מבקר המדינה

אבטחת המידע והגנת הסייבר במוסד לביטוח לאומי

חשוון התשפ"ה | נובמבר 2024

אבטחת המידע והגנת הסייבר במוסד לביטוח לאומי

מבוא

המוסד לביטוח לאומי (להלן - בט"ל) הוא תאגיד סטטוטורי הפועל מתוקף חוק הביטוח הלאומי [נוסח משולב], התשנ"ה-1995, ונתון לפיקוחו הכללי של שר העבודה. בט"ל פועל לצמצום העוני והפערים הכלכליים במדינת ישראל, ונועד להבטיח לאוכלוסיות ראויות לקידום ולמשפחות שנקלעו למצוקה זמנית או ממושכת בסיס כלכלי לקיומן, בין היתר באמצעות תשלום גמלאות ומתן שירותי שיקום, סיעוד ועוד, על פי המבחנים הקבועים בחוק.

בשנת 2022 התקבלו בבט"ל יותר מ-53 מיליון פניות מאזרחים, כ-40 מיליון מהן (כ-75%) דרך אתר המרשתת של בט"ל[1]. פניות אלו היו בתחומים שונים, ובהם זימון תורים, שירות אישי ואתר התשלומים. באותה שנה שילם בט"ל קצבאות בסכום של יותר מ-120 מיליארד ש"ח. הנגשה דיגיטלית של מרבית השירותים של בט"ל מצריכה ממנו לאפיין ולפתח את השירותים באופן מאובטח מבחינת הגנת הסייבר.

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. התרשים שלהלן מפרט את סוגי המידע המצוי במאגרי המידע של הביטוח הלאומי:

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

על פי נתוני המוסד לביטוח לאומי, בעיבוד משרד מבקר המדינה.

לפי תקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017 (להלן - תקנות אבטחת מידע)[2], מאגר מידע המכיל מידע על מצבם האישי או הרפואי או הכלכלי של אנשים ויש בו יותר מ-100,000

[1] אתר המרשתת של הביטוח הלאומי, "סיכום הפעילות בשנת 2022" (אפריל 2023).
[2] תקנה 1, התוספת הראשונה והתוספת השנייה בתקנות אבטחת מידע.

רשומות, נדרש לעמוד ברמת אבטחה גבוהה. התקנות מפרטות כיצד יש לשמור על רמת האבטחה שנקבעה למאגר. נוכח תקנות אלה, המאגרים של בט"ל נדרשים לרמת אבטחה גבוהה.

בבט"ל קיימות מאות מערכות מידע אשר פותחו במשך עשרות שנים על גבי תשתית משנת 1970 (להלן - מערכת מרכזית). בדצמבר 2009 השיק בט"ל את פרויקט תשתיות ביטוח לאומי (להלן - תב"ל) הכולל בניית תשתית טכנולוגית מודרנית ושדרוג הדרגתי של כלל מערכות המידע במוסד בתחומי הליבה. נכון למועד כתיבת הביקורת בפברואר 2024 הוסבו לתב"ל 10 מ-38 מערכות שהיה מתוכנן להסב. משרד מבקר המדינה פרסם בשנת 2020 דוח ביקורת על פרויקט תב"ל[3] ובמסגרת הפרסום לשנת 2024 נכלל דוח מעקב תיקון ליקויים על הדוח שנעשה בשנת 2020.

עד יולי 2023 בט"ל היה מונחה על ידי שב"כ בכל הקשור להגנה על סודות מדינה, בהתאם לתוספת השניה לחוק להסדרת הביטחון בגופים ציבוריים, התשנ"ח-1998 (להלן - החוק להסדרת הביטחון). החל משנת 2016 ועד יולי 2023 בט"ל היה מונחה מרצון על ידי מערך הסייבר בכלל היבטי ההגנה בסייבר בנוסף להנחיית השב"כ. בעקבות המלצה בדוח של מבקר המדינה[4] וקביעות נוספות של מערך הסייבר, ובתמיכתו של בט"ל, המליץ מערך הסייבר בחודש פברואר 2023 להגדיר את ביטוח לאומי כגוף שהוא תשתית מדינה קריטית (להלן - גוף תמ"ק). בהמשך להמלצה זו, ביולי 2023 החליטה ועדת היגוי עליונה להגנה על מערכות ממוחשבות במדינת ישראל[5] (להלן -ועדה ב/84) כי בט"ל עונה על התבחינים הנדרשים, וכי יש מקום להנחותו כגוף תמ"ק. לפיכך המליצה הוועדה על הוספת בט"ל לתוספת החמישית לחוק להסדרת הביטחון, כדי שבט"ל יהיה מונחה לפי חוק זה על ידי מערך הסייבר בכל הנושאים כולל הגנה על סודות מדינה והאחריות לכך הועברה מהשב"כ למערך הסייבר. 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 (כגון: זקנה, נכות, קיום, אבטלה, תגמולי מילואים). להלן דוגמה לאירוע אבטחת מידע חמור[6] 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.

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.

<u>פעולות הביקורת</u>

בחודשים יולי 2023 עד אפריל 2024 בדק משרד מבקר המדינה את נושא אבטחת המידע והגנת הסייבר בבט"ל והעמידה שלו בתקנות אבטחת מידע. בביקורת נבדקו בין היתר הנושאים האלו: המדיניות והנהלים בתחום הגנת הסייבר; ניהול הסיכונים; העברת מידע מבט"ל לגופים חיצוניים;

---

3 מבקר המדינה, **דוח שנתי 70ג** (2020), עמודים 577-533, "פרויקט תבל לשדרוג מערך המחשוב במוסד לביטוח לאומי". יצוין כי במהלך שנת 2024 צפוי מבקר המדינה לפרסם דוח מעקב על דוח זה.

4 מבקר המדינה, דוח שנתי (2023), "אסדרת אבטחת הסייבר במוסד לביטוח לאומי".

5 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.

6 אירוע אבטחה חמור במאגר מידע שחלה עליו רמת אבטחה גבוהה הוא אירוע שנעשה בו שימוש במידע מן המאגר בלא הרשאה או בחריגה מהרשאה, או שנעשתה פגיעה בשלמות המידע.

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).

הגופים האסדרתיים המדינתיים בתחום אבטחת המידע והגנת הסייבר

המחוקק התייחס לתחום אבטחת המידע והגנת הסייבר בחוק להסדרת הביטחון, בחוק הגנת הפרטיות, התשמ"א-1981 (להלן - חוק הגנת הפרטיות), ובתקנות אבטחת מידע. כמו כן קיבלה הממשלה כמה החלטות העוסקות בתחום זה[7].

בהתאם להחלטות הממשלה ולחוק, הנחיית תחום אבטחת הסייבר נחלקת למספר גורמים. להלן רשימת הגופים האסדרתיים המדינתיים בתחום הסייבר שאליהם מתייחס הדוח:

מערך הסייבר הלאומי (להלן - מס"ל): בשנת 2016, במסגרת מימוש החלטות הממשלה בדבר גורם לאומי בתחום הגנת הסייבר, עודכן החוק להסדרת הביטחון בגופים ציבוריים, התשנ"ח-1998, והאחריות להנחיית מרבית גופי התמ"ק הועברה משירות הביטחון הכללי (להלן - השב"כ) למערך הסייבר[8]. בהתאם לכך מנחה אגף הנחיה סקטוריאלית במערך הסייבר באופן ישיר את גופי התמ"ק המצוינים בתוספת החמישית לחוק, והוא אחראי ללוות את הגוף באופן שוטף ולסייע לו בין היתר בפעולות האלו: בניית תוכנית העבודה השנתית בתחום הגנת הסייבר ומעקב אחר ביצועה; ופיקוח על אופן היישום של תורת ההגנה הייעודית לגופי תמ"ק (להלן - תו"ל ייעודי). מערך הסייבר גם מבצע מבדקי חדירה ומחקרי תקשורת בגופים שהוא מנחה אותם. כמו כן, האגף הארצי לניהול אירועי סייבר במס"ל (להלן - CERT) יכול לסייע לגוף כשיש חשש לאירוע סייבר שעשוי להסב לו או לארגונים אחרים נזק חמור. נוסף על כך, מס"ל פרסם מדריך יישומי להגנת הסייבר בארגון, שהוא בגדר המלצה לכל ארגון במשק; שם המדריך - תורת ההגנה 2.0 (להלן - תורת ההגנה).

היחידה להגנת הסייבר בממשלה (להלן - יה"ב): היחידה הוקמה בעקבות החלטת הממשלה 2443. ייעוד היחידה הוא לכוון ולהנחות מקצועית בתחום הגנת הסייבר את כלל משרדי הממשלה ויחידות הסמך, למעט הגופים המיוחדים, ולהקים מרכז שליטה ובקרה ממשלתי להתמודדות עם איומי הסייבר (SOC ממשלתי). יה"ב פרסמה מסמך מדיניות להגנת הסייבר בממשלה והנחיית מסגרת להגנת הסייבר בממשלה, הכוללים נהלים והנחיות המחייבים את המשרדים ומגדירים ניהול תהליכים מרכזיים בנושא הגנת הסייבר. אף שהנחיות יה"ב אינן מחייבות את בט"ל, הן מגדירות נורמות מקובלות בתחום הגנת הסייבר עבור גופים ציבוריים הדומים לבט"ל.

הרשות להגנת הפרטיות: הרשות להגנת הפרטיות היא מאסדרת של כלל המשק ומופקדת על הגנת הזכות לפרטיות ובכלל זה אבטחת המידע בכלל מאגרי המידע הכוללים מידע אישי בישראל. לשם כך הרשות מוסמכת לבצע אכיפה מינהלית ואכיפה פלילית הן על גופים פרטיים והן על גופים ציבוריים, בהתאם להוראות חוק הגנת הפרטיות ותקנותיו. לצורך הפקת תמונת מצב מגזרית בנוגע לעמידה בהוראות החוק והתקנות ולצורך איתור כשלים הטעונים אסדרה קיים בידי הרשות מנעד של כלים, ובהם הכלי של פיקוח רוחב, הנעשה בעיקר במגזרים שיש בהם סיכון גבוה לפגיעה בפרטיות. נוכח מספרם הרב של הגופים המפוקחים מצד אחד ומגבלת המשאבים של הרשות מצד

---

7 החלטת ממשלה 2443, "קידום אסדרה לאומית והובלה ממשלתית בהגנת הסייבר" (15.02.2015), החלטת הממשלה 3611 "קידום היכולת הלאומית במרחב הקיברנטי", (7.8.2011), החלטת ממשלה 2444 "קידום ההיערכות הלאומית להגנת הסייבר" (15.02.2015).

8 גופי התקשורת נותרו באחריות השב"כ. רשימת הגופים והאחראים להם מוגדרת בחוק להסדרת הביטחון בגופים ציבוריים, התשנ"ח-1998.

שני, תוכניות האכיפה והפיקוח של הרשות להגנת הפרטיות מבוססות ברובן על ניהול סיכונים ותיעדוף. בקביעת תוכנית אכיפה, המתבססת על תוכנית העבודה השנתית והמדיניות הכוללת של הרשות, מובאים בחשבון עניינים שונים, ובין היתר מידת ההשפעה הרוחבית של פעילות האכיפה, מתן עדיפות לטיפול בגופים המחזיקים במידע רגיש בהיקף נרחב ומתן קדימות לנושאים רגישים. הרשות ביצעה כמה הליכים מינהליים מול בט"ל וכן ביצעה פיקוח רוחבי בבט"ל באוגוסט 2022 כחלק מפיקוח הרוחב שבוצע במגזר החברות הממשלתיות והתאגידים הסטטוטוריים בישראל.

שירות הביטחון הכללי (להלן - שב"כ): שב"כ הנחה את בט"ל לאורך השנים בהיבטי אבטחת מידע מסווג בלבד - אבטחת סודות מדינה (אס"מ). מיום אישור ועדה ב/84 של בט"ל כגוף תמ"ק, מס"ל מנחה את בט"ל בכלל ההיבטים של אבטחת מידע והגנת הסייבר לרבות הגנה על סודות מדינה.

כאמור לעיל, תקנות אבטחת מידע הן תקנות שחלות על בט"ל ומחייבות אותו. אשר לנושאי הגנת הסייבר שאינם מפורטים בתקנות, דוח זה רואה בתורת ההגנה 2.0 של מס"ל ובהנחיות יה"ב כמייצגות סטנדרטים מקובלים ונורמות מקובלות בתחומים אלה.

מדיניות ונהלים בתחום אבטחת המידע והגנת הסייבר ומסגרת ארגונית ליישומם

<u>מדיניות אבטחת מידע והגנת סייבר</u>

המדיניות להגנת הסייבר מבוססת על סיכונים למידע, למערכות המחשוב, למערכות המאחסנות את המידע ולרשתות התקשורת, בהתאם לצרכים התפעוליים והארגוניים. העקרונות במדיניות להגנת הסייבר משמשים בסיס לנוהלי העבודה בתחום הגנת הסייבר.

מסמך מדיניות אבטחת מידע של בט"ל הוא משנת 2014. נכתב בו כי מטרת המדיניות היא לציין לכל עובדי המשרד המטפלים או עוסקים או נעזרים במערכי המידע, השליטה והבקרה את העקרונות לאבטחת המידע שנקבעו על ידי ועדת ההיגוי לאבטחת המידע, ואשר מהם נגזרים נוהלי אבטחת המידע של בט"ל. עוד נכתב במסמך כי המדיניות תתוקף מדי שנה בשנה.

בט"ל מסר כי המדיניות והנהלים בתחום אבטחת המידע גובשו בשנת 2014 ומאז לא עודכנו או תוקפו. מערך הסייבר המנחה את בט"ל הגדיר עמו תאריך יעד לעדכון המדיניות - דצמבר 2023.

במהלך הביקורת, בנובמבר 2023, הועברה לצוות הביקורת טיוטת מסמך מדיניות עדכנית (להלן - הטיוטה) שטרם אושרה בידי הנהלת בט"ל, וכפופה עדיין לשינויים. בטיוטה התווספה התייחסות לנושאים שלא נכללו במסמך המדיניות הקיים ונדרשים לפי תקנים מקובלים כמו: שרשרת האספקה, התאמה לדרישות החוקים החלים על הארגון, פיתוח מאובטח ורכש. בטיוטת המדיניות יש נושא שחסר (ניהול וסיווג נכסים) ויש נושאים נוספים שכתובים ברמה כללית ואין להם פירוט. למשל: מהימנות עובדים ומידור, מערך הרשאות, אבטחה פיזית וגיבויים. כמו כן בטיוטה אין התייחסות מפורשת לתקנות אבטחת מידע ולמחויבות לבצע בקרות על עמידה בתקנות. זאת ועוד בטיוטת המדיניות נכתב כי גיבוש, עדכון ושינוי מדיניות אבטחת מידע הן מתפקידיה וסמכויותיה של ועדת היגוי.

בתוכנית העבודה של בט"ל לשנת 2024 שהוצגה לוועדת ההיגוי בינואר 2024 מופיעה משימה בנושא אישור מדיניות אבטחת מידע על ידי ועדת ההיגוי. במרץ 2024 אישר ממלא מקום מנכ"ל הבט"ל את טיוטת מסמך המדיניות.

נמצא כי 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 טיוטה 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.

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.

