשיתוף של משרד התחבורה ומערך הסייבר, נועד להסדיר את שלב המעבר מניסויים ברכבים אוטונומיים שבהם יושב נהג בטיחות כאמור, לנסיעות ניסיוניות ברכבים אוטונומיים ללא נהג כלל, ואף במסגרת של הסעת נוסעים בשכר או שלא בשכר. החוק כולל דרישות סייבר שעל המפעילים לעמוד בהן כתנאי לקבלת היתר הפעלה. משרד התחבורה

27 חוק לתיקון פקודת התעבורה (תיקון מס' 130), התשפ"ב-2022.

אחראי לבחון בשלב הניסויים, בליווי גורמים מומחים, את עמידת המפעילים בדרישות החוק. כן פרסם משרד התחבורה נוהל[28] שדורש מעבר במרכז הסייבר (אותו הקימו משרד התחבורה בשיתוף מערך הסייבר וחברת נתיבי איילון באמצעות קבוצת חברות שזכו במכרז) לבדיקות מקיפות של סייבר (ארבעה עד חמישה חודשי בדיקה) כתנאי למתן ההיתר.

מידת העצמאות של מערכות הנהיגה האוטונומיות מסווגת לחמש דרגות:

תרשים 12: **דרגות העצמאות של מערכות הנהיגה האוטונומיות**



המקור: מרכז המחקר והמידע של הכנסת, כלי רכב אוטונומיים - מדיניות ממשלתית, אתגרים והזדמנויות, דצמבר 2019, בעיבוד משרד מבקר המדינה.

28 הוראת נוהל - "הגנה בסייבר לרכב עצמאי" מיום 1.4.22.

דרגה 5 נוגעת לרכב המסוגל לבצע את מכלול פעולות הנהיגה. דרגה זו עדיין מצויה בפיתוח, ובהתאם לדברי ההסבר להצעת החוק, רכבים מסוג זה אינם צפויים להגיע לבשלות תפעולית בתקופה הקרובה.

משרד מבקר המדינה מציין לחיוב את הפעילות שנעשתה בתחום הרכב האוטונומי, לרבות תיקון החוק, פרסום הנוהל והקמת מרכז הניסויים בבאר שבע. עם זאת משרד התחבורה טרם החל בביצוע ביקורות בתחום זה.

מוצע שאגף הסייבר יבצע ביקורות באופן עצמאי על החברות שמבצעות ניסויים ברכב אוטונומי קודם הפעלת יכולת זו בכבישי ישראל ויחווה את דעתו בנוגע לסיכונים הקיימים בתחום זה ויוודא טיפול החברות בפערים שנמצאו בניסויים, ככל שאלו קיימים.

משרד התחבורה מסר בתשובתו מיולי 2022 כי ההצעה הוטמעה בחוק, המסמיך את מנהלת אגף הסייבר בשילוב גורמים מומחים לביצוע מעקב ובקרה. המשרד הוסיף כי הוראת הנוהל שפרסם באה לענות על דרישה זו והיא מיועדת להוות מסמך דרישות מפורט לבחינה מרגע הגשת הבקשה ועד למתן אישורי המשרד להפעלתם של רכבים עצמאיים בדרך ציבורית, כולל הוכחת היצרן להגנה בפני הגנת סייבר ואבטחת מידע.

שיתוף ידע בין הגורמים במגזר התחבורה

שיתוף ידע בין מתחרים

הגופים השונים במגזר התחבורה מתמודדים לרוב מול איומים דומים, ללא תלות בהגדרה של הגופים - גופי תמ"ק או גופים שאינם גופי תמ"ק, או בזהות החברה המפעילה. כך למשל, אירוע תקיפת סייבר המתרחש באחד מנמלי ישראל רלוונטי לידיעת כל יתר הנמלים כדי שיוודאו כי נתיב התקיפה של התוקפים אינו ניתן לניצול דומה בנמל אחר.

רשות התחרות פרסמה את עמדתה בנושא[29], ולפיה אף ששיתוף מידע בין מתחרים עשוי להוות, בנסיבות מסוימות, הסדר כובל על פי חוק התחרות הכלכלית, התשמ"ח-1988[30], אם שיתוף המידע אינו נוגע לפעילותם העסקית של הצדדים אלא אך ורק למידע הנדרש לצורך הגנת סייבר, כגון מידע על איומי סייבר, סממנים, חולשות, פוגענים ונוזקות וכן מתודולוגיות וכלי התמודדות עם איומי סייבר, רשות התחרות לא תראה בהעברתו כפעולה העלולה למנוע או להפחית את התחרות בעסקים, וזאת אף אם העברת המידע נעשית בין מתחרים. זאת מאחר ששיתוף מידע בעל ערך אבטחתי הוא חלק משמעותי מיכולת ההתמודדות של גופים עם איומי סייבר, ומדינת ישראל רואה חשיבות רבה בעידוד גופים במשק לשתף ביניהם מידע בעל ערך אבטחתי.

29 גילוי דעת 3/17: שיתוף מידע לצורך התמודדות עם איומי סייבר.

30 שמו המתוקן של חוק ההגבלים העסקיים.

בביקורת עלה כי אף שרשות התחרות לא רואה בהעברת מידע על איומי סייבר כפעולה העלולה לפגוע בתחרות, הרי שבפועל שיתוף המידע בין גופים דומים הוא חלקי. למשל: במערכות בתחום התחבורה - רק בשישה מתוך שנים עשר הגופים שנבדקו (50%) קיים שיתוף ידע בנושא הגנת הסייבר[31]; בתחום הים - נמצא כי נמל כ' ונמל כ"א, הנמצאים שניהם בתהליכים דומים לצורך שיפור רמת ההגנה בסייבר, אינם משתפים ידע אחד עם השני בתחום הגנת הסייבר.

היעדר שיתוף מידע בתחום איומי הסייבר עלול לגרום לכך שחברה אשר מצוי בידיה מידע קריטי (למשל ניסיון פגיעה באמצעות ניצול חולשה במערכת), לא תעביר מידע זה למקבילתה אף שבכך תוכל למנוע נזק משמעותי.

מומלץ כי משרד התחבורה יפעל למסד תשתית מתאימה (למשל באמצעות הקמת פורומים מקצועיים ומערכת שיתוף מידע) ולעודד את הגופים השונים לשתף האחד את השני במידע מקצועי בנושא הסייבר, גם כאשר הם מתחרים זה בזה, ובהתאם לכללי התחרות והסייגים לעניין הסייבר החלים עליהם. מומלץ כי המשרד ישקול להשתמש ב-SOC המגזרי גם כתשתית לשיתוף אירועים ופעולות לטיפול באירועים אלו שקורים בכלל המגזר. שימוש באופן זה אף עשוי להגביר את התועלת של הגופים משימוש ב-SOC.

חברת נמל כ"א מסרה בתשובתה ביוני 2022 כי שיתוף ידע בין הנמל לגורמים הנוספים מבוצע באמצעות מערך הסייבר אשר מעביר לידיעתם עדכונים בדבר אירועי אבטחת מידע שאירעו, לרבות בנמל כ', וכי אין לה התנגדות להשתתפות בפורומים משותפים ביוזמת משרד התחבורה.

חברת נמל כ' מסרה בתשובתה ביוני 2022 כי היא מברכת על ההמלצה ומעוניינת בשיתוף הידע, בתיווכו ובניהולו של מערך הסייבר.

הכנת תבנית לצורך פרסום מכרזים בתחום הסייבר

מינהל הרכש במשרד האוצר מפרסם מכרזים מרכזיים עם ספקים בתחום הסייבר עבור רכש תוכנה ושירותים במחירים ובתנאים שסוכמו בין המדינה לבין הספק[32]. מכרזים אלו מיועדים לשימוש משרדי הממשלה ויחידות הסמך בלבד.

במגזר התחבורה, בדומה למגזרים אחרים, כל גוף - לרבות חברות ממשלתיות המשמשות זרועות ביצוע של משרד התחבורה, מכין בעצמו את המכרזים. מכרזים אלו עוסקים לעיתים באותם הצרכים, וזוכים בהם אותם הספקים, למשל בנושאים כגון הקמת SOC ארגוני, רכש מערכות

---

31 מפורט להלן בממצאי השאלונים בפרק "מצב ההגנה בסייבר במגזר התחבורה".

