דוח מבקר המדינה | כסלו התשפ"ו | דצמבר 2025

משרד הביטחון

ניהול מאגרי מידע במשרד הביטחון ואבטחתם

ניהול מאגרי מידע במשרד הביטחון ואבטחתם

רקע

למשרד הביטחון תפקיד מרכזי במימוש יעדי הביטחון הלאומי של מדינת ישראל, ולצורך ביצוע משימותיו הוא משתמש במאגרי מידע רחבי היקף, ובהם מאגרי עובדים, ספקים, לקוחות, נכי צה"ל, משפחות שכולות, חללים, פדויי שבי ויועצים. מאגרים אלה כוללים מידע אישי, כגון נתונים על אישיותו של אדם, מעמדו האישי, מצבו הבריאותי, מצבו הכלכלי והכשרתו המקצועית. חשיפת המידע שבמאגרים עלולה לפגוע בזכות לפרטיות של האנשים שמידע רגיש לגביהם שמור בהם, שהיא אחת מזכויות האדם החשובות בישראל. כמו כן, עלולות להיות לכך השלכות על תפקודו של משרד הביטחון ועל ביטחון המדינה, כמתואר להלן:

השלכות אפשריות כתוצאה מחשיפת המידע שבמאגרי המידע של משרד הביטחון ופגיעה בהם

הסיכונים להגנת הפרטיות ולאבטחת המידע שבמאגרי המידע גברו במהלך מלחמת חרבות ברזל נוכח התעצמות מתקפות הסייבר, שהן חלק בלתי נפרד מהמלחמה המודרנית, ובהן מתקפות על מאגרי מידע של גופים ציבוריים והתגברות ניסיונות הודעות הדיוג (פישינג) המכוונים לגורמים בישראל, ובכלל זה לאנשי מערכת הביטחון לשעבר - ניסיונות שהפכו מתוחכמים יותר וממוקדים יותר ביעד התקיפה באמצעות איסוף מידע מקדים בנוגע לתחומי העיסוק ולתחומי העניין של היעד. בשנת 2024 חלה עלייה של 24% במספר אירועי הסייבר

שאימת מערך הסייבר הלאומי בהשוואה לשנת 2023 (17,078 אירועי סייבר בשנת 2024 לעומת 13,040 בשנת 2023). המתקפות הנפוצות ביותר היו אירועי דיוג (פישינג) - בשנת 2024 אומתו 10,084 אירועים לעומת 3,301 בשנת 2023; 44% מאירועי הדיוג בשנת 2023 (1,449) אירעו משבעה באוקטובר ועד סוף שנת 2023. כמו כן, אומתו בשנת 2024 1,771 אירועי חדירה למערכות מחשוב לעומת 1,714 בשנת 2023, מחצית מאירועים אלה בשנת 2023 (873) אירעו משבעה באוקטובר ועד סוף שנת 2023.

התממשות הסיכונים למאגרי המידע של משרד הביטחון עלולה לגרום למשל לחשיפה של מידע אישי על חיילים שנפצעו במלחמה (מאגר נכי צה"ל) או על חטופים מטבח שבעה באוקטובר ששוחררו מעזה (מאגר פדויי שבי) והפכו, בעל כורחם, לעניין ציבורי. נוסף על כך, חשיפת מידע או שיבוש מידע ממאגרים בעלי ערך ביטחוני, דוגמת מאגר עובדי משרד הביטחון ומאגר ספקי המשרד, שנדרש לשמור על חסיונם, עלולים לפגוע ברציפות התפקודית של משרד הביטחון וביכולתו לספק את האמצעים הנדרשים לצה"ל, לגרום לו נזק תדמיתי, לפגוע ביחסיו עם ספקים ולקוחות ולחשוף אותו לקנסות. יתרה מכך, לעניין זה השפעה תודעתית - הדבר עלול אף לזרוע בהלה ותחושת חוסר ביטחון בציבור ולפגוע בקשרי החוץ של המדינה בהקשרים ביטחוניים-מדיניים.

ואכן, במהלך מלחמת חרבות ברזל התממש הסיכון לדלף מידע ממשרד הביטחון: באפריל 2024 פורסם בכלי התקשורת כי באתר אינטרנט שהקימו פצחנים (האקרים) בין-לאומיים פורסם מידע שהודלף בידי גורמים עוינים מתוך פורטלים מינהליים של משרד הביטחון, ונכלל בהם מידע מזהה של עובדי המשרד, מידע על מכרזים ביטחוניים ועל מערכות טכנולוגיות של צה"ל, כגון פרטים על כלי רכב משוריינים, תשריטים הנדסיים ומידע טכני על מערכות צילום לווייניות.

