דוח מבקר המדינה | סייבר ומערכות מידע | התשפ"ג-2022

צבא הגנה לישראל

ניהול מידע ביומטרי בצה"ל והגנת הסייבר עליו

ניהול מידע ביומטרי בצה"ל והגנת הסייבר עליו

רקע

מידע ביומטרי הוא מאפיין אנושי פיזיולוגי ייחודי, הניתן למדידה ממוחשבת. הסיכונים הנשקפים למאגר מידע ביומטרי הם משמעותיים, היות שלהבדיל מאמצעי זיהוי אחרים כמו תעודה, סיסמה או אמצעי פיזי - מידע ביומטרי אי אפשר לבטל או להחליף בעקבות גניבה או דלף של מידע.

המידע הביומטרי בצה"ל נאסף ממתגייסים, משמש לזיהוי חללים ונשמר בשלושה מאגרים של אמצעי זיהוי (מאגר טביעות אצבע וכף היד, מאגר תצלומי שיניים ואוסף כתמי דם). בתהליך ההרכשה שבשרשרת החיול (שר"ח) נוטלים מכל חייל המתגייס לצה"ל את אמצעי הזיהוי האלו: טביעת אצבעות ותצלומי שיניים. כמו כן, בהסכמת המתגייס, ניטלים מכל מתגייס גם כתמי דם המשמשים להפקת דגימת דנ"א בעת הצורך. תהליך זיהוי החלל מתבצע באמצעות השוואת הנתונים הביומטריים שניטלו מהמתגייס לאלו שניטלו מהחלל.

צה"ל נדרש לפעול בהתאם למדיניות ההגנה שלו בתחום הסייבר, לחוק הגנת הפרטיות, התשמ"א-1981, ולתקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017 (תקנות אבטחת מידע). לפי תקנות אבטחת מידע, מאגר מידע המכיל מידע ביומטרי ויש בו יותר מ-100,000 רשומות, נדרש לעמוד ברמת אבטחה גבוהה. התקנות מפרטות כיצד יש לשמור על רמת האבטחה שנקבעה למאגר.

בצה"ל קיימות שלוש מערכות מידע מרכזיות לניהול תהליך הזיהוי: מערכת א' ומערכת ב' המנהלות את מאגרי אמצעי הזיהוי הוגדרו על ידי צה"ל בסיווג סודי ונדרשות לעמוד ברמת אבטחה גבוהה בהתאם לתקנות אבטחת מידע. מערכת מידע נוספת בשם מערכת ג' מנהלת ומתעדת את הטיפול בחלל ובכלל זה את תהליך זיהוי החלל. קצין אמצעי הלחימה (אמל"ח) במפקדת קצין משאבי אנוש ראשי (מקמש"ר) באגף כוח אדם (אכ"א) הוא מנהל הפרויקט של מערכות אמצעי הזיהוי שאחראי גם לגיבוש מענה הגנת הסייבר של המערכות. ענף תכלית ביחידת שחר אחראי לפיתוח ולתחזוקה של המערכות. המשתמשים העיקריים במערכות הם יחידת מיטב (בתהליך ההרכשה) וענף זיהוי וקבורה (זו"ק) ברבנות הצבאית (בתהליך זיהוי החלל).

להלן תרשים המציג את אמצעי הזיהוי ואת המידע הנשמר בהם:

מערכת א'
- טביעות עשר אצבעות הידיים
- טביעת כף יד של שתי הידיים

מערכת ב'
- תצלומי שיניים: אופטי ורנטגן
- מיקום כתמי הדם

אוסף כתמי דם
- כתמי דם שמהם ניתן להפיק דנ"א

נתוני מפתח

3 מערכות מידע
מנהלות את אמצעי הזיהוי

מאות אלפים
רשומות של טביעות אצבע שמורות במאגר אמצעי הזיהוי של צה"ל

7 שנים
מספר השנים שחלפו מאז עודכנה מדיניות ההגנה של צה"ל

26 שנים
לא עודכנו פקודות מטכ"ל בנושא הגנת הפרטיות, ולכן הן אינן מתייחסות לתקנות אבטחת מידע משנת 2017

0
מספר סקרי הסיכונים ומספר מבדקי החדירה שנעשו לבחינת מצב ההגנה של מערכות אמצעי הזיהוי מאז הקמתן בשנים 2006 - 2005 (לפני כ-16 שנים)

50%
2 מתוך 4 עמדות ההרכשה לאיסוף תצלומי חלל הפה בשר"ח מושבתות מאוגוסט 2021 (יותר מחצי שנה)

95%
מתצלומי השיניים של חלל הפה הקיימים במאגר אמצעי הזיהוי נמצאו באיכות שאינה מספקת

1 מכל 87
ממשרתי החובה והקבע כיום (1.15%) הרכיש רק אמצעי זיהוי אחד, דבר שמעלה חשש ליכולות הזיהוי שלו

פעולות הביקורת

בחודשים אוגוסט 2021 - אפריל 2022 בדק משרד מבקר המדינה את נושא "ניהול מידע ביומטרי בצה"ל והגנת הסייבר עליו". הביקורת נעשתה בצה"ל: באכ"א - בענף אסטרטגיה, דיגיטל ומערכות (אד"ם) ובמקמש"ר; במדור קליטה ומיון - ביחידת מיטב; ביחידת שחר - בענף תכלית; ברבנות הצבאית - בענף זו"ק. בדיקות השלמה נעשו בעמותה א', וברשות להגנת הפרטיות שבמשרד המשפטים.

הדוח שבנדון הומצא לראש הממשלה ביום 31.7.2022 והוטל עליו חיסיון עד לדיון בוועדת המשנה של הוועדה לענייני ביקורת המדינה.

מתוקף הסמכות הנתונה למבקר המדינה בסעיף 17(ג) לחוק מבקר המדינה, התשי"ח-1958 [נוסח משולב], ובשים לב לנימוקי הממשלה, לאחר היוועצות עם הגופים האמונים על אבטחת המידע הביטחוני ובתיאום עם יו"ר הכנסת, משלא התכנסה ועדת המשנה של הוועדה לענייני ביקורת המדינה בכנסת, הוחלט לפרסם דוח זה תוך הטלת חיסיון על חלקים ממנו. חלקים אלה לא יונחו על שולחן הכנסת ולא יפורסמו.

ממצאי דוח הביקורת והמלצותיו נכונים למועד המצאתו האמור לעיל.

תמונת המצב העולה מן הביקורת

מדיניות ההגנה בתחום הסייבר - מסמך מדיניות ההגנה של צה"ל כולל התייחסות לחלק מהנושאים שהיחידה להגנת הסייבר בממשלה (יה"ב) הגדירה שיש לכלול במסמך מדיניות להגנת הסייבר, כגון: הגנת רשומות, הגנה לוגית ופיזית והמבנה הארגוני, אך אינו כולל התייחסות לנושאים כגון ניהול וסיווג של נכסים, שרשרת האספקה, משאבי אנוש והתאמה לדרישות החוק (כמו תקנות אבטחת מידע). כמו כן, מסמך מדיניות ההגנה לא עודכן מאפריל 2015, במשך שבע שנים, שבמהלכן חלו שינויים טכנולוגיים וכן חלו שינויים בחובות החלות על צה"ל בנושא אבטחת מידע בעקבות פרסום תקנות הגנת הפרטיות (אבטחת מידע) משנת 2017.

מענה הגנה בתחום הסייבר - מערכת א' ומערכת ב' הוגדרו בסיווג סודי עם חסינות בינונית למרות שמערכות אלו נדרשות לעמוד ברמת אבטחה גבוהה לפי תקנות אבטחת מידע, ולמרות הנזק הרב שעלול להיגרם מדליפת מידע ביומטרי רגיש שמוחזק במערכות אלו. כמו כן למערכות אמצעי הזיהוי של צה"ל אין מענה הגנה מפורט במסמך הכולל את דרישות ההגנה הייעודיות למערכות אלו בהתאם לסיווג שלהן.

ממונה על אבטחת מידע - בצה"ל יש כמה גורמים העוסקים בהיבטים שונים בתחום אבטחת המידע של מערכות מידע, ובהם: יחידת הגנת הסייבר במרכז המחשבים ומערכות המידע (ממר"ם), מחלקת ביטחון מידע (מחב"ם), קצין האמל"ח וגורמי מדיניות ההגנה באגף התקשוב. אולם אין גורם אחד שנושא באחריות לכל היבטי אבטחת המידע של

מערכות אמצעי הזיהוי ותפקידו ותחומי אחריותו הוגדרו בהתאם לתקנה 3 בתקנות אבטחת מידע ובהתאם למדיניות ההגנה של צה"ל.

- **עמידה בתקנות אבטחת מידע** - אין בידי אכ"א תוכנית לבקרה שוטפת על מידת העמידה של מאגרי אמצעי הזיהוי בדרישות תקנות אבטחת מידע, וכן לא בוצעו ביקורות בנושאים אלו. עוד נמצא כי פקודות המטכ"ל בנושא הגנת הפרטיות לא עודכנו ממועד כתיבתן בשנת 1996 (פרק זמן של 26 שנים), לכן הן אינן מתייחסות לתקנות אבטחת מידע שפורסמו בשנת 2017. כמו כן הרשות להגנת הפרטיות לא ביצעה ביקורות ופעולות פיקוח רוחביות על מאגרי המידע בצה"ל בכלל ועל המאגרים הביומטריים לזיהוי חללים בפרט, כדי לוודא שהמאגרים עומדים בתקנות אבטחת המידע. זאת אף שצה"ל מחזיק במאגרי מידע שבהם שמור מידע רגיש ואישי על אזרחים רבים.

