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
מספר הגופים הפועלים במגזר התחבורה, לרבות בתחום הרכב הפרטי, התשתיות, התחבורה הציבורית, התעופה והים

4 מתוך 5
דירוג האיום על הפרטיות שקבעה הרשות להגנת הפרטיות בנוגע לתחום התחבורה

6 מתוך 30
20% מהגופים שמוגדרים כתשתיות מדינה קריטיות ומחזיקים במערכות ממוחשבות חיוניות שייכים למגזר התחבורה

7 שנים
משך העיכוב בחקיקת חוק הסייבר, שטרם הושלם, ביחס לנדרש בהחלטת ממשלה 2444 משנת 2015

36 מיליארד ש"ח
תקציב הפיתוח של משרד התחבורה לשנת 2022

6.3 מיליון ש"ח
התקציב שאושר לאגף הסייבר מתוך סך הדרישות שהגיש בסך 30 מיליון ש"ח (21%) נכון לדצמבר 2021

21 מתוך 35
60% מהגופים שמתוכננים להתחבר למרכז ניטור אירועי אבטחת מידע מגזרי (SOC) לא חוברו אליו עד מועד סיום הביקורת

0%
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 בתכננו, 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

הרשות להגנת הפרטיות - הגנת מידע אישי

מצב ההגנה בתחומים שנבדקו במסגרת שאלון על מערכות בתחום 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 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.