דוח מבקר המדינה - סייבר ומערכות מידע
אייר התשפ"ג | מאי 2023

המוסד לביטוח לאומי

אסדרת הגנת הסייבר במוסד לביטוח לאומי

אסדרת הגנת הסייבר במוסד לביטוח לאומי

רקע

בשנת 2021 הודלפו בעולם יותר מ-22 מיליארד רשומות עקב תקיפות סייבר[1]. שמות של אנשים ומספר ביטוח לאומי (ובהם SSN[2]) היו שני סוגי הנתונים שדלפו יותר מכל נתון אחר. נכון לנובמבר 2022, במוסד לביטוח לאומי (בט"ל) מתבצעות בכל יום כ-2.9 מיליון תקיפות סייבר בממוצע, ומהן כ-66,000 תקיפות עם פוטנציאל נזק.

בט"ל מעניק מגוון שירותים רחב למבוטחיו - תושבי מדינת ישראל - מהלידה עד הפטירה, ולפיכך למאגרי המידע של בט"ל רגישות מיוחדת הן בשל היקפם העצום והן מפני שהמאגרים מתממשקים לגורמים שמחוץ לבט"ל. להלן האסדרה הנורמטיבית העיקרית בנוגע להגנת הסייבר ואבטחת מידע: חוק הגנת הפרטיות, התשמ"א-1981, אשר מגדיר את החובות של בעל מאגר מידע, מחזיק מאגר מידע או מנהל מאגר מידע כהגדרתו בחוק, לאבטחת המידע שבו; תקנות הגנת הפרטיות (אבטחת מידע) התשע"ז-2017; וחוק להסדרת הבטחון בגופים ציבוריים, התשנ"ח-1998 (החוק להסדרת הביטחון), אשר קובע סמכויות ואחריות לאבטחה פיזית, אבטחת מידע ואבטחת מערכות מחשוב חיוניות של גופים ציבוריים שונים בתוכם, הן גופי ממשלה והן גופים בבעלות פרטית.

1 2021 Year End Report - Data Breach QuickView, RiskBased Security & Flashpoint (p. 3)

2 Social Security Number (יצוין כי בכמה מדינות כמו ארה"ב מספר ה-SSN שקול למספר ת"ז בישראל).

נתוני מפתח

22 מיליארד רשומות
דלפו בעולם בשנת 2021 עקב תקיפות סייבר

כ-2.9 מיליון
הממוצע היומי של תקיפות הסייבר על בט"ל

מאות טרה בייט (TB)
גודל בסיס הנתונים של בט"ל הכולל שדות על הנתונים האישיים של כ-9.5 מיליון מבוטחים בישראל

20 עובדים
בבט"ל (מהם 6 סטודנטים) מבצעים את הפיקוח על אבטחת המידע במערכות הממוחשבות שלו. לשם ההשוואה, לצה"ל המבצע גם הוא פיקוח עצמי יש אגף תקשוב וההגנה בסב"ר (סביבת רשת) בפיקוד קצין בדרגת אלוף

פעולות הביקורת

בחודשים אוקטובר - דצמבר 2022 בדק משרד מבקר המדינה את נושא אסדרת הגנת הסייבר בבט"ל. הבדיקה כללה מיפוי של הגופים המאסדרים את בט"ל כיום, בחינת הנזק האפשרי מהיעדר גורם מאסדר קבוע ובחינת הצורך בשינוי גורמי האסדרה. הביקורת נערכה בבט"ל, במערך הסייבר הלאומי, בשירות הביטחון הכללי וברשות להגנת הפרטיות במשרד המשפטים. ועדת המשנה של הוועדה לענייני ביקורת המדינה של הכנסת החליטה שלא להניח דוח זה במלואו על שולחן הכנסת אלא לפרסם רק חלקים ממנו, לשם שמירה על ביטחון המדינה, בהתאם לסעיף 17 לחוק מבקר המדינה, התשי"ח-1958 [נוסח משולב].

תמונת המצב העולה מן הביקורת

- **האסדרה של הרשות להגנת הפרטיות מול המוסד לביטוח לאומי** - בביקורת עלה כי מאז הקמת הרשות להגנת הפרטיות בשנת 2006 ועד מועד סיום הביקורת (יותר מ-16 שנה) ביצעה הרשות להגנת הפרטיות שישה הליכים מינהליים בנושא אבטחת מידע בבט"ל. אשר לפיקוח רוחב, רק באוגוסט 2022 החלה הרשות להגנת הפרטיות לבצע בפעם הראשונה פיקוח רוחב בבט"ל.

- **האסדרה של שירות הביטחון הכללי והממשק של מערך הסייבר הלאומי מול המוסד לביטוח לאומי** - בתוספת השנייה לחוק להסדרת הביטחון מופיעים הגופים הנדרשים להנחיה בנוגע לנושאים שסיווגם שמור עד סודי ביותר. גופים אלו מבצעים פיקוח עצמי, ויש בהם יחידות ייעודיות שמטרתן הגנה על מרחב הסייבר. בתוספת החמישית לחוק להסדרת הביטחון מופיעים הגופים המוגדרים בעלי תשתיות מידע קריטיות (תמ"ק) גופים אלו מונחים על ידי מערך הסייבר הלאומי (מס"ל). עלה כי בט"ל אומנם מופיע בתוספת השנייה אך אינו מוגדר בתוספת החמישית לחוק להסדרת הביטחון אף שהוא גוף שמחזיק במאגר מידע על תושבי מדינת ישראל. לפיכך, בט"ל מקבל הנחיה משב"כ בנוגע לנושאים המסווגים בלבד אך אינו נדרש להנחיה קבועה ממס"ל.

- **תהליך ה"הנחיה מרצון" של מערך הסייבר הלאומי** - החל בשנת 2016 החל מס"ל להנחות את בט"ל "הנחיה מרצון". משמעות הדבר היא שמס"ל מנחה את בט"ל כפי שהוא מנחה את גופי התמ"ק אולם לבט"ל אין חובה ליישם את ההנחיות. משיחות של צוות הביקורת עם בט"ל התברר כי רמת המעורבות של מס"ל לאורך השנים הלכה ופחתה: משנת 2016 עד 2020 ה"הנחיה מרצון" הייתה צמודה וכללה התייעצות שוטפת על בסיס יום-יומי; מסוף 2020 התחלפו שלושה מנחים וההנחיה הייתה מועטה ולא קבועה; ובמועד סיום הביקורת אין מנחה מטעם מס"ל אלא הקשר מתבצע באמצעות המוקד של מס"ל (CERT) המטפל בכלל אירועי הסייבר בישראל. לפיכך לבט"ל אין מענה שוטף ומערכתי לטיפול בכלל אירועי אבטחת מידע.