- **מסמך הגדרות מאגר מידע** - צה"ל לא גיבש מסמך הגדרות למאגרי אמצעי הזיהוי כנדרש בתקנות אבטחת מידע, הכולל מידע חיוני הקשור למאגרים ולאופן השימוש בהם, כמו פירוט הסיכונים העיקריים של פגיעה באבטחת המידע ואופן ההתמודדות עימם.

- **מידע עודף** - צה"ל לא בחן אחת לשנה כנדרש בתקנות אם שמור מידע עודף במאגרי אמצעי הזיהוי. במאגרי אמצעי הזיהוי קיים מידע עודף, למשל: מידע ביומטרי על חיילים אשר הלכו לעולמם (נפטרו) ואשר לא בוצע לגביהם תהליך זיהוי. מידע ביומטרי על נפטרים עלול לשמש ביתר קלות למטרת התחזות וגנבת זהות, שכן אין מי שיתלונן על השימוש שנעשה בו.

- **הגנה פיזית** - צה"ל לא גיבש נוהל אבטחה פיזית ייעודי למערכות אמצעי הזיהוי כנדרש בתקנה 4 לתקנות אבטחת מידע, זאת אף ששמור בהן מידע ביומטרי, אישי ורגיש החייב ברמת אבטחה גבוהה. כמו כן נמצאו פערים ברמת האבטחה הפיזית של המערכות ביחידה א' בנושאים: הגנה פיזית ובקרה על הכניסות והיציאות, הגנת סביבת העבודה והגנה סביבתית.

- **הגנה לוגית** - נמצאו פערים ברמת ההגנה הלוגית בנושאים שלהלן: הזדהות; הרשאות גישה; סקר בקרת גישה; בקרה על ביצוע פעולות לא מורשות; מנגנוני הצפנה; בקרה שוטפת לצורך תהליכי הגנה על יישומים.

- **המשכיות עסקית** - צה"ל לא פיתח לתהליך אמצעי הזיהוי תוכנית המשכיות עסקית שמכסה את כל התהליכים הקשורים לאמצעי הזיהוי ואת כל היחידות המעורבות בתהליכים אלו ולא הגדיר מהם החלקים בתהליך שהם קריטיים לאירוע חירום. כמו כן הוא לא ביצע תרגול הפעלה במתכונת חירום של כל המערך הנדרש לזיהוי חלל. זאת ועוד נמצאו הפערים האלה: צה"ל לא וידא כי המערכות נגישות באופן קבוע מאתרים חלופיים שנקבעו מראש; ביחידת ממר"ם לא נעשו תרגולים עיתיים של אחזור מגיבויים כדי לבדוק את תקינותם ואת העמידה ביעד אחזור הנתונים; האוסף הפיזי של כתמי הדם נשמר במקום יחיד ואין יתירות למידע שבו על ידי שמירתו במקום נוסף.

- **שלמות אמצעי הזיהוי** - מאגר הנתונים הביומטריים של צה"ל המכיל מאות אלפי רשומות אינו שלם. במאגר קיימות כמה עשרות אלפי רשומות של משרתי חובה וקבע שנכון למועד סיום הביקורת באפריל 2022, חסרים בהן אמצעי הזיהוי האלו: 0.5% מטביעות האצבע, 6.6% מתצלומי הרנטגן, 32.8% מתצלומי חלל הפה ו-3.8% מדגימות הדנ"א. כמו כן יש

חוסרים של מאות טביעות אצבע של חיילים שהתגייסו בשנים 2016 ו-2017 ושל כמה אלפי תצלומי שיניים עבור אנשי קבע שהתגייסו בשנים 1994 - 2004. נוסף על כך, מצא מדור זיהוי רפואי בביקורות שביצע בשנים 2018 - 2019 כי כ-95% מתצלומי השיניים של חלל הפה הם באיכות שאינה מספקת. איכות ההרכשה הירודה של תצלומי השיניים לא טופלה עד מועד סיום הביקורת באפריל 2022.

מתודולוגיה לניהול פרויקטים - המתודולוגיה לניהול פרויקטים בצה"ל (הק"א 10/1) שפרסם אגף תכנון אינה ייעודית לניהול פרויקטי מערכות מידע ועקב כך אינה כוללת התייחסות מפורטת לנושאי חובה שנדרשים במתודולוגיות מקובלות לניהול פרויקטי מערכות מידע. כמו כן המתודולוגיה אינה כוללת כלי עזר שיסייעו לגופים ביישומה: תקנים, קווים מנחים, נוהלי עבודה ותבניות אחידים בתחום ניהול הפרויקטים. זאת ועוד, המתודולוגיה לא כוללת התייחסות לניהול פרויקטים לפי השיטה "הזמישה"[1] אף שצה"ל מפתח מערכות לפי מתודולוגיה זו, למשל: מערכת ב' החדשה.

ניהול פרויקטים - במערכות אמצעי הזיהוי אין מסמכי יסוד כמו מסמכי דרישות מפורטים או תוצרי ביניים הנדרשים בתהליכי עבודה לפי מתודולוגיות מקובלות לניהול פרויקטי מערכות מידע ולפי הק"א 10/1, ללא מסמכי יסוד ותוצרי ביניים אלו נשקף סיכון שהמערכות המפותחות אינן תואמות לדרישות המשתמשים.

מנהל פרויקט - מערכות אמצעי הזיהוי לא נוהלו לפי מתודולוגיות מקובלות לניהול פרויקטים, ובכלל זה נמצאו פערים בנושאים האלו, אשר מנהל פרויקט אחראי להם: הכנת תוכניות עבודה ומעקב אחר ביצוען ניהול ושיתוף של הלקוח, העלאת הפרויקטים לדיון בישיבות של וועדות היגוי, ניהול סיכונים, ניהול שינויים וניהול תקלות.

זיהוי חללים בהתרחש אסון רב נפגעים (אר"ן) מעורב של אזרחים וחיילים - לא הוסדר השימוש במרכז איסוף נתוני חללים ("מרכז הצבי") של הרבנות הצבאית בהתרחש אר"ן מעורב של אזרחים וחיילים; כמו כן, אף שצה"ל מחזיק במאגר ובו מאות אלפי רשומות של אזרחים וחיילים הכולל אמצעי זיהוי ייחודיים כדוגמת טביעות עשר אצבעות וכן כפות ידיים, לא הושלמה הבחינה של אפשרות השימוש במאגרי אמצעי הזיהוי המוחזקים בצה"ל לצורך זיהוי חללים בהתרחש אר"ן.

הגברת ממשקי העבודה של צה"ל עם הרשות להגנת הפרטיות - במהלך שנת 2021 החל צה"ל, בשיתוף הרשות להגנת הפרטיות, בגיבוש תוכנית עבודה כוללת שתיתן מענה על נושאים שונים ובהם: מינוי ממונה הגנת הפרטיות ביחידות השונות, הסברה פנים-צה"לית בנושא חיזוק תפיסת הגנת הפרטיות בצה"ל, הכללת נושא הגנת הפרטיות בין שאר הנושאים שעליהם חלה הביקורת שמבצע אכ"א ותיקון פקודות מטכ"ל.

1 הלחם של המילים "זריזה" ו"גמישה" (Agile).

מיקור חוץ - במהלך הביקורת צה"ל נקט בפעולות כדי לוודא שיש לחברה ב', המספקת תמיכה טכנית למערכת א', גישה מאובטחת למערכות אמצעי הזיהוי וכדי לבקר גישה זו.

השלמת חוסרים באמצעי הזיהוי - בתקופה שבין הגיוסים בחודשים פברואר-מרץ 2022 צה"ל החל בהרכשת אמצעי זיהוי מהלוחמים בשטח באמצעות תחנה ניידת ובה עמדות הרכשה שהושאלו מהשר"ח.

עיקרי המלצות הביקורת

- מומלץ כי הממונה על היישומים הביומטריים יציג לצה"ל את מסמך ההסדרה שגיבש בדצמבר 2015 עם מחב"ם בצה"ל ויבחן יחד עמו את הצורך בעדכונו בהלימה למתכונת העבודה שהוסדרה עם גופים מיוחדים דומים.

- מומלץ כי מרכז צופן וביטחון (מצו"ב) בחטיבת ההגנה יעדכן את מסמך מדיניות הגנת הסייבר כך שיכלול את הנושאים המפורטים במסמכי מדיניות מקובלים בתחום הגנת הסייבר כמו ההנחיה בנושא מדיניות של יה"ב, וכן יעדכן אותה באופן עתי בהתאם לשינויים הטכנולוגיים ולסיכונים בתחום, באופן שיעמדו בדרישות החוק והתקנות הרלוונטיים.

- מומלץ כי מחב"ם יבחן מחדש ויתקף באופן עתי את סיווג מערכות אמצעי הזיהוי באופן שיביא בחשבון את הסיכונים העדכניים הנשקפים למידע שמוחזק במאגרים אלו וכן את הסיכון שקיים לנושאי המידע כתוצאה מדלף מידע. על מקמש"ר לוודא שעקרונות מדיניות ההגנה מעוגנים במסמך מענה הגנה וכן מיושמים במערכות אמצעי הזיהוי הנמצאות בשלבי פיתוח ותחזוקה. כמו כן, מומלץ שמדי שנה מקמש"ר יוודא שמענה ההגנה של המערכות מאפשר להתמודד באופן הולם עם הסיכונים הנשקפים באותה עת ועם תרחישי האיום העדכניים.