32 "מכרז הנערך מטעם החשב הכללי בעבור המשרדים" - הוראת תכ"ם בעניין "מכרז מרכזי והתחייבות ספק למחירים מרביים" קובעת כי "במקרים שבהם מצא מינהל הרכש כי מרבית משרדי הממשלה רוכשים טובין/שירותים/עבודות, שחלקם ברי תחרות וחלקם לא, יבחן עריכת מכרז מרכזי או חתימה על התחייבות ספק למחירים מרביים, במטרה להסדיר את תנאי ההתקשרות ולנצל את יתרון הגודל של כלל המשרדים".

הלבנה או גיוס יועצים בתחום הסייבר. תהליך הכנת מכרז בגוף ציבורי, משלב הכנתו ועד ההחלטה על הספק הזוכה, הוא תהליך מורכב שנמשך זמן רב וכרוך במשאבים רבים[33].

בשנת 2016 הכין מערך הסייבר תבנית אחידה לצורך גיוס יועצי סייבר על ידי משרדי ממשלה, המבוססת על מכרזים שפרסמו קודם לכן יחידות סייבר מגזריות שונות. בסופו של דבר לא אושרה תבנית זו והתהליך הופסק.

בשנת 2021, במסגרת תהליכי החשיבה המחודשת על החלטה 2443, צוין כי בנושא הרכש הממשלתי "דרוש שיפור של המנגנון ויישומו בפועל. אולי גם לעשות את הרכש המרוכז על ידי המערך, כדוגמה... נדרשת תפיסה הוליסטית בנושא".

בביקורת עלה כי לא קיימת תבנית לצורך פרסום מכרזים בתחום הסייבר לשימוש הגופים במגזר. מומלץ כי מערך הסייבר ואגפי הסייבר המגזריים, ובהם אגף הסייבר במשרד התחבורה, יעלו צרכים משותפים בתחום הסייבר לצורך הכנת תבניות שיוכלו לשמש את כלל הגופים במגזר (לדוגמא: גיוס יועצים; רכש כלים; רכש שירותי התערבות באירועים (IR); הקמת ותפעול SOC), תבניות אלו יוכלו לשמש את כותבי המכרז ולחסוך להם זמן וכן ליצור אחידות בדרישות הבסיס של כל תחום התקשרות, אליהם יוסיף כל גוף את הנושאים הרלוונטים לו.

33 ראו פירוט: מבקר המדינה, **דוח שנתי 69ב** (2019), "היבטים בהתקשרויות משרדי ממשלה בתחום התקשוב".

מצב ההגנה בסייבר במגזר התחבורה

פערי ידע בתחומים מסויימים

נמצא כי הנחיות מסויימות בנוגע למערכות בתחום התחבורה, כוללות פרקים אשר לא התעדכנו משנת 1981, ואינן כוללות את היבטי הגנת הסייבר הנדרשים על מערכות אלו. מומלץ כי משרד התחבורה יעדכן את ההנחיות כך שיכללו גם דרישות בנושא הגנת הסייבר.

בדיקת מצב הגנת הסייבר בתחום התחבורה באמצעות מבדק חדירה ושאלונים

משרד מבקר המדינה בדק את מצב הגנת הסייבר בתחום התחבורה באמצעות הכלים האלו: מבדק חדירה, תשאול בעלי תפקיד בתחום הגנת הסייבר והעברת שאלונים. מבדק החדירה והתשאול בוצעו בעירייה א'. שאלונים הבודקים את רמת הגנת הסייבר נשלחו לעשר רשויות מקומיות ולשתי חברות ממשלתיות.

תרשים 13: **שיטות הבדיקה של הגנת הסייבר**

משרד הפנים מופקד על תכנונה ויישומה של המדיניות הלאומית בנושאי השלטון המקומי. פעילות המשרד כמאסדר מתבצעת בשני מישורים: במישור הארצי - מתן הנחיות וקביעת מדיניות, ובמישור המחוזי - קיום קשר עם הרשויות באמצעות הדרג הביצועי. המשרד מפקח

מטעם הממשלה על הרשויות המקומיות ואחראי להכוונת פעולותיהן בהתאם לחוק ולמדיניות הממשלה[34].

אגף הסייבר במשרד הפנים: החלטת הממשלה 2443 עסקה במשרדי הממשלה המחילים את סמכויות הרגולציה שלהם על גופים או פעילויות החשופים לאיומי סייבר. בעקבות קבלתה של החלטת הממשלה האמורה, הוקם בשנת 2017 אגף הסייבר במשרד הפנים כיחידה מקצועית מגזרית בתחום הגנת הסייבר ואבטחת המידע הכפוף למינהל לשירותי חירום במשרד הפנים ובהנחיה מקצועית של מערך הסייבר, ובין היתר הוטלה על האגף האחריות להסדרת היערכותן של הרשויות המקומיות לאיומי סייבר. באגף מועסקים ארבעה יועצים חיצוניים המומחים לאבטחת מידע, אשר נותנים שירות לרשויות המקומיות. תפקיד היועצים ללוות את הרשויות המקומיות בתחום אבטחת המידע והגנת הסייבר, לייעץ להן באופן שוטף ולסייע בקביעת מדיניות ותוכניות עבודה ולהציב יעדים להגברת החוסן של הרשויות המקומיות.

אגף הסייבר במשרד התחבורה אחראי להנחיית מערכות בתחום התחבורה המנוהלות על ידי חברות התשתיות (שתי חברות ממשלתיות) ועירייה א'. במסגרת זאת אגף הסייבר סיווג את הגופים האלו כגופי A, והנחה אותם במסגרת פרסום המדיניות בינואר 2021, כמו את יתר גופי A, ליישם אותה עד ינואר 2023.

ממצאי השאלונים שעלו ממענה הרשויות המקומיות ושתי חברות ממשלתיות

פירוט הממצאים הכלליים שעלו בשאלונים

להלן סיכום מצב ההגנה בתחומים שנבדקו, על בסיס הממצאים שעלו בשאלונים:

34 בעניין זה ראו מבקר המדינה, **דוח שנתי 70ב** (2020), בפרק "ההיערכות הממשלתית ליישום טכנולוגיות מתקדמות ברשויות המקומיות - מיזם ערים חכמות", עמ' 412 - 413.

תרשים 14: מצב ההגנה בתחומים שנבדקו במסגרת שאלון בתחום התחבורה

תחום	השאלה	שיעור הגופים שבהם נמצא הליקוי
כללי	כתיבת דרישות בתחום הסייבר או אבטחת המידע במכרז לבחירת הספקים	שיעור גבוה
	קיום פורום לשיתוף ידע עם מערכות אחרות בתחום התחבורה	שיעור בינוני
ממשל תאגידי	ביצוע מבדקי חֲדירות לאיתור פרצות אבטחה	שיעור גבוה
	ביצוע סקרי סיכונים	שיעור גבוה
	קיום תוכנית להתאוששות עסקית	שיעור בינוני
	מינוי ועדת היגוי סייבר	שיעור בינוני
	מינוי בעלי תפקידים שאחראים להגנת הסייבר ולאבטחת המידע	שיעור נמוך
	קיום שרתי גיבוי	שיעור נמוך
ארכיטקטורה וטכנולוגיה	קיום סביבת בדיקות, שבה נבדקים היבטי סייבר	שיעור גבוה
	חיבור למערכת אבטחת מידע א'	שיעור גבוה
	חיבור למערכת אבטחת מידע ב'	שיעור גבוה
	התקנת עדכוני אבטחת מידע	שיעור בינוני
	קיום אנטי-וירוס	שיעור נמוך
	מערכות הפעלה ישנות	שיעור נמוך
	קיום חומת אש	שיעור נמוך
תיעוד וניטור	חיבור למרכז בקרה	שיעור גבוה
	קבלת התראה אוטומטית בנושא מסוים	שיעור נמוך
	שמירת לוגים	שיעור נמוך
ניהול משתמשים והרשאות	נושא א' בתחום ניהול המשתמשים וההרשאות	שיעור גבוה
	נוהל להסרת משתמשים	שיעור בינוני
	מנגנון בקרה מסוים	שיעור נמוך
גישה מרחוק	נוהל עבודה לגישה מרחוק של ספקי המערכת	שיעור בינוני
	הקלטה או שמירה של לוג של פעילות הספק בעת החיבור מרחוק	שיעור נמוך

שיעור גבוה | שיעור בינוני | שיעור נמוך

החלת המדיניות על הגופים שאליהם הועבר השאלון: במועד סיום הביקורת, המדיניות חלה על שלושה גופים בתחום התחבורה המוגדרים כגופי A[35]. כאמור, המדיניות קובעת כי גופי מגזר התחבורה יסווגו לשלוש רמות דירוג: A,B,C, בהתאם לחומרת הפגיעה האפשרית באינטרס חיוני למדינה כתוצאה מתקיפת סייבר. דירוג זה נקבע על ידי ועדה בראשות ראש אגף בכיר ביטחון חירום וסייבר במשרד התחבורה, כאשר אחת לשנה אמורה הוועדה לדון בהוספת או הסרת גופים מהרשימה בהתאם לקריטריונים ולאפיון הגופים.