נוהלי אבטחת מידע

תקנה 4ג לתקנות אבטחת מידע כוללת פירוט של הנושאים שנדרש לכלול בנוהל אבטחת מידע של כל ארגון. צוות הביקורת בחן אם בבט"ל יש נהלים בנושאים אלו (ראו פירוט בתרשים שלהלן). כמו כן תקנה 4ה קובעת כי בעל מאגר מידע יבחן אחת לשנה את הצורך בעדכון הנוהל, ובלי לגרוע מן האמור יבחן אם יש צורך בעדכונו של הנוהל במקרים אלה:

1. נעשו שינויים מהותיים במערכות המאגר או בתהליכי עיבוד המידע.
2. נודע על סיכונים טכנולוגיים חדשים הנוגעים למערכות המאגר.

בישיבה שקיימה ועדת אבטחת מידע בבט"ל ביוני 2022 הוחלט כי יש לבנות תוכנית עבודה לריענון נהלים ולהביאם לאישור הוועדה, אולם החלטה זו לא יושמה עד מועד סיום הביקורת באפריל 2024. בישיבה שקיימה ועדת אבטחת מידע בדצמבר 2022 נמסר כי נוהלי אגף הביטחון ונוהלי יחידת תקשוב ומערכות מידע מעודכנים לשנת 2016.

הרשות להגנת הפרטיות ביצעה בשנת 2022 פיקוח רוחב על בט"ל, ובמסגרתו העירה לבט"ל על החוסר בנהלים ועל שנוהל אבטחת מידע אינו מכסה 50% מהסעיפים שמפורטים בתקנות או אינו איכותי מספיק. בתגובת בט"ל על דוח פיקוח הרוחב נמסר תאריך היעד לתיקון הפערים: 30.12.23.

נמצא כי 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 4 (33%) מ-12 הנושאים, הנהלים הקיימים בעניינם לא עודכנו עשר שנים; ולגבי 2 (17%) מ-12 הנושאים, לא צוין המועד האחרון שבו עודכנו הנהלים בעניינם.

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.

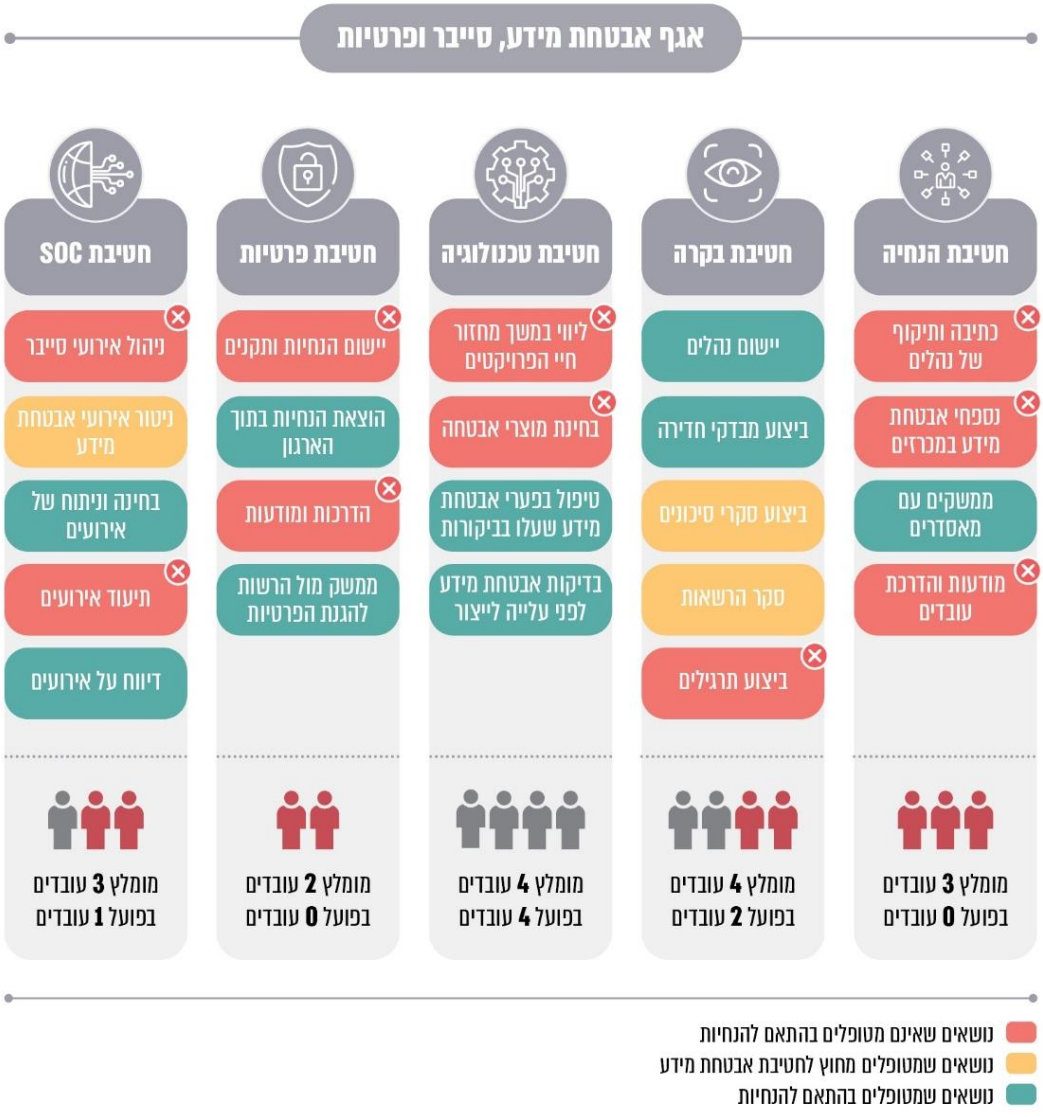
המסגרת הארגונית האחראית ליישום המדיניות

בבט"ל קיימת יחידת תקשוב ומערכות מידע (להלן - יחידת תמ"מ) בראשות סמנכ"ל תמ"מ. תחת יחידת תמ"מ יש אגפים, ותחת האגפים יש חטיבות. חטיבת אבטחת מידע כפופה לסמנכ"ל ואחראית לגיבוש וליישום של מדיניות אבטחת המידע, לביצוע מבדקי חדירה ולהנחיה של עובדי התשתיות. מנהל החטיבה משמש ממונה אבטחת המידע של המאגרים וממונה גופי תמ"ק. אגף הביטחון בבט"ל אחראי לאבטחה הפיזית ולסיווג העובדים.

מנהל חטיבת אבטחת מידע בבט"ל מסר כי חלק מן העובדים, למשל אלו העובדים במרכז הבקרה להגנת הסייבר (SOC), אינם כפופים אליו אלא למנהל אגף תשתיות, וכי עובדי החטיבה אינם יושבים במקום מרוכז, אלא מפוזרים בין שאר עובדי יחידת תמ"מ.

במסמך הדרישות של מס"ל בעניין מיצוב אגף אבטחת מידע, סייבר ופרטיות בבט"ל מאוגוסט 2023 צוינו הפערים האלה: משאבי חטיבת אבטחת מידע אינם מספיקים למילוי משימותיה; וממונה אבטחת המידע בבט"ל אינו מעורב בדיונים שבועיים לקידום נושאי פיתוח ותשתית. עוד נכתב במסמך כי כדי להבטיח את יכולת האגף לקיים את ייעודו נדרש שהממונה יקבל אחריות וסמכות מהמנכ"ל ומסמנכ"ל מערכות מידע לגבי הובלת משימותיו וכן יקבל תיעדוף לתקצוב כלל משימותיו. במסמך גם נכתב כי על בט"ל להיערך בדחיפות לשינוי המבנה הארגוני שלו, ובכלל זה להפיכת חטיבת אבטחת מידע לאגף שתחתיו יהיו כמה חטיבות שיעסקו בנושאים שונים, כפי שמופיע בתרשים שלהלן:

תרשים 2: **המבנה הארגוני שהציע מס"ל ומצב הנושאים שמטופלים כיום**



בעיבוד משרד מבקר המדינה.

באוקטובר 2023 התקיים דיון בהשתתפות מס"ל והגורמים האלו מבט"ל: סמנכ"ל תמ"מ, מנהל אבטחת מידע ומנהל תשתיות. בדיון הוצגו בין היתר הפערים בין המבנה הארגוני הקיים בבט"ל לבין זה המוצע על ידי מס"ל והוגדרו פעילויות של בט"ל לטיפול בפערים. בתשובת בט"ל ממרץ 2024 נמסר כי בדצמבר 2023 דנה הנהלת בט"ל בפערים במבנה הארגוני.

נמצא כי חטיבת אבטחת מידע בבט"ל אינה מטפלת בכמחצית הנושאים בתחום אבטחת מידע, כנדרש במסמך הדרישות של מס"ל בעניין מיצוב אגף אבטחת מידע, וזאת בשל מחסור בכוח אדם. הנושאים שאינם מטופלים הם למשל ניהול אירועי סייבר, יישום ההנחיות שנקבעו בתקנות אבטחת מידע, גיבוש נספחי אבטחת מידע במכרזים, בחינת מוצרי אבטחה וליווי הפרויקטים במשך מחזור החיים שלהם כדי לוודא שמשולבים בהם היבטי אבטחת מידע.

עוד נמצא כי יש נושאים מהותיים בתחום אבטחת המידע שמטופלים מחוץ לחטיבת אבטחת מידע, כמו ניטור אירועי אבטחת מידע, ולכן יש חשש שהעדיפות הניתנת להם אינה בהלימה לסיכון שבהם, או שממצאיהם לא יובאו לפני מנהל חטיבת אבטחת מידע, שהוא הממונה על תחום אבטחת המידע והממונה על גופי התמ"ק. עוד נמצא שמנהל החטיבה אינו מעורב בדיוני הנהלת בט"ל בנושאי פיתוח ותשתיות, ולכן יש חשש שהיבטי אבטחת מידע לא יקבלו בדיונים אלה את המשקל הראוי.

מומלץ כי הנהלת בט"ל תמשיך בתגבור כוח האדם וביישום השינוי במבנה הארגוני של חטיבת אבטחת המידע שהומלץ על ידי מס"ל ותוודא מתן מענה של בט"ל בנושאים המוטלים עליו מכח החוק ובתקנות אבטחת מידע אשר אינם מקבלים כיום מענה.

בתשובת בט"ל ממרץ 2024 נמסר כי כחלק מיישום תוכנית העבודה לשנת 2024, ובעקבות פערי הידע והמיומנות בקרב כוח האדם הקיים בחטיבת אבטחת המידע, מתוגברת חטיבת אבטחת מידע בכח אדם מקצועי. בחודש מרץ 2024 גויסו שני עובדים חדשים (יועץ אבטחת מידע לתחום הענן, עובדת ביטוח לאומי - אנליסטית אבטחת מידע) בנוסף לכך ישנן שתי משרות נוספות בהליכי גיוס (לרבות גיוס מתודולוג מומחה לנושא אבטחת המידע).

ועדת היגוי להגנת הסייבר

ועדת היגוי להגנת הסייבר היא מסגרת ארגונית ניהולית לקבלת החלטות אסטרטגיות בתחום הגנת הסייבר ולביצוע בקרה ניהולית על יישום הגנת הסייבר בארגון.

בהחלטת הממשלה 2443 נקבע כי על משרדי הממשלה להקים מסגרת ארגונית האחראית ליישום המדיניות בנושאי הגנת המידע והסייבר בראשות מנכ"ל. בהנחית יה"ב 5.1 בנושא "מדיניות להגנת הסייבר בממשלה" נכתב כי ועדת ההיגוי בכל משרד אחראית לגיבוש עקרונות המדיניות, להתוויית אסטרטגיות לפעילות, לאישור תוכנית האב ותוכניות העבודה השנתיות, לביצוע הערכת נזקים בעקבות תקלות ולגיבוש המלצות לטיפול על פי מסמך עקרונות המדיניות.

במסמך המדיניות של בט"ל נקבע כי באחריות ההנהלה למנות ועדת היגוי בראשות המנכ"ל או מנהל בכיר שהוסמך על ידו, שבה יהיו חברים בעלי תפקידים בכירים בבט"ל ואחראים בתחום האבטחה וההגנה של המידע והסייבר, לרבות אחראים בהיבטים טכנולוגיים, אבחנתיים ותפעוליים. עוד נקבע במסמך כי ועדת ההיגוי תתכנס לכל הפחות פעם בחצי שנה. תפקידי ועדת ההיגוי הם בין היתר לבצע מעקב ובקרה לגבי פרויקטים המחייבים אבטחת מידע ארגוני.

ועדת היגוי סייבר בראשות מנכ"ל שהייתה קיימת בבט"ל פוזרה בסוף שנת 2021. כחלק מתהליך הפיכת בט"ל לגוף תמ"ק פורסמו כתבי מינוי לחברי ועדת היגוי סייבר באוגוסט 2023, ונקבע כי הוועדה תתכנס אחת לרבעון. בכתב המינוי הוגדרו בין היתר מטרות הוועדה: קביעת מדיניות סייבר ואבטחת מידע בביטוח לאומי; אישור תוכניות עבודה שנתיות תיעדוף ומעקב על ביצוע; דיון באיומים ובחשיפות אבטחת מידע ובחינת דרכים לשיפור מתמיד של ההגנה מפני איומי סייבר; אישור הגדרת נכסי מידע מסווגים ותהליכים קריטיים; הצגת רמת ההגנה בסייבר לראש הארגון וכן פערים, אירועים משמעותיים ואיומים.

בשנת 2022 בהיעדר ועדת היגוי סייבר, הוקמה ועדה בראשות סמנכ"ל תמ"מ שתפקידיה הם לדון, לקבל החלטות ולבצע בקרה בנושאים הקשורים לאבטחת מידע ואיומי סייבר (להלן - ועדת אבטחת

מידע). ועדה זו התכנסה שש פעמים בין יוני 2022 ליולי 2023. בדיוני הוועדה שהתקיימו בפרק זמן זה לא עלו נושאים כמו עדכון מסמך המדיניות או אישור תוכנית העבודה, וכן לא בוצעה בקרה על החלטות שהתקבלו בוועדה על קידום נושאים כמו נוהלי עבודה והדרכות עובדים.

במהלך הביקורת, בינואר 2024, התכנסה לראשונה ועדת היגוי סייבר בראשות ממלא מקום מנכ"ל ובהשתתפות המנחים המקצועיים מטעם מס"ל. בוועדה הוצגו מטרות הוועדה, מונו ועדות משנה ואישרו את עיקרי תוכנית העבודה בתחום אבטחת מידע לשנת 2024.

נמצא כי 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 למנכ"ל בט"ל, לרבות פערים, אירועים משמעותיים ואיומים. עוד נמצא כי גם בדיון הראשון של ועדת ההיגוי, בינואר 2024, לא הוצגה רמת ההגנה בסייבר לממלא מקום מנכ"ל בט"ל, לא אושרה טיוטת המדיניות, ולא הוצגו נושאים מרכזיים אחרים שהוגדרו בכתב המינוי של הוועדה.

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 טיוטת המדיניות.

ניהול סיכוני אבטחת מידע וסייבר

<u>ניהול וסיווג של נכסי מידע</u>

לפי תקנה 5 לתקנות אבטחת מידע, על בעל מאגר מידע להחזיק מסמך מעודכן של מבנה המאגר וכן רשימת מצאי מעודכנת של מערכות המאגר, ובכלל זה תשתיות ומערכות חומרה, מערכות התוכנה המשמשות להפעלת המאגר, תוכנות וממשקים המשמשים לתקשורת בין מערכות המאגר למערכות אחרות ותרשים הרשת שפועל בה המאגר.