נתוני מפתח

14

מספר מאגרי המידע האישי[1] שרשם משרד הביטחון במרשם המאגרים; 8 מהם (57%) הם מאגרים שחלה עליהם רמת אבטחה גבוהה נוכח סיכוני האבטחה שהם מייצרים

2.84 מיליון אנשים

נכללים במאגרי המידע האישי של משרד הביטחון, לרבות 230,000 אנשים שפרטיהם נכללים במאגר נכי צה"ל, ובו מידע על מצבם הבריאותי והכלכלי, על בני משפחותיהם, על השירותים הניתנים להם ועוד, לרבות 18,000 פצועים ממלחמת חרבות ברזל

18 שנים חלפו

מאז שמשרד הביטחון מיפה לאחרונה (2007) את כלל המאגרים שבבעלותו כדי לדעת אם חלות עליו דרישות נוספות מתוקף חוק הגנת הפרטיות, ולכן ייתכן שיש בבעלותו מאגרי מידע נוספים

0

מספר הסקרים לאיתור סיכוני אבטחת מידע במאגרים ומבדקי החדירות למערכות של המאגרים שערך משרד הביטחון לצורך אבטחת המאגרים מפני סיכונים חיצוניים ופנימיים

עד 320,000 ש"ח

סכום העיצום הכספי לכל מאגר ברמת אבטחה גבוהה שמשרד הביטחון עלול להיות חשוף לו בגין אי-ביצוע סקרי סיכונים ומבדקי חדירות, עם כניסתו לתוקף של תיקון 13 לחוק הגנת הפרטיות

7 מכל 10

משתמשים חיצוניים[2] עם הרשאת גישה לרשת מחשב מרכזית של משרד הביטחון לא נכנסו לרשת יותר מחצי שנה, 60% מהם לא נכנסו אליה מעולם. 90% הם עובדי מיקור חוץ. לפיכך קיים סיכון שהם בעלי הרשאת גישה לרשת שלא לצורך

60%

מכלל המשתמשים החיצוניים שלא נכנסו לרשת יותר מחצי שנה משויכים לחמישה אגפים במשרד הביטחון שמידת הסיכון לחשיפת מידע ביטחוני מתוכם או לחשיפת מידע בנוגע לפרט מתוכם היא גבוהה

5 מכל 10

משתמשים חיצוניים עם הרשאת גישה למערכת המידע שבה מנוהל מאגר נכי צה"ל לא נכנסו למערכת יותר מחצי שנה. לפיכך קיים סיכון שהם בעלי הרשאת גישה למאגר נכי צה"ל שלא לצורך

1 כגון נתונים על אישיותו של אדם, מעמדו האישי, מצבו הבריאותי, מצבו הכלכלי והכשרתו המקצועית.

2 משתמשי מערכות המחשוב במשרד הביטחון נחלקים לשתי קבוצות: (א) קבוצת משתמשי משרד - משתמשים שפרטיהם האישיים מנוהלים במערכות כוח האדם של משרד הביטחון, ובהם עובדי המשרד, יועצים, בנות שירות לאומי, וחיילי צה"ל שמשרתים במשרד הביטחון; (ב) קבוצת המשתמשים החיצוניים - משתמשים שפרטיהם אינם מנוהלים במערכות כוח האדם של משרד הביטחון, ובהם עובדי מיקור חוץ, עובדי תעשיות ביטחוניות ומשתמשי צה"ל.

פעולות הביקורת

בחודשים אוגוסט 2024 עד ינואר 2025 בדק משרד מבקר המדינה את האופן שבו משרד הביטחון מנהל את מאגרי המידע שהוא בעל השליטה בהם ואת האופן שבו הוא מאבטח אותם בראי הדרישות החלות עליו כפי שנקבעו בחוק הגנת הפרטיות, התשמ"א-1981, ובתקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017 (תקנות אבטחת מידע). יצוין כי הביקורת לא עסקה באבטחת מידע בהיבטי סייבר. הביקורת נעשתה במשרד הביטחון - באגף תקשוב וניהול מערכות מידע (אגף התקשוב) ובאגף ביטחון; במשרד המשפטים - ברשות להגנת הפרטיות. בדיקות השלמה נעשו באגף שיקום נכים שבמשרד הביטחון.

יצוין כי מכיוון שתיקון מספר 13 לחוק הגנת הפרטיות ייכנס לתוקף באוגוסט 2025, לאחר מועד סיום הביקורת, נבדקה פעילותו של משרד הביטחון אל מול הוראות החוק טרם התיקון ובהלימה לדרישות שיחולו עליו בראייה צופה פני עתיד. בהתאם, ההגדרות והמונחים וכן ההמלצות המוצגים בדוח זה בהתייחס לחוק הגנת הפרטיות ולתקנות הגנת הפרטיות (אבטחת מידע) הם בהתאם לתיקון 13 לחוק.