- מומלץ כי צה"ל ימנה ממונה אבטחת מידע האחראי למערכות אמצעי הזיהוי כנדרש בחוק הגנת הפרטיות ובתקנות אבטחת מידע.

- על אכ"א להכין תוכנית לבקרה שוטפת על מידת העמידה של המאגרים בתקנות אבטחת מידע ולוודא את ביצועה אחת לשנתיים או במסגרת סקר סיכונים. עוד מומלץ כי אכ"א בשיתוף אגף התקשוב יפעלו להשלמת עדכון פקודות המטכ"ל בנושא הגנת הפרטיות.

- מומלץ כי בד בבד עם הליך תיקון החקיקה המתקיים תפעל הרשות להגנת הפרטיות להסדיר את יכולת הפיקוח והאכיפה על מאגרי המידע שברשות צה"ל, ובכללם מאגרי אמצעי הזיהוי. עוד מומלץ כי אכ"א בשיתוף הרשות להגנת הפרטיות יפעלו להוציא לפועל את תוכנית העבודה שגובשה כתוצאה מהפגישה במאי 2021, ובכלל זה יקדמו את ההדרכות בצה"ל בנושא עמידה בתקנות אבטחת מידע ויגבשו תוכנית להכשרת בעלי תפקיד שיוכלו לשמש מפקחים פנימיים בתוך צה"ל.

- על צה"ל לפעול לכתיבת נוהל אבטחה פיזית, כנדרש בתקנות אבטחת מידע. כמו כן על יחידה א' בשיתוף גורמי אבטחת המידע בצה"ל, לפעול למיגון המתחם שנבדק בביקורת.

- מומלץ כי ממונה אבטחת מידע בשיתוף מחב"ם יפעלו לצמצום הפערים שנמצאו ברמת ההגנה הלוגית.

- מומלץ כי צה"ל יגבש תוכנית התאוששות עסקית לתהליך אמצעי הזיהוי ובמסגרתה יבחן את מכלול התהליכים, הסיכונים וההשלכה של התממשותם, ויגדיר את רמת המענה שניתן לכל סיכון. עוד מומלץ כי צה"ל יערוך באופן עיתי תרגולי חירום כך שיכוסו כל התהליכים הקשורים לאמצעי הזיהוי וכל היחידות המעורבות בתהליכים אלו.

- מומלץ כי אכ"א יגביר את פעולתו לצמצום הפערים בהרכשת אמצעי הזיהוי החסרים, תוך תיעדוף ההשלמות לפי אופי שירותם של החיילים (שירות קרבי, רמות סיכון וכיו"ב), סוג אמצעי הזיהוי (טביעות אצבע) ומספר הפעמים שנקראו להשלמה. במסגרת המאמץ לצמצום הפערים מומלץ לקדם את היוזמה להפעלת תחנה ניידת להרכשת אמצעי זיהוי, בכלל זה תצלומי שיניים.

- מומלץ כי אכ"א יפעל בשיתוף אגף תכנון לעדכון הנהלים הרלוונטיים לניהול פרויקטי מערכות מידע (10/01 ו-10/6), באופן שיכללו התייחסות מפורטת לנושאי החובה הנדרשים במתודולוגיות מקובלות לניהול פרויקטי מערכות מידע ולהתאמת המתודולוגיה לניהול פרויקטים בשיטה "הזמישה". עוד מומלץ כי יגובשו כלי עזר ליישום המתודולוגיה ותבחן הקמת גוף תומך לניהול פרויקטים (כמו PMO) שייתן מענה לצורך זה.

- מומלץ כי מקמש"ר תנהל את מערכות אמצעי הזיהוי בהתאם למתודולוגיות מקובלות לניהול פרויקטי מערכות מידע, ובהתאם להק"א 10/1, ותגבש את מסמכי העבודה הנדרשים לפי מתודולוגיות אלו. על אכ"א לגבש תוכנית מסודרת להגדרת תחומי אחריותו של מקמש"ר כמנהל הפרויקט של מערכות אמצעי הזיהוי, לקראת השלבים הבאים בפיתוח המערכות ולפעול ליישומה לפי מתודולוגיות מקובלות.

- מומלץ כי רשות החרום הלאומית (רח"ל) בשיתוף הרשות לפינוי, לסעד ולטיפול בחללים בשעת חרום (פס"ח) יבחנו את המענה הקיים ואת המענה הדרוש לנושא זיהוי חללים בהתרחש אירוע רב נפגעים (אר"ן), יסדירו את חלוקת האחריות בין הגופים השונים ויפעלו לקידום השימוש במרכז הצבי כתחנת ריכוז חללים לאומית בהתרחש אר"ן. במסגרת זו מומלץ לבחון את ההיתכנות של הסתייעות במאגר של צה"ל ובמאגרים אחרים לשם זיהוי חללים בהתרחש אר"ן. מומלץ כי הנושא ייבחן בשיתוף נציגי הרשות להגנת הפרטיות ונציגי צה"ל: אכ"א, הרבנות הצבאית ונציגי הפרקליטות הצבאית.

הסיכונים הנשקפים למאגרי אמצעי הזיהוי

עמידת מאגרי אמצעי הזיהוי בדרישות תקנות אבטחת מידע

תקנה	נושא	ממצאי הביקורת
2	מסמך הגדרות המאגר	לא קיים
3	ממונה על אבטחת מידע	לא מונה
4	נוהל אבטחה	לא קיים
5	מיפוי מערכות המאגר וביצוע סקר סיכונים	קיים חלקית
6	אבטחה פיזית וסביבתית	קיים חלקית
7	אבטחת מידע בניהול כוח אדם	קיים חלקית
8	ניהול הרשאות גישה	קיים חלקית
9	זיהוי ואימות	קיים חלקית
10	בקרה ותיעוד גישה	קיים חלקית
11	תיעוד של אירועי אבטחה	קיים חלקית
12	התקנים ניידים	קיים
13	ניהול מאובטח ומעודכן של מערכות המאגר	קיים חלקית
14	אבטחת תקשורת	קיים
15	מיקור חוץ	קיים
16	ביקורות תקופתיות	לא קיים

סיכום

צה"ל מנהל מערכות מידע של אמצעי זיהוי שמטרתן לזהות חללים. מדובר במערכות שבאמצעותן מנוהלים מאגרי מידע ביומטריים הכוללים מידע רפואי, אישי ורגיש, ולכן נדרש כי רמת האבטחה של המאגרים תהיה גבוהה לפי תקנות אבטחת מידע.

ממצאיו של דוח זה משקפים פערים משמעותיים באבטחת המידע המצוי במערכות רגישות אלו, וכן הם מעידים על אי-קיום חלק מתקנות אבטחת מידע ועל אי-יישום דרישות שנכללו במסמכי מדיניות הגנת סייבר. מצב זה יוצר סיכון לפגיעה באמינות (שלמות), בזמינות ובסודיות של המידע שבמאגרים.

הדוח כולל ממצאים נוספים הנוגעים להליכי תפעול וניהול של מערכות המידע של אמצעי הזיהוי. בין היתר נמצא כי מערכות המידע אינן מנוהלות ביעילות ולפי מתודולוגיה סדורה לניהול פרויקטי מערכות מידע, ועקב כך יש חשש שמערכות אמצעי הזיהוי לא יוכלו למלא את ייעודן. כמו כן נמצא כי מנהל הפרויקט לא הכין תוכניות עבודה למערכות אמצעי הזיהוי ולא וידא שהקמתן וניהולן של המערכות עומדים ביעדים המקובלים של תכולה, לוחות זמנים, עלויות ושביעות רצון הלקוח.

על ראש אכ"א לפעול לתיקון הליקויים ולבחון את ההמלצות שבדוח זה.

ניהול מידע ביומטרי בצה"ל והגנת הסייבר עליו

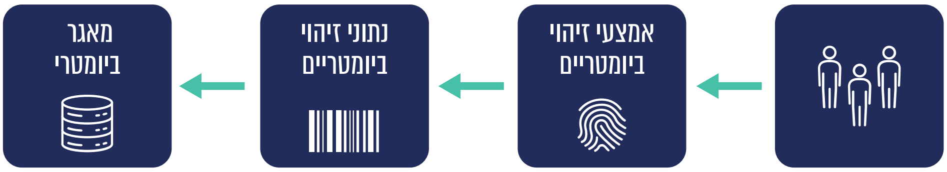
מבוא

מידע ביומטרי

על פי חוק הכללת אמצעי זיהוי ביומטריים ונתוני זיהוי ביומטריים במסמכי זיהוי ובמאגר מידע, התש"ע-2009 (להלן - חוק המאגר הביומטרי), ותקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017 (להלן - תקנות אבטחת מידע), מידע ביומטרי הוא מידע המשמש לזיהוי אדם, שהוא מאפיין אנושי פיזיולוגי ייחודי, הניתן למדידה ממוחשבת.

חוק המאגר הביומטרי מבחין בין "אמצעי זיהוי ביומטריים" לבין "נתוני זיהוי ביומטריים" (להלן - מידע ביומטרי) המופקים מהם אשר ניתן לעשות בהם שימוש לזיהוי. מידע ביומטרי עשוי להיות מופק מאמצעי זיהוי ביומטריים שהם תכונות פיזיולוגיות, כדוגמת טביעת אצבע, טביעת כף יד, תמונת פנים, תמונת קשתית העין, תמונת הרשתית של העין ודנ"א, או תכונות התנהגותיות כגון אופן הליכה, חתימת קול וקצב הקלדה. מידע ביומטרי יכול להישמר באמצעי אחסון כמו תעודה או במאגר מידע.

