

דוח מבקר המדינה - סייבר ומערכות מידע |
חשוון התשפ"ד | נובמבר 2024



המוסד לביטוח לאומי

**אבטחת מידע
והגנת הסייבר
במוסד לביטוח
לאומי**



אבטחת מידע והגנת הסייבר במוסד לביטוח לאומי

רקע

המוסד לביטוח לאומי (בט"ל) מחזיק במאגר גדול, המכיל מידע מארגונים וגופי ממשל רבים וגודלו טרה-בייט (TB) רבים. המאגר גדל בכ-10% בכל שנה. המאגר כולל מידע על כל תושבי מדינת ישראל מיום הלידה ועד יום הפטירה. המאגרים של בט"ל נדרשים לרמת אבטחה גבוהה לפי תקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017¹.

ביולי 2023 החליטה ועדת היגוי עליונה להגנה על מערכות ממוחשבות במדינת ישראל² כי בט"ל עונה על התבחינים הנדרשים, וכי יש מקום להנחותו כגוף תשתית מדינה קריטית (גוף תמ"ק). לפיכך המליצה הוועדה על הוספת בט"ל לתוספת החמישית לחוק להסדרת הביטחון בגופים ציבוריים, התשנ"ח-1998, כדי שבט"ל יהיה מונחה לפי חוק זה על ידי מערך הסייבר הלאומי (מס"ל). נכון לאפריל 2024, מועד סיום הביקורת, טרם התקבל אישור להוספת בט"ל לתוספת החמישית לחוק להסדרת הביטחון. במסגרת הפיכתו לגוף תמ"ק החל בט"ל לבצע פעילות יזומה לשיפור רמת ההגנה שלו, בהתאם למתודולוגיה הייעודית של גופי תמ"ק.

נכון לפברואר 2024, מתבצעים בכל יום עשרות אלפי ניסיונות לתקיפת סייבר נגד בט"ל. אירוע סייבר בבט"ל עלול לגרום לפגיעה חמורה בפרטיות של מיליוני אזרחים ותושבים המקבלים שירות מבט"ל, וכן עלול לגרום לפגיעה בעבודת בט"ל ואף לשיתוק של העבודה, ובעקבות כך לפגיעה ביכולת לשלם קצבאות (זקנה, נכות, קיום, אבטלה תגמולי מילואים). להלן דוגמה לאירוע אבטחת מידע חמור בבט"ל כהגדרתו בתקנות: בפברואר 2022 דווח על אירוע גניבת זהות שבעקבותיו מידע אישי על 2,000 אזרחים היה חשוף ונגיש למי שאינו מורשה לכך.

1 תקנה 1, התוספת הראשונה והתוספת השנייה בתקנות אבטחת מידע.

2 החלטת הממשלה ב/84 משנת 2002 שבה נקבע כי יש להקים ועדת היגוי עליונה להגנה על מערכות ממוחשבות במדינת ישראל, שתפקידה לבחון אילו גופים יוגדרו "חיוניים", ולכן זקוקים להגנה קיברנטית. האחריות להגנה זו הוטלה על שב"כ. בשנת 2016, במסגרת תיקון לחוק להסדרת הביטחון בגופים ציבוריים, התשנ"ח-1998, עברה אחריות זו מהשב"כ למס"ל.



נתוני מפתח

יותר משנתיים

פרק הזמן שבו לא התכנסה ועדת היגוי סייבר בראשות מנכ"ל - מראשית שנת 2022 עד לינואר 2024

עשרות אלפים

מספר ההתרעות להתקפות סייבר על בט"ל ביממה הדורשות תחקור על ידי אנליסט בודד שמאייש את מרכז שליטה ובקרה לטיפול באירועי סייבר (SOC) של בט"ל

10 שנים

לא עודכנה מדיניות הגנת הסייבר של בט"ל, אף שחלו שינויים משמעותיים מאז. 50% מהנהלים שלפי תקנות אבטחת מידע נדרש לכלול בנוהל אבטחת מידע של כל ארגון, אינם קיימים בבט"ל