הליקויים שעלו בשאלון נמצאו גם בעיריות שבהן מערכות בתחום התחבורה טרם סווגו, ולכן אינן נדרשות לעמוד בדרישות המדיניות.

בהתאם לתבחיני הנזק אשר למולם מתבצע תהליך דירוג הגופים, לדעת משרד מבקר המדינה העיריות העוסקות בהיבט שנבחן בדוח זה בתחום התחבורה עומדות בתבחינים לשם סיווגן כגוף A או B. לכן, מומלץ כי משרד התחבורה יעדכן את סיווג הגופים כך שעיריות אלו יידרשו לעמוד בדרישות המדיניות.

מתוך ראייה צופה פני עתיד, הדוח כולל המלצות גם עבור עיריות העוסקות בהיבט שנבחן בדוח זה בתחום התחבורה שאינן מסווגות כיום כגופי A או B ולפיכך המדיניות אינה מחייבת אותן כיום מבחינה פורמלית, אך צפויה לחייבן לאחר ביצוע עדכון סיווג הגופים על ידי משרד התחבורה.

עירייה י' מסרה בתשובתה כי היא רואה חשיבות בביצוע פעולות שתכליתן להיערך לקראת החלת המדיניות גם עליה, ולפיכך מינתה גורם בעירייה שיוכשר להתמודדות עם אתגרי הסייבר העומדים לפתחה.

היעדר מערכות בתחום התחבורה: עיריות מסוימות השיבו כי אין להן מערכת מרכזית בתחום זה.

ספקים: נמצא כי חברות אחדות נותנות שירות למערכות בתחום התחבורה לכל הגופים בתחום, וכן נמצא כי מערכות אלה מבוססות על מספר מועט של תוכנות.

אירועים שהתרחשו: כל הגופים דיווחו כי למיטב ידיעתם לא התרחשו אצלם אירועי סייבר הקשורים למערכות בתחום התחבורה בשנים 2019 עד 2021.

פירוט הממצאים העיקריים שעלו בשאלונים

1. מבנה ארגוני תומך הגנת הסייבר

לפי המדיניות, בגוף עליו חלה המדיניות, יש למנות לפחות את בעלי התפקידים האלה: ממונה הגנת הסייבר, מנהל הגנת הסייבר וכן ועדת היגוי להגנת הסייבר. יצוין כי בגופים רבים המחזיקים מאגרי מידע, בעלי תפקידים וחברי ועדות אלה מכהנים בתפקידם בגוף

35 משרד התחבורה מסר בתשובתו ביולי 2022 כי שני גופים אמנם מסווגים כגופי A, אך אינם כפופים לאגף הסייבר במשרד ונעזרים בשירותיו באופן וולנטרי וזמני.

ממילא מתוקף החובות לפי תקנות אבטחת מידע. נוסף על כך, לפי המדיניות, על ועדות היגוי הסייבר להתכנס אחת לחצי שנה לפחות.

התחום	השאלה
ממשל תאגידי	האם יש בגוף בעלי תפקידים שאחראים להגנת הסייבר ולאבטחת המידע במערכות בתחום התחבורה?
ממשל תאגידי	האם מונתה ועדת היגוי סייבר במסגרת הגוף?

נמצא כי בשיעור קטן בגופים שהשיבו על השאלון לא קיימים בעלי תפקידים שאחראים בצורה רשמית ומעשית להגנת הסייבר בגוף ככלל ובתחום התחבורה בפרט. בעירייה ה' נמצא כי קיימים בעלי תפקידים בתחום הגנת הסייבר, אך הם אינם עוסקים בתחום התחבורה. עוד נמצא כי בשיעור בינוני בגופים שנבדקו לא קיימות ועדות היגוי העוסקות בנושא הגנת הסייבר.

על העיריות האמורות למנות את בעלי התפקידים הנדרשים וכן למנות ועדת היגוי בנושא סייבר ולכנסה בקביעות. מינוי בעלי התפקידים והתכנסות ועדת ההיגוי יאפשרו להנהלת העירייה לקבל תמונת מצב ברורה של מצב הגנת הסייבר של מערכות הארגון ביחס לסיכונים הקיימים, לטפל בפערים הקיימים, לדון באירועי סייבר שהארגון חווה ולעקוב אחר העמידה במימוש תוכנית העבודה המוגדרת.

עירייה ח' מסרה בתשובתה כי היא מקבלת את ההערה בנושא ועדת היגוי סייבר, והיא תפעל להקים ועדה שכזאת עם בעלי התפקידים הרלוונטיים ברשות.

עירייה י' מסרה בתשובתה כי אף שהמדיניות אינה חלה על העירייה, היא תפעל למנות ממונה או מנהל הגנת סייבר וכן תפעל להקמת ועדת היגוי סייבר.

2. קיום דרישות בתחום הסייבר או אבטחת המידע במכרז לבחירת ספקים בתחום התחבורה

שרשרת האספקה משמשת במקרים רבים ערוץ לתקיפת הארגון: מחד התוקפים מנצלים את האמון הקיים בין הספק ללקוח, ומאידך את החולשות והפרצות אצל הספק שעלולות לאפשר גישה לרשת הארגון. לפיכך הארגון נדרש להבטיח את רמת ההגנה בסייבר גם אצל הספקים ואצל קבלני המשנה שלו. מערך הסייבר פרסם מתודולוגיה סדורה בנושא שרשרת האספקה וסיפק כלים לבחינת מידת ההגנה של הספק.

לגבי **התקשרויות קיימות**, הגוף נדרש למפות ולהעריך את הסיכונים הגלומים בהתקשרויות הקיימות עם כל אחד מהספקים הרלוונטיים, ועבור ספקים מהותיים יש לבצע מבדק בידי בודק תאימות סייבר שמוסמך לבדוק את שרשרת האספקה הארגונית. בהתאם לממצאי המבדקים והשאלונים, הגוף נדרש לגבש וליישם תוכנית לצמצום הסיכונים מול הספקים בכלים העומדים לרשותו. כלים אפשריים לדוגמה: סיום ההתקשרות עם הספק במקרה של סיכון חמור לארגון; בניית תוכנית משותפת עם הספק לטיפול בליקויים ופיצוי כספי במידת הצורך; ובקרות מפצות פנים-ארגוניות. **במכרזים והתקשרויות חדשות** הגוף

נדרש לכלול דרישות סייבר, בהתאם לדירוג הסיכון של הספק, כך שספקים מהותיים יידרשו להציג תעודת "ספק מאושר" מטעם גוף בדיקה מורשה.

התחום	השאלה
כללי	האם היו דרישות בתחום הסייבר או אבטחת המידע במכרז לבחירת ספקים של מערכות בתחום התחבורה?

נמצא כי בשיעור גבוה בגופים שנבדקו לא היו בהתקשרות עם ספקי מערכות בתחום התחבורה דרישות הנוגעות להגנת הסייבר. יצוין כי לספקים אלו יכולת התחברות למערכות ועדכון התוכניות מרחוק. עוד יצוין כי החוזים בתחום זה הם לעיתים ארוכי טווח - לדוגמה בעירייה ב' חלק מהחוזים יסתיימו בשנת 2031, ובעירייה ה' החוזה יסתיים בשנת 2025 עם אפשרות הארכה לחמש שנים נוספות.

מוצע כי העיריות האמורות ימפו ויעריכו את הסיכונים הגלומים בהתקשרויות קיימות שאינן כוללות דרישות סייבר, ויבצעו את דרישות המדיניות לגבי התקשרויות חדשות - נושא זה מהותי בעיקר בהתקשרויות שעתידות להסתיים בעוד שנים רבות.

עוד מוצע כי משרד התחבורה יכין בשיתוף מערך הסייבר ומשרד הפנים נספח דרישות סייבר אחיד הנוגע למערכות בתחום התחבורה.

עירייה ב' מסרה בתשובתה כי בחוזה יש דרישה למערכת בקרת גישה מסוימת וכי בימים אלה מיושמת המערכת.