תמונת המצב העולה מן הביקורת

עמידת משרד הביטחון בדרישות החלות עליו בתחום אבטחת המידע שבמאגרי המידע בהיבטי הגנת הפרטיות - אגף התקשוב במשרד הביטחון לא מימש את האחריות שהוא נושא בה לקיים את הדרישות החלות על משרד הביטחון בתחום אבטחת המידע במאגרי המידע בהיבטי הגנת הפרטיות, ובהן קביעת נוהל אבטחה וביצוע סקרי סיכונים, מבדקי חדירות והדרכה להגברת המודעות של העובדים; זאת משום שהוא נסמך על אגף ביטחון, שהוא הגורם המקצועי ובעל הסמכות בתחום אבטחת המידע של משרד הביטחון, בלא שווידא כי הפעולות שאגף ביטחון מבצע אכן נותנות מענה לכלל הדרישות הייחודיות בהיבט הגנת הפרטיות. יצוין כי אגף ביטחון מבצע פעולות לאבטחת מידע, אולם פעולות אלה דרושות לשם שמירה על מידע מסווג כהגדרתן בחוק להסדרת הביטחון בגופים ציבוריים, התשנ"ח-1998, שמכוחו פועל האגף, והן לא נותנות מענה מלא לאבטחת המידע במאגרי המידע בהיבט הגנת הפרטיות.

אי-עמידה בדרישות אבטחת המידע מתוקף תקנות הגנת הפרטיות מגבירה את הסיכונים הנשקפים למאגרי המידע, ובהם דֶלֶף מידע, שיבוש מידע או פגיעה בזמינותו, זאת בפרט נוכח האתגרים הייחודיים הקיימים באכיפה הנוגעת להגנת הפרטיות במאגרי מידע ממוחשבים. בשנים האחרונות דֶלֶף מידע מתוך משרד הביטחון הן כתוצאה מתקיפות סייבר מצד גורמים חיצוניים עוינים שהדליפו מידע מתוך פורטלים מינהליים של משרד הביטחון, לרבות מידע מזהה של עובדי המשרד, מידע על מכרזים ביטחוניים ומידע על מערכות

טכנולוגיות של צה"ל, ובכלל זה תשריטים הנדסיים ומידע טכני[3]; והן כתוצאה מטעויות אנוש של עובדים שפרסמו בשגגה מספרי תעודות זהות, שמות ומספרי רכב של בכירים במשרד הביטחון[4].

- **בקרת משרד הביטחון על יישום תקנות אבטחת מידע במאגרי המידע** - בניגוד לנדרש בחוק הגנת הפרטיות ובתקנות, שלפיהם ימונה ממונה אבטחת מידע למאגרי המידע שיבצע בקרה שוטפת על העמידה בדרישות שבתקנות אבטחת מידע, אין בעל תפקיד במשרד הביטחון שאחראי לזהות את הדרישות החלות על המשרד מתוקף החוק והתקנות, ובכלל זה לתקף את העמידה בהם ולבצע בקרה על כך. עוד עלה כי עד אוקטובר 2024 ראש אגף התקשוב במשרד הביטחון, המופקד על ניהול מאגרי המידע ונושא על פי חוק באחריות ישירה לאבטחת המידע שבמאגרי המידע במשרד הביטחון ולעמידה בחובות המנויות בתקנות בנוגע למאגרי המידע שמשרד הביטחון הוא בעל השליטה בהם, לא וידא שהממונה על אבטחת המידע במאגרי המידע ממלאת את תפקידיה בהתאם לנדרש בתקנות; וממילא הוא לא ביצע בקרה על עמידתו של משרד הביטחון בדרישות החלות על המשרד מתוקף התקנות, חרף חשיבותן של תקנות אלו להגנה על פרטיותם של אנשים שמידע רגיש לגביהם שמור במאגרים וחרף הסיכונים הרבים הנשקפים למאגרים והשלכותיהם הרוחביות - בהיבטי הפרט, הארגון וביטחון המדינה.

- **מיפוי ורישום מאגרי מידע במשרד הביטחון** - שלא בהתאם לנדרש בחוק הגנת הפרטיות, כי בעל שליטה במאגר מידע ירשום את המאגרים במרשם מאגרי המידע ויודיע על שינויים מסוימים הנוגעים למאגרים, אגף התקשוב לא מיפה את כלל המידע שבבעלות משרד הביטחון משנת 2007 כדי לדעת אם הוא כולל מידע אישי כהגדרתו בחוק ובתקנות, ואם חלות על משרד הביטחון דרישות נוספות מתוקף החוק, לרבות החובה לרשום מידע זה במרשם המאגרים.

במצב זה משרד הביטחון לא הכיר בכך שייתכן שיש בבעלותו מאגרי מידע נוספים שלגביהם הוא נדרש לפעול בהתאם להוראות שבחוק הגנת הפרטיות ובתקנות, ובכלל זה מאגרים שכוללים מידע אישי רגיש דוגמת מידע על צנעת חיי המשפחה של אדם; מצב בריאותו; עברו הפלילי; נתוני שכרו; אמונותיו הדתיות; מוצאו; הערכת מאפייני אישיותו המהותיים, ובכלל זה קווי אופי, יכולת שכלית ויכולת תפקוד בעבודה; נתוני מיקומו ונתוני תעבורה.