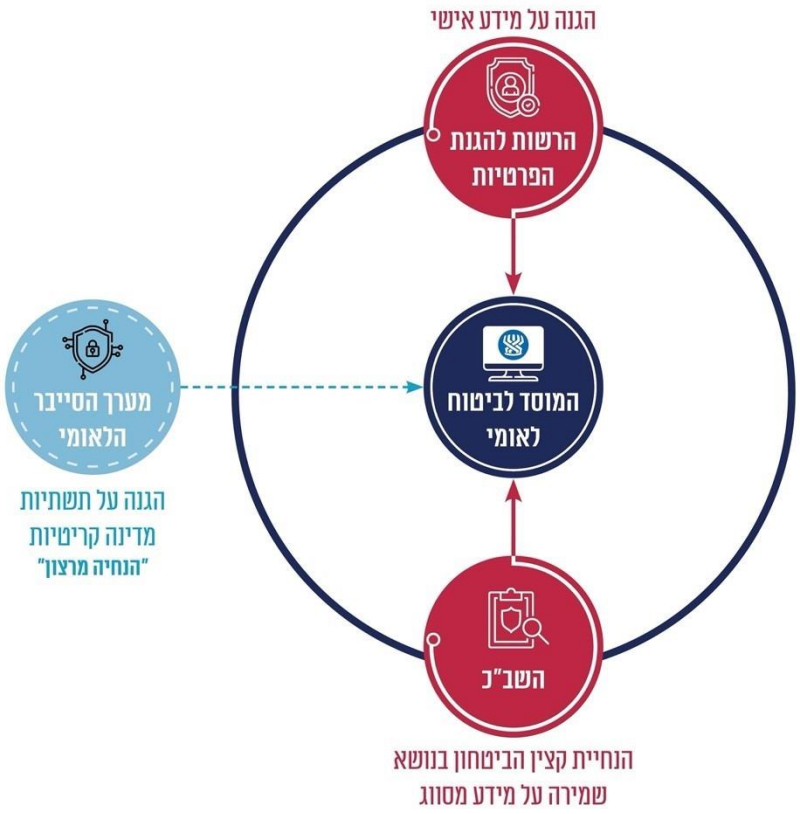
- **הניסיון להגדיר את בט"ל כגוף תשתיות קריטי (תמ"ק)** - בהחלטת הממשלה 84/ב משנת 2002 נקבע כי יש להקים ועדת היגוי עליונה[3] שתפקידה לבחון אילו גופים מוגדרים חיוניים ולכן זקוקים להגנה קיברנטית. נמצא כי נכון למועד סיום הביקורת - כשנתיים לאחר דיון בוועדת ההיגוי להגנה על מערכות ממוחשבות חיוניות שבו הוחלט להתחיל בחינה של בט"ל כגוף תמ"ק, מס"ל לא החל בהליך הבחינה. בבירור של צוות הביקורת במס"ל הועלה כי בכוונת מס"ל להתחיל בתהליך הבחינה של בט"ל כגוף תמ"ק ברבעון הראשון של שנת 2023. משמעות הדבר היא שבמועד סיום הביקורת בט"ל, המנהל מאגר מידע, אינו מונחה מקצועית באופן שוטף ומחייב, דבר העלול ליצור סיכון.

3 יו"ר ועדת ההיגוי הוא ראש מס"ל וחברים בה בין היתר נציגים ממשרד הביטחון, ממשרד המשפטים - ראש הרשות להגנת הפרטיות, מהמטה לביטחון לאומי, מצה"ל ומהשב"כ.

עיקרי המלצות הביקורת

- מומלץ כי ועדת ההיגוי להגנה על מערכות ממוחשבות חיוניות תקדם את הבחינה של בט"ל כגוף תמ"ק נוכח היקפי המידע השמורים בו והסיכונים לדליפתו.
- מומלץ כי עד סיום הבחינה של ועדת ההיגוי להגנה על מערכות ממוחשבות יוסדר ממשק מקצועי בין מס"ל לבט"ל לצורך מתן מענה ישיר, העברת דיווחים, בקרה על תיקון הליקויים וכיו"ב.
- מומלץ כי ועדת ההיגוי להגנה על מערכות ממוחשבות תבחן אם יש עוד גופים בעלי מאגרי מידע בהיקפים הדומים לבט"ל שיש לבחון את הגדרתם כגופי תמ"ק, ובכך תשפר את ההגנה על התשתיות החיוניות של מדינת ישראל.

גורמי האסדרה בתחום אבטחת המידע בבט"ל



סיכום

בדומה למדינות אחרות, ישראל חשופה לתקיפות סייבר לצורכי כופר וגניבת מידע. מלבד זאת, נוכח האקלים הגיאו-פוליטי המורכב ביטחונית, ישראל משמשת כר מטרות נרחב לתוקף הקיברנטי הפוטנציאלי, המעוניין לפגוע בחוסנה ובביטחון הלאומי שלה. גוף כדוגמת בט"ל, מחייב שיגובש עבורו מענה אסדרתי מספק הכולל הנחיה של מערך הסייבר הלאומי, הנחיה של הרשות להגנת הפרטיות ותיאום בין שניהם כדי להבטיח את ההגנה המיטבית. נוכח היקפי המידע השמורים בבט"ל והסיכונים לדליפתו מומלץ כי ועדת ההיגוי תקדם את הבחינה של בט"ל כגוף תמ"ק. מומלץ כי עד סיום הבחינה יוסדר ממשק מקצועי בין מס"ל לבט"ל לצורך מתן מענה ישיר, העברת דיווחים, בקרה על תיקון הליקויים וכיו"ב. כמו כן מומלץ כי ועדת ההיגוי תבחן אם יש עוד גופים בעלי מאגרי מידע בהיקפים הדומים לבט"ל שיש לבחון את הגדרתם כגופי תמ"ק, ובכך תשפר את ההגנה על התשתיות החיוניות של מדינת ישראל.

אסדרת הגנת הסייבר במוסד לביטוח לאומי

מבוא

בעשור האחרון גברו התקיפות במרחב הקיברנטי (להלן - תקיפות סייבר) על ארגונים ועל אנשים פרטיים ברחבי העולם. בשנת 2021 הודלפו בעולם יותר מ-22 מיליארד רשומות עקב תקיפות סייבר[4]; שמות של אנשים ומספר ביטוח לאומי (ובהם SSN[5]) היו שני סוגי הנתונים שדלפו יותר מכל נתון אחר. נכון לנובמבר 2022, במוסד לביטוח לאומי (להלן - בט"ל) מתבצעות בכל יום כ-2.9 מיליון תקיפות סייבר בממוצע, ומהן כ-66,000 תקיפות עם פוטנציאל נזק.

שכיחותן של תקיפות הסייבר כאמור הולכת וגדלה ממניעים שונים, ובהם כוונה לפגוע במערכות עצמן וכך לשבש את הפעילות התקינה והשוטפת של הארגון, החברה ואף המדינה, למטרת סחיטה, למטרת שינוי מידע כדי ליהנות מהטבות ומרווחים ואף במסגרת אתגר טכנולוגי לשמו. כך, בשנת 2021 טיפל מערך הסייבר הלאומי[6] (להלן - מס"ל) בכ-2,200 אירועי סייבר (עלייה של כ-33% בהשוואה לשנה הקודמת), איתר כ-9,000 חולשות אבטחה חמורות בכ-3,300 גופים והעביר כ-4,400 דיווחים ממוקדים לחברות ולגופים במשק הישראלי בגין הממצאים שאותרו. על פי מס"ל, בשנת 2021 נרשמה עלייה של 20% במספר הדיווחים שאותם הוא קיבל ואימת כאירועי סייבר בהשוואה לשנת 2020[7].

בט"ל מעניק מגוון שירותים רחב למבוטחיו - תושבי מדינת ישראל - מהלידה עד הפטירה. בכלל זה בט"ל משלם בכל שנה קצבאות בסך כ-122 מיליארד ש"ח[8]. נוסף על כך, בשנת 2020, בעת משבר הקורונה ובעקבות החלטת ממשלה, העבירה הממשלה באמצעות בט"ל למבוטחים שהוצאו לחל"ת עקב צעדי הממשלה למניעת הדבקה והתפשטות המחלה, כ-23.6 מיליארד ש"ח. לצורך מילוי משימותיו, ובכלל זה לצורך תשלום הקצבאות, מאגרי המידע של בט"ל כוללים מידע על כ-9.5 מיליון מבוטחים.