גופים רבים

מקבלים מידע מבט"ל באמצעות מערכות שיתוף מידע שהתגלו בהן פערי אבטחת מידע

87%

מתקנות אבטחת מידע מקוימות בבט"ל באופן חלקי בלבד. לא מתבצעת כלל ביקורת תקופתית על עמידה בתקנות

0

מבדקי חדירה התבצעו לגבי המערכת המרכזית של בט"ל

פעולות הביקורת

בחודשים יולי 2023 עד אפריל 2024 בדק משרד מבקר המדינה את נושא אבטחת המידע והגנת הסייבר בבט"ל ואת העמידה שלו בתקנות אבטחת מידע. בביקורת נבדקו בין היתר הנושאים האלו: המדיניות והנהלים בתחום הגנת הסייבר; ניהול הסיכונים; העברת מידע מבט"ל לגופים חיצוניים; הגנה לוגית; הגנה פיזית; המשכיות עסקית; התמודדות עם אירועי סייבר; ושרשרת האספקה. הביקורת נעשתה בבט"ל, במשרד ראש הממשלה - במערך הסייבר ובמשרד המשפטים - ברשות להגנת הפרטיות.

ועדת המשנה של הוועדה לענייני ביקורת המדינה של הכנסת החליטה שלא להניח על שולחן הכנסת ולא לפרסם חלקים מפרק זה לשם שמירה על ביטחון המדינה, בהתאם לסעיף 17(א) לחוק מבקר המדינה, התשי"ח - 1958 (נוסח משולב).



תמונת המצב העולה מן הביקורת



מדיניות אבטחת מידע והגנת הסייבר - בט"ל לא עדכן את מדיניות אבטחת המידע והגנת הסייבר שלו במשך כעשר שנים, משנת 2014, זאת אף שמאז הסיכונים בתחום השתנו במידה ניכרת, ואף שהדבר מנוגד למדיניות בט"ל, ולפיה מדיניות אבטחת מידע תידון ותתוקף מדי שנה בשנה. בעת ביצוע הביקורת עודכן מסמך המדיניות לרמה של טיטה ואושר במרץ 2024 בידי ממלא מקום מנכ"ל בט"ל, אולם טרם התקיים דיון בוועדת ההיגוי לאבטחת מידע בנוגע למדיניות כנדרש במסמך המדיניות. כמו כן במסמך המדיניות חסרה התייחסות מפורשת לנושאים שנדרשת להם התייחסות לפי תקנים מקובלים, כמו ניהול וסיווג של נכסים והמחויבות לבצע בקרות על עמידה בתקנות אבטחת מידע.



נוהלי אבטחת מידע - בט"ל לא התייחס בנוהל אבטחת מידע של הארגון ל-6 (50%) מ-12 הנושאים שנקבע בתקנות אבטחת מידע כי נדרש להסדיר אותם במסגרת נוהל אבטחת מידע. לגבי ארבעה (33%) מ-12 הנושאים, הנהלים הקיימים בעניינם לא עודכנו עשר שנים; ולגבי שניים (17%) מ-12 הנושאים לא צוין המועד האחרון שבו עודכנו הנהלים בעניינם.



ועדת היגוי להגנת סייבר - ועדת היגוי סייבר בראשות המנכ"ל לא התכנסה מתחילת שנת 2022 ועד ינואר 2024, וזאת בניגוד למדיניות בט"ל המחייבת כינוס של הוועדה בכל חצי שנה. מכיוון שהוועדה לא התכנסה בפרק הזמן האמור, לא היה בפרק זמן זה בבט"ל גורם שיאשר את מדיניות הגנת הסייבר, יאשר את תוכניות העבודה השנתיות ויבצע מעקב אחר יישומן ויציג את רמת ההגנה בסייבר לראש הארגון, לרבות פערים, אירועים משמעותיים ואיומים. כמו כן, גם בדיון הראשון של ועדת ההיגוי בינואר 2024 לא הוצגה רמת ההגנה בסייבר לממלא מקום מנכ"ל בט"ל, לא אושרה טיטת המדיניות, ולא הוצגו נושאים מרכזיים אחרים שהוגדרו בכתב המינוי של הוועדה.