עירייה ו' מסרה בתשובתה כי מוטמע בכל המכרזים החדשים נספח אבטחת מידע, אך ההסכם עם הספק נחתם קודם הטמעת הנספח וישולב בחידוש ההסכם הבא. העירייה הוסיפה כי היא מבצעת סקרי אבטחת מידע גם לתחום התחבורה ועומדת על השלמת התיקונים מול הספק.

עירייה ה' מסרה בתשובתה כי היא תידרש לבצע סקר סיכונים והגדרת דרישות אבטחת מידע וסייבר למול ספק בתחום התחבורה.

עירייה ז' מסרה בתשובתה כי היא תעביר דרישה לספק להחיל את דרישות הרגולציה בתחום אבטחת המידע במסגרת ההסכם בינו לבין העירייה.

עירייה ט' מסרה בתשובתה כי תשמח אם משרד התחבורה או משרד הפנים יוציאו הנחיות לשלטון המקומי המפרטות מה נדרש לכלול במכרזים אלו.

3. קיום פורום לשיתוף ידע בתחום התחבורה

מערכות בתחום התחבורה בגופים השונים מתמודדות עם איומים דומים ולעיתים אף זהים הנוגעים לתחום התחבורה. הקמת פורום לשיתוף ידע בין הגופים השונים עשויה לתרום להעלאת הרמה המקצועית של העוסקים בתחום, תוך שיתוף הדדי של מידע על הסיכונים ועל דרכי ההתמודדות שנקט כל גוף, על הכלים ועל הפתרונות שיושמו. דוגמאות לכך הינן:

תובנות מתהליכי יישום רכיבי אבטחה כמו חומת אש ואנטי וירוס; תובנות מתהליך חיבור למרכזי SOC בהם בחרו הגופים להשתמש; ושיתוף מידע אודות התקפות אותן חוו הגופים והדרך בה נקטו לטיפול בהן.

התחום	השאלה
כללי	האם יש לכם פורום לשיתוף ידע בתחום התחבורה?

הועלה כי אין פורום ממוסד לשיתוף מידע בין הגופים השונים העושים שימוש במערכות בתחום התחבורה. עוד עלה כי לשיעור בינוני בגופים שנבדקו אין קשר מקצועי עם גופים אחרים בעניין הגנת הסייבר על תחום התחבורה ברשות.

מוצע כי משרד התחבורה ייצור בשיתוף מערך הסייבר ומשרד הפנים, פורום לשיתוף ידע במערכות בתחום התחבורה, זאת לצורך שיפור רמת ההגנה בסייבר בתחום זה.

עירייה ה' מסרה בתשובתה כי אם יקום פורום לשיתוף ידע בתחום התחבורה, העירייה תשתתף בו, וכי קיים פורום מקצועי למנהלי אבטחת מידע ברשויות.

4. ניהול סיכונים

במדיניות נקבע כי הגוף המגזרי נדרש להכין תוכנית רב-שנתית ולבצע סקרי סיכוני סייבר ומבדקי חדירה תקופתיים למוצרי אבטחה, למערכות, לתשתיות ולתהליכים מרכזיים, וכי הטיפול בממצאי הסקרים ישולב בתוכניות העבודה השנתיות. התוכנית תכלול סקר מקיף של כלל תשתיות הארגון אחת לשנתיים, ומומלץ לשלב סקרי עומק ייעודים על מערכות או תשתיות ייעודיות באופן עיתי. קיום מבדקי חדירות וסקרי סיכונים יאפשר לארגון לקבל תמונת מצב מפורטת בנוגע לפערי ההגנה בסייבר הקיימים בתשתיות ובמערכות הארגון ולפעול לתיקונם.

התחום	השאלה
ממשל תאגידי	האם בוצעו סקרי סיכונים בעניין מערכות בתחום התחבורה בשנים 2019 - 2021?
ממשל תאגידי	האם בוצעו מבדקי חֲדִירוּת לאיתור פרצות אבטחה במערכות בתחום התחבורה בשנים 2019 - 2021?

נמצא כי בשיעור גדול בגופים שנבדקו לא בוצעו סקרי סיכונים בשנים 2019 עד 2021. כמו כן נמצא כי בשיעור גדול בגופים שנבדקו לא בוצעו מבדקי חדירה בשנים 2019 עד 2021.

על הגופים האמורים לקיים סקרי סיכונים בהתאם למדיניות הגנת הסייבר של משרד התחבורה.

על הגופים האמורים לקיים מבדקי חדירות בהתאם למדיניות הגנת הסייבר של משרד התחבורה.

חברה ז' מסרה בתשובתה כי היא בתהליך התקשרות עם יועץ לצורך ביצוע סקר סיכונים כולל למערכות הארגוניות, וכי לפי תוכנית העבודה של החברה יבוצעו בשנת 2023 מבדקי חדירה למערכות אלו.

עירייה ב' מסרה בתשובתה כי בדצמבר 2021 היא ביצעה סקר סיכונים, ובכוונתה לבצע מבדקי חדירות לאחר קבלת המסקנות וההמלצות ממנו, או בתוך 18 חודשים מביצוע הסקר, המוקדם שבהם.

עירייה ג' מסרה בתשובתה כי סקר סיכונים במערכות בתחום התחבורה בוצע בשנת 2017, וכי רוב המלצות הסקר בוצעו. העירייה הוסיפה כי סקר נוסף מתוכנן לשנת 2022.

עירייה ה' מסרה בתשובתה כי ההערה מקובלת, וכי סקרי סיכונים ומבדקי חדירות בתחום התחבורה יבוצעו עד סוף שנת 2022.

עירייה ז' מסרה בתשובתה כי היא תיזום התקשרות עם חברה שעוסקת באבטחת מידע לצורך ביצוע סקר סיכונים ומבדקי חדירות.

5. תוכניות המשכיות עסקית והתאוששות מאסון

במדיניות נקבע כי הנהלת הגוף המגזרי נושאת באחריות הכוללת להיערכות בסייבר למצבי משבר, ויהיה עליה לנהל את המשבר אם יתממש. במסגרת זו עליה להכין תוכנית המשכיות עסקית והתאוששות מאסון, הכוללת בין היתר תוכנית להתמודדות עם משבר שמקורו בסייבר, ולהקים אתר חלופי (DR) מופרד ומרוחק גיאוגרפית. כן יש ליזום ולבצע אחת לשנה לפחות תרגילים ניהוליים ותרגילים טכניים לבדיקת ההיערכות ויכולת ההתאוששות ממשבר, לזיהוי פערים ולהנעת תוכנית פעולה לשיפור.

התחום	השאלה
ממשל תאגידי	האם יש ברשותכם תוכנית להתאוששות עסקית הנוגעת לתחום התחבורה?
ממשל תאגידי	האם יש ברשותכם שרתי גיבוי?

נמצא כי בשיעור בינוני בגופים שנבדקו אין תוכנית התאוששות עסקית, וממילא הם לא תרגלו תוכנית זו.

על הגופים האמורים להגדיר תוכנית התאוששות עסקית הכוללת פירוט של התהליכים העסקיים, הסיכונים החלים עליהם והגדרת המענים הניהוליים והטכנולוגיים להתמודדות איתם.

עיריית ה' מסרה בתשובתה כי המערכת בתחום התחבורה נמצאת אצל הספק. ספק העירייה הוסיף כי אם יתבקש על ידי העירייה להכין תוכנית התאוששות עסקית הוא ישתף פעולה.

6. סביבת בדיקות להיבטי הסייבר במערכות בתחום התחבורה

להקמת סביבת בדיקות נודעת חשיבות רבה, וזאת כדי לאפשר בחינה מוגנת של תוכנות חדשות, עדכוני אבטחה וגרסאות תוכנה לתוכנות קיימות קודם העלאתם לסביבת הייצור.

התחום	השאלה
ארכיטקטורה וטכנולוגיה	האם יש ברשותכם סביבת בדיקות, שבה נבדקים היבטי סייבר?

נמצא כי בשיעור גדול בגופים שנבדקו אין סביבת בדיקות, וגם אם יש, היא משמשת לבחינה פונקציונלית ולא לבחינת היבטי סייבר. במצב זה העלאת עדכוני תוכנה עם נוזקה ישירות לסביבת הייצור עשויה לגרום לאירוע סייבר ואף להפסקת השירות לזמן ממושך.

עירייה ב' מסרה בתשובתה כי היא ביצעה בדצמבר 2021 סקר סיכונים, וכי לאחר יישום המלצותיו תישקל הקמת סביבת בדיקות.