פעולות הביקורת

בחודשים אוקטובר - דצמבר 2022 בדק משרד מבקר המדינה את נושא אסדרת הגנת הסייבר בבט"ל. הבדיקה כללה מיפוי של הגופים המאסדרים את בט"ל כיום, בחינת הנזק האפשרי מהיעדר גורם מאסדר קבוע ובחינת הצורך בשינוי גורמי האסדרה. הביקורת נערכה בבט"ל, במערך הסייבר הלאומי, בשירות הביטחון הכללי וברשות להגנת הפרטיות במשרד המשפטים. ועדת המשנה של הוועדה לענייני ביקורת המדינה של הכנסת החליטה שלא להניח דוח זה

4 2021 Year End Report - Data Breach QuickView, RiskBased Security & Flashpoint (p. 3)

5 Social Security Number (יצוין כי בכמה מדינות כמו ארה"ב מספר ה-SSN שקול למספר ת"ז בישראל).

6 גוף מבצעי טכנולוגי האמון על הגנת מרחב הסייבר בתחום האזרחי בישראל.

7 מבקר המדינה, **דוח 73א** (2022), "הגנת הסייבר על מערכות מידע במשרד החינוך ועל בחינות הבגרות וציוני הבגרות".

8 מתוך הירחון הסטטיסטי של בט"ל לשנת 2021, כללי פרק 1.5.1.

במלואו על שולחן הכנסת אלא לפרסם רק חלקים ממנו, לשם שמירה על ביטחון המדינה, בהתאם לסעיף 17 לחוק מבקר המדינה, התשי"ח-1958 [נוסח משולב].

היקפי המידע ורמת רגישות המידע בבט"ל: לצורך מתן השירותים הנדרשים למבוטחים פיתח בט"ל, עוד החל מתחילת שנות ה-80, מערכות מחשוב ייעודיות, שמטרתן טיפול בגמלאות שעליו לספק לזכאים להן בהתאם לחוק הביטוח הלאומי [נוסח משולב], התשנ"ה-1995. משנת 2010 החל בט"ל ביישום פרויקט "תבל" לשדרוג מערך המחשוב שלו. בדוח מבקר המדינה משנת 2020 שבחן את הפרויקט צוין בנוגע ל"תבל" כי אף שבט"ל יישם כמה מערכות חשובות ומתקדמות במסגרת הפרויקט, מדובר רק בחלק קטן מכלל המערכות שתוכננו במסגרתו[9]. מלבד פיתוח המערכות בט"ל גם מעדכן אותן בהתאם לשינויים שחלים בחוק וכן מתחזק אותן לצורך שמירה על כשירותן.

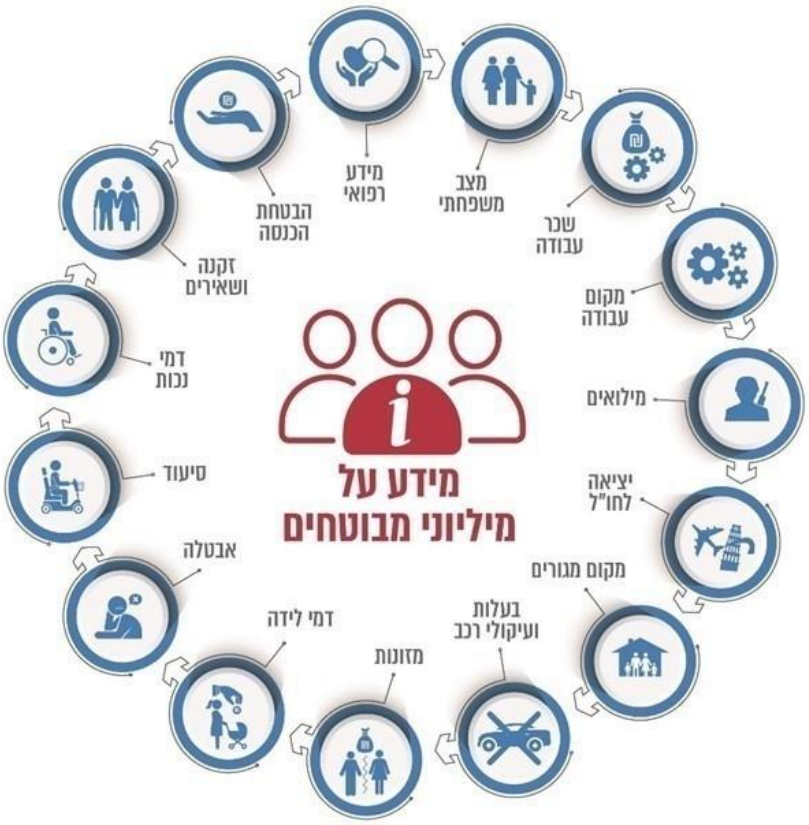
להתפתחות הטכנולוגית המחויבת מתלווה גם התגברות של הסיכונים והאיומים על המערכות ועל המידע האגור בהן ומכאן צורך במערך לשמירתם ולאבטחתם. הגופים המקצועיים בבט"ל האחראים לכך הם חטיבת אבטחת מידע וחטיבת סייבר הכפופים לסמנכ"ל מינהל תקשוב ומערכות מידע.

התשתית המרכזית של מערכות המחשוב בבט"ל משמשת גם כתשתית המחשובית שמספק בט"ל באתר השירות האישי. האתר מאפשר לכ-3.5 מיליון מבוטחים שנרשמו לאתר גישה אינטרנטית לאזור האישי שלהם ובאמצעותו לבצע פעולות, לקבל מידע, לשלוח שאילתות ובקשות וכיו"ב.

למאגרי המידע של בט"ל רגישות מיוחדת הן בשל היקפם העצום, הן בשל היותם מוגדרים כמידע רגיש על פי הקבוע בחוק הגנת הפרטיות התשמ"א-1981 (להלן - חוק הגנת הפרטיות) והן מפני שהמאגרים מתממשקים לגורמים שמחוץ לבט"ל, למשל לרשות המיסים, למשרד הרווחה והביטחון החברתי, לרשויות המקומיות ואף לגורמים פרטיים ובהם המעסיקים. בממשקים אלו קיימת תעבורת נתונים רבה אל בט"ל פנימה ומבט"ל החוצה. להלן תרשים המציג את סוגי המידע במאגרי המידע של בט"ל.

9 מבקר המדינה, **דוח שנתי 70ג** (2020), "פרויקט תבל לשדרוג מערך המחשוב במוסד לביטוח לאומי", עמ' 538.

תרשים 1: **סוגי המידע במאגרי המידע של בט"ל**



המקור: מבקר המדינה, דוח שנתי 70ג (2020), "פרויקט תבל לשדרוג מערך המחשוב במוסד לביטוח לאומי", עמ' 570.

עולה מהתרשים כי על מנת למלא את משימותיו נדרש בט"ל להיקף מידע עצום (לפחות על כלל המבוטחים) ולסוגי מידע מגוונים, שאת חלקם הוא מקבל מגורמים החיצונים לו. על כן ניתן לקבוע כי בט"ל מחזיק במאגר מידע על תושבי מדינת ישראל, דבר המגביר את חובת ההגנה על מערכות המחשוב והמידע שלו דבר שיאפשר להבטיח שהן יתפקדו באופן יעיל, זמין, תקין, אמין ורציף.