לפי תורת ההגנה, השלב הראשון בניהול סיכונים הוא הגדרת יעדי ההגנה העיקריים של הארגון (תהליכים עסקיים או נכסים דיגיטליים). בקרה 1.2 בתורת ההגנה נועדה לוודא כי ברשות הארגון מיפוי עדכני הכולל את רשימת יעדי ההגנה שלו. כמו כן, לפי הבקרה יש לוודא כי לכל יעד הגנה שמופה נקבעה בשנה האחרונה רמת ערכיות (עד כמה יעד ההגנה קריטי לארגון). סיווג הנכסים יתבצע לפי הסבירות להתממשותם, מידת הנזק הפוטנציאלי במקרה של התממשות הסיכון, בחינת הבקרות הקיימות לגבי כל סיכון וקביעת סיכון שיורי.

לבט"ל אין מסמך מיפוי נכסים כולל, כנדרש בתקנות אבטחת מידע ובתורת ההגנה. לשם ביצוע סקר לאיתור סיכוני תקשוב נעשה מיפוי חלקי של המערכות: יחידת תמ"מ בחרה חלק מהמערכות החשובות והקריטיות מתוך כלל המערכות הקיימות בבט"ל, ומהן מופו כשליש מהמערכות שהוגדרו החשובות ביותר, ונקבע שמערכות אלה ייבחנו בסקר. כמו כן, לצורך ביצוע סקר סיכוני סייבר לגבי מערכות תב"ל נערך מיפוי חלקי של נכסי המידע במערכות אלו. תכולת הסקר לגבי מערכות תב"ל לא כללה את סיווג הנכסים בהתאם לרמת הקריטיות שלהם לארגון.

נמצא כי בט"ל אינו מנהל רשימת מצאי של כלל הנכסים והתהליכים העסקיים שלו ואינו מסווג אותם לפי רמת הקריטיות שלהם לארגון, וזאת בניגוד לנדרש בתקנות אבטחת מידע ובניגוד לנורמות מקובלות בתחום הסייבר, ובהן הנורמות הכלולות בתורת ההגנה. 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.

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

סקרי סיכונים

לפי תקנה 5(ג) לתקנות אבטחת מידע, בעליו של מאגר מידע שחלה עליו רמת אבטחה גבוהה אחראי לביצוע סקר לאיתור סיכוני אבטחת מידע. לאחר שיקבל בעל מאגר המידע את ממצאי הסקר עליו לדון בהם ולבחון את הצורך בעדכון מסמך הגדרות המאגר או נוהל אבטחת המידע, ואם התגלו ליקויים בתחום האבטחה - לפעול לתיקונם. יש לבצע סקר סיכונים אחת ל-18 חודשים לפחות.

לפי מסמך המדיניות של בט"ל, ניהול הסיכונים יהיה מושתת על הערכת סיכונים לגבי מידת הפגיעות של המידע והמאגרים והמערכות שהוא שמור בהם ; והערכת האיומים, השפעותיהם ומידת היתכנות התממשותם. עוד נכתב במסמך המדיניות כי מנהל חטיבת אבטחת מידע יערוך סקר סיכוני מידע ויחליט על פיו לגבי הצורך בהצפנת מידע רגיש.

עד מאי 2023 היה קיים בבט"ל אגף לניהול סיכונים שהיה כפוף למנכ"ל. מיולי 2023 האחריות לטיפול בנושא עברה באופן זמני לאגף ביקורת פנים. נציגי אגף ביקורת פנים בבט"ל מסרו כי הוחלט להעביר את נושא ניהול הסיכונים לאחריות סמנכ"ל התקציבים. בכל אגף וחטיבה (כולל תמ"מ) יש ממלא תפקיד של מנהל סיכונים. כל מנהל אגף מגבש את מפת הסיכונים שבתחום אחריותו.

נמצא כי עריכת סקרי סיכונים בתחום אבטחת מידע לגבי מאגרי המידע אינה באחריות חטיבת אבטחת מידע, אף שהיא היחידה המקצועית הרלוונטית לעריכת סקרי סיכוני אלו. נוכח זאת קיימת פגיעה ביכולת של בט"ל לקדם את הטיפול בנושא באופן מיטבי.

בישיבה של ועדת אבטחת מידע שהתקיימה ביוני 2022 נאמר כי לראשונה מתאפשרת התקשרות עם חברה חיצונית לצורך גיבוש תוכנית לניהול סיכונים. בישיבה צוין כי הנושאים הראשונים לביצוע סקרי סיכונים יהיו האתר האישי ודלף מידע וגיבויים, וכי הרשימה המלאה תגובש עם החברה שתיבחר. בישיבת ועדת אבטחת מידע שהתקיימה בנובמבר 2022 נמסר כי חברה א' וחברה ב' נבחרו לביצוע הסקרים, וכי יש התקדמות ברישום המצאי החלקי שנבחר לצורכי הסקרים.

בט"ל מסר לצוות הביקורת תוצאות של סקר סיכונים שבוצע על ידי חברה א'. הסקר מתייחס לסיכונים של מנהל תמ"מ בנושאים שונים, אולם אינו עוסק בנושאי אבטחת מידע. סקר סיכונים נוסף בוצע על ידי חברה ב' לגבי מערכות תב"ל, ונכללו בו עשר מערכות, עשרה שרתים ושני בסיסי נתונים שנבחרו שלא על פי סיווג הנכסים. במועד כתיבת הדוח, פברואר 2024, מבוצע סקר סיכוני תקשוב לגבי מערכות המידע של בט"ל, אך סקר זה מתייחס לניהול סיכוני טכנולוגיות מידע (IT) ואינו כולל בדיקה של סיכוני אבטחת מידע וסייבר.

מס"ל מסרו כי ביצוע סקרי סיכונים נמצא באחריות בט"ל, וכי מס"ל לא נחשף לסקרי הסיכונים שבוצעו בבט"ל.

נמצא כי בט"ל אינו מבצע סקרי סיכוני אבטחת מידע אחת ל-18 חודשים לגבי מאגרי המידע שלו, כנדרש על פי תקנות אבטחת מידע מארגונים שיש להם מאגרי מידע שחלה עליהם רמת אבטחה גבוהה. עוד נמצא כי בחירת המערכות בתב"ל שלגביהן בוצע סקר סיכונים נעשתה לפי חשיבותן העסקית של המערכות ולא על בסיס מיפוי וסיווג של פוטנציאל הנזק שייגרם עקב פגיעה במערכות אלו, כנדרש במתודולוגיות מקובלות, כמו תורת ההגנה של מס"ל.

מומלץ כי בט"ל, בהנחיית מס"ל, יבצע תהליך סדור של סקרי סיכוני אבטחת מידע בהתאם למתודולוגיות מקובלות, כמו תורת ההגנה, ויוודא 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.

בתשובת מס"ל מאפריל 2024 נמסר כי חשוב שבט"ל יבצע סקר סיכוני אבטחת מידע בנוגע לכלל מערכות המידע בארגון ויפעל לסגור את הפערים שימצאו בסקר זה. עוד נכתב בתשובת מס"ל כי במסגרת תוכנית העבודה יעקוב מס"ל אחר ביצוע סקר הסיכונים וסגירת הפערים.

מבדקי חדירה

לפי תקנה 5(ד) לתקנות אבטחת מידע, בעליו של מאגר מידע שחלה עליו רמת אבטחה גבוהה אחראי לביצוע מבדקי חדירה למערכות המאגר, לשם בחינת עמידותן בפני סיכונים פנימיים וחיצוניים. את מבדקי החדירה למערכות המאגר יש לבצע אחת ל-18 חדשים לפחות. על בעל המאגר לדון בממצאיהם של מבדקי החדירה, ואם יתגלו במבדקים ליקויים - לפעול לתיקונם.

במסמך מדיניות אבטחת מידע של בט"ל נכתב כי מנהל אבטחת המידע והסייבר יערוך מבדקי חדירה פנימיים, על פי תוכנית העבודה ועל פי הצורך. עוד נכתב כי תבוצע בקרה על יישום הממצאים ותיקון הליקויים שעלו בביקורות.

משרד מבקר המדינה מציין לחיוב את העובדה שבט"ל מעסיק צוות בודקי חוסן מיומנים במשרה מלאה, אשר מבצע באופן שוטף מבדקי חדירה תשתיתיים ואפליקטיביים למערכות ויישומים. כמפורט בהמשך, לא מתבצעים מבדקים על המערכת המרכזית.

מנהל אבטחת המידע בבט"ל מסר כי לא קיימת תוכנית עבודה לביצוע מבדקי חדירה וכי חטיבת אבטחת מידע אינה מבצעת בקרות על תיקון הליקויים שנמצאו מבדקי החדירה. מנהל אבטחת המידע ציין כי לגבי כל ממצא בדוח ניתנות רשימת המלצות והנחיות לתיקון הליקויים, וכי האחריות לתיקון הליקויים היא של הגורם המיישם.

לצוות הביקורת נמסרו דוחות על 41 מבדקי חדירה שבוצעו בשנים 2021 - 2023. מניתוח הדוחות האמורים עולה התמונה שלהלן:

1. שום מבדק לא בוצע על המערכת המרכזית, בשל מחסור בידע בתחום זה בבט"ל, במס"ל ובארץ בכלל.
2. רק כ-7% מהמבדקים בוצעו על מערכות שמקושרות למערכת המרכזית.
3. במבדקים שבוצעו עלו ליקויים חוזרים וליקויים רוחביים שמצביעים על כך שהליקויים שנמצאו בביקורות קודמות לא תוקנו. להלן דוגמא: במבדק שבוצע לגבי שרתי תב"ל לבחינת ליקויים חוזרים, התגלו ליקויים שלא תוקנו בתשעה (82%) מ-11 הממצאים שנבדקו, שמונה מהם היו בדרגת חומרה גבוהה ומעלה.

בפיקוח הרוחבי שביצעה הרשות להגנת הפרטיות בבט"ל עלה כי בט"ל אינו מבצע מבדקי חדירה לכל המאגרים הרלוונטיים בהתאם לתקנות אבטחת מידע (ראו בפרק "פיקוח הרשות להגנת הפרטיות על בט"ל").

נמצא כי בט"ל אינו מבצע מבדקי חדירה לגבי מאגרי המידע שברשותו, כמתחייב מתקנות אבטחת מידע וכן ממסמך המדיניות שלו. לדוגמה, רק כ-7% מהמבדקים שבוצעו היו על מערכות שמקושרות למערכת המרכזית, אשר בה נמצאים כל מאגרי המידע של בט"ל. עוד נמצא כי בט"ל אינו עוקב אחר תיקון הליקויים שנמצאו במבדקים, וכי נמצאו ליקויים חוזרים וליקויים רוחביים ברמת חומרה גבוהה שלא תוקנו, דבר החושף את בט"ל לסיכון.

עוד נמצא כי בט"ל אינו מבצע מבדקי חדירה למערכת המחשב המרכזית, וכי קיים מחסור במידע וידע בביצוע מבדקים אלו בבט"ל ובמס"ל.

בתשובת בט"ל ממרץ 2024 נמסר כי מבדקי חדירה למערכת המרכזית אינם מבוצעים משום שלא קיים ידע מקצועי בישראל. בט"ל חיפש לאורך שנים גורם מקצועי המסוגל לבצע מבדקי חדירה למערכת המרכזית ללא הצלחה. עוד נמסר כי בט"ל איתר מוצר ייחודי בעולם לביצוע סקר סיכונים (לא מבדק חדירות) למערכת המרכזית. בט"ל מבצע POC לגבי מוצר זה ובהתאם לממצאים יחליט אם להרחיב את הפעילות בתחום.

מומלץ כי בט"ל ייעזר במומחי תוכן 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 מערכתי לאומי לביצוע מבדקים על מערכות אלו.

תוכנית עבודה ותקציב להגנת הסייבר

לפי החלטת הממשלה 2443, תפקידיו של ממונה הגנת הסייבר הם בין היתר בניית תוכנית עבודה להגנת הסייבר על פי המדיניות; ניתוח והערכה שוטפים של תוכנית הגנת הסייבר והמדיניות בהתאם לצרכים, לאיומים ולמענים; ניתוח והערכה שוטפים של ההיערכות הארגונית להתמודדות עם אירועי סייבר; וגיבוש תוכנית תקציבית לטיפול בהגנת הסייבר ולניהולה השוטף. עוד קובעת ההחלטה[9] כי המנכ"לים של משרדי הממשלה ומנהלי יחידות הסמך יסדירו במסגרת סמכותם ואחריותם את מבנה התקציב השנתי של המשרדים והיחידות כך שלפחות 8% מתקציב תחום טכנולוגיית המידע יופנה להגנת הסייבר.

מדיניות אבטחת המידע והסייבר של בט"ל קובעת כי על ראש אגף הביטחון ועל מנהל אבטחת המידע והסייבר להגיש תוכנית עבודה מסודרת, כולל תקציב, לאישור ועדת ההיגוי לאבטחת מידע וסייבר. התוכנית המאושרת על ידי ועדת ההיגוי תועבר להנהלת בט"ל לקבלת אישורה. באחריות ועדת ההיגוי לבצע מעקב שוטף אחר ביצוע תוכנית העבודה המאושרת.

בט"ל מסר לצוות הביקורת דוח תכנון לשנת 2022, ללא לוחות זמנים וללא נתוני ביצוע. כמו כן התקבלה תוכנית עבודה לשנת 2023 הכוללת משימות כלליות, ללא פירוט לוחות זמנים לביצוע המשימות וללא פירוט מצב הביצוע של המשימות. בתקופה זו (2022-2023) לא הייתה קיימת ועדת היגוי סייבר, שאחראית לדון בתוכניות עבודה ולאשרר אותן. בינואר 2024 אישרה ועדת היגוי את תוכנית העבודה לשנת 2024. התוכנית אינה מפורטת ואינה כוללת לוחות זמנים.

כאמור, מס"ל מנחה את בט"ל כגוף תמ"ק. במסגרת הנחיה זו גיבשו שני הגופים יחד תוכנית עבודה למחצית השנייה של שנת 2023. עקב מלחמת חרבות ברזל תוכנית זו עודכנה, והמשימות שבה הועברו לשנת 2024. נציגי מס"ל מסרו כי ביצוע תוכנית העבודה הוא באחריות בט"ל.

בט"ל מסר לצוות הביקורת מסמכים של תקציב מאושר לשנת 2022 והצעת תקציב לשנת 2023. התקציב של אבטחת מידע שמופיע בדוח לשנת 2023 הוא כ-8 מליוני ש"ח שמהווים כ-2% מתקציב תמ"מ. סמנכ"ל תמ"מ מסר כי התקציב של אבטחת מידע נכלל גם בסעיפים נוספים של שכירות תוכנה ואחזקת תוכנה. לא התקבל פירוט של רכיבי אבטחת מידע בסעיפים אלו.

נמצא כי תוכנית העבודה של בט"ל בתחום אבטחת מידע לשנים 2022 - 2024 איננה מפורטת ברמת המשימות, לא נקבעו לנושאים המופיעים בה לוחות זמנים. עוד נמצא כי תוכנית העבודה לשנים 2022 - 2023 לא נידונה ולא אושרה בוועדת היגוי סייבר. מאחר שבט"ל לא ביצע מיפוי נכסים וסקר סיכונים, קיים סיכון שהמשאבים שלו מושקעים שלא בהלימה לסדרי העדיפויות ולסיכונים, או שלא מושקעים די משאבים כדי להתמודד עם סיכוני אבטחת המידע הנשקפים לארגון.

עוד נמצא כי אין לבט"ל יכולת להעריך את שיעור התקציב המיועד לאבטחת המידע מכלל התקציב המיועד לתחום טכנולוגיית המידע נוכח העובדה שעלויות הנוגעות להיבטי אבטחת מידע מופיעות

[9] החלטת הממשלה 2443, נספח ו', סעיף 4א.

