

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 סייבר¹. שמות של אנשים ומספר ביטוח לאומי (ובהם SSN²) 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 מתממשים 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

<p>20 עובדים</p> <p>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</p>	<p>מאות טרה ביט (TB)</p> <p>גודל בסיס הנתונים של בט"ל הכולל שדות על הנתונים האישיים של כ-9.5 מיליון מבוטחים בישראל</p>	<p>כ-2.9 מיליון</p> <p>הממוצע היומי של תקיפות הסייבר על בט"ל</p>	<p>22 מיליארד רשומות</p> <p>דלפו בעולם בשנת 2021 עקב תקיפות סייבר</p>
--	---	---	--

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 הנק 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 "ההנחיה 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 עליונה³ 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 ממוסד הביטחון, ממוסד המשפטים - ראש הרשות להגנת הפרטיות, מהמטה לביטחון לאומי, מצה"ל ומהשב"כ.

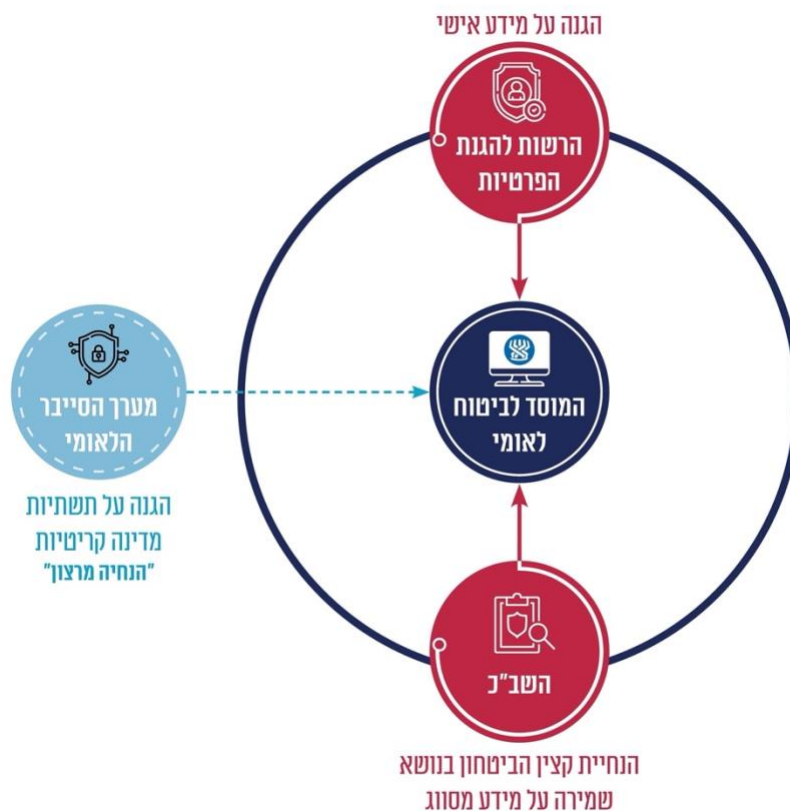
עיקרי המלצות הביקורת

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 הגיאוגרפי 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.