מידע אישי רגיש מסוג זה עשוי להיכלל למשל במאגרי המידע של מבדקי התאמה מהימנותיים וביטחוניים שמבצע משרד הביטחון לכלל האוכלוסיות שמועסקות בו ובמאגרי המידע של מבדקי הערכה לגיוס עובדים. לפיכך משרד הביטחון אינו מודע לכך שייתכן שחלות עליו חובות נוספות בנוגע למידע אישי שהוא בעל השליטה בו וכן חובות מתוקף

3 כפי שפורסם בכלי התקשורת באפריל 2024 (למשל, **ישראל היום**, "האקרים הצליחו לחדור למערכות משרד הביטחון: חשש שמידע רגיש דלף" (9.4.24) https://www.israelhayom.co.il/tech/tech-news/article/15573329). משרד הביטחון מסר לכלי התקשורת כי נפרץ אתר שאינו רגיש ואישר את תגובתו זו למשרד מבקר המדינה בדצמבר 2024, לרבות מסירת התחקיר שבוצע בעקבות המקרה והפעולות שנקט לטיפול בפרצת האבטחה.

4 כפי שפורסם בשנת 2022 בכלי התקשורת (למשל, **דה מרקר**, "טעות קטנה באקסל חשפה ברשת פרטים של בכירים במשרד הביטחון", (24.8.22), https://www.themarker.com/captain-internet/2022-08-24/ty-article/.premium/00000182-cf9f-d1de-a7c3-dfdf3bca0000). משרד הביטחון אישר את הפרטים למשרד מבקר המדינה בספטמבר 2024.

תקנות הגנת הפרטיות (הוראות לעניין מידע שהועבר לישראל מהאזור הכלכלי האירופי), התשפ"ג-2023, שעמידה בהן מקלה על קיום קשרי מסחר עם המדינות החברות באיחוד האירופי, והיעדרה עלול לפגוע בקשרי החוץ עם מערכות ביטחון זרות שלהן חשיבות רבה למימוש יעדי הביטחון הלאומי של מדינת ישראל.

- **סיווג המאגרים וגיבוש מענה ההגנה עבורם** - בניגוד לנדרש בתקנות אבטחת מידע, שלפיהן יוכן מסמך הגדרות מאגר שמתאר היבטים מרכזיים שנוגעים לו, וכי המאגר יסווג בהתאם לסיכוני האבטחה שהוא מייצר, אגף התקשוב במשרד הביטחון לא הכין מסמך כאמור לכל אחד ממאגרי המידע שהוא בעל השליטה בהם, והוא לא סיווג את מאגרי המידע בהתאם לרמות האבטחה החלות עליהם (בינונית או גבוהה). במצב זה אין לאגף התקשוב תמונת מצב מלאה ועדכנית בנוגע לכל המאגרים שהוא מנהל אשר תאפשר לו להתאים את מענה ההגנה הנדרש עבורם בהתאם לסיכונים שהם מייצרים. יתרה מכך, מאוגוסט 2025, עם כניסתו לתוקף של תיקון 13 לחוק הגנת הפרטיות, עלול משרד הביטחון להיות חשוף לעיצומים כספיים בסכום שבין 20,000 ש"ח ל-320,000 ש"ח בגין הפרות שונות של תקנות אבטחת מידע בנוגע לכל מאגר.

- **ניהול הרשאות גישה במערכת ניהול זהויות**[5]

  - בביקורת עלה כי לפי ניתוח שביצע משרד מבקר המדינה, 7 מכל 10 משתמשים חיצוניים בעלי הרשאת גישה לרשת מחשב מרכזית של משרד הביטחון, שהיא שער כניסה למאגרי מידע, לא נכנסו לרשת זו יותר מחצי שנה, מרביתם (60%) לא נכנסו אליה מעולם. במצב זה עולה חשש כי הם בעלי הרשאת גישה שלא לצורך ביצוע תפקידם. עוד עלה כי מרבית המשתמשים שלא נכנסו לרשת יותר מחצי שנה (90%) הם עובדי מיקור חוץ, וחלק גדול מהם (60%) משויכים לחמישה אגפים שמידת הסיכון לחשיפה של מידע ביטחוני מתוכם או של מידע בנוגע לפרט מתוכם, היא גבוהה. מאחר שרשת זו היא שער הכניסה למאגרי מידע, וקיימים בה נכסים, חלקם רגישים, וכן תשומות המשרתים תהליכים עסקיים ותהליכי הצטיידות של צה"ל, גובר הסיכון לחשיפת מידע אישי בפני מי שאינם מורשים לכך.

  - בביקורת עלה עוד כי אגף התקשוב במשרד הביטחון לא הסדיר שיטת דיווח מצד הגורמים דורשי ההרשאות מאגפי משרד הביטחון וצה"ל בנוגע לסיום תפקידם של משתמשים מקבוצת המשתמשים החיצוניים לצורך ביטול הרשאותיהם. זאת אף שכתוצאה מהיעדר דיווח סדור קיימות הרשאות פעילות שלא לצורך בקבוצת המשתמשים החיצוניים, ובכלל זה הרשאות לרשתות מחשבים ולמערכות מידע שהן שער כניסה למאגרי מידע.