ניהול סיכונים - בט"ל אינו מנהל רשימת מצאי של כלל הנכסים והתהליכים העסקיים שלו ואינו מסווג אותם לפי רמת הקריטיות שלהם לארגון כנדרש בתקנות אבטחת מידע ובנורמות מקובלות בתחום הסייבר, ובהן הנורמות הכלולות בתורת ההגנה³. בט"ל בחר חלק מהמערכות החשובות והקריטיות מתוך כלל המערכות הקיימות בבט"ל, ומהן מופו כשליש מהמערכות שהוגדרו החשובות ביותר, ונקבע שמערכות אלה ייבחנו בסקר. קיום הליך של ניהול סיכונים שלא על בסיס מיפוי מלא של כלל נכסי הארגון מעלה חשש כי ניהול הסיכונים לא ישקף בצורה מיטבית את הסיכונים העיקריים שאליהם חשוף הארגון, וכי המשאבים והפעולות המופנים להתמודדות עם סיכונים אינם מוקצים בהלימה לרמת הסיכון הנשקפת לנכסי הארגון. כמן כן, בט"ל אינו מבצע סקרי סיכונים אחת ל-18 חודשים לגבי מאגרי המידע שלו, כנדרש מארגונים שיש להם מאגרי מידע שחלה עליהם רמת אבטחה גבוהה.



3 מערך הסייבר הלאומי, מדרך יישומי להגנת הסייבר של הארגון גרסה 2.0 (יוני 2021).



מבדקי חדירה - בט"ל אינו מבצע מבדקי חדירה לגבי מאגרי המידע שברשותו, כמתחייב מתקנות אבטחת מידע וכן ממסמך המדיניות שלו. כך, רק כ-7% מהמבדקים שבוצעו היו על מערכות שמקושרות למערכת המרכזית, אשר בה נמצאים כל מאגרי המידע של בט"ל. כמו כן, בט"ל אינו עוקב אחר תיקון הליקויים שנמצאו במבדקים, ונמצאו ליקויים חוזרים וליקויים רחביים ברמת חומרה גבוהה שלא תוקנו, דבר החושף את בט"ל לסיכון. זאת ועוד, בט"ל אינו מבצע מבדקי חדירה למערכת המרכזית וקיים חוסר במידע וידע אודות ביצוע מבדקים מסוג זה בבט"ל ובמס"ל.

הגנה לוגית - נמצאו פערים בהגנה הלוגית בבט"ל במספר נושאים.

זיהוי אירועי סייבר וטיפול בהם - נמצאו פערים ביכולת של בט"ל לזהות אירועי סייבר ולטפל בהם: אין בבט"ל צוותים ייעודיים לניהול משבר - צוות ניהול אירוע (IR) וצוות לביצוע חקירה פורמזית (DFIR); צוות הנהלה לניהול אירוע סייבר שהוקם בסוף ינואר 2024 לא התכנס, לא הוכשר ולא תורגל; נמצא פער בהפעלת ה-SOC; הצוות שמאייש את ה-SOC לא עבר הכשרה ייעודית לנושא; ה-SOC אינו נמצא באחריות חטיבת אבטחת מידע, אלא באחריות אגף תשתיות; יש חוסר הלימה בין הצורך בתחקור עשרות אלפי ההתערות ביממה, ובין איש ה-SOC באנליסט אחד בלבד. נוכח זאת קיים חשש כי לא מתאפשר לזהות את אירועי האמת בזמן סביר או בכלל.

המשכיות עסקית - נמצאו פערים ביכולת ההמשכיות העסקית של בט"ל בנושאים שלהלן: טיוטת נוהל התאוששות עסקית שקיימת בבט"ל איננה כוללת נושאים הנדרשים כחלק מתוכנית המשכיות עסקית, ובהם מיפוי עדכני של התהליכים החיוניים והסיכונים הכרוכים בהם, הגדרת יעדי התאוששות מדידים והקצאת משאבים ותשומות נדרשים. כמו כן, טיוטת הנוהל כוללת סדרי עדיפות להתאוששות משנת 1991, אשר אושרו בשנת 2013 ואינם עדכניים. נוסף על כך, בט"ל לא ביצע תרגול של תוכנית התאוששות מאסון בשלוש השנים האחרונות; נמצאו פערים ביכולת לשחזר מידע מגיבויים.