עירייה ג' מסרה בתשובתה כי עדכוני תוכנה מבוצעים ישירות על השרתים עם יכולת חזרה לאחור ברזולוציה של שעה, וכי לא קיימת סביבה או יכולת לבדיקות סייבר של תוכנות. העירייה הוסיפה כי עדכוני תוכנה או קושחה אינם יכולים להתבצע מרחוק.

עירייה ו' מסרה בתשובתה כי ברשותה מערכת אבטחת מידע ב' לסריקת עדכונים קודם הכנסתם לרשת המוגדרת כרשת רגישה ונפרדת, וכי שרת המערכת הווירטואלי מוקשח לגישה רק מכתובות IP ספציפיות.

משרד מבקר המדינה מציין כי הכלים שצוינו בתשובות חלק מהעיריות אינם נותנים מענה מלא לסיכון שקיים בהכנסת פוגען או חולשה ישירות לסביבת הייצור, זאת בהיעדר שימוש בסביבת בדיקות.

מוצע לגופים האמורים לבחון העלאת עדכוני תוכנה ועדכוני אבטחה לסביבה שונה מסביבת הייצור, אם על ידי שימוש בשרת צדדי ואם על ידי הקמת סביבת בדיקות מלאה. עוד מוצע כי משרד התחבורה יבחן את הסיכון הקיים בהיעדר סביבת בדיקות במרבית הגופים ויקים סביבת בדיקות אחודה עבור הגופים השונים במסגרת המרכז לסייבר בתחבורה חכמה הממוקם בבאר שבע.

7. עדכוני אבטחת מידע

שימוש במערכות הפעלה ישנות שאינן נתמכות עוד על ידי היצרן: מערכת הפעלה היא תוכנה המנהלת את משאבי החומרה והתוכנה במחשב. יצרניות מערכות ההפעלה מפיצות מפעם לפעם עדכוני תוכנה, ובהם כאלה המיועדים לצורך תיקוני פרצות אבטחה שהתגלו במערכת. מערכות ההפעלה נתמכות שנים אחדות לאחר הפצתן, ולאחר מכן היצרן מפסיק להפיץ עדכונים למערכת, לרבות עדכוני אבטחה. כלומר, כדי להמשיך ולקבל את עדכוני האבטחה, על משתמשי מערכות ההפעלה לדאוג לשדרוג הגרסאות מפעם לפעם לצורך המשך קבלת העדכונים מצד היצרן.

עדכוני אבטחת מידע למערכות בתחום התחבורה: בדומה למערכות ההפעלה, גם לרכיבים בתחום התחבורה מופצים מפעם לפעם עדכוני תוכנה על ידי היצרנים, ובהם כאלה המיועדים לצורך תיקוני פרצות אבטחה שהתגלו במערכת.

התחום	השאלה
ארכיטקטורה וטכנולוגיה	אילו מערכות הפעלה משמשות את המערכות בתחום התחבורה? השאלה נועדה לבחון אם נעשה שימוש במערכות הפעלה שאינן נתמכות על ידי היצרן.
ארכיטקטורה וטכנולוגיה	באיזו תדירות ביצעתם בשנים 2019 - 2021 עדכוני אבטחת מידע במערכות בתחום התחבורה?

שימוש במערכות הפעלה ישנות שאינן נתמכות עוד על ידי היצרן: באף אחד מהגופים שנבדקו לא קיימת גרסה ישנה של מערכת הפעלה אשר אינה נתמכת עוד על ידי יצרן המערכת.

עדכוני אבטחת מידע במערכות בתחום התחבורה: נמצא כי בשיעור בינוני בגופים שנבדקו לא בוצעו בשנים 2019 עד 2021 התקנות סדירות של עדכוני אבטחת המידע (כלומר בתדירות של פעם בשנה לפחות), ובעירייה ז' לא בוצעו כלל עדכונים אלו.

על העיריות האמורות לקיים תהליך ניהול עדכונים שוטף לצורך טיפול בחולשות אבטחה המתגלות מפעם לפעם בתשתיות המחשוב שבאחריותן כדי להפחית את הסיכון להתרחשותם של אירועי סייבר.

עירייה ז' מסרה בתשובתה כי היא תבחן לשלב את המערכות בתחום התחבורה בנוהל עדכוני אבטחת המידע של כלל מערכות העירייה.

8. רכיבי אבטחה המותקנים במערכות בתחום התחבורה

קיימים כמה רכיבי הגנה מקובלים המיושמים ברשתות מחשבים רגישות בכלל וברשתות המשמשות את תחום התחבורה בפרט: חומת אש - רכיב ברשתות מחשבים החוסם או מאפשר תעבורת רשת על פי סט קבוע או משתנה של חוקים; אנטי-וירוס - תוכנה שמיועדת לאתר וירוסי מחשב ולהגן על המחשב מפני פעילותם.

התחום	השאלה
ארכיטקטורה וטכנולוגיה	אנא ציינו אם כל אחד מרכיבי האבטחה הבאים מיושם במערכות בתחום התחבורה:
	חומת אש
	אנטי-וירוס
	מערכת אבטחת מידע א'
	מערכת אבטחת מידע ב'

חומת אש: נמצא כי רכיב זה מיושם בכל הגופים שנבדקו.

אנטי-וירוס: נמצא כי רכיב זה מיושם בשיעור גדול בגופים שנבדקו.

מערכת אבטחת מידע א': נמצא כי מערכת זו אינה מיושמת בשיעור גדול בגופים שנבדקו. כן נמצא כי בעירייה ו' רכיב זה מיושם חלקית.

מערכת אבטחת מידע ב': נמצא כי מערכת זו אינה מיושמת בשיעור גדול בגופים שנבדקו.

חברה ז' מסרה בתשובתה כי בוצעה בחינה על ידי החברה, ונמצא כי פתרונות מערכת אבטחת מידע א' אינה מתאימה ליישום בסביבת המערכות בתחום התחבורה של החברה, ולפיכך החברה פועלת להגדרת בקרות מפצות ונמצאת לקראת ביצוע הוכחת היתכנות (POC) לבחינת הפתרון המתאים.

עירייה ב' מסרה בתשובתה כי קיימת ברשותה מערכת דומה למערכת אבטחת מידע ב' והיא סבורה שאין לה צורך במערכת אבטחת מידע ב'.

עירייה ג' מסרה בתשובתה כי מערכות א' וב' לא יושמו מפאת היעדר תקציב.

עירייה ד' מסרה בתשובתה כי אכן מערכת אבטחת מידע א' אינה מיושמת. עם זאת, מאחר שהמערכת בתחום התחבורה היא מערכת עצמאית שאינה מקושרת למערכות העירייה, אין לדעתה צורך במערכת.

עירייה ה' מסרה בתשובתה כי היא תבצע סקר סיכונים מול ספק מסוים בתחום התחבורה, ובמסגרתו יועברו המלצות לתיקון פערים אם יימצאו.

עירייה ז' מסרה בתשובתה כי היא תפעל בהקדם להתקנת אנטי וירוס ומערכת אבטחת מידע א' בתחום התחבורה.

עירייה ו' מסרה בתשובתה כי היא תבחן את הנושא.

על הגופים האמורים לבחון את הצורך ביישום כל אחד מרכיבי ההגנה לעיל שאינם מיושמים אצלם ולהתקינם במידת הצורך. יובהר כי כל אחד מרכיבי ההגנה מספק מענה לצורך אחר ואינם מהווים תחליף האחד לשני.

9. תיעוד וניטור

קיום תהליכי תיעוד וניטור אפקטיביים הוא מרכיב חשוב במעטפת ההגנה בסייבר בארגון, המאפשר לזהות אירועי סייבר בזמן אמת ולקיים תחקור טכני של האירועים לצורך התמודדות איתם ומניעת חזרתם.

נמצאו פערים בתחום התיעוד והניטור של מערכות בתחום התחבורה. נושאים אלו הוצגו לגופים והם מסרו בתשובתם כי הם פועלים לטיפול בממצאים.

התחום	השאלה
תיעוד וניטור	האם קיים חיבור למרכז בקרה?
תיעוד וניטור	האם מתקבלת התראה אוטומטית בנושא מסוים?
תיעוד וניטור	האם נשמרים לוגים של הפעילות במערכות בתחום התחבורה?

חיבור למרכז בקרה: נמצא כי בשיעור גדול בגופים שנבדקו מערכות בתחום התחבורה אינן מחוברות למרכז בקרה בנושא מסוים.