פגיעה במערכות המידע ובנתונים של בט"ל יכולה להתרחש בזדון או שלא בזדון. פגיעה בזדון יכולה למשל להיות לצורך שינוי המידע כדי לזכות בהטבות כלכליות, לצורך שיבוש תפעולי של המערכות, כפעולת סחיטה וכמתקפת סייבר בידי גורם עוין. פגיעה שלא בזדון יכולה להיות למשל חשיפת מידע למי שאינו מורשה או כפעולה שגויה בתהליך עסקי שעלולה למחוק מידע או לשבש אותו.

ניתן לחלק את הנזק הנגרם מהפגיעות כמתואר לעיל לשלושה סוגים עיקריים: פגיעה בפרטיות, פגיעה או שיתוק עבודת הארגון ופגיעה אחרת.

פגיעה בפרטיות: הזכות לפרטיות וחובת השמירה על צנעת הפרט עוגנו בחקיקה - הזכות לפרטיות מוגנת על פי סעיף 7 לחוק-יסוד: כבוד האדם וחירותו, הקובע כי כל אדם זכאי לפרטיות ולצנעת חייו"; חוק הגנת הפרטיות קובע איסור על פגיעה בפרטיותו של אדם.

כאמור, בסיס המידע של בט"ל מכיל מידע אישי רגיש שנאגר ומעובד לשם מתן שירות למבוטחים וכן לצורך מיצוי זכויות מיטבי. בג"ץ עמד על חשיבות ההגנה על הפרטיות בעידן הדיגיטלי בפסיקתו וציין כי "התפתחויות בעולם המדע והטכנולוגיה הופכות מהירות יותר מאשר בעבר ועל כן ניצב בית המשפט בפני אתגרים חדשים בתכיפות גדולה מאשר בעידן הקודם... אמצעי המחשוב המודרניים והטכנולוגיה המתקדמת בתחום התקשורת מביאים עימם ברכה רבה בצד סכנות גוברות לפגיעה בזכותו של האדם לפרטיות"[10].

חוק הגנת הפרטיות קובע כי האחריות לאבטחת המידע במאגר חלה על בעל מאגר המידע, מחזיק מאגר המידע או מנהל מאגר המידע כהגדרתו בחוק. תקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017 (להלן - תקנות הגנת הפרטיות אבטחת מידע), קובעות את החובות שחלות על בעל מאגר מידע, מחזיק מאגר המידע או מנהל מאגר המידע[11], בשינויים המחויבים ולפי העניין. רמת רגישות המידע ורמת האבטחה הדרושה נקבעות לפי סוג המידע, היקף נושאי המידע ומספר בעלי הרשאות הגישה למאגר בהתאם לאמור בתוספת הראשונה והשנייה בתקנות הגנת הפרטיות אבטחת מידע. התקנות קובעות שלוש רמות אבטחה למאגרי מידע שונים: בסיסית, בינונית וגבוהה, בהתאם לסוג המידע שהם כוללים, היקפו ומספר בעלי ההרשאה אליו[12]. מטרת התקנות היא להגביר ולחזק את ההגנה על המידע האישי של האזרחים באמצעות דרישות אבטחת מידע ברורות שבהן על הגופים והארגונים לעמוד, בהתאם לרגישות ולהיקף של המידע האישי שמנוהל או מוחזק בהם.

הרשות להגנת הפרטיות בישראל (להלן - הרשות) מסרה לצוות הביקורת כי היות שהמאגר של בט"ל הוא מאגר מידע של גוף ציבורי, ככלל חלה עליו רמת אבטחה בינונית. עם זאת, בשל היקפי המידע הקיימים במאגר המידע, רמת האבטחה שחלה על המאגר היא רמת אבטחה גבוהה[13].

פגיעה או שיתוק עבודת הארגון: התקפות מניעת שירות (Denial of Service) נפוצות מאוד, והן מתבצעות באופן יום-יומי על ארגונים שונים. במקרים רבים ההתקפות הללו מנסות להשבית או לשבש את השירותים שמספק הארגון על ידי העמסה חריגה על המשאבים הקריטיים של הארגון באמצעות אוסף של טכניקות, כמו בקשות חוזרות לעיבוד הצורכות משאבים גדולים.

סיכון זה קיים גם באשר למערכות המידע של בט"ל: לבט"ל יש מערכות ורכיבים שהשבתה שלהם עלולה לשתק את פעילות הארגון; מערכות נוספות אחרות אמנם לא ישתקו את הארגון כולו, אך פעילותן השוטפת תשובש משמעותית. שיתוק הפעילות השוטפת או שיבושה באופן

10 בג"ץ 8070/98 **האגודה לזכויות האזרח בישראל נ' משרד הפנים**, פסק דין נ"ח (4), 842, עמ' 864 (2004).

11 לפי תקנה 19 לתקנות על המחזיק יחולו כלל החובות למעט החובות לעניין מסמך הגדרות המאגר ומיקור חוץ תקנות 2 ו-15(א).

12 ראו את המדריך המלא לתקנות הגנת הפרטיות אבטחת מידע באתר: www.gov.il/he/departments/Guides/data_security_guide

13 על פי התוספת השנייה לתקנון, מאגר מידע שיש בו מידע על אודות 100,000 איש ומעלה, תחול עליו רמת אבטחה גבוהה.

משמעותי עלולים לגרום לפגיעה מהותית בציבור, למשל להפסקת העברת קצבאות למבוטחים - חלק מהקצבאות הן ממש קריטיות למבוטחים שכן הן מאפשרות המשך מחייתם כמו קצבאות הנכות לסוגיהן וקצבת הבטחת הכנסה.

פגיעה אחרת: סיכון נוסף שעלול להתממש הוא בשל פריצה למאגרי המידע של בט"ל; סיכון זה עלול להוות סיכון אחר היות ומדובר במאגר מידע הכולל מידע אישי ובו מיליוני רשומות. בנסיבות אלו, במתקפת סייבר, מתקיים סיכון של חשיפה בשל דליפת מידע רגיש ממערכות המידע של בט"ל.

תמונת המצב האסדרתית

להלן האסדרה הנורמטיבית העיקרית בנוגע להגנת הסייבר ואבטחת מידע: חוק הגנת הפרטיות מגדיר את החובות של בעל מאגר מידע, מחזיק מאגר מידע או מנהל מאגר מידע לאבטחת המידע שבו; תקנות הגנת הפרטיות (אבטחת מידע); חוק להסדרת הביטחון בגופים ציבוריים התשנ"ח-1998, אשר קובע סמכויות ואחריות לאבטחה פיזית, אבטחת מידע ואבטחת מערכות מחשוב חיוניות של גופים ציבוריים שונים בתוכם, הן גופי ממשלה והן גופים בבעלות פרטית; והחלטת ממשלה 2443 בדבר "קידום אסדרה לאומית והובלה ממשלתית בהגנת הסייבר"[14].

האסדרה של הרשות להגנת הפרטיות מול בט"ל: הרשות מופקדת על הגנת המידע האישי במאגרי מידע דיגיטליים ועל ביצורה של הזכות לפרטיות. בידי הרשות סמכויות אכיפה פליליות וסמכויות אכיפה מינהליות על כלל הגופים בישראל - פרטיים, עסקיים וציבוריים, המחזיקים או מעבדים מידע אישי דיגיטלי. הרשות נוקטת שני הליכים אסדרתיים עיקריים:

1. **פיקוח רוחב:** מדי שנה בשנה מבצעת הרשות סקר סיכונים המבוסס על "שולחנות עגולים" בהשתתפות גופים במשק, גופים מהמגזר הציבורי ואנשי אקדמיה. בהתאם לסקר הסיכונים, הרשות בוחרת חמישה עד שבעה מגזרים שבהם יש רמת סיכון מוגברת, ובוחנת את רמת העמידה של הגופים השייכים לאותם מגזרים בחוק הגנת הפרטיות ובתקנותיו (להלן - פיקוח רוחב). הפיקוח מבוסס על תשובות שאלונים שמילאו הגופים הנבדקים. תוצר הפיקוח מציג דוח המדרג (במדד גבוה, בינוני או נמוך) כל גוף שנבדק לפי רמת העמידה בחוק ובתקנות הגנת הפרטיות אבטחת מידע.