גם בסעיפים תקציביים אחרים. כך למשל, בתקציב של שנת 2023 סעיף אבטחת מידע הוא כ-2% מסך התקציב המיועד לטכנולוגיית מידע, ואין לדעת מהו שיעור ההקצאה התקציבית הכולל ואם הוא מגיע להקצאה המקובלת במשרדי הממשלה ויחידות הסמך (8%).

בתשובת בט"ל ממרץ 2024 נמסר כי הנושא התקציבי לא היווה חסם לביצוע רכש או משאבים עבור אבטחת המידע בבט"ל וכי שיעור התקציב לתחום אבטחת המידע, לרבות כוח אדם חיצוני, מכלל התקציב גדול מ-2%.

מומלץ כי בט"ל יפרט את רכיבי אבטחת המידע בסעיפי התקציב השונים באופן שישקף את המשאבים שהושקעו בנושא זה ויוודא כי המשאבים המושקעים כדי להתמודד עם סיכוני אבטחת המידע הנשקפים לו הם בשיעור המקובל בארגונים בסדר גודל של בט"ל.

בקרה, ביקורת ותאימות לדרישות החוק והתקנות בתחום הגנת הסייבר

עמידה בדרישות החוק והתקנות

לפי תקנה 3(3) לתקנות אבטחת מידע, על ממונה אבטחת מידע להכין תוכנית לבקרה שוטפת על העמידה בדרישות התקנות, לבצע אותה ולהודיע לבעל מאגר המידע הרלוונטי ולמנהל המאגר על ממצאיו. תקנות 16(א) ו-16(ב) קובעות לגבי מאגר מידע שחלה עליו רמת אבטחה בינונית או גבוהה, כי בעל המאגר אחראי לכך שתיערך אחת ל-24 חודשים לפחות ביקורת פנימית או חיצונית על ידי גורם בעל הכשרה מתאימה לביקורת בנושא אבטחת מידע שאינו ממונה האבטחה של המאגר, כדי לוודא שהמאגר עומד בהוראות התקנות. בדוח שיגבש הגורם שביצע את הביקורת הוא ידווח בעניין התאמת אמצעי האבטחה לנוהל אבטחת מידע ולתקנות אבטחת מידע, יציין ליקויים ויציע אמצעים לתיקונם.

כאמור, במסמך המדיניות של בט"ל משנת 2014 אין אזכור לחובה לבצע בקרה על עמידה בתקנות אבטחת מידע. בטיוטת מסמך המדיניות העדכני של בט"ל מדצמבר 2023 נכתב כי באחריות מנהל אבטחת המידע והסייבר לוודא כי כל יחידות בט"ל פועלות בהתאם לדרישות החוק, התקנות, האסדרות שנקבעו ודרישות בעלי עניין בהיבטי הגנת המידע, הפרטיות והסייבר. עוד נכתב במסמך המדיניות כי פעילויות אלו יוגדרו בתוכנית העבודה השנתית.

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 מאגר גדול וכולל מידע רגיש בנפח של טרה-בייט (TB) רבים, מחייב קיום תוכנית סדורה כזו, כדי להבטיח רמת אבטחה נאותה. כמו כן, עד מועד סיום הביקורת, אפריל 2024, בט"ל לא ביצע ביקורת כדי לוודא שהוא עומד בדרישות תקנות אבטחות מידע.

משרד מבקר המדינה בדק את מידת העמידה של בט"ל בתקנות אבטחת מידע, כפי שיפורט בפרקים הבאים. להלן תרשים המסכם את תוצאות הבדיקה:

תרשים 3 : **מידת עמידתו של בט"ל בתקנות אבטחת מידע**

הוכן בידי משרד מבקר המדינה.

בט"ל מחזיק במאגרי מידע מהגדולים והרגישים הקיימים במדינה. מהתרשים עולה כי רובן המכריע של תקנות אבטחת מידע (13 מ-15 תקנות - 87%) מקוימות בבט"ל באופן חלקי בלבד. נוסף על כך, בט"ל אינו מקיים כלל את התקנה לגבי ביצוע ביקורת תקופתית על עמידה בתקנות.

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.

בתשובת הרשות להגנת הפרטיות ממרץ 2024 נמסר כי לנוכח ממצאי הביקורת המצביעים על רמת אבטחת מידע נמוכה בבט"ל עקב אי-עמידה בתקנות אבטחת מידע, באופן אשר מעמיד בסיכון גבוה מאגר מידע גדול ורגיש ביותר, הרשות תקצה משאבים לשם קידום עמידת בט"ל בתקנות.

<u>פיקוח הרשות להגנת הפרטיות על בט"ל</u>

לצורך הפקת תמונת מצב מגזרית בנוגע לעמידה בהוראות החוק והתקנות ואיתור כשלים הטעונים אסדרה, קיים בידי הרשות להגנת הפרטיות מנעד רחב של כלים, ובכלל זה נקיטת פעולות מודיעיניות והליכי אכיפה מינהליים שונים, ובהם פיקוחי רוחב ופיקוחי עומק.

מערך פיקוחי רוחב (Audit) מופעל על ידי הרשות משנת 2018. מדובר בהליך אכיפה "רך" אשר נועד בעיקרו להתניע ולהגביר מודעות ותהליכי ציות לחוק ולתקנות בקרב הגופים המפוקחים, להסיק מסקנות בדבר דגשים נדרשים לצמצום פערים קיימים הן ברמת הגופים המפוקחים והן ברמת המגזר, וכן להציג תמונת מצב לציבור בנוגע לדרישות הציות להגנת הפרטיות ואבטחת המידע בקרב המגזר הנבחר.

מחלקת האכיפה ברשות להגנת הפרטיות מבצעת פיקוח רוחב שנתי על כחמישה מגזרים שנבחרים על בסיס סקר סיכונים שנתי שמבצעת הרשות. כל פיקוח רוחב נעשה בכ- 20 עד 50 גופים מדגמיים מכל מגזר שנבחר, ובסיומו נשלח לגוף המפוקח דוח ליקויים. על הגוף המפוקח למסור לרשות את תגובתו על דוח הליקויים, ובכלל זה לוחות זמנים לטיפול בהם והתחייבות של נושא משרה לתיקונם.

במסגרת פיקוח רוחב שקיימה הרשות להגנת הפרטיות במגזר החברות הממשלתיות והרשויות הסטטוטוריות נשלח לבט"ל באוקטובר 2022 שאלון מקוון, לצורך בדיקת עמידתו בהוראות חוק הגנת הפרטיות ותקנות אבטחת מידע (להלן - שאלון פיקוח רוחב). במרץ 2023 שלחה הרשות להגנת הפרטיות לבט"ל דוח שבו פורטו הליקויים והפעילות המתקנת הנדרשת. במאי 2023 שלח בט"ל את תגובתו על הדוח. בדרישה שהעבירה הרשות לבט"ל לגבי תיקון הליקויים ניתנה הנחיה לנקוט גישה מבוססת סיכון, ולתת עדיפות ככל הניתן לטיפול בליקויים בתחום אבטחת המידע ולאחר מכן לתיקון הליקויים בנושאים האלה: עיבוד מידע במיקור חוץ, ניהול מאגרי מידע, בקרה ארגונית וממשל תאגידי והעברת מידע בין גופים ציבוריים.

שקלול התשובות על שאלון פיקוח הרוחב שנשלח לבט"ל העלה כי בט"ל קיבל ציון גבוה. הליקויים העיקריים שצוינו בדוח הפיקוח נוגעים למספר קטן של נושאים, כמו קיום נוהלי אבטחת מידע, אופן ההזדהות בכניסה למאגר וכן ביצוע מבדקי חדירה. בתגובת בט"ל על הממצאים שצוינו בדוח נכתב כי בט"ל מקבל את ההמלצה לתיקון שני הליקויים הראשונים.

הרשות להגנת הפרטיות מסרה כי הציון שניתן למוסד לביטוח לאומי, כמו כל גוף מפוקח בפיקוח רוחב, עוסק במהותו בהוראות ציות ואחריותיות תאגידית. קרי, עמידת הגוף המפוקח בקריטריונים המשקפים מודעות לתקנות אבטחת מידע וציות להן. בעוד שהשאלון שנשלח במסגרת פיקוח הרוחב מותאם לרמת האבטחה הנדרשת במאגרי המידע של הגופים המפוקחים, ההליך אינו מעניק משקל לגודל הגוף המפוקח, גודל המאגרים או מספרם. יחד עם זאת, לנוכח העובדה כי הליך פיקוח הרוחב מעצם טיבו וטבעו מתמקד בעצם קיום נהלים ובקרות, וכן נסמך על תשובות הגופים המפוקחים ומספר מצומצם של מסמכים מאמתים - תהליך פיקוח הרוחב אינו מהווה בהכרח סוף פסוק ובידי הרשות יש כלי נוסף, משלים או עומד בפני עצמו, של אכיפה מינהלית - "פיקוח עומק" - שבוחן לעומק את רמת האבטחה של הגוף בהתאם לתקנות אבטחת מידע. הליכי פיקוח העומק יכולים, ככלל, להתבצע במספר ארגונים המשתייכים לאותו מגזר או בארגון אחד שהוא בעלים או מחזיק של מספר מאגרי מידע משמעותיים.

נמצא כי הרשות להגנת הפרטיות ביצעה בבט"ל בין השנים 2022-2023 פיקוח רוחב, באמצעות בדיקת ציות לתקנות אבטחת מידע ואחריותיות תאגידית, והעניקה לבט"ל ציון גבוה שאינו בהלימה לציון בבדיקת הציות לתקנות אבטחת מידע שבוצעה על ידי משרד מבקר המדינה. פער זה נובע, בין היתר, מכך שפיקוח הרוחב של הרשות להגנת הפרטיות אינו כולל בדיקות עומק וכן בדיקות במערכות עצמן כדי לוודא את שלמות המענים שהתקבלו. עוד נמצא כי פיקוח הרוחב לא שיקף פערים בנושאים שנדרש לפי התקנות לעמוד בהם, כמו מיפוי מערכות המאגר, ניהול הרשאות גישה, בקרה על הגישה ותיעוד שלה, מיקור חוץ וביקורות תקופתיות.

מומלץ כי הרשות להגנת הפרטיות תבחן מחדש את שיטת ההערכה של הפיקוח הרוחבי, כדי לדייק את הציון הניתן לגוף המפוקח באופן שישקף, את מידת הציות של בט"ל לתקנות אבטחת מידע. עוד מומלץ כי נוסח השאלון שמועבר במסגרת פיקוח הרוחב יותאם למורכבות הגוף ולכמות המאגרים שבבעלותו כך שיתקבל ממנו מענה המשקף את המצב בכלל המאגרים. כמו כן, מומלץ

כי הרשות להגנת הפרטיות תבחן דרכים נוספות לבחינת האסמכתאות המגבות את הדיווח של הגופים.

בתשובת הרשות להגנת הפרטיות ממרץ 2024 נמסר כי מערך פיקוחי הרוחב מצוי בהליך בחינה מתמשך, מאז הוקם בשנת 2018. הרשות הוסיפה כי בכל שנה הוחלו שינויים הן בשאלות הכלולות בשאלון המופנה לגופים המפוקחים, הן במערכת הממוחשבת למענה על השאלון והן בהנחיות שניתנו למשרדי רואי החשבון בנוגע לבחינת המענים שניתנים על ידי הגופים המפוקחים בהתאם לכך, וכן בהמשך לשיח שהתקיים בין הרשות למשרד מבקר המדינה על רקע הנכתב בדוח הביקורת, הרשות פועלת גם כעת לטיוב שאלון פיקוחי הרוחב, כדי שישקף באופן המיטבי ביותר (בהתאם למהות ההליך) את עמידתו של הגוף המפוקח בקריטריונים המשקפים מודעות לתקנות אבטחת מידע.

מסמך הגדרות המאגר

תקנה 2 לתקנות אבטחת מידע מחייבת בעל מאגר להכין "מסמך הגדרות מאגר" ולציין בו פרטים לגבי מידע חיוני ואופן השימוש בו, ובכלל זה תיאור כללי של פעולות איסוף המידע ושל השימוש בו; תיאור מטרות השימוש במידע; סוגי המידע הכלול במאגר; סיכוני אבטחת מידע שהמאגר חשוף אליהם ודרכי ההתמודדות עימם; פרטי מנהל המאגר וממונה אבטחת המידע בו (אם מונה בעל תפקיד כזה).

בט"ל מסר לצוות הביקורת מסמך ובו רשימה של מאגרי המידע שרשומים בבט"ל, הכוללת את שם המאגר, סוגי המידע שבו (דמוגרפי, רפואי, מצב כלכלי) וייעודו. סמנכ"ל תמ"מ מסר כי לא ידוע לו על קיום מסמך הגדרות מאגר, וכי נדרש ליצור מסמך כזה.

נמצא כי בט"ל אינו מחזיק במסמך הגדרות מאגר לגבי אף אחד מהמאגרים שלו, אף שמדובר במאגרים גדולים ומשמעותיים, ואף שהדבר נדרש בתקנה 2 לתקנות אבטחת מידע.

על בט"ל להכין מסמך הגדרות מאגר, בדגש על המאגרים הגדולים והמשמעותיים שבידיו, ולכלול בו מידע כמו תיאור כללי לגבי פעולות איסוף המידע והשימוש בו, סוגי המידע הכלולים במאגר וסיכוני אבטחת המידע שהמאגר חשוף אליהם ודרכי ההתמודדות של הארגון עימם. מסמכים אלו נדרשים גם לצורך ביצוע תהליך של ניהול סיכונים ארגוני.

העברת מידע מבט"ל לגופים חיצוניים

בט"ל מחזיק במידע על כלל אזרחי ישראל מיום הולדתם ועד פטירתם. מידע זה יכול לשמש גופים ציבוריים לצורך מילוי תפקידם. לדוגמה, הוא יכול לשמש את הלשכה המרכזית לסטטיסטיקה (להלן - הלמ"ס) לביצוע מחקרים, את רשות המיסים לקבלת מידע על נישומים ואת משרד התחבורה לבדיקת זכאות לנכות.

פרק ד' בחוק הגנת הפרטיות[10] מגדיר בין היתר את התנאים והדרישות שלהלן לגבי העברת מידע בין גופים ציבוריים:

1. מסירת המידע דרושה למטרת ביצוע כל חיקוק או למטרה במסגרת הסמכויות או התפקידים של מוסר המידע או מקבלו.
2. גוף ציבורי המוסר דרך קבע מידע יפרט עובדה זו על כל דרישת מידע בהתאם לחוק.
3. גוף ציבורי המקבל דרך קבע מידע, והמידע נאגר במאגר מידע, יודיע על כך לרשם, ועובדה זו תיכלל בפרטי רשימת מאגרי המידע.
4. גוף ציבורי שקיבל מידע לא ישתמש בו אלא במסגרת הסמכויות או התפקידים שלו.

[10] חוק הגנת הפרטיות - פסקאות 23 ג' ו 23 ד'.

5. לעניין חובת השמירה על סודיות לפי כל דין, מידע שנמסר לגוף ציבורי מכוח חוק זה כמוהו כמידע שהגוף המקבל השיג מכל מקור אחר, ונוסף על כך יחולו על הגוף המקבל כל ההוראות החלות על הגוף המוסר.

ערוצי העברת מידע

בט"ל מעביר מידע לגופים חיצוניים באמצעות מערכות שיתוף מידע.