תרשים 1: **תהליך הקמת מאגר מידע ביומטרי**



בעיבוד משרד מבקר המדינה.

זיהוי ביומטרי הוא אמצעי מהימן ביותר לזיהוי אדם. הזדהות ביומטרית משמשת בין היתר לכניסה לחשבון הבנק ולביצוע פעולות, לכניסה למקום העבודה ולמגוון יישומים רבים אחרים. צריכת שירותים רבים המסופקים כיום לאזרחי מדינת ישראל מותנית בהזדהות של מבקש השירות.

הסיכונים הנשקפים למאגר מידע ביומטרי הם משמעותיים, היות שלהבדיל מאמצעי זיהוי אחרים כמו תעודה, סיסמה או אמצעי פיזי - מידע ביומטרי אי אפשר לבטל או להחליף בעקבות גנבה או דלף מידע. כמו כן, מידע ביומטרי כמעט אינו משתנה במהלך חייו של אדם (ראו פירוט בפרק הסיכונים למידע ביומטרי).

לפי תקנות אבטחת מידע[2], מאגר מידע המכיל מידע ביומטרי ויש בו יותר מ-100,000 רשומות נדרש לעמוד ברמת אבטחה גבוהה. התקנות מפרטות כיצד יש לשמור על רמת האבטחה שנקבעה למאגר.

מערכות המידע בצה"ל המשמשות לזיהוי חללים

בצה"ל קיימים מאגרים ביומטריים המשמשים לזיהוי חללים. על פי חוק שירות ביטחון (נוסח משולב), התשמ"ו-1986 ותקנות שירות ביטחון (אמצעי-זיהוי), התשמ"ט-1989, יש ליטול ממועמד לשירות ביטחון המתגייס לצה"ל את אמצעי הזיהוי האלו: טביעת אצבעות ותצלומי שיניים. כמו כן, בהסכמת המתגייס ובהסתמך על פקודת ארגון (להלן - פק"א) הרבנות הצבאית, ניטלים מכל מתגייס גם כתמי דם המשמשים להפקת דגימת דנ"א בעת הצורך.

בצה"ל קיימות שלוש מערכות מידע מרכזיות לניהול תהליך הזיהוי (להלן - מערכות אמצעי הזיהוי):

1. **מערכת א':** תוכנת מדף, שנרכשה בשנת 2006 והותאמה לדרישת צה"ל. המערכת משמשת לשמירה של טביעות האצבע של המתגייסים וכן להשוואה בין טביעת האצבע של החלל לטביעות הקיימות במערכת. נכון לפברואר 2022 יש במאגר המידע של המערכת מאות אלפי רשומות, לכן זהו מאגר הנדרש לעמוד ברמת אבטחה גבוהה על פי תקנות אבטחת מידע.
2. **מערכת ב':** מערכת בפיתוח עצמי של צה"ל שהוכנסה לפעולה (להלן - מבצוע) בשנת 2005. המערכת משמשת, בין היתר, לשמירת תצלומי השיניים. נכון לפברואר 2022 יש במאגר המידע מאות אלפי רשומות, לכן זהו מאגר הנדרש לעמוד ברמת אבטחה גבוהה על פי תקנות אבטחת מידע. במערכת זו צפוי להתבצע שדרוג טכנולוגי ושינויים בממשק המשתמש בשנת 2022 (להלן - מערכת ב' החדשה).
3. **מערכת ג':** מערכת בפיתוח עצמי של צה"ל. המערכת מובצעה בדצמבר 2021. מטרת המערכת היא לנהל ולתעד את הטיפול בחלל ובכלל זה את תהליך זיהוי החלל. במערכת זו צפויים שינויים ושיפורים במהלך החציון השני של שנת 2022.

נוסף על מערכות אלו, בצה"ל שמור אוסף פיזי של כתמי דם. במערכת ב' נמצא קישור למיקום כתם הדם באוסף הפיזי.

2 תקנה 1, תוספת ראשונה ותוספת שנייה בתקנות אבטחת מידע.

להלן פירוט הפרויקטים במערכות אמצעי הזיהוי, השלב במחזור החיים שבו הן נמצאות ומועדי ההתחלה והסיום הצפוי שלהם:

לוח 1: **הפרויקטים במערכות אמצעי הזיהוי**

הפרויקט	שלב במחזור החיים	מועד תחילת הפרויקט	מועד מבצוע
מערכת ב'	תחזוקה	2005	אין - מערכת בתחזוקה
מערכת א'	תחזוקה	2006	אין - מערכת בתחזוקה
שדרוג מערכת ב' (מערכת ב' החדשה)	בדיקות (לפני מבצוע)	יולי 2021	יוני 2022 (מתוכנן)
מערכת ג' שלב א'	תחזוקה	תחילת 2018	אין - מערכת בתחזוקה
השלמות למערכת ג' שלב א'	אפיון	יולי 2022	סוף 2022 (מתוכנן)

להלן יוצגו אמצעי הזיהוי הביומטריים הניטלים לצורכי זיהוי חלל ומאגרי המידע שהם נשמרים בהם:

תרשים 2: **מאגרי אמצעי הזיהוי**

בעיבוד משרד מבקר המדינה.

הגורמים המנהלים את מערכות אמצעי הזיהוי בצה"ל

הגורמים העיקריים בצה"ל המעורבים בניהול מערכות אמצעי הזיהוי הם:

1. **אגף כוח אדם (להלן - אכ"א)**

   א. **מפקדת קצין משאבי אנוש ראשי (להלן - מקמש"ר):** קצין אמצעי הלחימה (אמל"ח) במקמש"ר אחראי לאפיון הדרישות של המערכות לניהול אמצעי הזיהוי, ניהול הפרויקטים להקמתן ולתחזוקתן של מערכות אלו והגדרת מענה הגנת הסייבר של המערכות.

   ב. **ענף אסטרטגיה, דיגיטל ומערכות מידע (להלן אד"ם):** אחראי בין היתר להגדרת האסטרטגיה של מערכות המידע באכ"א, היבטי הגנת הפרטיות של המידע הנשמר במאגרים, הגדרת יכולת ההתאוששות העסקית של מערכות המידע ותכנון טכנולוגיות חדשות והשוואה לטכנולוגיות בשוק האזרחי.

2. **ענף תכלית ביחידת שחר:** הענף מוגדר כקצין הפרויקט ואחראי לתכנון, פיתוח ותחזוקה של מערכות אמצעי הזיהוי.

3. **יחידת מיטב בבסיס קליטה ומיון:** היחידה אחראית להרכשת אמצעי הזיהוי במסגרת שרשרת החיול (להלן - שר"ח).

4. **הרבנות הצבאית, ענף זיהוי וקבורה (להלן - זו"ק):** הענף אחראי לזיהוי חללים. עובדי הענף הם המשתמשים העיקריים במערכות אמצעי הזיהוי.

תהליכי העבודה

ניהול אמצעי הזיהוי נחלק לשני תהליכים עיקריים: הרכשה וזיהוי חלל. להלן יתוארו התהליכים והגורמים העיקריים בצה"ל המעורבים בביצועם:

תרשים 3: **תהליכי ניהול אמצעי הזיהוי**

בעיבוד משרד מבקר המדינה.

תהליך הרכשה של אמצעי זיהוי

יחידת מיטב מרכישה את אמצעי הזיהוי במהלך יום הגיוס במסגרת השר"ח. כל אמצעי זיהוי ניטל בתחנת הרכשה נפרדת, ובכל תחנה יש כמה עמדות הרכשה. המתגייס מזדהה בכל תחנה באמצעות סריקת מדבקת ברקוד ובה פרטיו האישיים. בסיום תהליך ההרכשה מתבצע תהליך של בקרת איכות שמטרתו לוודא כי אמצעי הזיהוי יוכלו לשמש לזיהוי בעת הצורך.

תהליכי ההרכשה ובקרת האיכות מתבצעים בהתאם לאמצעי הזיהוי:

1. **טביעות אצבע:** הרכשת טביעות אצבע מתבצעת באמצעות קוראים אופטיים[3]. טביעות באיכות שהוגדרה על ידי הרבנות כמספקת (הכוללות לפחות 12 נקודות זיהוי) מועברות במישרין למערכת א' (תמונה ונקודות זיהוי). טביעות אצבע שמזוהות במערכת ככאלו שאינן באיכות מספקת (כ-30%) עוברות תהליך טיוב במעבדת טביעת אצבע על ידי חייל בתפקיד

3 עם טביעת האצבעות ניטלת גם תמונת הפנים, שלא למטרת זיהוי חללים.

"מקודד". אם הטיוב הצליח נשמרת במאגר טביעת האצבע המטויבת. טביעות אשר לא הצליחו לטייבן (כ-0.2% מהטביעות) מסומנות כחסרות לצורך ביצוע הרכשה חוזרת.

2. **תצלומי שיניים:** הרכשת תצלומי השיניים מתבצעת בשתי תחנות נפרדות: צילום רנטגן וצילום אופטי של חלל הפה. התמונות מועברות באופן מיידי לשרתי האחסון, ומדור זיהוי רפואי ברבנות מבצע בקרת איכות ידנית באופן מדגמי, לפי כמה קריטריונים הבוחנים את איכות התצלום. ממצאי בקרת האיכות משמשים בסיס ללמידה ולשיפור בתהליך ההרכשה.