שמירת לוגים של הפעילות במערכות בתחום התחבורה: בכל הגופים שנבדקו נשמרים הלוגים במערכות בתחום התחבורה ונבדקים בידי בעלי תפקידים שונים בהתאם לצורך. נמצא כי בעירייה ד' אומנם הלוגים נשמרים, אך הם אינם נבדקים בידי אף גורם.

התראה אוטומטית בנושא מסוים: בשיעור גדול בגופים שנבדקו נשלחת התראה למרכז הבקרה בנושא מסוים, למעט בעיריות ב' וד'.

10. ניהול משתמשים והרשאות במערכות בתחום התחבורה

נמצאו פערים בתחום ניהול המשתמשים וההרשאות. נושאים אלו הוצגו לגופים והם מסרו בתשובתם כי הם פועלים לטיפול בממצאים.

ישנם כלים המאפשרים ניהול ושליטה מרכזיים של משתמשי המחשוב ומשאבי המחשוב בארגון וכן החלת מדיניות ארגונית, הגדרת הרשאות עבור משתמשים והתקנת תוכנות מרחוק. שימוש נכון בכלים אלו משפר את רמת אבטחת המידע באמצעות ניהול הרשאות יעיל ואף חוסך עלויות באמצעות ייעול ניהול המחשוב בארגון.

שינוי סיסמאות באופן עיתי והסרת משתמשים שאינם פעילים מקטינים את הסיכון לחדירה לארגון מצד גורם זדוני.

התחום	השאלה
ניהול משתמשים והרשאות	האם מבוצע מנגנון בקרה מסוים?
ניהול משתמשים והרשאות	נושא א' בתחום ניהול המשתמשים וההרשאות.
ניהול משתמשים והרשאות	האם קיים נוהל להסרת משתמשים (למשל לא פעילים או כאלו שעזבו את הארגון)?

הסרת משתמשים: נמצא כי בשיעור בינוני בגופים שנבדקו לא קיים נוהל להסרת משתמשים - למשל משתמשים שאינם פעילים או כאלה שעזבו את הארגון. בעירייה ד' ציינו כי אומנם קיים נוהל, אך בשנים 2019 עד 2021 בוצעה בעירייה בקרה בתדירות "נמוכה מאוד" על כך שלא קיימים משתמשים לא פעילים. יצוין כי לעיתים מדובר בעובדים בעלי מודעות נמוכה לאבטחת מידע, ובהם עובדי הארגון ועובדי הספק המתחברים מרחוק, שלהם הרשאות גישה לכלל התחום ולכן יש חשיבות עליונה להסרתם בעת שהם הופכים למשתמשים שאינם פעילים.

מומלץ לגופים האמורים ליישם את השינויים הנדרשים בתחום ניהול המשתמשים וההרשאות.

עירייה ה' מסרה בתשובתה כי ייקבעו למול ספק מסוים בתחום התחבורה דרישות אבטחה והגנת הסייבר מותאמים לדרישות מערך הסייבר הלאומי.

עירייה ו' מסרה בתשובתה לגבי הסרת משתמשים כי הרשאותיו של משתמש שעוזב את הארגון נמחקות מהרשת, וקיים דוח בקרה המוודא כי אין עובדים שעזבו וברשותם משתמש פעיל ברשת. כן הוסיפה העירייה כי תפעל לסגירת הפער.

11. גישה מרחוק

יכולת גישה מרחוק של עובדי הארגון או ספקיו לתשתיות הארגון מאפשרת לארגון לבצע את משימותיו בצורה אפקטיבית. עם זאת, החיבור מגדיל את "משטח התקיפה" ומשית סיכונים רבים על הסודיות, הזמינות והמהימנות של המידע בארגון. באחריות הארגון לבצע ניהול סיכונים לתהליך הגישה מרחוק וליישם בקרות מתאימות להגנה בסייבר על מנת להתמודד איתם. כך לדוגמה, באפריל 2022 היו בעירייה א' 38 משתמשים המורשים להשתמש בהיבט מסוים בתחום התחבורה - מתוכם 11 משתמשים חיצוניים שהם עובדי חברות פרטיות המספקות שירות לעירייה (מפתחים, טכנאי ויועץ), והם בעלי הרשאה לגישה מרחוק.

התחום	השאלה
גישה מרחוק	האם יש נוהל עבודה המסדיר את אופן הגישה מרחוק של ספקי המערכת?
גישה מרחוק	האם יש הקלטה או שמירה של לוג של פעילות של ספקי המערכת בעת החיבור מרחוק?

נמצא כי בכלל הגופים קיימת גישה מרחוק לתשתיות הארגון עבור ספקים ומפתחים. עם זאת, נמצא כי בחלק מהארגונים מענה ההגנה בסייבר הקיים בתשתית הגישה מרחוק אינו מותאם לסיכונים הרבים הנשקפים בגישה מרחוק.

נוהל עבודה המסדיר את אופן הגישה מרחוק של ספקי מערכות בתחום התחבורה: נמצא כי בשיעור בינוני בגופים שנבדקו לא קיים נוהל כאמור.

הקלטה או שמירה של לוג של פעילות ספקי המערכת בעת החיבור מרחוק: נמצא כי בשיעור קטן בגופים שנבדקו אין הקלטה או שמירה של לוג כאמור.

על הגופים האמורים לקיים תהליך ניהול סיכונים ובחינת מענה ההגנה המיושם בתהליך הגישה מרחוק ולפעול לטיפול בליקויים שיימצאו בתהליך זה.

☆

נוכח הממצאים שעלו מהשאלון, על הגופים שנבדקו לקיים הערכת מצב ולקבוע תוכנית עבודה לתיקון הליקויים.

מבדק חדירה במערכות בתחום התחבורה של עירייה א'

משרד מבקר המדינה ביצע בעירייה א' מבדק חדירה. מטרת המבדק הייתה לזהות חולשות העשויות לגרום לסיכונים הנוגעים לזמינות, למהימנות ולסודיות התשתיות, זאת באמצעות תרחישי תקיפה שונים העושים שימוש בחולשות אבטחה.

הבדיקה בוצעה בסביבת הייצור, ולכן ננקטו פעולות להפחתת הסיכונים שהשפיעו על תכנון המבדק ובהן: ביצוע המבדק רק על רכיבים ייעודיים שנבחרו בשלב תכנון המבדק; ביצוע המבדק על שרתי גיבוי ככל הניתן; הפעלת כלים אוטומטיים באמצעות סריקה מדורגת כדי שלא לפגוע בעומסים על השרתים; תשאול בנוגע לחלק מהרכיבים שהועלה חשש מהפעלת כלים עליהם; והיעדר ניצול חולשות שנמצאו במבדק אלא רק הוכחת יכולת.

משרד מבקר המדינה מציין לחיוב את שיתוף הפעולה מצד עירייה א' בכל שלבי מבדק החדירה: החל בתכנונו, דרך ביצועו, תהליך הצגת הממצאים והנכונות לשפר את התהליכים הקיימים וכלה בטיפול בחלק מהליקויים שנמצאו בזמן קצר ביותר.

להלן פירוט הממצאים שעלו במבדק החדירה בלבד. יצוין כי מבדק החדירה אומנם בוצע רק בעירייה א', אולם הממצאים העולים מהשאלונים הרוחביים מלמדים כי הליקויים בתחום זה על

פי רוב אינם ייחודים לרשות כזו או אחרת, זאת עקב העובדה כי תחום התחבורה ברשויות רבות דומה.

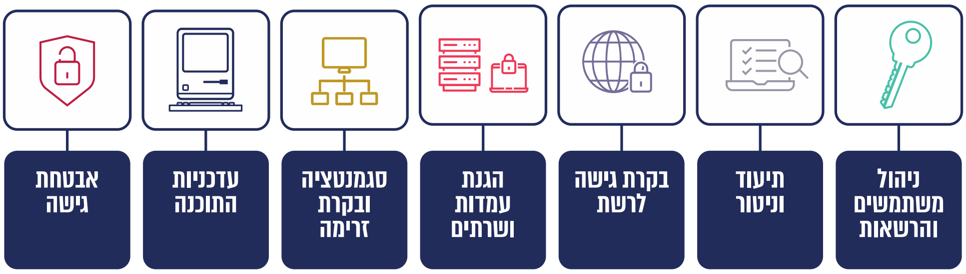
להלן תרשים המציג את השלבים בתהליך מבדק החדירה:

תרשים 15: **שלבי מבדק החדירה***

* המבדק לא כלל שלב של ניצול חולשות שהתגלו כדי שלא לייצר סיכון לרשת התפעולית.