לפי תקנה 13(ג) בתקנות אבטחת מידע, בעל מאגר נדרש לעדכן באופן שוטף את מערכות המאגר, מערכות החומרה ומערכות התוכנה, בהתאם להנחיות היצרן, כדי לנטרל פגיעויות וחולשות המתגלות מפעם לפעם. לא ייעשה שימוש במערכות (חומרה או תוכנה) שהיצרן שלהן הפסיק את התמיכה בהיבטי האבטחה שלהן. בתקנה 5 לתקנות אבטחת מידע, שעניינה מיפוי מערכות המאגר, נקבע בסעיף 5(א)(3) כי מערכות המאגר כוללות "תוכנות וממשקים המשמשים לתקשורת אל מערכות המאגר ומהן". מכאן שהממשק של העברת המידע מהמאגר של בט"ל באמצעות מערכת שיתוף מידע הוא חלק ממערכות המאגר, ולכן תקנה 13(ג) לתקנות חלה על מערכות שיתוף המידע המשמשות להעברת מידע מהמאגר.

מדיניות סיסמאות מגדירה את האורך ואת המורכבות של הסיסמה באופן שיקשה על תוקף לנחש אותה וכן את תוקפה.

נמצא כי בט"ל מעביר לגופים חיצוניים רבים מידע, באמצעות מערכות לשיתוף מידע שהתגלו בהן פערי אבטחת מידע.

בתשובת בט"ל ממרץ 2024 נמסר כי בט"ל נמצא בשלב מתקדם מאוד של תהליך החלפת הטכנולוגיה לעומת שאר גופי הממשלה. מדובר בפרויקט שיימשך כמה שנים לאור העובדה שנדרשים שינויים והיערכות לשינוי הטכנולוגיה גם בצד המקבל את המידע ולא רק בבט"ל. יצוין כי בט"ל העבירה למשרד מבקר המדינה תכנית להחלפת הטכנולוגיה.

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

בט"ל מסר כי קיים ערוץ נוסף להעברת מידע בין בט"ל לגופים חיצוניים.

נמצא כי בט"ל מאפשר לגופים חיצוניים, גישה למאגרי המידע של בט"ל באופן שבו קיים סיכון לחשיפת מידע עודף לגופים חיצוניים.

מומלץ כי בט"ל יאפשר גישה ייעודית מאובטחת עבור גופים חיצוניים, בהתאם לצרכים של אותם גופים.

בקרה על המידע המועבר לגופים ציבוריים

בבט"ל קיימת ועדה להעברת מידע בראשות סמנכ"לית מחקר ותכנון, הכוללת נציג אבטחת מידע, יועץ משפטי ועובדים אחרים. הוועדה דנה בבקשות לקבלת מידע ויכולה לדחות או לאשר את העברת המידע בכפוף להתניות. אחרי הדיון בוועדה הטופס מוגש לחתימות של סמנכ"ל תמ"מ, ממונה אבטחת המידע והיועץ המשפטי שבודק ומאמת את החתימות. כל בקשה קצובה לתקופה מרבית של חמש שנים, ובסיומן הגוף הציבורי שמבקש את המידע נדרש להגיש בקשה חדשה.

לפי נוהל העברת מידע של בט"ל, המידע המופק יועבר לבדיקת הנציג הרלוונטי באגף הבקרה, וזה יבדוק את התאמת המידע המופק למידע שאושר למסירה על ידי הוועדה להעברת מידע. עם קבלת

מידע מהוועדה להעברת מידע על תפוגת האישור להעברת מידע לגורם חוץ - יודיע עוזר סמנכ"ל תמ"מ למנהלת אגף בקרה ובדיקות מידע שיש להפסיק את העברת המידע השוטפת.

מנהל אבטחת מידע ומנהל אגף הבקרה בבט"ל מסרו כי אין מעקב אחרי תפוגת תוקף הממשק להעברת מידע בתום חמש שנים להפעלתו. כמו כן, אין מעקב אחרי המעבר של הנתונים בפועל, לעומת האישור של הוועדה או ההתניה שנכתבה בטופס אישור הממשק וכי הנושא נכלל בתוכנית העבודה לשנת 2024. לדוגמה, העברת מידע עודף התגלתה תוך כדי דיון בוועדת היגוי על הרחבת מערכת ה' שמרכזת את הבקשות של חברות לקבלת מידע על לקוחות. נוסף על כך, נמסר כי אין לבט"ל מסמכים שבהם מתועדים באופן מלא הממשקים הקיימים, וכי המערכת הנוכחית אינה מנפיקה דוחות, ולפיכך יש קושי להפיק מידע על ממשקים קיימים בקלות.

לפי נוהל העבודה של הוועדה להעברת מידע בבט"ל, יש לפרסם באתר המרשתת של בט"ל רשימה של הגופים הציבוריים המקבלים מידע מבט"ל ואת סוגי המידע המועבר דרך קבע. באתר המרשתת של בט"ל לא נמצא מידע בגין העברות מידע כאמור.

נמצא כי בט"ל אינו מנהל רשימה של הממשקים הקיימים אצלו להעברת מידע לגופים חיצוניים ואינו מפרסם ממשקים אלו לציבור, בניגוד לנוהל שלו. כמו כן, בט"ל אינו מבצע בקרה על התאמת המידע שמועבר לגופים ציבוריים למידע שאישרה הוועדה להעברת מידע למסור. עוד נמצא כי בט"ל אינו מקיים בקרות עיתיות על תפוגת תוקף הממשק להעברת המידע ואינו מפסיק את העברת המידע לאחר חמש שנים.

בתשובת בט"ל ממרץ 2024 נמסר כי כחלק מתוכנית העבודה לשנת 2024 החל תהליך מיפוי ובקרה לגבי תהליכי העברת המידע, לרבות מיפוי המצב הקיים.

מערך הדיגיטל הלאומי (לשעבר רשות התקשוב הממשלתי) פרסם במאי 2019 הנחיה בנושא העברת המידע הממשלתי. בהתאם לנדרש בסעיף 5(ב) להחלטת הממשלה 1933[11] ובתקנות אבטחת מידע, פיתח מערך הדיגיטל הלאומי את מערכת מוע"ד לניהול עבודת הוועדות להעברת מידע. המערכת החלה לפעול בנובמבר 2017. כל משרדי הממשלה ויחידות הסמך מחויבים לפי ההנחיה לנהל את תהליכי הבקשות להעברת מידע במערכת מוע"ד, ואין להגיש בקשה להעברת מידע אלא באמצעות המערכת.

הוועדה למסירת מידע בבט"ל מסרה כי רוב הבקשות להעברת מידע מגיעות בדואר האלקטרוני ולא באמצעות מערכת מוע"ד, היות שבמערכת אין אפשרות לצרף מסמכים לבקשות. כמו כן, במערכת אין אפשרות בסיום הטיפול בבקשות לצרף את טופס האישור של הוועדה לבקשה.

נמצא כי מערך הדיגיטל פיתח מערכת ממוחשבת ייעודית לתיעוד העברת מידע בין משרדי הממשלה ויחידות הסמך (מערכת מוע"ד), ומשרדי הממשלה מחויבים לפי הנחיה של מערך הדיגיטל להשתמש בה. ואולם מרבית משרדי הממשלה שעובדים מול בט"ל אינם מעבירים את הבקשות באמצעות המערכת, בין היתר בשל היעדר היכולת לצרף מסמכים.

מומלץ כי מערך הדיגיטל יפעל לשדרוג מערכת מוע"ד, בהתאם לדרישות שעלו מן המשתמשים. עוד מומלץ שמערך הדיגיטל יבחן את הסיבות לכך שמשרדי הממשלה לא עובדים עם המערכת ויפעל כדי לתת להם מענה.

בתשובת מערך הדיגיטל ממרץ 2024 נמסר כי מפותחת מערכת חדשה - מערכת ח' - עבור תהליך העברת מידע בין משרדים. מערך הדיגיטל ציין כי המערכת תושק בחודש מאי, בתחילה עם מספר מצומצם של משתמשים, ותורחב בהדרגה עד לכלל הפוטנציאל האפשרי, וכי יתאפשר בה צירוף מסמכים לבקשות. כמו כן, יש דרישה שבמערכת החדשה תוטמע האפשרות לצרף את תשובת הועדה ואת פרוטוקול הועדה.

---

[11] החלטת הממשלה 1933, "שיפור העברת המידע הממשלתי והנגשת מאגרי המידע לציבור" (30.8.16).

הגנה פיזית

תקנה 6 לתקנות אבטחת המידע מגדירה את החובות של בעל מאגר ברמת אבטחה גבוהה בהיבטי אבטחה פיזית וסביבתית[12]. מערכות המאגר יישמרו במקום מוגן שלא מתאפשרת כניסה אליו בלי הרשאה, והתואם את אופי פעילות המאגר ורגישות המידע שבו. כמו כן, בעל המאגר ינקוט אמצעים לבקרה על הכניסה לאתרים שבהם מצויות המערכות המפורטות בתקנה 5(א)(1)[13] ועל היציאה מהם ולתיעוד הכניסה והיציאה כאמור, וכן אמצעים לבקרה על הכנסה והוצאה של ציוד אל מערכות המאגר ומהן ולתיעוד הכנסה והוצאה כאמור.

תורת ההגנה[14] קובעת כי ההגנה הפיזית והסביבתית היא נדבך חשוב בהגנת הסייבר של הארגון, והיא נועדה למנוע מתוקף לחדור לסביבת הסייבר באמצעים פיזיים.

ההגנה הפיזית והסביבתית כוללת את אתרי חדרי המחשבים, אתרי ריכוזי התקשורת, המשרדים והסניפים של בט"ל. חדר המחשבים הפעיל של בט"ל נמצא באתר אירוח של ספק א'. לבט"ל יש24 סניפים ראשיים, ולהם יש כ-54 סניפי משנה ואשנבים בכל רחבי הארץ. אתר ההתאוששות בשעת חירום וחדר המחשבים בשעת חירום של בט"ל (להלן - אתר DR) נמצא נכון להיום באחד הסניפים וצפוי לעבור למקום אחר.

בבט"ל קיים נוהל אבטחת מידע במחשב. בנוהל נכתב כי חדרי המחשב המרכזיים יוקמו ויתוחזקו כחדרים מאובטחים באמצעות מערכות הגנה מתאימות, בקרת כניסה מחמירה, קבלת עובדים בהתאם לנוהל סינון ביטחוני, מערכות התרעה מאש, עשן ופריצה, מערכות לשמירת חומר וכו'.

<u>חדר המחשבים - אתר הגיבוי (DR)</u>

חדרי מחשב ובפרט חדר מחשב המשמש את הארגון לצרכי גיבוי במקרה של אסון (להלן - DR) צריכים לפי מתודולוגיות מקובלות ובהן הנחיות יה"ב לאפשר גישה רק לאנשים מורשים היות ופגיעה בשרתים ובמידע השמור בהם יגרמו לפגיעה בהמשכיות התפקודית של הארגון.

חדר המחשבים (אתר ה-DR) שהיה פעיל בתקופת הביקורת נמצא באותו מתחם שבו נמצא בית כנסת, ובכניסה למתחם כולו יש דלת נעולה בקודן. לדברי השומרים, בזמני התפילה נמצא באזור מאבטח חמוש המונע מעבר לאזור אתר ה-DR. חדר המחשבים נמצא בקצה חלל ללא דלת, ובמעבר המוביל לחדר נמצאו מחשבים מונחים על הרצפה. בכניסה לחדר המחשבים יש דלת הנשלטת על ידי כרטיס קִרבה, ולא מותקנת בה "מערכת דלת מוטרדת"[15]. רשימת המורשים כוללת גם את המאבטח, שהוא ברמת סיווג חמש. בחדר המחשבים יש כמה מאווררי עמוד, שנמצאים בחדר עקב בעיות מיזוג אוויר בו. בחדר נמצאו כמה מחשבים על שולחנות המשמשים עמדות עבודה ועמדות שליטה.

נמצא כי בקרת הגישה לאתר הגיבוי (DR) של בט"ל שהיה פעיל בתקופת הביקורת איננה לפי הסטנדרטים המקובלים, למשל הסטנדרטים שנקבעו בהנחיות יה"ב: אתר הגיבוי נמצא באותו מתחם שבו קיים בית כנסת, ולכן הגישה למתחם נגישה גם לאנשים שאינם מורשים. נוסף על כך, דלת הכניסה לאתר הגיבוי אינה בעלת מנגנונים של דלת מוטרדת, ולכן אם הדלת נשארת פתוחה אין התראה על כך. כמו כן, בט"ל הגדיר שהגישה לחדר עצמו מתאפשרת גם לאחד העובדים החיצוניים מצוות האבטחה, שהוא ברמת סיווג נמוכה. עוד נמצא כי אף שרק חלק ממערכות המחשוב פעילות, מערכת המיזוג בחדר המחשבים אינה עומדת בעומס החום, ולכן התבצע בנוסף

---

12 המונח "אבטחת סביבתית" נוגע לשמירת המערכות מפני נזקים, כגון אש ומים.

13 תשתיות ומערכות חומרה, סוגי רכיבי תקשורת ואבטחת מידע.

14 מערך הסייבר, תורת ההגנה 2.0, פרק 6.2 זיהוי 18.

15 "מערכת דלת מוטרדת" - אמצעי ניטור בדלת שנותרה פתוחה זמן קצוב. במקרה כזה תתקבל התרעה במוקד או התרעה קולית.

לה שימוש במאוחרים. נוכח כל אלה, אתר ה-DR חשוף לסיכונים אשר עלולים לגרום לפגיעה בכשירותו וביכולות בט"ל להתאושש מאסון או מאירוע חמור.

במועד סיום הביקורת עבר בט"ל לאתר גיבוי חדש. משרד מבקר המדינה ביקר באתר הגיבוי החדש של בט"ל ומצא כי כלל הפערים שנמצאו באתר הגיבוי הישן לא רלוונטיים לאתר החדש וכי הוא עומד בתקנים מקובלים. משרד מבקר המדינה מציין לחיוב את בט"ל על העתקת אתר הגיבוי (DR) למקום החדש עוד במהלך הביקורת במרץ 2024.

חדר תקשורת סניפי

בביקורת פיזית שערך צוות הביקורת בסניף א' עלה כי ציוד התקשורת בסניף מרוכז בחדר תקשורת שבו דלת עץ עם מנעול ומפתח רגילים. אין מערכת לבקרת כניסה, אין תיעוד של הנכנסים, ואין מערכת מצלמות בכניסה לחדר או בחדר עצמו. פגיעה בחדר זה עלולה להשבית את כלל הפעילות בסניף. בחדר נמצאים כמה מחשבים שמשמשים כשרתי מערכת לניהול תורים, והמפתחות לחדר נמצאים אצל שני תומכי התקשורת וצוות האבטחה. הימצאות מחשבים פעילים בחדר תקשורת משנה את ההתייחסות לחדר התקשורת כמו לחדר שרתים.

נמצא כי חדר התקשורת באחד הסניפים הראשיים של בט"ל שנבדק פיזית על ידי צוות משרד מבקר המדינה, משמש בחלקו גם חדר מחשב, ועקב כך ההגנה הפיזית שלו אינה עונה על הדרישות המצוינות בנוהל אבטחת מידע של בט"ל. כמו כן, נמצא שחדר התקשורת אינו מוגן מפני שריפה בקומה עצמה. נוכח זאת, החדר, על כל ציוד התקשורת והמחשוב שבו, נמצא בסיכון גבוה לפגיעה. כאמור, פגיעה בחדר עלולה להשבית את כלל הפעילות והעבודה בסניף.

מומלץ כי מס"ל יוציא הנחיות מפורטות בנושא ההגנה הפיזית על חדרי המחשב, ובפרט על חדר מחשב המשמש אתר DR, וכן על חדרי התקשורת ויפעל להטמעתן בכל האתרים בגופים המונחים שבהם יש חדר מחשב.