3. **כתמי דם:** דגימות דם ניטלות מן המתגייסים על גבי כרטיס FTA[4] פיזי ומשונעות לאוסף כתמי הדם הנמצא בארכיון צה"ל. בדיקת איכות ראשונית מתבצעת באוסף כתמי הדם כדי לוודא כי כתם הדם ממלא כ-80% משטח העיגול המוקצה לכך, וכי יש חתימה של המתגייס בכרטיס ה-FTA. אם נמצאו בבדיקה דגימות כתמי דם לא תקינות, הן מסומנות במערכת ב' כחסרות לצורך ביצוע הרכשה חוזרת. דנ"א מופק מכתמי הדם רק כשיש צורך בזיהוי חלל או לצורך בקרת איכות. בתהליך בקרת האיכות ניטלות דגימות מתקופות זמן שונות למעבדת הדנ"א כדי לבדוק אם אפשר לפענח אותן ולהפיק מהן פרופיל דנ"א.

תהליך זיהוי חלל

תהליך הזיהוי מוסדר בפקודות מטכ"ל העוסקות בטיפול בחללים בעיתות שגרה וחירום[5] והוא כולל זיהוי של החלל באמצעות נתוני זיהוי ביומטריים. את איסוף אמצעי הזיהוי מחללים מבצעת הרבנות הצבאית במרכז איסוף נתוני חללים (להלן - מאנ"ח). מהחלל נאספים חפצים אישיים (כגון דיסקית, בגדים, מסמכים) שהם "מכווני זיהוי" המספקים השערה ביחס לזהותו של החלל וכן אמצעי זיהוי ביומטריים.

זיהוי החלל מתבצע באמצעות לפחות שני אמצעי זיהוי: היכרות אישית ואמצעי זיהוי ביומטרי אחד (טביעת אצבע, תצלומי שיניים, דנ"א) או שני אמצעי זיהוי ביומטריים. ענף זו"ק ברבנות הצבאית הוא שמבצע את הזיהוי, באמצעות השוואת הנתונים הביומטריים שניטלו מהחייל בשר"ח קודם המוות (AM - Ante Mortem) לאלו שניטלו מהחלל לאחר המוות (PM - Post Mortem). להלן יוצג אופן התיעדוף של אמצעי הזיהוי שנעשה בהם שימוש בתהליך הזיהוי:

1. **זיהוי באמצעות טביעת אצבע:** חיפוש טביעת האצבע של החלל בקרב כל טביעות האצבע השמורות במאגר טביעות האצבע (חיפוש 1:N). החיפוש מתבצע באמצעות השוואה ממוחשבת של טביעת האצבע, ללא שימוש במידע מזהה נוסף. חייל בתפקיד "משווה" בוחן במעבדה את התוצאות שהתקבלו מהמערכת ומאמת את התוצאה הטובה ביותר שהתקבלה. לאחר אישוש של משווה נוסף או של מומחה, מתקבל הזיהוי. בשלב זה, מופק מסמך זיהוי המועבר לרבנות כחוות דעת מומחה לצורך קביעת הזיהוי.

2. **זיהוי באמצעות תצלומי שיניים:** לצורך הזיהוי נדרשת זהות חלל משוערת, והוא מתבצע באמצעות איתור תמונות השיניים (רנטגן ואופטי) של החייל שהוערך כי הוא החלל, והשוואה ידנית של הצילומים במעבדה.

4 FTA (Fast Technologies for Analysis) - טכנולוגיה על בסיס נייר ייחודי הסופג דם או רוק. הנייר מבצע פירוק של התאים וקושר את הדנ"א אל תוך סיבי הנייר.

5 פקודות מטכ"ל 38.0105 ו- 38.0103

3. **זיהוי באמצעות דנ"א:** לצורך הזיהוי נדרשת זהות חלל משוערת, והוא מתבצע באמצעות השאלה של כתם דם AM של החייל שמוערך כי הוא החלל מאוסף כתמי הדם. דגימת ה-AM וכן דגימת ה- PM מהחלל מועברות למעבדת הדנ"א, ובה ממצים את הדנ"א מהדגימות ומשווים ביניהן לצורך זיהוי או אימות הזיהוי.

הסיכונים למידע הביומטרי

שמירת מידע ביומטרי של חיילי צה"ל חיונית לצורך זיהוי חללים. עם זאת, החזקת מאגרים ביומטריים טומנת בחובה סיכונים בהיבטי אבטחת המידע וההגנה על הפרטיות.

המידע במאגרי אמצעי הזיהוי חשוף לשלושה סוגי סיכונים (לפי מבחן ה- CIA[6]), אשר מקורם באירועי סייבר או באירועים תפעוליים:

1. **פגיעה בסודיות הנתונים (Confidentiality)**

א. **גנבת זהות:** אם נתונים ביומטריים ייחשפו וייקשרו לאדם מסוים ולנתוניו האישיים, עלולה להיגרם פגיעה של ממש בזהותו (עד כדי גנבת זהותו) או בפרטיותו. לדוגמה, אפשר לבצע "השתלת" טביעות אצבע של אנשים חפים מפשע, שנגנבו מהמאגר, בזירת פשע.

ב. **חשיפת מידע ביטחוני או מודיעיני:** אמצעי הזיהוי עלולים להסגיר מידע שיש לשמור על חסיונו.

ג. **חשיפת מידע רגיש:** מידע אשר לפי חוק הגנת הפרטיות, התשמ"א-1981 (להלן - חוק הגנת הפרטיות), כולל נתונים על אישיותו של אדם, צנעת אישיותו ומצב בריאותו - אמצעי זיהוי ביומטריים כמו דנ"א עשויים לספק מידע על המצב הבריאותי או האישי של אותו אדם.

2. **פגיעה באמינות (שלמות) הנתונים (Integrity):** אם נתוני אמצעי הזיהוי ישובשו, באופן מלא או חלקי, או יימחקו ייתכן שלא יהיה אפשר לזהות חללים או שיהיו אמצעי זיהוי חסרים או באיכות נמוכה שיקשו את תהליך הזיהוי.

3. **פגיעה בזמינות הנתונים (Availability):** אירועי טילים ואסונות טבע כמו רעידות אדמה עשויים להשבית את מערכות המידע ואת המכשור המשמש להרכשה ולניהול של אמצעי זיהוי החללים לטווח ממושך. כמו כן, נשקף סיכון שבעת אסון רב-נפגעים או בעת אירוע לחימה התשתית הטכנולוגית לא תצליח להתמודד עם עומס הבקשות לזיהוי חללים. כמו כן, מתקפת סייבר על השרתים ועל תשתיות התקשורת עלולה אף היא לפגוע בזמינות הנתונים.

6 מבחן מקובל בתחום הסייבר ואבטחת המידע לבחינת הנזק העלול להיגרם באמצעות חלוקה לשלוש קטגוריות: Confidentiality, Integrity, Availability.

בתרשים להלן מוצגים הסיכונים הנשקפים למידע הביומטרי:

תרשים 4: **הסיכונים הנשקפים למאגרי אמצעי הזיהוי**

בעיבוד משרד מבקר המדינה.

פעולות הביקורת

בחודשים אוגוסט 2021 - אפריל 2022 בדק משרד מבקר המדינה את נושא "ניהול מידע ביומטרי בצה"ל והגנת הסייבר עליו". הביקורת נעשתה בצה"ל: באכ"א - בענף אסטרטגיה, דיגיטל ומערכות (אד"ם) ובמקמש"ר; במדור קליטה ומיון - ביחידת מיטב; ביחידת שחר - בענף תכלית; ברבנות הצבאית - בענף זו"ק. בדיקות השלמה נעשו בעמותה א' וברשות להגנת הפרטיות שבמשרד המשפטים.

הדוח שבנדון הומצא לראש הממשלה ביום 31.7.2022 והוטל עליו חיסיון עד לדיון בוועדת המשנה של הוועדה לענייני ביקורת המדינה.

מתוקף הסמכות הנתונה למבקר המדינה בסעיף 17(ג) לחוק מבקר המדינה, התשי"ח-1958 [נוסח משולב] ובשים לב לנימוקי הממשלה, לאחר היוועצות עם הגופים האמונים על אבטחת המידע הביטחוני ובתיאום עם יו"ר הכנסת, משלא התכנסה ועדת המשנה של הוועדה לענייני ביקורת המדינה בכנסת, הוחלט לפרסם דוח זה תוך הטלת חיסיון על חלקים ממנו. חלקים אלה לא יונחו על שולחן הכנסת ולא יפורסמו.

ממצאי דוח הביקורת והמלצותיו נכונים למועד המצאתו האמור לעיל.

מדיניות הגנת הסייבר על מערכות אמצעי הזיהוי

מדיניות להגנת הסייבר מבוססת על סיכונים למידע, למערכות המחשוב, למעבדות המאחסנות אותו ולרשתות התקשורת, תוך התאמה לצרכים התפעוליים והארגוניים. העקרונות במדיניות להגנת הסייבר משמשים בסיס לנוהלי העבודה בתחום הגנת הסייבר.

בשנים 2011 עד 2015 התקבלו שלוש החלטות ממשלה[7] בנושא קידום היכולת הלאומית במרחב הסייבר, אסדרה לאומית והסדרת האחריות לטיפול בתחום הסייבר. מכח החלטות אלו הוקמו הרשות הלאומית להגנת הסייבר (כיום מערך הסייבר הלאומי) והיחידה להגנת הסייבר בממשלה (להלן - יה"ב) ברשות התקשוב. גופים אלו אחראים בין היתר להנחיה ולהכוונה בתחום הגנת הסייבר, ובהחלטות אלו הוסדרו תחומי האחריות של כל אחד מהם. כמו כן, הממשלה החליטה כי ההגנה על תפקודו התקין והבטוח של מרחב הסייבר מהווה יעד ביטחוני לאומי חיוני של המדינה.