2. **הליך מינהלי:** הליך זה נעשה כתולדה של אחד מאלו: אירוע אבטחת מידע בגוף הנבדק; חשד מודיעיני לאירוע; חשש להפרה של חוק הגנת הפרטיות או של תקנות הגנת הפרטיות (אבטחת מידע); קבלת תלונה קונקרטית; וכאשר הגוף מבצע שינויים מערכתיים העלולים לייצר אירוע של אבטחת מידע. במקרים שבהם הרשות להגנת הפרטיות סבורה כי מחזיק מאגר המידע או בעל מאגר המידע הפרו את הוראות החוק או את הוראות התקנות או לא מילאו אחר דרישות שהוצגו להם, יש בידי הרשות מספר כלים הקבועים בחוק ובהם הטלת קנס מינהלי, הנחיה לתיקון ליקויים, התליית תוקפו של רישום המאגר לתקופה מסוימת או אף ביטול רישומו בפנקס מאגרי המידע[15].

14 החלטת הממשלה 2443 (15.2.15, עדכון 28.7.15).

15 חוק הגנת הפרטיות, התשמ"א-1981, סעיף 10(ו).

בביקורת עלה כי מאז הקמת הרשות להגנת הפרטיות בשנת 2006 ועד מועד סיום הביקורת (יותר מ-16 שנה) ביצעה הרשות שישה הליכים מינהליים בנושא אבטחת מידע בבט"ל. אשר לפיקוח רוחב, רק באוגוסט 2022 החלה הרשות להגנת הפרטיות לבצע בפעם הראשונה פיקוח רוחב בבט"ל.

האסדרה של שירות הביטחון הכללי והממשק של מערך הסייבר הלאומי מול בט"ל: החוק להסדרת הביטחון קובע את הסמכויות והאחריות של שירות הביטחון הכללי (השב"כ) לאבטחה פיזית, אבטחת מידע ואבטחת מערכות מחשוב חיוניות בגופי ממשלה ובגופים בהחזקה פרטית או ציבורית. בתוספת השנייה לחוק מנויים גופים שמונחים על ידי השב"כ בנוגע לאבטחת מידע בנושאים שסיווגם שמור עד סודי ביותר ובהם בט"ל. המשמעות היא שהיחידה מנחה את בט"ל בהיבטי אבטחת מידע מסווג.

מס"ל: באוגוסט 2011 החליטה הממשלה על "קידום היכולת הלאומית במרחב הקיברנטי"[16]. ההחלטה התייחסה לקידום היכולת הלאומית במרחב הקיברנטי[17]; לשיפור יכולת ההתמודדות עם האתגרים במרחב הקיברנטי; לשיפור ההגנה על תשתיות לאומיות חיוניות ועוד. בדצמבר 2017 הופקד מס"ל על הגנת הסייבר בישראל מכוח החלטת הממשלה 3270. על מס"ל הוטל בין היתר לבנות ולחזק את חוסנו של כלל המשק להתמודדות עם התקפות סייבר. עוד קבעה הממשלה בהחלטתה כי מס"ל יקבל את האחריות להנחיית הגופים המוגדרים כבעלי תשתיות מידע קריטיות (להלן - תמ"ק). בתוספת החמישית לחוק מנויים הגופים שמס"ל תהיה אחראית להנחות אותם ובהם משרד האוצר, הלשכה המרכזית לסטטיסטיקה ובנק ישראל וכן חברות תשתית ותחבורה ובהן חברת החשמל לישראל, חברת נמל אשדוד ורשות שדות התעופה. הנחיית מס"ל לגוף תמ"ק כוללת מתן מענה מערכתי ובכלל זה ליווי של הגוף באופן שוטף וסיוע בפעולות האלה: 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 מבדקי חדירה. כמו כן אגף תמ"ק במס"ל מלווה את גוף התמ"ק ומסייע לו כשיש חשש לאירוע סייבר[18].

בתוספת השנייה לחוק להסדרת הביטחון מופיעים הגופים הנדרשים להנחיה בנוגע לנושאים המסווגים שמור עד סודי ביותר.

עלה כי בט"ל אומנם מופיע בתוספת השנייה אך אינו מוגדר בתוספת החמישית לחוק להסדרת הביטחון המתייחסת לגופים המוגדרים כבעלי תשתיות מידע קריטיות, אף שהוא גוף שמחזיק במאגר מידע על תושבי מדינת ישראל. לפיכך, בט"ל מקבל הנחיה משב"כ בנוגע לנושאים המסווגים בלבד אך אינו נדרש להנחיה קבועה ממס"ל.

היחידה להגנת הסייבר בממשלה: בהחלטת הממשלה 2443 מפברואר 2015 בנושא קידום אסדרה לאומית והובלה ממשלתית בהגנת הסייבר, הוחלט על הקמת היחידה להגנת הסייבר

16 החלטת הממשלה 3611 (7.8.11).

17 המתחם הפיזי והלא פיזי שנוצר או מורכב מחלק או מכל הגורמים הבאים: מערכות ממוכנות ממוחשבות, רשתות נחשבים ותקשורת, תוכנות, מידע ממוחשב, תוכן שמועבר באופן ממוחשב, נתוני תעבורה, ובקרה והמשתמשים של כל אלה.

18 מבקר המדינה, **דוח שנתי 73א** (2022), "הגנת הסייבר במגזר התחבורה", עמ' 54.

בממשלה (להלן - יה"ב) אשר תפעל לשיפור רמת הגנת הסייבר, תכווין את משרדי הממשלה ואת יחידות הסמך שלה ותנחה אותם.

בט"ל הוא תאגיד אשר הוקם לפי חוק הביטוח הלאומי [נוסח משולב], התשנ"ה-1995, ועל כן הוא אינו מונחה בידי יה"ב, המנחה כאמור משרדי ממשלה ויחידות סמך.

פיקוח עצמי: על פי החוק להסדרת הביטחון ישנם גופים המבצעים פיקוח עצמי. בגופים אלו יש יחידות ייעודיות שמטרתן הגנה על מרחב הסייבר. למשל בצה"ל יש אגף תקשוב וההגנה בסב"ר (סביבת רשת) בפיקוד קציץ בדרגת אלוף. האגף אמון על הפעלת הכוח וכן על גיבוש מדיניות התקשוב בצה"ל ומימושה ובכלל זה על ניהול הגנת הסייבר. כמו כן האגף מפעיל את חיל הקשר וכמה יחידות מסווגות[19].

הגופים המקצועיים בבט"ל האחראים לאבטחת המידע במערכות הממוחשבות שלו הם חטיבת אבטחת מידע וחטיבת סייבר, והם כפופים לסמנכ"ל מינהל תקשוב ומערכות מידע ומונים 20 עובדים[20].