  - כמו כן, עלה בביקורת כי אגף התקשוב אינו מבצע סקירת הרשאות סדורה ומובנית על אלפי המשתמשים המנוהלים במערכת ניהול זהויות ועל עשרות אלפי סוגי ההרשאות שבה לצורך עדכון רשימות המשתמשים, אלא הוא מבצע מפעם לפעם בדיקות ממוקדות של הרשאות לקבוצת משתמשים מצומצמת לפי שיקול דעתו ובאופן ידני. זאת, שלא בהתאם לדרישה בתקנות לנהל רישום מעודכן של המשתמשים ושל

5 מערכת ממוחשבת שבה מנוהלים חשבונות משתמשים של בעלי תפקידים שלהם הרשאות שונות לרשתות המחשוב של משרד הביטחון, למערכות המידע ולמאגרי המידע המקושרים אליהן.

הרשאות הגישה שניתנו להם לביצוע תפקידם ואף שאגף התקשוב מודע לקיומן של הרשאות שאינן לצורך בקבוצת המשתמשים החיצוניים.

ניהול הרשאות גישה למאגר נכי צה"ל

- בביקורת עלה כי לפי ניתוח שביצע משרד מבקר המדינה, 5 מכל 10 משתמשים בעלי הרשאת גישה פעילה למערכת שמש[6] (263 משתמשים מתוך 481) לא נכנסו למערכת זו יותר מחצי שנה, חלקם (29% מהם, שהם 78 משתמשים) לא נכנסו אליה מעולם. במצב זה עולה חשש כי הם בעלי הרשאת גישה שלא לצורך ביצוע תפקידם.

- עוד עלה בביקורת כי אגף התקשוב במשרד הביטחון לא הסדיר שיטת דיווח מצד הגורמים דורשי ההרשאות בנוגע לסיום תפקידם של משתמשים חיצוניים במערכת שמש לצורך ביטול הרשאותיהם. זאת אף שכתוצאה מהיעדר דיווח סדור קיימות הרשאות פעילות שלא לצורך למערכת שמש בקבוצת המשתמשים החיצוניים. לדוגמה, היו הרשאות פעילות שלא לצורך לעובדים שהועסקו באמצעות ספק חיצוני, דוגמת המוקד הטלפוני של אגף שיקום נכים, שמונה עשרות עובדים ומתאפיין בתחלופה של עובדים, וכן לספקים חיצוניים שיכלו להתחבר מרחוק למערכת שמש, וזאת אף שהם סיימו את תפקידם.

כתוצאה מכך, בנסיבות מסוימות עלולים גורמים בלתי מורשים להיחשף למידע אישי לרבות מידע בעל רגישות מיוחדת במאגר נכי צה"ל שכולל פרטים על אודות יותר מ-230,000 אנשים, ובכלל זה מצבם הבריאותי, מצבם הכלכלי, בני משפחותיהם והשירותים הניתנים להם. סיכון זה גובר נוכח הגידול של כ-18,000 פצועים שנוספו למאגר נכי צה"ל בשל מלחמת חרבות ברזל והגידול בעקבות זאת במספר נותני השירותים באגף שיקום נכים המשתמשים במערכת שמש. עם כניסתו לתוקף של תיקון 13 לחוק הגנת הפרטיות תוכל הרשות להגנת הפרטיות להטיל על משרד הביטחון עיצומים כספיים בגין אי-ביטול הרשאות גישה למשתמשים מיד עם סיום תפקידם בסכום של 160,000 ש"ח למאגר ברמת אבטחה גבוהה, דוגמת מאגר נכי צה"ל.

נוהל אבטחה למאגרי המידע - אגף התקשוב לא קבע נוהל אבטחה למאגרי המידע כנדרש בתקנות. נושאים מסוימים שאותם יש לכלול בנוהל קיימים בנהלים שקבע אגף הביטחון, דוגמת ניהול אירועי סייבר, הגנה בעבודה עם התקנים ניידים ומדיניות סיסמאות, שהיא חלק ממדיניות הגישה למאגרים; אולם נושאים כגון הסיכונים שלהם חשופים מאגרי המידע, אופן קביעת הסיכונים והטיפול בהם ואופן הבקרה על השימוש במאגרים, אינם מקבלים מענה בנהלים מצד אף גורם במשרד הביטחון.

בהיעדר נוהל אבטחה למאגרי המידע נותר משרד הביטחון בלא מדיניות אבטחה סדורה ושלמה להתמודדות עם סיכוני האבטחה שלהם חשוף המידע שבמאגרי מידע ובלא כלי לעריכת ביקורות תקופתיות שיאפשרו לו לוודא את קיומם של אמצעי האבטחה הנדרשים לפי הנוהל ואת תקינותם.