במישור הלאומי, מדיניות בתחום הגנת הסייבר מתבססת על הקווים המנחים הבאים:

1. תורת ההגנה 2.0, שפרסם מערך הסייבר הלאומי: מדריך יישומי להגנת הסייבר בארגון (רלוונטי לכל המשק).

2. מדיניות להגנת הסייבר בממשלה והנחיית מסגרת להגנת הסייבר בממשלה (להלן - הנחיית מסגרת), שפרסמה יה"ב: מדיניות ומסגרת של נהלים והנחיות המחייבים את המשרדים ומגדירים ניהול תהליכים מרכזיים בנושא הגנת הסייבר.

3. תקן ISO27001: לפי החלטת ממשלה 2443 משנת 2015, על המנכ"לים של משרדי ממשלה להגדיר בתוך 120 יום מיום קבלת ההחלטה תכנית מדורגת להטמעה, התעדה והסמכה לתקן אבטחת מידע ארגוני ממשפחת ת"י ISO27001.

מכלול ההוראות והנורמות האמורות מהווה נורמות מקובלות במישור הלאומי ואולם אלו אינן מחייבות את צה"ל.

יישומים ביומטריים מכילים מידע רגיש, לכן בהתאם להחלטת הממשלה[8] הממונה על היישומים הביומטריים במערך הסייבר הלאומי (להלן - הממונה על היישומים הביומטריים) גיבש מדיניות לאומית ייעודית ליישומים ביומטריים הכוללת קווים מנחים כלליים ליישום המדיניות. כמו כן גיבש הממונה כלי עזר שמטרתם לסייע לגופים לבחון את מידת עמידתם במדיניות הלאומית ליישומים ביומטריים, להלן פירוט הכלים:

7 החלטת הממשלה 3611, "קידום היכולת הלאומית במרחב הקיברנטי" (7.8.2011); החלטת הממשלה 2444, "קידום ההיערכות הלאומית להגנת הסייבר" (15.2.15); החלטת הממשלה 2443, "קידום אסדרה לאומית והובלה ממשלתית בהגנת הסייבר" (15.2.15).

8 החלטת ממשלה 4510, "תפקידיו וסמכויותיו של הממונה על היישומים הביומטריים" (1.4.2012).

1. מחשבון "תבחינים ובקרות - יישומים ביומטריים" - כלי עזר המאפשר לארגון לסווג יישומים ביומטריים לאחת משלוש רמות סיכון ובהתאם לכך לקבל את רשימת הבקרות (הנחיות) שעל הגוף לעמוד בהן.

2. נספח "קווים מנחים" - כלי עזר שמסייע לגוף להבחין אלו סעיפים בקווים המנחים הכלליים במדיניות ליישומים ביומטריים חלים על היישום בהתאם לסיווגו.

בהחלטת הממשלה 4510 נקבע כי המדיניות ליישומים ביומטריים לא תחול על הגופים המיוחדים ובכללם צה"ל, וכי על הגופים המיוחדים יחולו הסדרים מיוחדים כפי שיסוכמו בינם ובין הממונה. במסמך ההסדרה[9] שגובש בדצמבר 2015 בין מחלקת ביטחון מידע (להלן - מחב"ם) בצה"ל ליחידת הממונה על היישומים הביומטריים (להלן - מסמך ההסדרה) נקבע כי יישומים מרכזיים, שבהם מעובדים נתונים ביומטריים של חיילים או אזרחים רבים, ואשר המידע שלהם נשמר לאורך זמן ממושך, סיווגם יהיה "סודי" או "סודי ביותר" ומדיניות הביטחון בהגנה עליהם תהיה בהלימה למדיניות הביטחון המקובלת בצה"ל לגבי אותו סיווג ביטחוני. במסמך ההסדרה מול צה"ל אין התייחסות לעמידה במדיניות הלאומית ליישומים ביומטריים ולא נקבע מנגנון לבחינת עמידה בקווים המנחים של היישומים הביומטריים בהתאם לרמת הסיכון שלהם.

מסמכי ההסדרה שגיבש הממונה על היישומים הביומטריים עם גופים מיוחדים אחרים גובשו על בסיס הקווים המנחים לניהול יישומים ביומטריים שהוגדרו במדיניות ליישומים ביומטריים, בהתאמות הנדרשות. במסמכי ההסדרה עם חלק מהגופים אף גובש מנגנון לעדכון הדדי אחת לשנה ולתיקוף הסדרים קיימים.

בתשובת צה"ל מיוני 2022 (להלן - תשובת צה"ל) נמסר כי מחב"ם, האמונה על ביטחון המידע בצה"ל, לא הכירה את מסמך ההסדרה, וכי לא ברורים לה התבחינים שלפיהם המידע עשוי להגיע עד לרמת סיווג "סודי ביותר".

מומלץ כי הממונה על היישומים הביומטריים יציג לצה"ל את מסמך ההסדרה שגיבש בדצמבר 2015 עם מחב"ם ויבחן יחד עמו את הצורך בעדכונו בהלימה למתכונת העבודה שהוסדרה עם גופים מיוחדים דומים.

צה"ל, כאמור, איננו כפוף לקווים המנחים שהוזכרו במישור הלאומי, אלא למדיניות הגנת מערכות תקשוב של צה"ל[10] (להלן - מדיניות ההגנה) שגובשה על ידי יחידת מרכז צופן וביטחון (להלן - מצו"ב)[11] בחטיבת ההגנה בצה"ל בשנת 2012, ועודכנה לאחרונה בשנת 2015. מדיניות ההגנה של צה"ל מפורטת בהוראת קבע אגפית (להלן - הק"א) שפרסם אגף התקשוב לראשונה בשנת 2001[12] (להלן - הוראות המדיניות).

9 במסגרת החלטת הממשלה 4510, "תפקידיו וסמכויותיו של הממונה על היישומים הביומטריים" (1.4.2012), הוגדר צה"ל כ"גוף מיוחד" שעליו לא תחול ההחלטה אלא יחולו הסדרים מיוחדים כפי שייקבעו בינו לבין הממונה על היישומים הביומטריים.

10 פקודת מטכ"ל 3.0303 בנושא "הגנת מערכות תקשוב והמידע האגור בהן".

11 היחידה אחראית לפיתוח פתרונות צופן והגנה בסייבר לגופים הביטחוניים השונים.

12 הק"א 3.001, "מדיניות צה"ל להגנת מערכות מידע".

מלבד מדיניות ההגנה, על המאגרים הביומטריים בצה"ל חלים חוק הגנת הפרטיות, ותקנות אבטחת מידע. הרשות להגנת הפרטיות אחראית ליישום של החוק והתקנות שחלים על צה"ל למעט סייגים שמופיעים בחוק בעניין פיקוח ואכיפה.

בהיעדר מדיניות הגנה מלאה ועדכנית בתחומים שנסקרו בדוח זה, משרד מבקר המדינה השווה את הגנת הסייבר בצה"ל לנורמות בין-לאומיות מקובלות, להנחיות שפרסמו רשות התקשוב ומערך הסייבר הלאומי (נורמות אשר מחייבות את כלל משרדי הממשלה) ולתקנות אבטחת מידע שמחייבות את צה"ל. להלן יוצגו הנורמות שלאורך נבחנו הנושאים בפרקים הבאים:

תרשים 5: **הנורמות שחלות על צה"ל בתחום מדיניות הגנת הסייבר**

בעיבוד משרד מבקר המדינה.

מדיניות הגנת הסייבר

הנחיות יה"ב וכן תורת ההגנה בסייבר של מערך הסייבר הלאומי יוצרות מסגרת של מוסכמות בתחום המדיניות על הגנת סייבר. בהנחיה 5.1 שפרסמה יה"ב בספטמבר 2016 בנושא "מדיניות להגנת הסייבר בממשלה" (להלן - ההנחיה בנושא מדיניות) מפורטים עיקרי הנושאים שיש לכלול במסמך המדיניות של משרדי הממשלה, כמפורט בתרשים להלן:

תרשים 6: **עיקרי הנושאים שיש לכלול במסמך המדיניות להגנת הסייבר**

הגנה פיזית
הגנה על הציוד והמידע מפני גישה פיזית של גורמים לא מורשים

הגנת רשומות
הגדרת התהליכים וכלי הטיפול להגנה על אמצעים פיזיים ולוגיים נושאי מידע

ניהול המשכיות תפקודית
הגדרת עקרונות שיאפשרו את המשך פעילות המחשוב התפקודית החיונית בעת חירום

ניהול וסיווג נכסים
סיווג נכסי מידע וניהולם
קביעת גורם אחראי לכל נכס מידע

תוכנית עבודה ותקציב
גיבוש תוכנית עבודה ותקציב בתחומי הגנת הסייבר שיסייעו בעמידה ביעדים הממשלתיים

הגנה לוגית
מעגלי הגנה על המידע בתחומי המחשוב והתקשורת

התאמה
עמידה בדרישות החוק והתקנות הישראליות הנוגעות להגנת הסיבר

פיתוח ורכש
שילוב הגנת הסייבר בתהליכי הפיתוח והרכש

שרשרת האספקה
צמצום הסיכון הנובע מחשיפה של ספקים חיצוניים למערכות ולמידע השמור בהן

משאבי אנוש
- הגדרת עקרונות הגנת המידע והמערכות התומכות בו בכל הקשור לעובדי המשרד, עובדי קבלן ועובדי מיקור חוץ.
- תהליכי קליטה ועזיבה, מודעות עובדים

המבנה הארגוני
- הגדרת בעלי התפקידים אשר יישמו את המדיניות ויפקחו עליה
- הגדרת סמכויותיהם ויחסי הגומלין ביניהם

בעיבוד משרד מבקר המדינה.