תהליך ה"הנחיה מרצון" של מס"ל: בשנת 2016 החל מס"ל להנחות את בט"ל "הנחיה מרצון", וזאת בעקבות פניות של בט"ל אליו בעניין זה. משמעות הדבר היא שמס"ל מנחה את בט"ל כפי שהוא מנחה את גופי התמ"ק אולם לבט"ל אין חובה ליישם את ההנחיות. נכון למועד סיום הביקורת (דצמבר 2022) הנחו את בט"ל ארבעה מנחים מטעם מס"ל.

משיחות של צוות הביקורת עם בט"ל התברר כי רמת המעורבות של מס"ל לאורך השנים הלכה ופחתה: משנת 2016 ועד 2020 ה"הנחיה מרצון" הייתה צמודה וכללה התייעצות שוטפת על בסיס יום-יומי; מסוף 2020 התחלפו שלושה מנחים וההנחיה הייתה מועטה יותר ולא קבועה; ובמועד סיום הביקורת אין מנחה מטעם מס"ל אלא הקשר מתבצע באמצעות המוקד של מס"ל (CERT[21]) המטפל בכלל אירועי הסייבר בישראל. לפיכך לבט"ל אין מענה שוטף ומערכתי לטיפול בכלל אירועי אבטחת מידע.

סיכום הגופים האסדרתיים הנוגעים לבט"ל: להלן לוח המציג את הגופים האסדרתיים המרכזיים ואת סמכויותיהם בכל הנוגע לבט"ל.

19 מתוך אתר אגף התקשוב וההגנה בסב"ר במרשתת.

20 חטיבת אבטחת מידע, המונה שמונה עובדים, אחראית על מדיניות אבטחת מידע, גיבוש נהלים, אכיפה ובקרה בנושאי אבטחת מידע והגנת הפרטיות בארגון; חטיבת הסייבר אחראית על יישום אבטחת מידע והגנת הסייבר בארגון, לרבות הפעלת מוקד SOC לניטור ומתן מענה מידי לאירועי סייבר הפועל 24/6. החטיבה מונה 6 עובדים ובנוסף, 6 מוקדנים העובדים במשמרות במוקד SOC (Secuity Operation Center – מרכז שליטה ובקרה לאבטחת מידע לזיהוי פעילות חריגה במערכות המידע הארגוניות).

21 Cyber Emergency Response Team

לוח 1: **הגופים האסדרתיים המרכזיים בתחום הגנת הסייבר ואבטחת המידע**

	החוק שעל פיו פועל הגוף	סמכות	גופים כפופים	מאסדרים של בט"ל לפי חוק
הרשות להגנת הפרטיות	חוק הגנת הפרטיות ותקנות הגנת הפרטיות	סמכויות אכיפה פליליות ומינהליות	כלל הגופים בישראל - פרטיים, עסקיים וציבוריים, המחזיקים או מעבדים מידע אישי דיגיטלי	✓
השב"כ	החוק להסדרת הביטחון בגופים ציבוריים - התוספת הראשונה, השנייה ולא מופיעים בתוספת החמישית (לגבי פעולות לאבטחת מידע) והרביעית לחוק	הנחיות מחייבות לאבטחת מערכות מסמכים ותשתיות אשר מוגדרים מסווגים	למשל: משרד החוץ בט"ל הסוכנות היהודית חברות תקשורת	✓ נתונים מסווגים וכן מערכות
מס"ל[22] - תמ"ק	החוק להסדרת הביטחון בגופים - התוספת החמישית ולגבי גופים המופיעים בתוספת השנייה והחמישית	הנחיות מחייבות לאבטחת מערכות מידע חיוניות וכן מניעת פגיעה במידע	למשל: משרד האוצר בנק ישראל וכן חברות תשתית ותחבורה ובהן: חברת החשמל לישראל ורשות שדות התעופה (מופיעים בתוספת השנייה והחמישית)	✗
יה"ב	החלטת הממשלה 2443 בנושא קידום אסדרה לאומית והובלה ממשלתית בהגנת הסייבר	הכוונה והנחיה מקצועיות בתחום הסייבר	משרדי הממשלה ויחידות הסמך	✗
פיקוח עצמי	החוק להסדרת הביטחון בגופים - סעיף 21 ו-21א	גופים המוחרגים מאחריות הנחיית השב"כ בהיבטים הקיברנטיים	בעיקר גופי ביטחון רגישים, ובהם: השב"כ, המוסד למודיעין ותפקידים מיוחדים וצה"ל, המגנים על עצמם ואינם מחויבים בדיווח או בפיקוח חיצוני על אופן התנהלותם	✗
הנחיה מרצון	הנחיית מס"ל בדומה לגופי תמ"ק לפי שיקול דעת של הגוף המונחה			✓

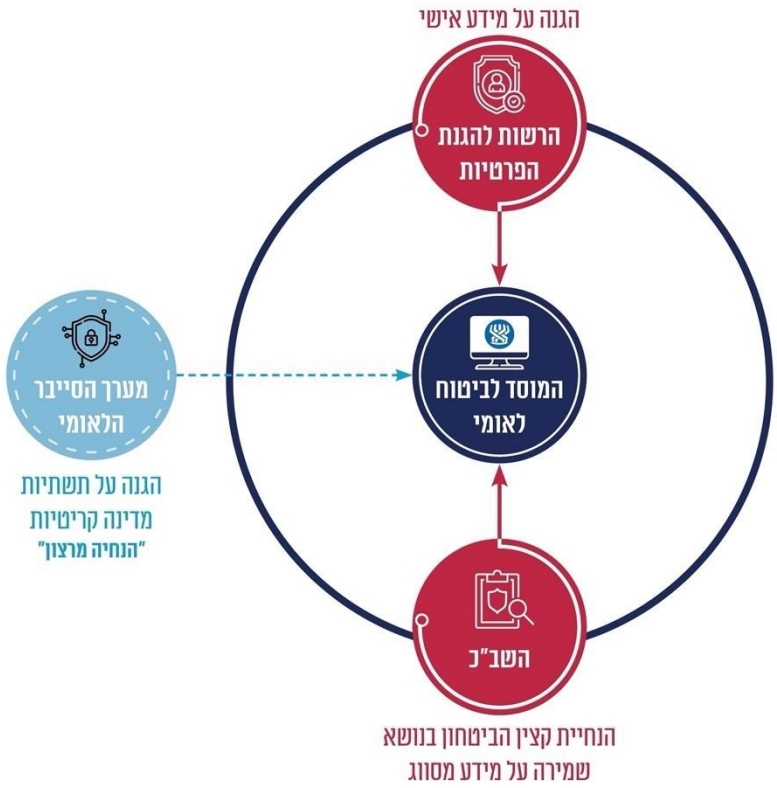
22 מס"ל מורכב משני אגפים: האחד - אגף תמ"ק (ראו פירוט בלוח 1); והשני - אגף מגזר, המנחה מגזרים באופן עקיף באמצעות יחידה מגזרית במשרד הממשלתי הרלוונטי, למשל הוא מנחה את בתי החולים דרך משרד הבריאות במגזר הבריאות.

מלוח 1 עולה כי הרשות להגנת הפרטיות מנחה את כלל הגורמים ובכללם בט"ל בנושאים של הגנה על המידע האישי שבמאגרי המידע. נוסף על כך בט"ל מונחה על ידי השב"כ בכל הנוגע לענייני אבטחת מידע על נתונים מסווגים ומערכות. בט"ל אינו מונחה על ידי מס"ל, המנחה גופים שלהם מערכות מידע חיוניות (תמ"ק), ועל ידי יה"ב, המנחה את כל משרדי הממשלה ויחידות הסמך.