ניהול הסיכונים מצד שרשרת האספקה - לבט"ל אין נוהל בנושא שרשרת אספקה, ואין לו מיפוי של כלל ספקי התקשוב שלו והסיווג שלהם לפי רמת הסיכון הנשקף מהם. כמו כן, במכרזים של בט"ל אין נספח אבטחת מידע שמחייב עמידה של הספק בבקורות התואמות את הנדרש במתודולוגיית שרשרת האספקה. זאת ועוד, בט"ל אינו מבצע ביקורות על ספקי התקשוב שלו. נוכח זאת קיים סיכון לפגיעה בבט"ל באמצעות פגיעה באחד הספקים המהותיים שלו. במספר מקרים מצומצם שבהם ביצע בט"ל ביקורות התגלו ליקויים.

העברת מידע מבט"ל לגופים חיצוניים - בט"ל מעביר לגופים חיצוניים רבים מידע באמצעות מערכות לשיתוף מידע שהתגלו בהן פערי אבטחת מידע. כמו כן, בט"ל אינו מבצע בקרה על התאמת המידע שמועבר לגופים חיצוניים למידע שאישרה הוועדה להעברת מידע למסור. זאת ועוד בט"ל אינו מקיים בקורות עיתיות על תפוגת תוקף הממשק להעברת המידע ואינו מפסיק את העברת המידע לאחר חמש שנים כנדרש לפי נהליו.

עמידה בדרישות החוק והתקנות - נמצא כי אין בידי בט"ל תוכנית לבקרה שוטפת על העמידה של מאגרי המידע בדרישות תקנות אבטחת מידע, כנדרש בתקנה 3 לתקנות אלה. מאגר המידע של בט"ל, הנחשב למאגר גדול וכולל מידע רגיש בנפח של טרה-בייט (TB) רבים, מחייב קיום תוכנית סדורה כזו, כדי להבטיח רמת אבטחה נאותה. עוד נמצא כי רובן



המכריע של תקנות אבטחת מידע (13 מ-15 תקנות - 87%) מקוימות בבט"ל באופן חלקי בלבד.




צוות מבדקי חדירה פנימי - בט"ל מעסיק צוות בודקי חוסן מיומנים במשרה מלאה, אשר מבצע באופן שוטף מבדקי חדירה תשתיתיים ואפליקטיביים למערכות ויישומים. כאמור, לא מתבצעים מבדקים על המערכת המרכזית.


שרשרת האספקה - במכרזים החדשים בט"ל הוסיף בפרק אבטחת מידע נושאים כמו ביקורות אצל ספקים וחובת הדיווח שלהם על אירועים.


מלחמת חרבות ברזל - במהלך מלחמת חרבות ברזל נדרש בט"ל לבצע פעולות דחופות לטיפול בנפגעי פעולות האיבה, במשפחות החטופים, במשפחות המפונים ובמשרתי המילואים. פעולות אלו כללו בין היתר פיתוח שירותים חדשים לטיפול באוכלוסיות אלו; פיתוח ממשקים להעברת מידע לגופים אחרים; ומציאת פתרונות חדשים המאפשרים עבודה מהבית של עובדי בט"ל, כדי שהשירות לא יפגע.


אתר הגיבוי (DR) - משרד מבקר המדינה מציין לחיוב את בט"ל על העתקת אתר הגיבוי (DR) למקום החדש במרץ 2024, במהלך הביקורת.

עיקרי הממצאות הביקורת

על בט"ל לעדכן את מסמך מדיניות אבטחת המידע והגנת הסייבר שלו בנושאים שנדרשת להן התייחסות לפי תקנים מקובלים ולהציגו בוועדת ההיגוי לאבטחת מידע, וכן עליו לוודא כי המסמך יעודכן באופן עיתי ובהתאם לסיכונים המשתנים בתחום כפי שמתחייב במדיניות אבטחת המידע והגנת הסייבר של בט"ל. 