בתשובת מס"ל מאפריל 2024 נמסר כי נושא מעגלי האבטחה מוסדר בתו"ל ייעודי לגופי תמ"ק ולפיו מונחים הגופים. מס"ל הוסיף כי על בסיס תו"ל זה נדרש מנהל הביטחון בגוף המונחה להוציא הנחיות פרטניות לגוף. עוד בתשובת מס"ל נמסר כי הפער שנמצא באחד הסניפים הראשיים של בט"ל מלמד על כך שאין חשש שאירוע מהסוג המדובר יגרום לפגיעה במערכות הליבה של הגוף, וכי גם במקרה שבו יושבת הסניף - התבחינים שבגינם הוגדר הגוף מלכתחילה כגוף תמ"ק אינם מתממשים.

בכדי לשמור על אחידות ועל רמת הגנה פיזית ראויה על חדרי המחשב והתקשורת של גופי תמ"ק, על מס"ל להגדיר ולפרט בתו"ל הייעודי את דרישות הסף לאבטחה פיזית של חדרי מחשב וחדרי תקשורת בגופי תמ"ק ולפקח על יישום ההנחיה.

אבטחה פיזית של קלטות הגיבוי

קלטות גיבוי נועדו להיות עוד קו הגנה ולשמש את הארגון אם המידע במערכות שלו שובש. בט"ל מעתיק את כלל המידע באופן עיתי לקלטות.

נמצאו פערים באבטחה הפיזית של קלטות הגיבוי. בתהליך הקיים יש סיכון לזליגת חומרים ולאיבוד היכולת לשחזור המידע הארגוני.

מומלץ כי בט"ל יפעל לסגירת הפערים באבטחה הפיזית של קלטות הגיבוי ולתיעוד של התהליך הנדרש לכך, וכי מס"ל יוציא הנחיות מפורטות בנושא.

הגנה לוגית

בהנחיית המסגרת להגנת הסייבר בממשלה[16] נקבע כי ההגנה הלוגית היא השכבה העיקרית והבסיסית ביותר בהגנה על המידע השמור במערכות המחשוב והתקשורת, וכי בהיעדר יישום נכון של שכבה זו נחשף המידע לפעילויות שונות אשר חלקן עלול להסב נזק רב.

עוד נקבע בהנחיית המסגרת כי ממונה הגנת הסייבר יתווה רמת הגנה לוגית מחייבת עבור רכיביהן השונים של מערכות המחשוב והתקשורת. רובדי ההגנה על המידע יקיפו את הנדבכים המרכזיים האלו: הזדהות, הרשאות ובקרת גישה לוגית, הגנה על התקני קצה וניטור שלהם, הגנה על מערכי תקשורת וניטור שלהם, הגנה על תשתיות מחשוב וניטור שלהם, הגנה על תשתיות אחסון וניטור שלהם, הגנה על תשתיות ניטור ובקרה מובנות.

נמצאו פערים בהגנה הלוגית בבט"ל במספר נושאים.

הגורם האנושי

הגורם האנושי נחשב לחוליה החלשה בתהליכי אבטחת המידע של הארגון, ותוקפים רבים מנצלים חוליה חלשה זו, למשל תוקפים בשיטות דִיוּג (Phishing). לכן הדרכה והגברת המודעות של העובדים והמנהלים בארגון חיונית לשמירת רמת אבטחת מידע נאותה בארגון.

<u>הדרכה והגברת המודעות של העובדים</u>

לפי תקנה 7(ג) לתקנות אבטחת מידע, בעל מאגר מידע שחלה עליו רמת האבטחה הגבוהה יקיים פעילות הדרכה תקופתית לבעלי הרשאות למאגר בדבר מסמך הגדרות המאגר, נוהל האבטחה והוראות אבטחת המידע לפי החוק ולפי תקנות אלה, בהיקף הנדרש לביצוע תפקידיהם. כמו כן תעסוק ההדרכה בחובות בעלי ההרשאות לפי נוהל האבטחה, החוק והתקנות. הדרכה כאמור תיערך אחת לשנתיים לפחות, ולגבי הסמכה של בעל הרשאה לתפקיד חדש - סמוך ככל האפשר למועד תחילת הסמכתו.

לפי מסמך המדיניות של בט"ל, עובדים חדשים או נותני שירותים יהיו חייבים לקבל הדרכת אבטחת מידע על המדיניות המנחה ועל הנהלים הנובעים ממנה. כמו כן, עליהם לחתום על מסמך התחייבות לקיום הדרישות המפורטות במדיניות ובנהלים. עוד נכתב במסמך המדיניות כי בט"ל ידאג להדרכת העובדים, הספקים וכל מי שבא במגע אתו בנושא מדיניות אבטחת המידע כפי שנקבעה בנהלים, וכי מערך הדרכה בנושאי אבטחת המידע, המדיניות והנהלים יפותח על ידי גוף מונחה מטעם ועדת ההיגוי לאבטחת מידע ובשיתוף חטיבת אבטחת מידע.

בפרוטוקול ישיבת ועדת אבטחת מידע שהתקיימה ביוני 2022 נכתב כי קיימת מערכת למידה ארגונית, וכן נשלח דואר אלקטרוני שבועי ממוקד הסייבר, דבר שמקיים את החובה החוקית של ההדרכה. עוד נכתב כי הוועדה החליטה על מינוי מוביל לעדכון הלומדה מול ההדרכה, וכן החליטה לבנות תהליך של חובה שנתית לכל עובד לבצע את הלומדה.

מנהל אבטחת מידע מסר לצוות הביקורת בדצמבר 2023 כי לא מועברת הדרכה לעובדים חדשים על מדיניות אבטחת המידע והסייבר. יתר על כן, המדיניות לא עודכנה זה עשר שנים, ולכן לא בוצעו לגביה הדרכות ריענון לעובדים ותיקים.

---

16 יה"ב, הנחייה 5.2 סעיף 11.1 וסעיף 11.2.

בט"ל מסר כי תרגילים להגברת המודעות לנושא הדיוג (פישינג) התקיימו לפני כמה שנים, וכי אין בידי מנהל אבטחת מידע מסמכים בדבר תוצאות התרגילים. באירוע תקיפה אמיתי שהתרחש בינואר 2024 ובו הועבר קישור לאתר זדוני, עלה כי ארבעה עובדים לחצו על הקישור.

נמצא כי בט"ל אינו מקיים הדרכות סדורות לעובדים חדשים בנושא אבטחת מידע, וכן אינו מקיים הדרכות עיתיות ותרגולים לאנשי ההנהלה ולעובדים לשם הגברת מודעותם לנושא זה, זאת בניגוד לתקנות אבטחת מידע ולמדיניות שלו עצמו.

מומלץ כי בט"ל יקיים הדרכות סדורות לעובדים חדשים בנושא אבטחת מידע, וכן יקיים הדרכות עיתיות ותרגולים לאנשי ההנהלה ולעובדים, לשם הגברת מודעותם לנושא זה.

בתשובת בט"ל ממרץ 2024 נמסר כי תוכנית העבודה לשנת 2024 כוללת קיום הדרכות וימי עיון בנושא אבטחת מידע. כאמור, במרץ 2024 התקיים יום עיון לכ-60 מנהלי מערכות מידע בנושא אבטחת מידע, בהתמקדות בנושאים של secure by design ו- zero trust.

ניהול הסיכונים מצד שרשרת האספקה

שרשרת אספקה היא מונח המתייחס לכלל המשאבים והתהליכים הקשורים בספקים, בלקוחות ובקבלני ביצוע אשר דרושים לאספקת מוצר או שירות בארגון. מתקפות סייבר המתבצעות באמצעות שרשרת האספקה מכוונות לפגוע באחד מספקי הארגון ולחדור באמצעותו אל הארגון, תוך ניצול האמון שהארגון נותן בספק שלו.

בדוח שפרסם מערך הסייבר בדצמבר 2023, בעת מלחמת חרבות ברזל[17], נכתב כי מראשית המלחמה מזוהה פעילות, המתעצמת בהדרגה, של תוקפים מסוגים שונים נגד ארגונים במרחב הסייבר הישראלי. התוקפים פועלים במנעד רחב של שיטות וטכניקות - ממתקפות פשוטות ולא מתוחכמות, כגון השחתת אתרים או מתקפות מניעת שירות, ועד לתקיפות ממוקדות נגד גופים המעורבים בשרשרת האספקה של ארגונים רבים במשק, במטרה לגרום נזק רחב.

תקנה 15 לתקנות אבטחת מידע מגדירה את דרכי ההתמודדות עם סיכוני אבטחת מידע הכרוכים בהתקשרות עם גורם חיצוני.

מס"ל פיתח מתודולוגיה ייעודית לניהול סיכוני סייבר מצד שרשרת האספקה[18] (להלן - מתודולוגיית שרשרת האספקה), שמחייבת את משרדי הממשלה ואת גופי התמ"ק. לפי המתודולוגיה, על הארגון למפות את הספקים שלו בתחום התקשוב ולסווג אותם לפי פוטנציאל הנזק הנשקף מהם. כמו כן, על הארגון להגדיר את היבטי הגנת המידע והסייבר בחוזים עם הספקים, כמו הסמכות של הארגון לבצע ביקורות סייבר בחצרות הספק, וחובת הספק לעדכן מיד את הארגון על התרחשותו של אירוע סייבר אשר עשוי להשפיע על הארגון או על לקוחותיו. נוסף על כך, לפני יציאה למכרז או לפני התקשרות חדשה או חידוש התקשרות קיימת של ארגון יש להביא זאת לידיעת ממונה הגנת מידע וסייבר של הארגון. במסמך הנחיות שהוציא מס"ל לגופי תמ"ק ביוני 2023 בנושא שרשרת האספקה נכתב כי תיקוף, מיפוי ודירוג של כלל הספקים יתבצע בליווי וסיוע של מנחה הגוף.

הנחיית יה"ב 5.19 בנושא שרשרת האספקה מחייבת את המשרדי הממשלה לצרף לכל מכרז ממשלתי נספח אבטחת מידע, ומצורף לה נספח לדוגמה. נספח אבטחת מידע הוא מסמך המפרט את אחריות הספק בנושאים שונים הנוגעים לאבטחת מידע במסגרת ההתקשרות. בט"ל מסר לצוות הביקורת דוגמאות שונות לנספחי אבטחת מידע שאינם כוללים חלק מהנושאים הנדרשים בהנחיית יה"ב, כמו ביצוע ביקורות על ספקים, ואינם כוללים את החובה לעמידה במתודולוגיית שרשרת האספקה.

17 מערך הסייבר, "מלחמת חרבות ברזל במימד הסייבר: תובנות ודרכי התמודדות" (דצמבר 2023).
18 https://www.gov.il/he/departments/guides/supply_chain_guide

לבט"ל אין נוהל בנושא שרשרת אספקה. תוכנית העבודה שגיבש מס"ל עם בט"ל הגדירה לוחות זמנים ליישום מתודולוגית שרשרת האספקה ובכלל זה מיפוי וסיווג ספקים עד דצמבר 2023 ובקרה על הספקים המהותיים עד אמצע מרץ 2024. בט"ל העביר לצוות הביקורת מסמך טיוטה הכולל רשימה של שישה ספקים מובילים. רשימה זו לא כוללת את כל ספקי התקשוב של הארגון. כמו כן הרשימה כוללת שלושה ספקים שנחשפים למידע רגיש וכן שני ספקים אשר יש להם התחברות לרשת מרחוק. יצוין כי במכרזים החדשים עם שני הספקים שמחזיקים מידע רגיש, בט"ל התייחס בפרק אבטחת מידע לנושאים כמו ביקורות אצל ספקים וחובת הדיווח שלהם על אירועים ואולם אין נספח אבטחת מידע אחיד לכלל המכרזים המתייחס לכלל הנושאים הנדרשים.

במספר מצומצם של התקשרויות עם ספקים חיצוניים התגלו פערי אבטחת מידע.

נמצא כי לבט"ל אין נוהל בנושא שרשרת אספקה, ואין לו מיפוי של כלל ספקי התקשוב שלו והסיווג שלהם לפי רמת הסיכון הנשקף מהם. כמו כן, נמצא כי במכרזים של בט"ל אין נספח אבטחת מידע שמחייב עמידה של הספק בבקרות התואמות את הנדרש במתודולוגיית שרשרת האספקה. זאת ועוד, נמצא כי בט"ל אינו מבצע ביקורות על כל 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.

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 בבקרות, בהתאם למתודולוגיית שרשרת האספקה של מערך הסייבר.

המשכיות עסקית

בנייה ויישום של תוכנית להמשכיות עסקית מבטיחים שהפעילויות הקריטיות בארגון ימשיכו להתבצע גם בהתרחש אירוע המסכן את הארגון - מלחמה, אסון טבע, תקיפת סייבר או כל אירוע המשבית את הפעילות הסדירה של הארגון או פוגע בה.

לפי הנחיה 1.3.06 של ראש רשות התקשוב הממשלתי בנושא "היערכות להמשכיות עסקית ותפקודית במצב חירום", פיתוח תוכנית המשכיות עסקית נחלק לשלבים העיקריים האלו:

1. ניתוח התהליכים הרלוונטיים והגדרה של השלבים החיוניים בכל תהליך אשר נדרש כי ימשיכו להתבצע גם בעת אירוע חירום.

2. מיפוי וניתוח של האיומים על קיום התהליך, תרחישי ייחוס אפשריים ומידת השפעתם.

3. הגדרת יעדי התאוששות מדידים:
   א. יעד משך ההתאוששות (RTO) - הגדרת היקף הפעילות הנדרש בכל שלב בתהליך בהתרחש אירוע חירום, ופרק הזמן הנדרש להחזרת הפעילות בהיקף האמור מרגע קרות האירוע.
   ב. יעד אחזור הנתונים (RPO) - היקף אובדן המידע שהארגון מוכן להכיל בהתרחש אירוע חירום[19].

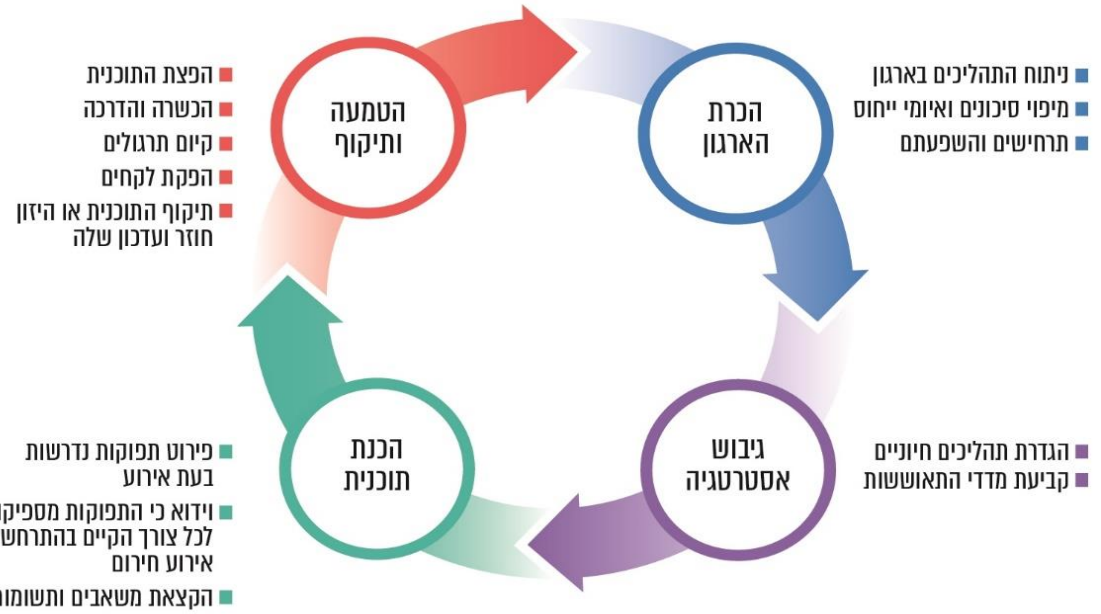
4. הכנת תוכנית התאוששות מאסון (DRP) - אוסף התהליכים שעל הארגון לבצע כדי לחזור לכשירות בקרות אירוע, בהלימה ליעדי ההתאוששות שהארגון הגדיר בתוכנית ההמשכיות

[19] הגדרה מפורטת של המונח "יעד אחזור הנתונים" (RPO - Recovery Point Objective) אפשר למצוא באתר זה: www.isaca.org/resources/glossary.