6 מערכת המידע המרכזית של אגף שיקום נכים, המקושרת למאגר המידע של נכי צה"ל.

סקרי סיכונים ומבדקי חדירות - אגף התקשוב לא ביצע סקרים לאיתור סיכוני אבטחת מידע במאגרי המידע שהם ברמת אבטחה גבוהה ולא ערך מבדקי חדירות למערכות של המאגרים האלה לצורך בחינת עמידותן בפני סיכונים פנימיים וחיצוניים, כפי שנדרש בתקנות הגנת הפרטיות (אבטחת מידע). אגף התקשוב ואגף הביטחון מבצעים סקרי סיכונים ומבדקי חדירות ברשתות ובמערכות מידע שונות במשרד הביטחון ובאתרי אינטרנט של משרד הביטחון שמפתחות חברות במיקור חוץ כדי לוודא שאין בהם חולשות אבטחה; אולם, אף גורם במשרד הביטחון לא ביצע סקרי סיכונים ומבדקי חדירות ייעודיים בנוגע ל-14 מאגרי המידע שמשרד הביטחון הוא בעל השליטה בהם - הוא לא זיהה, לא ניתח ולא העריך את התרחישים האפשריים להתממשות אירוע אבטחה במאגרים באופן פרטני או בשלבי התהליך העסקי שנוגע אליהם ואת סבירותם להתממש; הוא לא התבסס על מיפוי מאפייני מערכות המידע המעבדות מידע מהמאגרים; והוא לא כלל מיפוי של הבקרות הקיימות בארגון למול הבקרות שראוי ליישם למזעור הסבירות להתממשות הסיכונים. ממילא משרד הביטחון לא בחן את הצורך בעדכון מסמך הגדרות המאגר או בעדכון נוהל אבטחה למאגרי מידע; הוא לא קבע את הבקרות הנדרשות; ולא בחן את יעילות הבקרות ומנגנוני ההגנה הקיימים.

בהיעדר סקרי סיכונים ומבדקי חדירות למאגרי מידע אין למשרד הביטחון את הכלים להעריך את רמת הבשלות שלו להתמודדות עם איום לפגיעה בשלמות המידע האגור במאגרי המידע, בסודיות שלו ובזמינותו; לזהות את נקודות החולשה באבטחת המידע; לקבוע סדרי עדיפויות לטיפול בסיכונים אלו; להבין את הבקרות שעליו ליישם בתוכניות העבודה שלו; ולבחון את יעילות הבקרות ואת מנגנוני ההגנה הקיימים.

מינוי ממונה על אבטחת מידע במאגרי המידע שבמשרד הביטחון - בעקבות ביקורת זו מינה ראש אגף התקשוב ממונה חדשה על אבטחת המידע במאגרי המידע שבמשרד הביטחון והקנה לה סמכויות ותפקידים בהלימה לתקנות אבטחת מידע. זאת לאחר שעד אוקטובר 2024 ראש אגף התקשוב לא וידא שהממונה על אבטחת מידע במשרד הביטחון ממלאת את תפקידיה בהתאם לנדרש.

מיפוי מאגרים - בעקבות הביקורת, בדצמבר 2024, הנחה ראש אגף התקשוב את ראשי האגפים והיחידות במשרד הביטחון לבצע מיפוי של מאגרי המידע באגפיהם וביחידותיהם. יצוין כי הנחייתו נגעה רק למידע שהועבר ממשרד הביטחון לגורמים מחוץ למשרד או התקבל מהם. נכון למועד סיום הביקורת, ינואר 2025, טרם הסתיים המיפוי.

עיקרי המלצות הביקורת

על משרד הביטחון לעמוד בדרישות החלות עליו בהיבטי הגנת הפרטיות כמתחייב בחוק ובתקנות, ובפרט לאור תיקון 13 לחוק שייכנס לתוקף באוגוסט 2025 המתאים את החוק לאתגרים העכשוויים. כמו כן, נוכח הממצאים שעלו בניתוח הנתונים שביצע משרד מבקר המדינה, מומלץ כי משרד הביטחון יבדוק את תהליכי ניהול ההרשאות בכלל מערכות

המידע שמקושרות למאגרי המידע של משרד הביטחון. עוד מומלץ כי מנכ"ל משרד הביטחון יסדיר את תחומי האחריות והסמכות בין אגף התקשוב ובין אגף ביטחון בתחום אבטחת המידע במאגרי המידע בראי הגנת הפרטיות. זאת, כדי לצמצם את הסיכונים לפגיעה בפרטיות ולפגיעה במימוש ייעודו של משרד הביטחון.