עולה כי מרבית מערכות המידע של בט"ל, שאינן מסווגות, אינן מונחות על ידי גורם מאסדר חיצוני כלשהו באופן שוטף ומערכתי, וזאת על אף הרגישות הרבה של מערכות מידע אלו ורמת הסיכון הגבוהה שלהן.

להלן תרשים המציג את כלל הגופים המנחים את בט"ל:

תרשים 2: **גורמי האסדרה בתחום אבטחת המידע בבט"ל**



על פי נתוני בט"ל, בעיבוד משרד מבקר המדינה.

מלוח 1 ומתרשים 2 עולה כי לעומת משרדי הממשלה, שלחלקם מאגרי מידע מצומצמים, המונחים בידי יה"ב, בט"ל האחראי למאגר מידע מבצע פיקוח עצמי על מרבית המידע שלו, לפעמים בסיוע מס"ל באמצעות "הנחיה מרצון".

המשמעות של הנחיה מרצון

כאשר גוף מקבל עליו באופן וולונטרי הנחיות של גורם מאסדר, הוא אינו מחויב למלא את ההוראות כפי שהן, והמאסדר אינו יכול לאכוף עליו את קיום ההנחיות. על כן, עלול להיווצר מצב בו המאסדרים לא יבחנו את הציות של גופים הנתונים לאסדרתם מרצון. כך למשל בדוח בנושא "אבטחת סייבר: אתגרים באבטחת רשת החשמל"[23] של מבקר המדינה האמריקאי משנת 2012 צוין כי המאסדר האמריקאי (NERC) לא בחן את הציות של חברות החשמל בארצות הברית להנחיותיו בנושא הגנת הסייבר כיוון שמדובר היה ב"הנחיה מרצון", ואין חובה ליישם את הנחיותיו.

להלן שני אירועים שהתרחשו בתקופת ה"הנחיה מרצון" של מס"ל. אירוע א' מציין כשל בהתנהלות בט"ל ואת הצורך בהנחיה מחייבת של מס"ל, ואירוע ב' מתאר את היתרון שיש בהנחיה של מנחה קבוע מטעם מס"ל.

אירוע א', שבמסגרתו עלה פער מסוים בבקרה מסוימת, כאשר אין לבט"ל הנחיות מחייבות בהתנהלותו השוטפת בסוגיות אבטחה והגנת סייבר,הנהלת הארגון נדרשת להכריע בין הגנת הסייבר ואבטחת המידע לבין הנטל הצפוי והכרוך בכך עבור הארגון ועבור מקבל השירות. אם מדובר במסגרת כללים מחייבת שאינה ניתנת לגמישות הרי שהנורמות ידועות והחובה ליישמן ברורה, גם במחיר של פגיעה מסוימת בשירות למבוטח. לחלופין, אם מדובר ב"רצון" לקבל את הנורמות, קיים פתח להנהלת הארגון לא ליישם פתרונות נדרשים ובכך לוותר על הצורך להתמודד עם הסיכונים האפשריים.

הרשות להגנת הפרטיות מסרה למשרד מבקר המדינה בפברואר 2023 כי בקרה מסוימת היא דרישה הקבועה בתקנות. עוד הוסיפה הרשות כי היא עוסקת במתן הנחיות לגופים כיצד ליישם בקרה מסוימת שאינה יוצרת נטל על הפעילות השוטפת, ועם זאת אינה פוגמת ברמת האבטחה. עוד ציינה הרשות כי אירוע א' מצוי בבחינה במסגרת הליך פיקוח.

אירוע ב' - אירוע העברת מידע לגורם חיצוני במסגרת הסכם מסוים: בשנת 2016 נחתם הסכם עם גורם חיצוני שכלל בין השאר בקשה של הגורם החיצוני לגישה למערכות בט"ל כדי למשוך נתונים ומידע.

בעקבות זאת העלה "המנחה מרצון", מטעם מס"ל באותה העת, את המשמעות הנגזרת ממתן גישה ישירה לאותו גורם למערכות המחשוב של בט"ל. בחשיבה משותפת עם הגורמים המקצועיים בבט"ל גובש פתרון שאיפשר את מתן הגישה למערכות בט"ל באופן שלא יפגע באבטחת המידע.

23 Cybersecurity :Challenges in Securing the Electricity Grid. GAO-12-926T (2012)

המנחה הדגיש לפני צוות הביקורת את הרגישות של בסיסי המידע בבט"ל האוגרים מידע שלם על האזרחים והתושבים בישראל מרגע לידתם ועד מותם. עוד ציין המנחה כי נוכח המידע הרגיש והסיכונים שלהם בט"ל חשוף, לדעתו בט"ל צריך לקבל הנחיה ממס"ל על פי חוק באמצעות מנחה ייעודי בהתאם לחוק הסדרת הביטחון.

אירוע ב', שעסק במתן גישה לגורם חיצוני למערכות בט"ל, מצביע על החיונויות הטמונה בהנחיה מקצועית שוטפת לבט"ל. בשל הערנות שגילה המנחה דאז, שליווה באופן שוטף את בט"ל וזיהה את הסיכון שבחשיפת המידע לגורם חיצוני, נמנע מימושו. אולם, אירוע ב' מצביע גם על הסיכון שעלול להתממש לנוכח אי-אסדרת ההנחיה של מס"ל בכל הנוגע למאגרי המידע של בט"ל.

נציגי בט"ל מסרו לצוות הביקורת כי בט"ל מתמודד בימים אלו (אוקטובר-דצמבר 2022) עם אירוע אבטחת מידע של התחזות, ואף שמס"ל מודע לאירוע אבטחה זה, לא ניתן לבט"ל ליווי וייעוץ צמוד בנושא אלא באמצעות מוקד CERT של מס"ל, אשר מטפל בכלל אירועי הסייבר בישראל.

מכלל האמור לעיל עולה כי היקף המידע שבידי בט"ל ורגישותו הרבה, מצריכים הגנה ומתן מענה שוטף במקרים של חשש לאירועי אבטחה. מן הראוי לוודא כי לבט"ל ניתנת הנחיה מקצועית מיטבית לטיפול במקרים אלה, בין אם כהנחיה מחייבת ע"י מס"ל ובין אם הנחיה ע"י גורמים אחרים.

הניסיון להגדיר את בט"ל כגוף תמ"ק

חלוקת סמכויות בין מאסדרים: נושא חלוקת הסמכויות בין המאסדרים השונים בתחום הגנת הסייבר נדון במסגרת ועדת החוץ והביטחון בשנת 2016. במסגרת זו הוקמה ועדת משנה אשר בחנה את משמעויות החלטת הממשלה על הקמת רשות הסייבר הלאומית ואופן מימושה[24]. ועדת המשנה סיכמה את עבודתה בדוח בנושא[25] אשר קבעה כי רשות הסייבר הלאומי צריכה להיות הגורם האחראי להגנת הסייבר בישראל, וכי תפקידה לחזק את החוסן המדינתי, להכווין את צורכי ההגנה הרלוונטיים בסייבר ולהתמודד עם אירועי תקיפת סייבר על יעדים ישראליים. עוד צוין בדוח כי יש צורך בשיתוף פעולה בין הגוף שעיסוקו הבלעדי הוא הגנת הסייבר, המביא בחשבון שיקולים אזרחיים-מדינתיים, לבין גופי הביטחון שהם בעלי מומחיות בהיבטים הביטחוניים והמודיעיניים במרחב זה.