העסקית. במסגרת פיתוח התוכנית יש לוודא כי ליחידות הרלוונטיות מוקצים משאבים ותשומות שיאפשרו חזרה לכשירות כאמור.

להלן תיאור השלבים השונים בתהליך הטמעת תוכנית המשכיות עסקית:

תרשים 4: **תהליך הטמעת תוכנית המשכיות עסקית**



בעיבוד משרד מבקר המדינה.

בבט"ל קיים נוהל המשכיות עסקית, אולם ללא ציון התאריך שבו הוא נכתב וללא היסטוריית שינויים. לפי הנוהל, נדרש לפתח תהליך לניהול ולקיום של המשכיות עסקית לגבי רשת התקשוב של בט"ל. במהלך הביקורת התקבלה טיוטת נוהל המבוסס על נוהל שעת חירום ועתיד להחליף את נוהל המשכיות עסקית הקיים. בטיוטת הנוהל הוגדר היעד להתאוששות עסקית במצב של אסון, בהתאם לסדרי העדיפות שהוגדרו על ידי מנהלת בט"ל בשנת 1991 ואושררו בשנת 2013. לפי טיוטת הנוהל, יש לבדוק את התוכנית להמשכיות עסקית באופן סדיר, כדי להבטיח שהיא מעודכנת ואפקטיבית. בדיקות כאלה גם יבטיחו שכל חברי צוות ההתאוששות ועובדים רלוונטיים אחרים מודעים לתוכנית. במסמך המדיניות של בט"ל נכתב כי אחת לתקופה, אך לא יותר משלוש שנים, כפי שנקבע בתוכנית, יש לבצע ניסוי לבחינת מערך השיקום וההתאוששות של בט"ל.

נמצא כי טיוטת נוהל התאוששות עסקית שקיימת בבט"ל מאוקטובר 2023 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 אושררו בשנת 2013 ואינם עדכניים.

כמו כן, בט"ל לא ביצע תרגול של התאוששות מאסון בשלוש השנים האחרונות. נוכח זאת קיים חשש כי תוכנית ההמשכיות העסקית והמשאבים שהוקצו ליישומה לא ישקפו את הנכסים שיש להגן עליהם ואת המדדים שעל בט"ל לעמוד בהם כדי להמשיך לתת שירות נאות לציבור, וכי בזמן אמת בט"ל לא יוכל ליישם את התוכנית.

<u>גיבויים</u>

גיבויים אפקטיביים, אמינים וזמינים הם חשובים ביותר לתהליך המשכיות עסקית יעיל, ונדרש לבדוק אותם באופן שוטף.

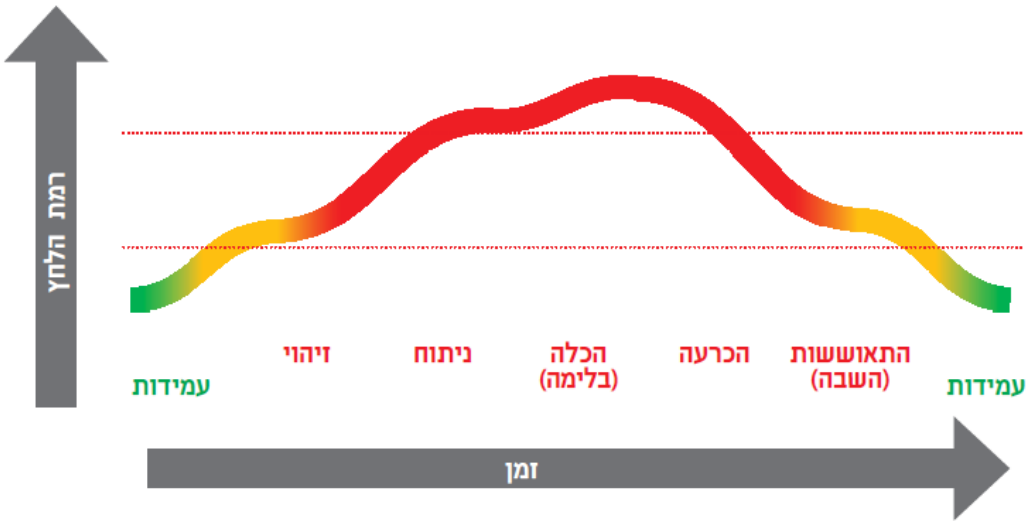
נמצאו פערים ביכולת לשחזר מידע מגיבויים.

אירועי סייבר

בשנים האחרונות הפכו אירועי סייבר לנפוצים בארץ ובעולם. התחכום ההולך וגובר של התוקפים, מורכבות האירועים והנזק הפוטנציאלי העצום לארגונים - כל אלה מחייבים היערכות ניהולית במגוון רבדים - משפטיים, תדמיתיים, עסקיים וכמובן טכנולוגיים. הארגון נדרש למומחיות תוכן, לכלים ולטכנולוגיות כדי להתמודד עם איומים אלו. ללא מענה מיומן ומקצועי הולם - איום הסייבר יכול להתרחב ולהעמיק בארגון ואף להתפשט לארגונים מקבילים וללקוחות הארגון. אירוע סייבר או תקיפת סייבר עלולים לשבש את ההתנהלות העסקית השוטפת, עד כדי פוטנציאל לפגיעה חמורה ומהותית בארגון, והם מחייבים מעורבות ישירה של הנהלת הארגון.

בהינתן שתוקף יצליח להתגבר על מאמץ המניעה ולהשיג גישה לארגון כדי לתקוף אותו, מטרת הארגון תהיה לגלות את התקיפה זמן קצר ככל האפשר לאחר שאירעה (באמצעות יכולות זיהוי), לנתח ולחקור את האירוע, לנסות למנוע את התפשטותו (להכיל אותו), להסיר את האיום ולהתאושש ממנו, ולעיתים אף להשיב את הארגון לתפקוד. בסוף התהליך על הארגון לבצע הפקת לקחים ולתקן ליקויים (שלב העמידות), ראו בתרשים שלהלן את שלבי ההתמודדות עם אירוע סייבר:

תרשים 5: **שלבי ההתמודדות של ארגון עם אירוע סייבר**



המקור: אתר ENISA, סוכנות של האיחוד האירופי לביטחון רשתות ומידע.

בבט"ל התרחשו כמה אירועי מניעת שירות (DDoS) שחלקם גרמו להשבתת האתר למשך יותר משעה. כמו כן אירעו בבט"ל כמה אירועי גניבת זהות של אזרחים שכתוצאה מהם שינה בט"ל את תהליך ההזדהות. זאת ועוד, בט"ל סובל מתופעת התחזות לאתר של הארגון שאחת מתוצאותיה הייתה

גניבת פרטי כרטיס האשראי של אזרחים. ממאי 2022 ועד מאי 2023 דווחו 25 מקרים של התחזויות למוקד 119[20].

התמודדות עם אירוע סייבר

לפי סעיף 11 לתקנות אבטחת מידע, בנוהל האבטחה יקבע בעל מאגר המידע גם הוראות לעניין התמודדות עם אירועי אבטחת מידע, לפי חומרת האירוע ומידת רגישות המידע, לרבות לעניין ביטול הרשאות וצעדים מידיים אחרים שיש לנקוט וכן לעניין דיווח לבעל המאגר על אירועי אבטחה ועל פעולות שננקטו בעקבותיהם.

מס"ל פרסם במאי 2021 המלצות למנהלים בעניין אופן ניהול אירוע סייבר[21]. כהכנה לקראת אירוע סייבר ממליץ מס"ל לדאוג בעוד מועד לנושאים האלה:

1. **הכנת צוות מולטי-דיסציפלינרי לטיפול באירוע:** מומלץ לוודא כי קיים צוות המעלה לדיון משמעויות ושיקולים במגוון ההיבטים הרלוונטיים - הטכנולוגי, העסקי, התקשורתי, המשפטי, האסדרתי, רציפות התפקוד, המוניטין ועוד.

2. **הכנת "תוכנית מגירה" וצוות IR:** מומלץ לוודא כי במקרה של אירוע סייבר או תקיפת סייבר יהיה ניתן להפעיל בקלות את תהליך העבודה המובנה שגובש בארגון, בהתאם לאופי האירוע.

3. **צוות DFIR:** מומלץ לוודא כי צוות ה- IR יכלול אנשי צוות מומחי תוכן טכנולוגיים (אנשי DFIR) אשר ינטר את הארגון ויבצע את החקירה הפורנזית, כולל חקירת המערכות, החשבונות, הרשת, מתווה התקיפה, והנזק לנכסים ולמידע.

תיק שטח הוא אסופה של מסמכים הנוגעים לסביבת התקשוב בארגון ולנהלים הרלוונטיים ומשמש את צוותי ה-IR בתהליכי הטיפול באירוע סייבר[22]. במענה לשאלון של משרד מבקר המדינה בנושא יכולת ההתמודדות של ארגונים עם אירועי סייבר נמסר כי בט"ל לא מנהל תיק שטח. עוד נמסר במענה לשאלון כי תהליכי התגובה לאירוע לא כוללים פעולות הכלה וניקוי[23].

בבט"ל קיים נוהל טיפול באירועי סייבר ללא ציון התאריך שבו הוא נכתב וללא היסטוריית שינויים. הנוהל כולל כמה נושאים, כמו דיווח על אירועי סייבר ועל נקודות תורפה ברשת המחשב של בט"ל, טיפול באירועי סייבר, ניהול אירועי אבטחת מידע וניהול שיפורים. בנוהל גם מוגדר צוות פעולה המורכב מסמנכ"ל תמ"מ, ראש אגף ביטחון ומנהל אבטחת מידע. לגבי תחומי האחריות של הצוות מצוין בנוהל נושא האבטחה באופן כללי. אשר לצוות ניהול אירוע סייבר (IR), הוא כולל רק את מנהל אגף תשתיות, ולא הוגדרו בנוהל תחומי האחריות שלו. נוסף על כך, חסר בנוהל פירוט של ממשקי התקשורת והתקני הרשת שבהם יש לטפל בקרות אירוע.

נמצא כי בנוהל טיפול באירועי אבטחת מידע של בט"ל חסרה התייחסות לנושאים האלה: התייחסות מפורטת לשלבי הטיפול באירוע סייבר: זיהוי, ניתוח, הכלה, הכרעה, התאוששות והפקת לקחים; והגדרת תחומי האחריות של הגורמים השונים בקרות אירוע. כמו כן, נמצא כי

---

20 מרכז 119 של מערך הסייבר הלאומי לדיווח על אירועי סייבר, מאויש 24 שעות ביממה באנליסטים ובאנליסטיות שתפקידם לזהות את סוג האיום, לאמוד את היקף הנזק הנשקף ממנו, ולספק את המענה המותאם לאזרח ולארגון.

21 https://www.gov.il/he/departments/general/cyber_attack_management

22 NIST 800-61r2, סעיף 3.1.1 - Preparing to Handle Incidents תחת הכותרת: Incident Analysis Resources

23 גידור הנזק מהתקיפה וסילוק הקבצים החשודים.

בט"ל אינו מנהל תיק שטח המיועד לצוותי התגובה על האירוע (IR). נוכח זאת קיים חשש כי בעת התרחשות אירוע סייבר לא יבוצעו הפעולות הדרושות לטיפול בו.

מנהל אבטחת מידע בבט"ל מסר כי אגף התשתיות הוא למעשה צוות ה-IR של בט"ל, וכי לא קיים צוות מוגדר של התאוששות מאירוע. בנוהל טיפול באירועי סייבר מופיע רק מנהל אגף תשתיות בצוות IR. בכינוס ועדת היגוי אבטחת מידע שהתקיים בינואר 2024 מונה צוות הנהלה בראשות מנכ"ל בט"ל לניהול אירוע בעת משבר סייבר.

במהלך מלחמת חרבות ברזל היה חשד לאירוע סייבר בבט"ל, ונדרשה בעניין חקירה פורנזית. בט"ל חקר את האירוע והסתייע במס"ל כדי לחקור קובץ זדוני.

נמצא כי אין בבט"ל צוותים ייעודיים לניהול משבר: צוות ניהול אירוע (IR) וצוות לביצוע חקירה פורנזית (DFIR). בסוף ינואר 2024, במהלך הביקורת, הוקם צוות הנהלה לניהול אירוע סייבר, אולם הוא לא התכנס, לא הוכשר ולא תורגל. היעדרם של צוותים ייעודיים מוכשרים ומתורגלים יפגע בהכרח באיכות המענה והתגובה שיינתנו בקרות אירוע סייבר.

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.

<u>מרכז שליטה ובקרה לטיפול באירועי סייבר (SOC)</u>

שימוש יעיל במערכת לגילוי אירועי סייבר ולהתרעה עליהם מצריך מערך של אנשי מקצוע הצופים בהתרעות של המערכת, מבצעים חקירה של אירועים ומעדכנים את המערכת.

נוהל הפעלת מוקד סייבר בבט"ל קובע כי מנהל חטיבת הסייבר נושא באחריות לקיום ייעודו של המוקד. בט"ל מסר כי ה-SOC עבר לאחרונה מאחריות חטיבת אבטחת מידע לאחריות אגף התשתיות. כאמור, מערך הסייבר המליץ כי חטיבת ה-SOC תוכפף למנהל אגף אבטחת מידע וסייבר.

בקרה 18.2 בתורת ההגנה של מערך הסייבר קובעת כי יש לוודא קיומה של בקרה רציפה ומתמשכת (Continuous Monitoring). דוגמה ליישום הבקרה: הטמעת מערכת SIEM עם צוות SOC הזמין 24 שעות ביממה, שבעה ימים בשבוע. מן הניסיון המצטבר בעולם עולה כי אירועי סייבר רבים מתרחשים בסופי שבוע ובחגים[24].

צוות ה-SOC במרכז השליטה והבקרה לאירועי סייבר בבט"ל פועל זה 13 שנים במתכונת רחבה. ההתרעות ממערך הסייבר נכנסו בעבר למערכת החוקים של ה-SIEM בתהליך אוטומטי, אולם כיום התהליך הוא ידני. צוות ה-SOC מורכב מבעלי התפקידים האלו: מנהלת אדמיניסטרטיבית; אנליסטית; עובד מצוות התשתיות; שבעה אנשי מוקד (סטודנטים) שעובדים בתורנות; שלושת הראשונים עובדים בשעות הפעילות בלבד. בט"ל מסר כי צוות ה- SOC לא עבר הכשרות פורמליות בתחום אבטחת מידע והכשרה רלוונטית לגילוי ולזיהוי של אירועים.