נמצא כי מסמך מדיניות ההגנה של צה"ל כולל התייחסות לחלק מהנושאים שיה"ב הגדירה שיש לכלול במסמך מדיניות להגנת הסייבר כגון: הגנת רשומות, הגנה לוגית ופיזית והמבנה הארגוני אך אינו כולל התייחסות לנושאים כגון ניהול וסיווג נכסים, שרשרת האספקה, משאבי אנוש והתאמה לדרישות החוק (כמו תקנות אבטחת מידע).

לפי המדיניות הלאומית ליישומים ביומטריים, יש לעדכן את מסמך המדיניות מעת לעת בהתאם לתנאי השטח המשתנים ובהתבסס על הפקת הלקחים מתהליך ניהול הסיכונים. גם את מסמך המדיניות להגנת הסייבר בממשלה נדרש יה"ב לעדכן לפי הצורך.

נמצא כי מסמך מדיניות ההגנה של צה"ל לא עודכן מאפריל 2015, במשך 7 שנים, שבמהלכן חלו שינויים טכנולוגיים וכן חלו שינויים בחובות החלות על צה"ל בנושא אבטחת מידע בעקבות פרסום תקנות אבטחת מידע משנת 2017. במצב זה מסמך מדיניות ההגנה אינו מספק מענה עדכני לסיכונים שנשקפים בתחום זה כנדרש.

מומלץ כי מצו"ב יעדכן את מסמך המדיניות כך שיכלול את הנושאים המפורטים במסמכי מדיניות מקובלים בתחום הגנת הסייבר כמו ההנחיה בנושא מדיניות של יה"ב, וכן יעדכן אותה באופן עתי בהתאם לשינויים הטכנולוגיים ולסיכונים בתחום, באופן שיעמדו בדרישות החוק והתקנות הרלוונטיים.

מענה ההגנה למערכות אמצעי הזיהוי

כאמור, לפי תקנות אבטחת מידע, מאגר מידע המכיל מידע ביומטרי ויש בו יותר מ-100,000 רשומות נדרש לעמוד ברמת אבטחה גבוהה, לכן מאגרי המידע של מערכת א' ומערכת ב' נדרשים על פי התקנות לעמוד ברמת אבטחה גבוהה.

סיווג מערכות אמצעי הזיהוי

לפי מדיניות ההגנה בצה"ל, קצין האמל"ח, שהוא ראש הפרויקט, יהיה הגורם האחראי לגיבוש רמת ההגנה הנדרשת על מערכת תקשוב (להלן - מענה ההגנה) בתהליך הרכש שלה או בתהליך פיתוח עצמי של מערכת כאמור. רמת ההגנה נקבעת לפי שני רכיבים:

1. רמת הסודיות - משקפת את הנזק העלול להיגרם למדינה עקב דלף מידע. הגדרה זו נקבעת על ידי קצין האמל"ח בהתאם להגדרות מחב"ם[13].
2. רמת החסינות - משקפת את הנזק העלול להיגרם עקב פגיעה בזמינות ובאמינות של מערכת תקשוב ובמידע האגור בה. הגדרה זו נקבעת על ידי קצין האמל"ח בהתאם להגדרות המשתמש המוביל.

נמצא כי מערכת א' ומערכת ב' הוגדרו בסיווג סודי עם חסינות בינונית למרות שמערכות אלו נדרשות לעמוד ברמת אבטחה גבוהה לפי תקנות אבטחת מידע, ולמרות הנזק הרב שעלול להיגרם מדליפת מידע ביומטרי רגיש שמוחזק במערכות אלו.

מומלץ כי מחב"ם יבחן מחדש ויתקף באופן עיתי את סיווג מערכות אמצעי הזיהוי באופן שיביא בחשבון את הסיכונים העדכניים הנשקפים למידע שמוחזק במאגרים אלו וכן את הסיכון שקיים לנושאי המידע כתוצאה מדלף מידע.

13 פקודת מטכ"ל 21.0101 - "אבטחת רשומות"

בתשובת מחב"ם מיוני 2022 נמסר כי הם מקבלים את ההמלצה, וכי הם יבחנו ויתקפו את הסיווגים של מערכות אמצעי הזיהוי.

מענה ההגנה של מערכות אמצעי הזיהוי

לפי הוראות המדיניות יש להגדיר את דרישות ההגנה במסמך אשר יכלול את ההיבטים האלו:

1. סקירת איומים - איומים הנובעים מאופייה של המערכת, איומים מודיעיניים כלליים וקונקרטיים, איומים טכנולוגיים ואיומים הנובעים מתצורת השימוש המוגדרת באפיון המבצעי.

2. פירוט דרישות ההגנה למערכת המידע - איסוף כלל הדרישות למערכת על פי רמת ההגנה הנדרשת בנושאים האלה: הזדהות, הרשאות, בקרה, תשתיות תוכנה, ממשקים ותקשורת, סביבת הפיתוח, אבטחה פיזית ומהימנות כוח אדם.

עוד נקבע במדיניות ההגנה כי נוסף על האמור לעיל, רמת ההגנה על המערכת תיקבע גם בהתאם לצורך ולעניין הקונקרטיים ותעודכן מפעם לפעם.

נמצא כי למערכות אמצעי הזיהוי של צה"ל אין מענה הגנה מפורט במסמך הכולל את דרישות ההגנה הייעודיות למערכות אלו בהתאם לסיווג שלהן. עקב כך לא ניתן לבחון את מידת עמידת מערכות אמצעי הזיהוי בדרישות אבטחת המידע שנקבעו במדיניות ההגנה. כמו כן נמצא פער ביישום דרישות ההגנה במערכות אמצעי הזיהוי כפי שמפורט בפרקים רלוונטיים.

על מקמש"ר לוודא שעקרונות מדיניות ההגנה מעוגנים במסמך מענה הגנה וכן מיושמים במערכות אמצעי הזיהוי הנמצאות בשלבי פיתוח ותחזוקה. כמו כן, מומלץ שמדי שנה מקמש"ר יוודא שמענה ההגנה של המערכות מאפשר להתמודד באופן הולם עם הסיכונים הנשקפים באותה עת ועם תרחישי האיום העדכניים.

ועדות היגוי בנושא סייבר

על פי הנחיית המסגרת להגנת הסייבר בממשלה[14], ועדת ההיגוי המשרדית לנושא הגנת הסייבר היא פורום ניהולי שממונה על ידי מנכ"ל המשרד אשר יושב בראשו. ועדת ההיגוי אחראית לגיבוש עקרונות המדיניות, להתוויית אסטרטגיה לפעילות, לפיקוח על תוכנית האב ותוכניות העבודה השנתיות, להערכת נזקים בעקבות תקלות ולגיבוש המלצות לטיפול בתקלות אלה על פי עקרונות מסמך המדיניות והמסגרת להגנת הסייבר הממשלתית. כמו כן ועדת ההיגוי אחראית לביצוע בקרה על יישום המדיניות על פי מתווה הנחיות המסגרת להגנת הסייבר בממשלה.

בהוראות מדיניות ההגנה של צה"ל יועדה ועדת הגנת מערכות מידע שתפקידה לאשר את פתרונות ההגנה שניתנו לכל פרויקט ואת עמידתו במדיניות. הצגת הפרויקט לפני הוועדה מוטלת

---

14 הנחיית יה"ב 5.2, סעיף 6.1

על קצין האמל"ח של הפרויקט. אם יידרש אישור לחריגה מהמדיניות, הנושא יועלה לדיון בוועדת הגנת מערכות מידע המטכ"לית.

בפגישה שקיים צוות הביקורת עם רע"ן תכלית נאמר כי צה"ל מקיים ועדות היגוי בנושאי סייבר, אך אלו לא דנות במערכות בשלבי תחזוקה עם כמות משתמשים מצומצמת כדוגמת מערכת א' ומערכת ב'.

נמצא כי למרות שמערכות אמצעי הזיהוי הן מערכות הכוללות מידע ביומטרי רגיש, הן אינן מוגדרות ככאלו המטופלות במסגרת עבודתה של ועדת הגנת מערכות מידע שמתפקידה לעקוב אחר יישום מדיניות הגנת הסייבר הלכה למעשה.

על מקמש"ר להעביר לאישור ועדת הגנת מערכות מידע את מענה ההגנה שיגובש למערכות אמצעי הזיהוי. כמו כן על מקמש"ר לוודא שהוועדה בוחנת באופן עיתי את מידת העמידה של המערכות במדיניות ההגנה בהתאם לסיכונים הכרוכים במידע האגור בהן.

ממונה על אבטחת מידע

לפי סעיף 17ב לחוק הגנת הפרטיות, גוף ציבורי חייב במינוי אדם בעל הכשרה מתאימה שיהיה ממונה על אבטחת מידע (להלן - ממונה אבטחת מידע) ויישא באחריות לאבטחת המידע שבמאגרים המוחזקים ברשות הגוף.

בהתאם לתקנה 3 לתקנות אבטחת מידע, על ממונה אבטחת מידע להכין נוהל אבטחת מידע ולהביאו לאישור בעל המאגר. כמו כן, על ממונה אבטחת מידע להכין תוכנית לבקרה שוטפת על העמידה בדרישות תקנות אבטחת מידע, לבצע אותה ולהביא את ממצאיו לידיעתם של בעל מאגר המידע ומנהל מאגר המידע.