החשיבות שבאסדרת האחריות בין הגופים השונים העוסקים בסייבר עלתה גם בדוח מבקר המדינה משנת 2016[26], ובו עלה, בין היתר, כי בעבודת המטה ובתהליך קבלת ההחלטות על אסדרת האחריות לטיפול בתחום הקיברנטי במדינת ישראל נפלו ליקויים מהותיים.

24 בהחלטת הממשלה 2444 הוחלט להקים "רשות לאומית להגנת הסייבר". על פי ההחלטה, מטה הסייבר והרשות יהוו יחד את "מערך הסייבר הלאומי" ובראשו יעמוד ראש מטה הסייבר.

25 הכנסת, ועדת חוץ וביטחון, דין וחשבון בנושא: בחינת חלוקת האחריות והסמכות בנושא הגנת הסייבר בישראל, אוגוסט 2016.

26 מבקר המדינה , **דוח שנתי 67א** (2016), "היבטים בהיערכות המדינה להגנת המרחב הקיברנטי".

הגדרת דפוסי הפעולה והסמכויות בנוגע להגנת הסייבר של ישראל בדגש על תשתיות חיוניות נקבעה בהחלטת הממשלה 84/ב משנת 2002 בנושא "אחריות להגנה על מערכות ממוחשבות במדינת ישראל" של ועדת השרים לענייני ביטחון לאומי. בהחלטה נקבע כי יש להקים ועדת היגוי עליונה שתפקידה לבחון אילו גופים מוגדרים "חיוניים" ולכן זקוקים להגנה קיברנטית.

יו"ר ועדת ההיגוי הוא ראש מס"ל וחברים בה בין היתר נציגים ממשרד הביטחון, ממשרד המשפטים - ראש הרשות להגנת הפרטיות, מהמטה לביטחון לאומי, מצה"ל ומהשב"כ. אחד מתפקידי הוועדה הוא לבחון באופן תקופתי את האפשרות להכניס גופים נוספים לתוספת החמישית לחוק הסדרת הביטחון - היינו להנחיות המחייבות, או לגרוע גופים שאינם זקוקים לכך. בכלל זה, עליה לבחון בהתאם לסעיף 22ב(א) לחוק הסדרת הביטחון אם להוסיף גופים לרשימת הגופים המנויים גם בתוספת השנייה וגם בתוספת החמישית לחוק. החוק קובע כי מס"ל ינחה את הגופים בכל הנוגע לפעולות לאבטחת מידע ברמת סיווג עד "שמור" בהתאם לעקרונות חוק שירות הביטחון הכללי, התשס"ב-2002, בעניין שמירה על מידע מסווג. לעניין פעולות לאבטחת מידע ברמה הגבוהה מ"שמור", מס"ל ינחה את הגופים בהתאם להוראות השב"כ בעניין שמירה על מידע מסווג.

אסדרת בט"ל כגוף תמ"ק: במסגרת דיון ועדת היגוי להגנה על מערכות ממוחשבות חיוניות שהתקיימה בדצמבר 2020 הציג ראש אגף בכיר תמ"ק במס"ל לאישור הוועדה גופים אשר מולם מתכנן מס"ל להתחיל תהליך בחינה כגופי תמ"ק - דהיינו לשלבם בתוספת החמישית לחוק; בט"ל תועדף ראשון מבין הגופים שנדונו. ואולם, בסיכום הדיון הנחה ראש מס"ל דאז להתחיל בתהליך בחינה של גוף אחר במהלך שנת 2021 ואחר כך להמשיך בבחינת הגופים לפי התיעדוף שהציע ראש אגף תמ"ק במס"ל.

דוח מבקר המדינה משנת 2022[27] העלה כי לעיתים תהליך הגדרת גוף כתמ"ק עלול להימשך כמה שנים. כך לדוגמה, מס"ל המליץ להגדיר חברה בתחום הספנות והנמלים כגוף תמ"ק בנובמבר 2018, אולם רק באפריל 2022 התהליך הושלם. עוד ציין המבקר כי העיכובים בהגדרת גופי תמ"ק עלולים להביא לסיכונים בנושאים שטרם מטופלים וכן לניצול משאבים לא יעיל.

נמצא כי נכון למועד סיום הביקורת - כשנתיים לאחר הדיון בוועדת ההיגוי - מס"ל לא החל בהליך הבחינה של בט"ל כגוף תמ"ק. בבירור של צוות הביקורת במס"ל הועלה כי בכוונתו להתחיל בתהליך הבחינה של בט"ל כגוף תמ"ק ברבעון הראשון של שנת 2023. משמעות הדבר היא שבמועד סיום הביקורת בט"ל, המנהל מאגר מידע, אינו מונחה מקצועית באופן שוטף ומחייב, דבר העלול ליצור סיכון ברמה הלאומית.

בט"ל מסר למשרד מבקר המדינה בפברואר 2023 כי הוא מקבל את ההמלצות המופיעות בטיוטת הדוח ומייחס חשיבות רבה לנושא אבטחת המידע וההגנה על מערכות המחשוב ומאגרי המידע בארגון. בהתאם לכך בט"ל יישם בשנים האחרונות הנחיה מרצון. עוד מסר בט"ל כי הוא רואה ערך רב בליווי והנחיה של הגופים הרלוונטיים לעמידה באירועי סייבר ולהתמודדות איתם. עם זאת, כגוף ציבורי שמטרתו בראש ובראשונה מתן שירות לציבור, תהליכי הנחיה חייבים ליצור איזון בין השמירה על רמת שירות גבוהה התואמת לסטנדרט שלו מצפה ציבור האזרחים, לבין השמירה על רמת אבטחת המידע וההגנה בסייבר.

27 מבקר המדינה, **דוח שנתי 73א** (2022), "הגנת הסייבר במגזר התחבורה", עמ' 72.

מס"ל מסר למשרד מבקר המדינה בפברואר 2023 כי לאחר קבלת טיוטת הדוח הוא החל בתהליך הבחינה של בט"ל כגוף תמ"ק, ואף התקיימה פגישה ראשונה עם בט"ל. מס"ל הוסיף כי עד סיום הבחינה מס"ל יעמוד בקשר מקצועי עם בט"ל.

סיכום

בדומה למדינות אחרות, ישראל חשופה לתקיפות סייבר לצורכי כופר וגניבת מידע. מלבד זאת, נוכח האקלים הגיאו-פוליטי המורכב ביטחונית, ישראל משמשת כר מטרות נרחב לתוקף הקיברנטי הפוטנציאלי המעוניין לפגוע בחוסנה ובביטחון הלאומי שלה. על כן, היות שבט"ל הוא גוף שמחזיק במאגר מידע והיות שלו ממשקים רבים עם גופים ממשלתיים נוספים, הדבר מחייב שיגובש עבורו מענה אסדרתי מספק הכולל הנחיה של מערך הסייבר הלאומי, הנחיה של הרשות להגנת הפרטיות ותיאום בין שניהם כדי להבטיח את ההגנה המיטבית.

נוכח היקפי המידע השמורים בבט"ל והסיכונים לדליפתו מומלץ כי ועדת ההיגוי תקדם את הבחינה של בט"ל כגוף תמ"ק. מומלץ כי עד סיום הבחינה יוסדר ממשק מקצועי בין מס"ל לבט"ל לצורך מתן מענה ישיר, העברת דיווחים, בקרה על תיקון הליקויים וכיו"ב. כמו כן מומלץ כי ועדת ההיגוי תבחן אם יש עוד גופים בעלי מאגרי מידע בהיקפים הדומים לבט"ל שיש לבחון את הגדרתם כגופי תמ"ק, ובכך תשפר את ההגנה על התשתיות החיוניות של מדינת ישראל.