נמצא פער בהפעלת ה-SOC. עוד נמצא כי הצוות שמאייש את ה-SOC לא עבר הכשרה ייעודית לנושא. כמו כן ה-SOC אינו נמצא באחריות חטיבת אבטחת מידע אלא באחריות אגף תשתיות, שלא בהתאם לנוהל של בט"ל ושלא בהתאם להמלצות מס"ל. נוכח זאת קיים סיכון כי אירועי סייבר לא יתגלו על ידי ה-SOC.

---

[24] https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-243a
https://www.cybereason.com/hubfs/dam/collateral/ebooks/ransomware-attackers-dont-take-holidays-2022.pdf

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.

בתשובת בט"ל ממרץ 2024 נמסר כי "לאחר הטמעת תהליכי העבודה וייצוב כל תחום אחריות בנפרד תישקל שוב האפשרות להפריד תחומים אלו לרבות כפיפות ניהולית".

צוות ה- SOC בבט"ל מסר כי מגיעים אליו לטיפול עשרות אלפי חשדות לאירועים ביממה. בט"ל מסר לצוות הביקורת דוחות מה- SIEM אודות התרעות שהתקבלו במערכת במשך עשר יממות במהלך ינואר 2024. הדוחות מכילים עשרות אלפי התרעות מכ-30 סוגים של חוקים שמעלים חשד לפעילות עוינת. לדוגמה התקבלו התרעות על חשד לפעילות של נוזקה ידועה אשר מתרחשת בשעה קבועה בלילה. צוות ה- SOC לא תחקר את ההתרעות הללו כדי לבחון האם מדובר בסיכון ממשי או לחילופין, במידה ומדובר בפעילות לגיטימית - לטייב את החוק ולהסיר את ההתרעה.

עוד מסר צוות ה-SOC כי לא מתבצע מעבר שיטתי על ההתרעות בכדי לטייב את החוקים או בכדי לפתור את מקור ההתרעות ברמה מערכתית וכי אין שיטת עבודה המגדירה תיעדוף לטיפול באירועים.

נמצא כי בט"ל אינו מתחקר באופן סדור התרעות שמתקבלות ב-SOC כדי לעמוד על מקורן, וכי אין שיטת עבודה המגדירה תיעדוף לטיפול באירועים. לדוגמה, התרעות על חשד לפעילות של נוזקה ידועה אשר מתרחשת בכל לילה בשעה קבועה לא תוחקרו. כמו כן, יש חוסר הלימה בין הצורך בתחקור עשרות אלפי ההתרעות ביממה, לבין איוש ה- SOC באנליסט אחד בלבד. נוכח זאת קיים חשש כי לא מתאפשר לזהות את אירועי האמת בזמן סביר או בכלל.

מומלץ כי בט"ל יבחן את מנגנון הטיוב של מנוע החוקה ב-SIEM, כך שהאירועים שיגיעו לבחינת האנליסטים יהיו האירועים הרלוונטיים ביותר. עוד מומלץ לתגבר את מספר האנליסטים שיתחקרו את האירועים בהתאם למדדי ביצוע ולמספר האירועים החשודים שמגיעים לטיפולם. כמו כן, מומלץ להטמיע תהליך סדור של תחקור אירועים והתרעות.

תיעוד ותחקור של אירועי סייבר

לפי סעיף 11 לתקנות אבטחת מידע, בעל מאגר מידע אחראי לתיעוד כל אירוע המעורר חשש לפגיעה בשלמות המידע, לשימוש בו בלא הרשאה או לחריגה מהרשאה. בנוהל האבטחה ייקבעו הוראות לעניין ההתמודדות עם אירועים כאמור, לפי חומרת האירוע ומידת רגישות המידע. לגבי מאגר מידע שחלה עליו רמת האבטחה הגבוהה, בעל המאגר יקיים דיון אחת לרבעון לפחות באירועי האבטחה ויבחן את הצורך בעדכונו של נוהל האבטחה.

בנוהל טיפול באירועי סייבר של בט"ל נכתב כי צוות מוקד אבטחת מידע, מנהל חטיבת הסייבר ובדיקות החוסן, מנהל חטיבת אבטחת מידע ומנהל חטיבת שרתים יתכנסו לפגישה חודשית לתיאום הפעילות ביניהם. עוד נכתב בנוהל כי יש לתעד אירועים במערכת ניהול אירוע.

צוות ה-SOC מסר כי אין רישום מסודר של טיפול באירוע וסגירתו במערכת ה-SIEM, וכי אירועים חשודים נרשמים באופן ידני בקלסר. עוד מסר צוות ה- SOC כי אין תיעוד אודות ניהול החוקים (Rules) במערכת - טיוב ועדכון חוקים קיימים והגדרת חוקים חדשים. כמו כן, אין בסיס נתונים לגבי התרעות ואירועים היסטוריים ושימור ידע (Knowledge Base) ולא מתקיימות פגישות עיתיות של צוות ה- SOC עם אנשי התשתיות ואבטחת מידע כדי לדון באירועים וכדי לגבש שיטות עבודה מוסכמות.

בדצמבר 2021 התרחשה תקיפת מניעת שירות (DDoS) שהשביתה את האתר של בט"ל למשך שעה וחצי. במענה על פנייה של הרשות להגנת הפרטיות נמסר כי כלל הבדיקות בדבר האירוע נעשו פנימית בארגון, וכי לא קיים בבט"ל תיעוד על בדיקות בנוגע למתקפות מסוג זה.

בנוהל טיפול באירועי סייבר של בט"ל נכתב כי לאחר סיום האירוע יתכנס פורום אבטחת מידע מורחב לצורך הפקת לקחים ממנו.

סמנכ"ל תמ"מ מסר כי לא קיים בבט"ל תהליך של תחקור אירועים.

נמצא כי בט"ל אינו מתעד באופן שיטתי אירועי סייבר, אינו עוקב אחר האירועים, אינו מקיים דיון אחת לרבעון באירועי האבטחה ואינו בוחן את הצורך בעדכון נוהלי האבטחה בהתאם לסעיף 11 בתקנות אבטחת מידע. עוד נמצא כי לא מתקיים תהליך סדור של תחקור והפקת לקחים בעקבות אירועי סייבר.

מומלץ להטמיע תהליך סדור של תיעוד אירועי סייבר, שבו יפורט בין השאר לגבי זיהוי האירוע; סיווגו; התיעדוף לטיפול שהוגדר לו; ממצאי החקירה; התיקון שבוצע ברמת החוק (rule), המערכת או תהליך ספציפי אשר קשורים לאירוע; והפקת הלקחים מן האירוע. כן מומלץ להגדיר ולהטמיע תהליכי שיתוף ושימור של ידע.

<u>דיווח על אירועי סייבר</u>

לפי תקנה 11 לתקנות אבטחת מידע, במקרה של אירוע אבטחה חמור על בעל המאגר להודיע לרשם על כך באופן מיידי וכן לדווח לרשם על הצעדים שנקט בעקבות האירוע.

בנוהל אירוע סייבר של בט"ל נכתב כי על מנהל אבטחת מידע לדווח למערך הסייבר ולרשות להגנת הפרטיות בהתאם למצב הכוננות ובאופן מיידי בקרות אירוע.

באירוע שהתרחש בינואר 2022 התקבלה פנייה של אזרחית בדבר קבלת סיסמה לאתר בט"ל, בלי שנפתח משתמש ובוצעה הרשמה לאתר. נוסף על כך, התגלה דלף מידע לגבי כ-2,000 אזרחים בעקבות חולשה בתהליך ההזדהות הדו-שלבי באתר בט"ל, והאתר הוקשח בעקבות האירוע. התברר כי אירוע זה לא דווח לרשות להגנת הפרטיות כאירוע אבטחת מידע חמור.

נמצא כי בט"ל לא דיווח על אירועי סייבר לגורמים האסדרתיים, ובכלל זה לא דיווח לרשות להגנת הפרטיות על אירוע סייבר חמור (כהגדרתו בתקנות אבטחת מידע) של דלף מידע לגבי כ-2,000 אזרחים, זאת בניגוד למתחייב לפי תקנה 11 בתקנות אבטחת מידע ובניגוד למתחייב לפי נוהלי בט"ל.

בתשובת הרשות להגנת הפרטיות ממרץ 2024 נמסר כי במסגרת תיקון 14 לחוק הגנת הפרטיות[25] תוקנה לרשות הסמכות להטיל עיצומים כספיים ניכרים על גופים שלא ימסרו דיווח מיידי בגין אירוע אבטחת מידע חמור כמתחייב בתקנות.

במאי 2023 התקיים דיון התנעה של ועדת היגוי בנושא התחזויות בהשתתפות מערך הסייבר, המשטרה ובט"ל. בדיון עלה כי קיימים יותר מקרי התחזויות מאלו שדווחו למוקד 119, וכי חלק מהדיווחים מגיעים למשטרה וחלק אחר ישירות לבט"ל, ולכן חשוב לסנכרן את כלל המידע למאגר אחוד. עוד עלה בפגישה כי לא התקיים דיון בנושא חדשנות טכנולוגית לצמצום התופעה, לדוגמה שימוש בכלי טכנולוגי - Digital Brand Protection (DRP) לטובת הגנה מתופעת ההתחזויות. זאת ועוד, בדיון ציינה נציגת המשטרה שאין למשטרה בשלב זה את הכלים וכוח האדם לצמצום התופעה.

[25] הצעת חוק הגנת הפרטיות (תיקון מס' 14), התשפ"ב-2022 (טרם אושרה).

נמצא כי למס"ל ולמשטרה אין את המשאבים האנושיים והטכנולוגיים לטיפול בתופעת ההתחזויות לבט"ל ואין להם יכולות למנוע אותה. נוכח זאת, אירועי ההתחזות ממשיכים להתקיים באופן שפוגע בתדמית בט"ל. עוד נמצא כי כל אחד מהגופים (מס"ל והמשטרה) מקבל רק דיווח חלקי על אירועי ההתחזות.

מומלץ כי מס"ל יבחן שימוש בכלים שקיימים בשוק וכלים שנמצאים בשימוש ארגונים מקבילים בעולם להתמודדות עם תופעת ההתחזויות ויציע פתרונות להתמודדות עם התופעה. עוד מומלץ כי מס"ל והמשטרה יקימו תשתית דיווח אחודה על התחזויות.

בתשובת המשטרה ממרץ 2024 נמסר כי ניטור מרחב המרשתת ופעולות סיכול ומניעה בו בנושא האמור נתונים בידי מערך הסייבר הלאומי והגופים עצמם. המשטרה ציינה כי אם הנושא מובא לידיעתה במסגרת תלונה או מידע מודיעיני, היא פועלת בשיתוף מס"ל לאיתור מוביל חקירתי לצד ניסיונות להפלת התשתית. המשטרה ציינה כי עבודת מטה להרחבת פעילות מרכז הסייבר הארצי (מס"א) אשר פועל בחטיבת הסייבר במשטרה לשם סיכול ומניעה לא תועדפה לביצוע בשנים 2023 - 2024. לדברי המשטרה אם עבודת המטה תתקדם ותמומש, ניתן יהיה לטייב את המענה הכולל לתופעות הדיוג במדינת ישראל. עוד נמסר בתשובה כי חטיבת הסייבר של משטרת ישראל נמצאת בימים אלה בתהליך השמשה של מערכת שמטרתה לזהות תשתית דיוג, אם מקרים אלו מדווחים למשטרה. ואולם קשה לזהות מקרים כאלה, בשל יכולות הסוואה ושימוש בתשתיות אנונימיות וחד פעמיות של החשודים, אשר רובם ככולם פועלים מחו"ל.

בתשובת מס"ל מאפריל 2024 נמסר כי מס"ל מודע לתופעה הפסולה ופועל בנושא זה, בשיתוף המשטרה. בעת קבלת עדכון על פעילות התחזות ודיוג לבט"ל, לאחר בחינה וכן עדכון המשטרה, פועל מערך הסייבר לעדכן את חברת האחסון וגורמים רלוונטיים נוספים לפי הצורך, כדי שיבחנו אם יש מקום לפעולות מצידם, במטרה לצמצם פגיעה בציבור.

<u>תרגול אירועי סייבר</u>

הסיכונים בעולם הסייבר ואבטחת המידע משתנים מיום ליום. התרגולים התקופתיים לצוות העובדים וההנהלה של הארגון נועדו לוודא את מוכנות הארגון לתקיפת סייבר בהתאם למגמות חדשות ואיומים רלוונטיים לתקופה.

בנוהל אירוע סייבר של בט"ל נכתב כי יש לתרגל את נוהל אירוע סייבר באופן לימודי וכן לערוך תרגול יבש פעם בחצי שנה.

במענה לשאלון של משרד מבקר המדינה בנושא יכולת ההתמודדות של ארגונים עם אירועי סייבר נמסר כי בט"ל לא ביצע תרגיל לצוות הנהלה לניהול משבר סייבר וכן לא ביצע תרגיל מעשי לצוות הטכנולוגי המדמה לפחות אחד מתרחישי האיום. כמו כן הארגון לא השתתף בתרגיל סייבר מגזרי או לאומי.

נמצא כי בט"ל אינו מקיים תרגול של אירועי סייבר להנהלה ולעובדים, כמתחייב בנוהל אירוע סייבר שקבע הוא עצמו.

על מנת שבט"ל יוכל להתמודד כראוי עם אירוע סייבר שמתרחש בזמן אמת, עליו לקיים תרגול של אירועי סייבר להנהלה ולעובדים כמתחייב בנוהל אירוע סייבר שלו.

בתשובת בט"ל ממרץ 2024 נמסר כי ברבעון השני של שנת 2024 מתוכנן תרגול הנהלת בט"ל בהתמודדות עם אירוע סייבר.

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.

מילון מושגים

Security Information and Event Management (SIEM) - מערכת המנתחת לוגים המגיעים מרכיבי תקשורת ומרכיבי תוכנה שונים. המערכת מקבלת נתונים ממערכות ארגוניות שונות, מנתחת אותם ומאפשרת בקרה על תהליכים ואירועים, הפקת דוחות, זיהוי פרצות אבטחה ותגובה על מתקפות המתרחשות בזמנים שונים.

מרכז בקרה להגנת סייבר Security Operation Center (SOC) - יחידה ריכוזית בארגון האחראית לתהליכים וטכנולוגיה ונועדה לפקח באופן רציף על רמת האבטחה של הארגון ולשפר אותה, תוך ביצוע פעולות מניעה, איתור, ניתוח ותגובה לגבי אירועי אבטחת רשת.

תוכנית המשכיות עסקית Business Continuity Plan (BCP) - תוכנית פעולה מקיפה הקובעת את הנהלים והמערכות הדרושים להבטחת המשך הפעילות של גוף במצב חירום ולהתאוששותו.

Incident Response Team (IR) - צוות ניהול אירוע סייבר הפועל למזער את הנזק הארגוני בהתרחש אירוע כזה.

Digital Forensics Incident Response Team (DFIR) - צוות מומחי תוכן טכנולוגיים אשר ינטר את הפעילויות ברשת הארגון בעת אירוע סייבר ולאחריו ויבצע את החקירה הפורנזית, כולל חקירת המערכות, החשבונות, הרשת, מתווה התקיפה והנזק לנכסים ולמידע.

מתקפת מניעת שירות מבוזרת Distributed Denial of Service (DDoS) - הרחבה של מתקפת DoS. במתקפת DoS נשלחת כמות מסיבית של פניות ובקשות לקבלת שירות הפוגעת ביכולת האתר או השרת לתת שירות ללקוחות. מתקפת DDoS מנוהלת על ידי גורם מרכזי (המכונה המאסטר) אשר שולט בו זמנית במחשבים תמימים רבים (המכונים bots או zombies), המבצעים את התקיפה באופן מתואם ובמקביל.

משרד מבקר המדינה
ונציב תלונות הציבור