נוכח החשש כי נושאים עיקריים באבטחת המידע של בט"ל אינם מטופלים בהתאם לשינויים בסביבה הארגונית, לאיומי הסייבר החדשים ולסיכונים, על בט"ל לעדכן את נוהל אבטחת המידע שלו כך שיכלול את הנושאים שנדרשים לפי תקנות אבטחת מידע. אשר לנהלים הקיימים, יש לעדכן את הנושאים שלא עודכנו בשנתיים האחרונות. 

נוכח חילופי ממלא מקום המנכ"ל בבט"ל לאחר כינוס ועדת היגוי סייבר בראשונה ונוכח העובדה שבדיון הוועדה לא הוצגו נושאים משמעותיים כמו רמת ההגנה בסייבר של בט"ל, מומלץ כי בט"ל יכנס בהקדם את ועדת היגוי סייבר, כדי להציג לפניה את נושא רמת ההגנה בסייבר ונושאים מרכזיים אחרים שנכללו בכתב המינוי של הוועדה ולאשר את טיטוט המדיניות. 

על בט"ל לערוך מיפוי של כלל הנכסים והתהליכים העסקיים שלו ולסווג אותם לפי רמת הקריטיות שלהם לארגון וזאת בהתאם לנדרש בתקנות אבטחת מידע. 



מומלץ כי בט"ל, בהנחיית מס"ל, יבצע תהליך סדור של סקרי סיכוני אבטחת מידע בהתאם למתודולוגיות מקובלות, כמו תורת ההגנה, ויודא כי בסקרי הסיכונים יובאו בחשבון סיכונים הנשקפים לגופי תמ"ק ברמה הלאומית. עוד מומלץ כי ממצאי הסקר והתוכנית לתיקון הליקויים שעלו בו יועברו למס"ל המשמש כמנחה מקצועי של בט"ל.

מומלץ כי בט"ל ייעזר במומחי תוכן בנושא המערכת המרכזית לצורך ביצוע מבדקי חדירה למערכת המרכזית. היות שחלק מגופי התמ"ק מחזיקים גם הם במערכות דומות, מומלץ כי מס"ל יקים פורום לשיתוף ידע בין הגורמים הרלוונטיים, שבין היתר יבחן מענה מערכתית לאומי לביצוע מבדקים על מערכות אלו.

מומלץ כי בט"ל יקים צוותים ייעודיים לניהול משבר: צוות ניהול אירוע (IR) וצוות לביצוע חקירה פורנזית (DFIR). עוד מומלץ כי בט"ל יפעל לכנס ולתרגל את צוות ההנהלה לניהול אירוע סייבר.

מומלץ כי בט"ל, בשיתוף מערך הסייבר, ישפר את היכולות של ה-SOC לגלות ולזהות אירועי סייבר וכן יפעל לסגירת הפער בהפעלת ה-SOC. עוד מומלץ כי מערך ה-SOC יהיה כפוף לחטיבת אבטחת מידע.

מומלץ כי בט"ל, בליווי ובסיוע של מס"ל, יבצע מיפוי מלא של כל הספקים שלו, כנדרש בהנחיית מס"ל בנושא. עוד מומלץ כי בט"ל יגבש תבנית של נספח אבטחת מידע במכרזים שכוללת את המחויבויות של הספק במסגרת ההתקשרות ואת הדרישות ממנו לעמידה בבקורות, בהתאם למתודולוגיית שרשרת האספקה של מערך הסייבר.

על בט"ל לערוך סקרי סיכונים ומבדקי אבטחת מידע למערכות שיתוף המידע הפעילות. במידה ויתגלו במערכות אלו פערי אבטחת מידע, על בט"ל להטמיע בקורות מפצות.

על בט"ל לבצע בהקדם ביקורת על מידת העמידה של המאגרים המשמעותיים שברשותו בתקנות אבטחת מידע וזאת כנדרש בתקנות. בנוסף עליו לבצע את הביקורת באופן עתי.