להלן התחומים שבהם נמצאו ליקויים במסגרת מבדק החדירה:

תרשים 16: **התחומים שבהם נמצאו ליקויים במבדק החדירה (חלקם תוקנו עד מועד סיום הביקורת)**



הממצאים דורגו על פי שני תבחינים: **חומרת הנזק** הגלומה בהם, הנקבעת בהתאם לרמת ההשפעה על יכולת עירייה א' לקיים את התהליכים התפעוליים במקרה של התממשות הסיכון; ו**הסבירות להתממשות הסיכון**, המתייחסת לכל ממצא בנפרד ומביאה בחשבון את רמת

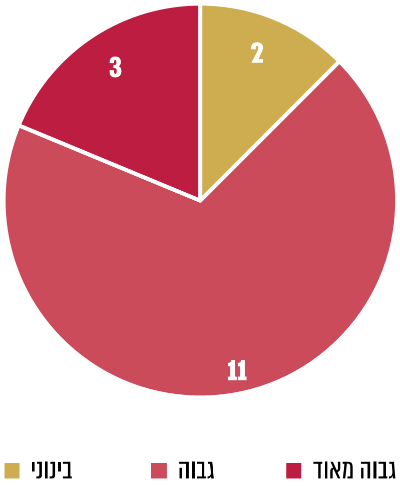
מורכבות ניצול הפער שהתגלה במסגרת הממצא. לכל תבחין ארבע דרגות אפשריות: גבוהה מאוד, גבוהה, בינונית ונמוכה. המכפלה בין שני התבחינים יוצרת את הערך הנקרא **רמת הסיכון**.

תרשים 17: **טבלת דירוג ניהול הסיכונים**

גבוהה מאוד				
גבוהה				
בינונית				
נמוכה				
חומרה / סבירות	**נמוכה**	**בינונית**	**גבוהה**	**גבוהה מאוד**

במהלך מבדק החדירה והתשאול שהתבצעו בעירייה א' זוהו 16 ממצאים משמעותיים בתחומים הבאים: ניהול משתמשים והרשאות; תיעוד וניטור; בקרת גישה לרשת; הגנת עמדות ושרתים; סגמנטציה ובקרת זרימה; עדכניות התכנה; ואבטחת הגישה. ממצאים אלו הוצגו לעירייה א' כבר בדצמבר 2021 לצורך תיקון וטיפול בהם וחלקם תוקנו עד מועד סיום הביקורת. להלן פילוח הממצאים לפי חומרתם:

תרשים 18: **פילוח הממצאים במבדק החדירה לפי חומרתם**



עירייה א' מסרה בתשובתה מיוני 2022 כי היא קיבלה את דוח הביקורת ולמדה היטב את ממצאיו במטרה לשפר באופן מתמיד את השירות שהיא מעניקה לציבור, והיא תפעל לתקן את הליקויים המופיעים בדוח.

נוכח הממצאים שעלו ממבדק החדירה, על עירייה א' לקיים הערכת מצב ולקבוע תוכנית עבודה לתיקון הליקויים.

☆

בסקר שערך משרד מבקר המדינה בעשר עיריות ובשתי חברות ממשלתיות עלו פערים מהותיים בין מצב הגנת הסייבר במערכות בתחום התחבורה לבין דרישות הסייבר של משרד התחבורה.

משרד התחבורה מסר בתשובתו מיולי 2022 כי אין לו סמכות הנחיה על מערכות בתחום התחבורה המופעלות ומתוקצבות על ידי הרשויות המקומיות עצמן, למעט מערכות בתחום התחבורה המנוהלות על ידי חברות התשתית ובעירייה א'.

משרד הפנים מסר בתשובתו מיולי 2022 כי הטיפול במערכות העירוניות בתחום התחבורה אינו בתחום עיסוקו, וכי הוא מסייע לרשויות המקומיות רק בנושאי מחשוב הקשורים לרשתות המינהלתיות הפנימיות שלהן. עוד מסר כי קיימים תחומי מחשוב נוספים שהעירייה אמונה עליהם והם אינם מטופלים על ידי אגף הסייבר במשרד הפנים, למשל מים וביוב.

מערך הסייבר מסר בתשובתו מיוני 2022 כי מערכות עירוניות בתחום התחבורה הן באחריות מלאה של הרשויות המקומיות הרלוונטיות, וכל היבטי התפעול בתחום זה נעשים על ידי הרשות.

יצוין כי בדוח מבקר המדינה משנת 2022 בנושא "ניהול מערכות מידע ברשויות מקומיות"[36] צוין כי משרד הפנים ומערך הסייבר לא השלימו את הסדרת הסמכויות החסרות בכל הנוגע לאסדרה ולהנחיה מקצועית של הרשויות המקומיות בתחומי אבטחת מידע והגנת הפרטיות, וכפועל יוצא מכך זה שנים הרשויות פועלות ללא הנחיות מקצועיות ברורות בנושא, וכל רשות פועלת בעניין לפי ראות עיניה.

נמצא כי כל המערכות בתחום התחבורה (למעט אלו המופעלות על ידי חברות התשתית ועירייה א') אינן מונחות על ידי משרד הפנים או משרד התחבורה, אף שיש בהם כאלו שפגיעה בהם עשויה לגרום לפגיעה כלכלית ניכרת ואף לפגיעה בחיי אדם.

נוכח הממצאים שעלו מהשאלון וממבדק החדירה בנושא הגנת הסייבר, מומלץ כי משרד הפנים ומשרד התחבורה בשיתוף מערך הסייבר יפעלו יחד להסדרת תחומי האחריות ביניהם ולקביעת נהלים מתאימים כך שנושא הגנת הסייבר במערכות בתחום התחבורה ברשויות המקומיות יקבל את המענה האסדרתי ההולם. זאת על מנת שגורם מנחה יבצע פיקוח ובקרה על תיקון הליקויים ועל הגנת המערכות מפני תקיפות סייבר.

36 מבקר המדינה, **דוח על הביקורת בשלטון המקומי** (2022), "ניהול מערכות מידע ברשויות מקומיות", עמ' 1269.

הממצאים שעלו בביקורות שביצע משרד התחבורה

לפי שגרות הניהול, על יחידות הסייבר המגזריות להעביר למערך הסייבר דיווחים עיתיים, בין היתר, בדבר ביקורות וסקרים בגופי המגזר.

בשנת 2021 ביצע אגף הסייבר במשרד התחבורה ביקורות בחלק מגופי A כדי לבחון את מצב הגנת הסייבר שלהם ואת מידת יישום המדיניות החדשה שפרסם. יצוין כי עקב היעדר איוש מלא של תקני כוח האדם באגף הסייבר בוצעה הביקורת באמצעות תשאול ושאלון למילוי עצמי. להלן תמונת המצב שעלתה מהביקורת שביצע משרד התחבורה:

תרשים 19: **תמונת המצב העולה מהביקורות שביצע משרד התחבורה**

גוף	דירוג	ניהול סייבר	טכנולוגיות הגנה	ניטור	תגובה	כללי
חברה ל"ג	A	גבוה	גבוה	גבוה	גבוה	גבוה
חברה ז'	A	גבוה	גבוה	בינוני	גבוה	גבוה
חברה ט'	A	גבוה	גבוה	גבוה	בינוני	בינוני
חברה ו'	A	בינוני	בינוני	בינוני	גבוה	בינוני
חברה ח'	A	בינוני	בינוני	נמוך	בינוני	נמוך
חברה נ'	A	בינוני	בינוני	נמוך	נמוך	נמוך
חברה כ"ב	A	בינוני	בינוני	נמוך	נמוך	נמוך
חברה י"א	A	אין נתונים	אין נתונים	אין נתונים	אין נתונים	אין נתונים
חברה ש'	A	בינוני	נמוך	בינוני	בינוני	נמוך
חברה כ"ג	A	בינוני	גבוה	בינוני	נמוך	נמוך
חברה כ"ד	A	גבוה	גבוה	בינוני	בינוני	גבוה
גוף א'	A	בינוני	בינוני	נמוך	נמוך	נמוך
גוף ג'	A	נמוך	בינוני	נמוך	נמוך	נמוך

גבוה   בינוני   נמוך   אין נתונים

על פי נתוני משרד התחבורה, בעיבוד משרד מבקר המדינה.