- על ראש אגף התקשוב, המופקד על ניהול מאגרי המידע במשרד הביטחון, לוודא כי ביכולתה של הממונה על אבטחת המידע שבמאגרי המידע לבצע את תפקידה כנדרש, כי היא תקבל את ההכשרה הנדרשת, וכי יוקצו לנושא המשאבים הדרושים. על הממונה על אבטחת המידע במאגרי המידע שבמשרד הביטחון לממש את תפקידה כנדרש בתקנות ובכלל זה להכין תוכנית לבקרה שוטפת על העמידה בדרישות שבתקנות, לבצע את הבקרה ולהביא את ממצאיה לידיעתם של כלל הגורמים הנוגעים בדבר. על מנכ"ל משרד הביטחון למנות מפקח פרטיות כמתחייב בתיקון 13 לחוק הגנת הפרטיות שייכנס לתוקף באוגוסט 2025, לוודא כי קיימת חלוקת תפקידים ברורה בין הממונה על אבטחת המידע שבמאגרי המידע ובין מפקח הפרטיות שימונה במשרד הביטחון, ולעקוב אחר ביצוע תפקידם.

- על ראש אגף התקשוב להנחות את ראשי האגפים וראשי היחידות במשרד הביטחון לבצע מיפוי מלא של כלל המידע האישי שקיים אצלם, ולא רק בנוגע למידע שמועבר ממשרד הביטחון לגורמים מחוץ למשרד או מתקבל מהם. כמו כן, עליו לוודא כי המיפוי יתייחס גם לתקנות הגנת הפרטיות (הוראות לעניין מידע שהועבר לישראל מהאזור הכלכלי האירופי), התשפ"ג-2023. לאחר מכן, על ראש אגף התקשוב לזהות את הדרישות החלות על משרד הביטחון בהתאם לממצאי המיפוי, לרבות החובה לרשום אותם במרשם המאגרים.

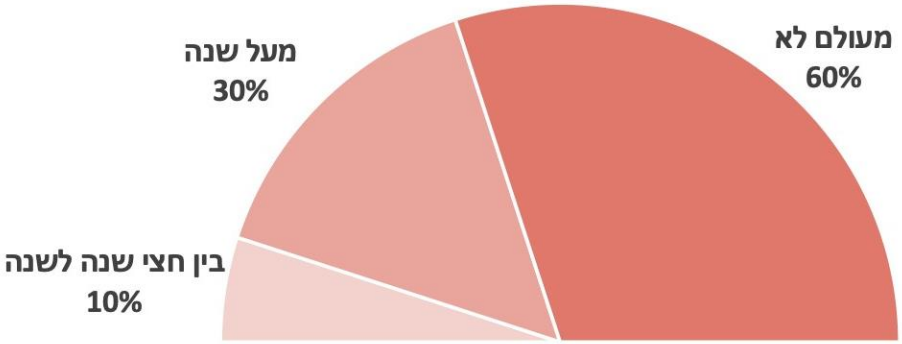
- על אגף התקשוב לבדוק באופן עיתי את כלל ההרשאות הקיימות במערכות המידע שמקושרות למאגרי המידע במשרד הביטחון, לרבות מערכת שמש שמקושרת למאגר נכי צה"ל, ולבטל הרשאות פעילות שאינן נחוצות למשתמשים לצורך מילוי תפקידם. כמו כן, מומלץ כי אגף התקשוב יבחן גם את תהליכי ניהול ההרשאות במערכות המידע. דבר זה יסייע לו לצמצם את הסיכון לחשיפת מידע אישי, לרבות מידע בעל רגישות מיוחדת, בפני מי שאינם מורשים לכך, וכן לצמצם את הסיכון לדלף של מידע זה, לפגיעה בזמינותו ולשיבושו; ובכך יפחת הסיכון לפגיעה בפרטיותם של האנשים שמידע אישי לגביהם שמור במאגרי המידע.

- מומלץ כי מנכ"ל משרד הביטחון יסדיר את תחומי האחריות והסמכות בתחום אבטחת המידע במאגרי המידע מתוקף חוק הגנת הפרטיות ותקנות אבטחת מידע, לדוגמה באמצעות מינוי גורם אחד שיישא באחריות הכוללת ויהיה בעל ראייה מתכללת בנוגע לכלל היבטי אבטחת המידע, לרבות בראי הגנת הפרטיות; באמצעות הקמת צוות בין-אגפי לחיזוק אבטחת המידע במאגרי המידע, שיכלול למשל נציגים מאגף ביטחון, מאגף התקשוב, מאגף היועץ המשפטי למערכת הביטחון ומאגפים שמשתמשים במאגרי המידע; או בכל דרך אחרת שימצא לנכון. עוד מומלץ כי חלוקת האחריות, הסמכות והתפקידים השונים, לרבות בהתייחס לתיקון 13 לחוק הגנת הפרטיות, יעוגנו בנוהל משרדי.

פוטנציאל הסיכון של משתמשים חיצוניים בעלי הרשאה שלא לצורך לרשת מחשב מרכזית של משרד הביטחון

שיעור המשתמשים החיצוניים שלא נכנסו לרשת יותר מחצי שנה מכלל המשתמשים החיצוניים בעלי הרשאת גישה פעילה לרשת

התפלגות מועד הכניסה האחרון של המשתמשים החיצוניים שלא נכנסו לרשת יותר מחצי שנה



על פי נתוני אגף התקשוב, בעיבוד משרד מבקר המדינה.