מידת עמידתו של בט"ל בתקנות אבטחת מידע

ממצאי הביקורת	הנושא
קיים חלקית	מסמך הגדרות המאגר
קיים חלקית	ממונה על אבטחת מידע
קיים חלקית	נוהל אבטחה
קיים חלקית	מיפוי מערכות המאגר וביצוע סקר סיכונים
קיים	אבטחה פיזית וסביבתית
קיים חלקית	אבטחת מידע לגבי ניהול כוח אדם
קיים חלקית	הגנה לוגית - נושא 1
קיים חלקית	הגנה לוגית - נושא 2
קיים חלקית	הגנה לוגית - נושא 3
קיים חלקית	תיעוד של אירועי אבטחה
קיים חלקית	התקנים ניידים
קיים חלקית	ניהול מאובטח ומעודכן של מערכות המאגר
קיים חלקית	אבטחת תקשורת
קיים חלקית	מיקור חוץ
לא קיים	ביקורת תקופתית

הוכן בידי משרד מבקר המדינה.



סיכום

בט"ל מחזיק במאגר גדול, בנפח של טרה-בייט (TB) רבים, הכולל מידע על כל תושבי מדינת ישראל מיום הלידה ועד יום הפטירה. מאגר זה נדרש לרמת אבטחה גבוהה בהתאם לחוק הגנת הפרטיות ולתקנות אבטחת מידע, וכן משום שהוא יעד מרכזי לניסיונות תקיפה (עשרות אלפי חשדות לאירועים ביממה), ופגיעה בו עלולה להיות קריטית בייחוד בתקופה זו של מלחמת חרבות ברזל, שבה ממלא בט"ל תפקיד חיוני בטיפול בנפגעים, במפונים ובאנשי המילואים.

ביוני 2023 הוגדר בט"ל כתשתית מדינה קריטית (גוף תמ"ק) והחל בתהליכי אסדרה של הגנת הסייבר בהתאם לתו"ל ייעודי לגופי תמ"ק, בהנחיית מערך הסייבר. במהלך מלחמת חרבות ברזל נדרש בט"ל לבצע פעולות דחופות לטיפול בנפגעי פעולות האיבה, במשפחות החטופים, במשפחות המפונים ובמשרתי המילואים. פעולות אלו כללו בין היתר פיתוח שירותים חדשים לטיפול באוכלוסיות אלו; פיתוח ממשקים להעברת מידע לגופים אחרים; ומציאת פתרונות חדשים המאפשרים עבודה מהבית של עובדי בט"ל, כדי שהשירות לא ייפגע.

ממצאיו של דוח זה משקפים פערים ניכרים בכל הנוגע לניהול אבטחת המידע בבט"ל ולהיערכותו לאיומי סייבר. פערים רבים עלו בנוגע למכלול תחומי הפעילות הרלוונטיים לאבטחת המידע וביניהם: פערים בגילוי אירועי סייבר ובטיפול בהם; ליקויים ברמת האבטחה הלוגית; תוכנית המשכיות עסקית שאינה עדכנית; ויכולת התאוששות נמוכה במקרה של אסון. הממצאים שהועלו בדוח זה, כמכלול, וכל ממצא בפני עצמו מהווים סיכון לפגיעה בסודיות, באמינות ובזמינות של המידע שבמאגרי בט"ל.

הדוח כולל ממצאים נוספים הנוגעים לקיום חלקי ביותר של תקנות אבטחת מידע ולחוסר יכולת של חטיבת אבטחת מידע בארגון למלא חלק מתפקידיה.

על ממלא מקום מנכ"ל בט"ל, הנהלת בט"ל וועדת היגוי סייבר, בשיתוף מס"ל, כמנחה מקצועי, לפעול בהקדם למיפוי סיכוני הסייבר המהותיים הניצבים בפני הארגון ולגבש תוכנית עבודה לטיפול בפערי אבטחת המידע, ובהם הפערים שצוינו בדוח זה.