בביקורות שביצע מצא משרד התחבורה עלו ליקויים רוחביים בגופים שונים במגזר ביחס לדרישות שפורטו במדיניות. בהם ניתן למנות את הנושאים האלו:

1. ניטור ובקרה: ארגונים ללא ניטור או ניטור ברמה שאינה מספקת.
2. כוח אדם: בחלק מהארגונים אין כוח אדם ייעודי לניהול תחום הסייבר.

3. ניהול סיכונים בשרשרת האספקה: היעדר סיווג, היעדר נהלים, היעדר בקרות והיעדר שאלונים.

4. נהלים: פער בנוהלי ארגון בסיסים לניהול סייבר.

5. תקצוב: העדר תקציב הפוגע בתוכנית עבודה לקידום ולשיפור, לרכש מערכות ולרישיונות.

כך לדוגמה, בחברה ו' נמצאו פערים בתחום ניהול שרשרת האספקה; נמצא כי כל המשתמשים בחברה מוגדרים כמנהלי מערכת מקומיים, דבר המהווה חולשה ומעצים את יכולת התוקף לנצל את ההרשאות המקומית; נמצא כי אין מיצוי מיטבי של שירות ה-SOC של החברה; ונמצא כי אין תוכנית המשכיות עסקית לארגון.

משרד התחבורה מצא בביקורות שביצע שורה של ליקויים רוחביים המחייבים טיפול מערכתי. מומלץ כי המשרד יסייע לגופים לטפל בליקויים הרוחביים שעלו באמצעות ייעוץ והכוונה וכן יבחן לספק לגופים במגזר שירותים רוחביים שיקצרו את טווח הזמן לטיפול בליקויים. למשל, בתחומי הניטור והתגובה: התקשרות עם צוות תגובה שמשרד התחבורה יגיש לטובת כלל המגזר לטיפול במשברי סייבר; כתיבת תבניות סטנדרטיות למכרזי רכש לרבות התקשרות עם שירותי SOC/SIEM ויועצי סייבר; הנגשת נוהלי סייבר בנושאים כלליים; רכישת מוצרים לביצוע מבדקי חדירה ואפשרות לבצע ביקורות באמצעותם בכלל הגופים במגזר.

בביקורת נמצא כי משרד התחבורה לא ביצע מעקב אחר תיקון הליקויים שמצא בביקורות שביצע. מומלץ כי משרד התחבורה יבצע מעקב על הליקויים שמצא, תוך קביעת לוח זמנים לתיקונם על ידי הגופים.

חברה ז' מסרה בתשובתה ביוני 2022 כי הוגדרו בחברה תקני כוח אדם ייעודיים בתחומי הסייבר למימוש הפעילות, אך בשל תנאי השכר המגבילים שהיא יכולה לשלם ולאור הביקוש הגבוה במשק למקצועות אלה, נוצר קושי משמעותי בגיוס התקנים הללו. חברה ז' הוסיפה כי לגבי נושא התקצוב, קיימים פערים תקציביים משמעותיים בין הדרישות במדיניות לבין התקציבים הייעודיים שיש להקצות לנושא ושבלעדיהם לא ניתן יהיה לממש את הדרישות באופן מלא ושוטף. להלן חלק מהדרישות שפירטה חברה ז' שלגביהן קיים פער תקציבי: הדרישה לעמידה בתקן ISO27001 או תורת ההגנה 2.0; הדרישה להקצות תקציב ייעודי להגנת הסייבר בגובה 8% מתקציב ה-IT וכן 10% מתקציב הטכנולוגיות של פרויקטים חדשים; הדרישה להכין תוכנית המשכיות עסקית והתאוששות מאסון; והדרישה להבטיח את רמת הגנת הסייבר גם אצל הספקים וקבלני המשנה.

SOC בגופי מגזר התחבורה

אחד מהתחומים שבהם נמצאו פערים רוחביים במרבית גופי ה-A במגזר התחבורה הוא הקמת SOC ארגוני. לפי המדיניות, כל הגופים במגזר התחבורה נדרשים ליישם מנגנוני רישום ואיסוף אירועים לצורך ניטור אירועים חריגים, זיהוים והתראה עליהם. ניטור זה יופעל עבור מערכות הגנה, ממשקי ניהול של מערכות ההגנה, תשתיות, מערכות תפעוליות מרכזיות ומאגרי מידע של המשרד, ויבוצע באמצעות SIEM/SOC פנים-ארגוני או באמצעות שירות של חברה חיצונית (MSSP).

חיבור הגופים עצמם ל-SOC משלהם משפיע גם על אפשרות החיבור ל-SOC המגזרי, שכן חלק גדול מהנתונים המוצגים בו משתקפים ממרכזי ה-SOC של הגופים ומקלים על החיבור ל-SOC המגזרי.

מוצע כי אגף הסייבר בשיתוף הגופים ימפה בהקדם את הפעולות הדרושות להקמת SOC בארגונים שחסרים יכולות ניטור או לחיבורם ל-SOC המגזרי כמתן מענה ראשוני גם לארגון, תוך מתן עדיפות לגופי A שאינם בעלי יכולות ניטור.

זאת ועוד, מוצע שאגף הסייבר יגדיר מתודולוגיה סדורה להקמת SOC ארגוני המבוססת על ניסיונו בתחום, יבצע רכש מרכזי למוצר או לשירות MSSP וילווה את הגופים ליישום הפתרון ולהפעלתו, כדי לנהל את אירועי הסייבר ולהתריע בזמן אמת על התקפות במגזר התחבורה.

סיכום

תשתיות התחבורה נועדו להבטיח את הבטיחות והיעילות של התחבורה הימית, התחבורה האווירית והתחבורה היבשתית עבור כל משתמשי הדרך. ככל שתשתית מסוימת חיונית יותר לחיי היום-יום של התושבים, כך היא מושכת יותר את התוקפים וככל שהיא תלויה יותר בממד הסייבר, כך היא פגיעה יותר לתקיפות שעשויות לגרום לשיבושים בתפקודה התקין ואף להשבתתה המלאה, לפגיעה כלכלית ניכרת ולפגיעה בחיי אדם.

ממצאי דוח זה משקפים בעיה מבנית ותפקודית יסודית בכל הנוגע להערכות של מדינת ישראל לאיומי הסייבר במגזר התחבורה. במהלך הביקורת חל שיפור בכמה תחומים שבהם פועל אגף הסייבר במשרד התחבורה, ובהם: הקמת SOC מגזרי, פרסום מדיניות וביצוע ביקורות בחלק מהגופים המונחים לבחינת עמידת הגופים בה; קידום אסדרת תחום הרכב האוטונומי, לרבות תיקון החוק, פרסום נוהל והקמת מרכז הניסויים בבאר שבע. עם זאת עדיין קיימות כמה בעיות יסודיות:

חסרה הסדרת תחומי האחריות והסמכות של מערך הסייבר ומשרד התחבורה בכל הנוגע לגופים שאינם תמ"ק; משרד התחבורה אחראי לפעילויות המגזר אולם אין בידיו תמונה מלאה של מצב ההגנה של הגופים בו; היעדר הלימה בין האיומים והמענים להם במגזר כולו לבין המשאבים של משרד התחבורה; היעדר דרישות סייבר בהתקשרויות בחלק ניכר מהפעילויות במגזר והיעדר הקצאת המשאבים הנדרשים לכך על ידי הגופים.

הבעיה התפקודית והמבנית שהועלתה בדוח זה אפשר כי היא רלוונטית למגזרים גדולים נוספים, ולכן טיפול מערכתי בנושאים אלו עשוי לשפר את מוכנות המשק והמגזרים הגדולים הפועלים בו להתמודד עם אירועי סייבר.

במסגרת ביקורת זו בוצע מבדק חדירה על ידי צוות הביקורת בתחום התחבורה של עירייה א'. חשיבותה של פעולה חדשנית זו, שיושמה לראשונה בדוח ביקורת של משרד מבקר המדינה, הינה בכך שהיא מאפשרת להעריך את מוכנותו האמיתית של הגוף לעמוד בפני התקפות סייבר, באמצעות שימוש בכלים החושפים חולשות אבטחה בסביבת העבודה התפעולית של הגוף ולסייע בכך באופן מעשי וממשי לשיפור רמת ההגנה של הגופים המבוקרים.

על משרד התחבורה ועל מערך הסייבר לוודא כי תשתיות התחבורה ובפרט התשתיות הקריטיות, מבצעות הערכת סיכונים באופן שוטף ומשפרות את מידת עמידתן בפני מתקפות סייבר אפשריות.