מאחר שרשת זו היא שער הכניסה למאגרי מידע, וקיימים בה נכסים, חלקם רגישים, וכן תשומות המשרתים תהליכים עסקיים ותהליכי הצטיידות של צה"ל, גובר הסיכון לחשיפת מידע רגיש בפני מי שאינם מורשים לכך, בייחוד משום ש-90% מהמשתמשים החיצוניים שלא נכנסו לרשת יותר מחצי שנה הם עובדי מיקור חוץ.

סיכום

משרד הביטחון הוא בעל שליטה במאגרים הכוללים מידע אישי, כגון נתונים על אישיותו של אדם, מצבו הבריאותי ומצבו הכלכלי. הסיכונים להגנת הפרטיות ולאבטחת המידע שבמאגרים אלו התגברו לנוכח מלחמת חרבות ברזל והתממשותם עלולה לפגוע ביכולתו של משרד הביטחון לספק את האמצעים הנדרשים לצה"ל, לגרום לו נזק תדמיתי, לפגוע ביחסיו עם ספקים ולקוחות ולחשוף אותו לקנסות. יתרה מכך, הדבר אף עלול לזרוע בהלה ותחושת חוסר ביטחון בציבור ולפגוע בקשרי החוץ של המדינה בהקשרים ביטחוניים-מדיניים.

בשנים האחרונות דָלַף מידע מתוך משרד הביטחון הן כתוצאה מתקיפות סייבר מצד גורמים חיצוניים עוינים והן כתוצאה מטעויות אנוש של עובדי המשרד, לרבות מידע מזהה על בעלי תפקידים במשרד הביטחון.

תמונת המצב העולה מדוח זה מצביעה על פערים חמורים באופן שבו משרד הביטחון מנהל את 14 מאגרי המידע שהוא בעל השליטה בהם ואת אבטחתם, ושבהם קיימים נתונים אישיים בנוגע ל-2.84 מיליון איש. בביקורת עלה כי אגף התקשוב, הנושא באחריות לקיים את הדרישות החלות על משרד הביטחון מתוקף חוק הגנת הפרטיות ותקנות אבטחת מידע, לא מיפה את כלל המאגרים שבבעלות משרד הביטחון משנת 2007, הוא לא קבע נוהל אבטחה למאגרי המידע, לא ביצע סקרים לאיתור סיכוני אבטחת מידע במאגרי המידע שהם ברמת אבטחה גבוהה ולא ערך מבדקי חדירות למערכות של המאגרים האלה לצורך בחינת עמידותן בפני סיכונים פנימיים וחיצוניים.

נוסף על כך, בדוח עלו ליקויים בנוגע לניהול הרשאות המשתמשים במערכת ניהול זהויות ובמערכת המידע המקושרת למאגר נכי צה"ל - מאגר שבו אגור מידע על אודות כ-230,000 אנשים ובהם גם כ-18,000 פצועים שנוספו אליו בשל מלחמת חרבות ברזל, לרבות מידע על מצבם הבריאותי, מצבם הכלכלי, בני משפחותיהם והשירותים הניתנים להם. מניתוח שביצע משרד מבקר המדינה עלה כי 5 מכל 10 משתמשים חיצוניים (עובדי מיקור חוץ) בעלי הרשאת גישה פעילה למערכת המידע המקושרת למאגר נכי צה"ל, לא נכנסו אליה יותר מחצי שנה. גם יועצים, שמנוהלים במערכות כוח האדם של משרד הביטחון בדומה לעובדי המשרד, לא נכנסו למערכת יותר מחצי שנה, ושיעורם מסך כל המשתמשים שלא נכנסו למערכת היה 20%. במצב זה עולה החשש כי הם בעלי הרשאות למאגר נכי צה"ל שלא לצורך.

על משרד הביטחון לעמוד בדרישות החלות עליו בהיבטי הגנת הפרטיות כמתחייב בחוק ובתקנות, ובפרט לאור תיקון 13 לחוק, שייכנס לתוקף באוגוסט 2025, המתאים את החוק לאתגרים העכשוויים. כמו כן, נוכח הממצאים שעלו בניתוח הנתונים שביצע משרד מבקר המדינה, מומלץ כי משרד הביטחון יבדוק את תהליכי ניהול ההרשאות בכלל מערכות המידע שמקושרות למאגרי המידע של משרד הביטחון. עוד מומלץ כי מנכ"ל משרד הביטחון יסדיר את תחומי האחריות והסמכות בין אגף התקשוב ובין אגף ביטחון בתחום אבטחת המידע במאגרי המידע בראי הגנת הפרטיות. זאת, כדי לצמצם את הסיכונים לפגיעה בפרטיות ולפגיעה במימוש ייעודו של משרד הביטחון.