גם לפי הנחיית יה"ב, יש למנות ממונה על הגנת הסייבר שיהיה אחראי לניהול תחום הגנת הסייבר, להנחיה מקצועית שוטפת בתחום זה וליישום בפועל של ההחלטות והסיכומים של ועדת ההיגוי להגנת הסייבר.

כאמור, בצה"ל יש כמה גורמים העוסקים ביישום של אבטחת מידע ובהנחיה בנושא:

1. יחידת הגנת הסייבר במרכז המחשבים ומערכות המידע (להלן - ממר"ם): אחראית ליישום מדיניות ההגנה בתשתיות המחשוב ורשת התקשורת, ולא אחראית ברמת המערכות הספציפיות.

2. קצין ביטחון מידע (להלן - קב"ם): בכל יחידה בצה"ל, לרבות ברבנות, ממונה קב"ם שהוא נציג מטעם מחב"ם. הקב"ם אחראי ליישום הנהלים בתחום ביטחון המידע ובין תפקידיו: נוהלי מסירת מידע לגורם שמחוץ לצה"ל ונוהלי העסקת עובדים אזרחים במתקנים צבאיים.

3. קצין האמל"ח: לפי מדיניות ההגנה, הוראות ההגנה להפעלת מערכת התקשוב יגובשו על ידי קצין האמל"ח ויובאו לאישורה של ועדת הגנת מערכות תקשוב.

4. ראש אגף התקשוב או מי שיוסמך לכך מטעמו: כאמור במדיניות ההגנה, באחריותם לפקח על יישום פעולות הגנת מערכות התקשוב ועל עדכניותן.

נמצא כי בצה"ל יש כמה גורמים העוסקים בהיבטים שונים בתחום אבטחת המידע של מערכות מידע ובהם: יחידת הגנת הסייבר בממר"ם, מחב"ם, קצין האמל"ח וגורמי מדיניות ההגנה באגף התקשוב, אולם אין גורם אחד שנושא באחריות לכל היבטי אבטחת המידע של מערכות אמצעי הזיהוי ותפקידו ואחריותו הוגדרו בהתאם לתקנה 3 בתקנות אבטחת מידע ובהתאם למדיניות ההגנה של צה"ל.

מומלץ כי צה"ל ימנה ממונה אבטחת מידע האחראי למערכות אמצעי הזיהוי כנדרש בחוק הגנת הפרטיות ובתקנות אבטחת מידע.

בתשובת צה"ל נמסר כי עד מועד סיום הביקורת באפריל 2022 לא מונה ממונה אבטחת מידע של מאגר כוח האדם הצה"לי.

נוהלי אבטחת מידע

נוהל אבטחה

תקנה 4 בתקנות אבטחת מידע מגדירה את הנושאים שיש לכלול בנוהל האבטחה במטרה להבטיח את יישום מדיניות האבטחה הנדרשת במאגר. בנוהל יש לכלול, בין השאר, נושאים אלה: הוראות בעניין האבטחה הפיזית והסביבתית של אתרי המאגר; הרשאות גישה למאגרי המידע ולמערכות המאגר; הסיכונים שחשוף להם המידע שבמאגר, לרבות אלה הנובעים ממבנה מערכות המאגר, אופן קביעת סיכונים אלו ואופן הטיפול בהם, לרבות על ידי מנגנוני הצפנה מקובלים; אופן ההתמודדות עם אירועי אבטחת מידע; הוראות לעניין ניהול של התקנים ניידים ושימוש בהם.

נמצא כי הגורמים העוסקים באבטחת המידע לא גיבשו ואישרו נוהלי אבטחה למערכות אמצעי הזיהוי כנדרש בתקנות אבטחת מידע שיבטיחו את רמת האבטחה הנדרשת במאגר. כתוצאה מכך מסמכים שמתייחסים להיבטי אבטחה מסוימים נכתבו על ידי גורמים שונים באופן שאינו מספק את המענה הדרוש על פי התקנות. למשל, הרבנות כתבה נוהל הרשאות משתמשים למערכת א' אשר מכיל הגדרות בעלי תפקידים אך חסר בו מידע כמו הצורך במידור - הגדרת הרשאות לפי תפקידים כמקובל במסמכי ניהול הרשאות; נאסר להכניס טלפון נייד למעבדת טביעות האצבע, אך הגבלה זו אינה מתועדת בנוהל כתוב; לא קיים נוהל פיתוח מאובטח (ראו תת-פרק בהמשך).

מומלץ כי ממונה אבטחת מידע יגבש ויאשר נהלים בתחום אבטחת המידע למערכות אמצעי הזיהוי, בדומה לנוהלי יה"ב שיבטיחו את רמת האבטחה הנדרשת במערכות ובמאגרי המידע שלהן.

תיעוד אירועי אבטחת מידע

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 (להלן - אירועי אבטחת מידע). בנוהל האבטחה ייקבעו הוראות לעניין ההתמודדות עם אירועי אבטחת מידע, לפי חומרת האירוע ומידת רגישות המידע.

לפי מדיניות ההגנה בצה"ל, במקרה של תקלה במערכות התקשוב או במצע אחסון מידע צה"ליים, הטיפול התקשובי בהם יהיה בהתאם לסיווג התקלה אשר יתבסס על מידת הנזק העשוי להיגרם בגינה למערכת התקשוב ומידת תפוצתה של התקלה ברשת הצה"לית. במידת הצורך, במקביל לטיפול התקשובי תיערך גם חקירה ביטחונית של המקרה.

נמצאו פערים באופן תיעוד האירועים, מוצע כי צה"ל יפעל לתקנם.

בקרה, ביקורת ותאימות של הגנת הסייבר

מיפוי מערכות אמצעי הזיהוי

לפי תקנה 5 לתקנות אבטחת מידע על בעל מאגר מידע להחזיק מסמך מעודכן בעניין מבנה מאגר המידע וכן רשימה מעודכנת בדבר המצאי של מערכות המאגר. ובכלל זה:

1. תשתיות ומערכות חומרה, סוגי רכיבי תקשורת ואבטחת מידע.
2. מערכות התוכנה המשמשות להפעלת מאגר המידע, לניהול המאגר ולתחזוקתו, לתמיכה בפעולתו, לניטור שלו ולאבטחתו.
3. תוכנות וממשקים המשמשים לתקשורת עם מערכות המאגר.
4. תרשים של הרשת שפועל בה המאגר, המציג בין היתר את הקשרים בין רכיבי המערכת השונים ואת מקומם הפיזי של רכיבים אלה.
5. תאריך העדכון האחרון של המסמך ושל רשימת המצאי.

ענף תכלית הכין תרשים רשת של מערכת א' ומערכת ב', המציג בין היתר את המבנה הפונקציונלי שלהן. עם זאת, נמצא כי תרשים הרשת של מערכת א' ומערכת ב' לא מכיל את כל הפירוט הנדרש בתקנות אבטחת מידע, ובכלל זה פירוט בנוגע לתשתיות ולמערכות החומרה, לסוגי תקשורת ולרכיביה, ולמערכות התוכנה המשמשות להפעלת המאגר. כמו כן, בתרשים לא צוין מועד העדכון האחרון שלו. היעדר מיפוי עדכני בדבר הטכנולוגיות הקיימות עלול לפגוע ביכולת של צה"ל לזהות את הסיכונים והאיומים הנשקפים למאגרים ובכלל זה לזהות פרצות אבטחה ידועות בחלק מהרכיבים ולהתגונן מפני הסיכונים הנשקפים בגינן.

מומלץ כי ענף תכלית יעדכן את תרשים הרשת של מערכות אמצעי הזיהוי כנדרש בתקנות אבטחת מידע.

סקרי סיכונים

לפי תקנה 2 לתקנות אבטחת מידע, במסמך הגדרות מאגר יש לפרט, בין היתר, את הסיכונים העיקריים של פגיעה באבטחת המידע ואת אופן ההתמודדות מולם. הבנת הסיכונים והאיומים הנשקפים למאגרים היא הבסיס לקביעת תוכנית העבודה ולביצוע הבקרות הנדרשות להגנה על המידע הנשמר במאגרים הללו.

תקנה 15 לתקנות אבטחת מידע קובעת שגם בהתקשרות עם גורם חיצוני יש לבחון את סיכוני אבטחת המידע הקשורים בהתקשרות.

הנחת העבודה בממר"ם היא שרמת ההגנה על הרשת הצה"לית גבוהה ביותר, ומכאן שאיום הייחוס העיקרי על מאגרי המידע הוא האיום הפנימי של דלף מידע.

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

לצוות הביקורת נמסר כי על פי מדיניות הגנת הסייבר, צה"ל מכין סקר סיכונים בנוגע למערכות המידע רק במועד הקמת המערכות ובמסגרת תהליכי ההגנה עליהן. האחראי לביצוע הסקר הוא גורם האמל"ח, ומשתתפים בתהליך גם ענף תכלית והקב"ם של המשתמש המוביל. ועדת ההגנה מוסמכת לאשר את הסקר.

נמצא כי ממועד הקמת מערכת א' ומערכת ב' בשנים 2005 - 2006 ועד למועד סיום הביקורת באפריל 2022 (פרק זמן של יותר מ-16 שנים) צה"ל לא ביצע סקרי סיכונים בנוגע למערכות. זאת אף שלפי תקנות אבטחת מידע נדרש לבצע במערכות אלו שחלה עליהן רמת אבטחה גבוהה, סקר סיכונים מדי 18 חודשים.

על אכ"א לוודא ביצוע סקרי סיכונים בנוגע למערכות אמצעי הזיהוי שנדרשות לעמוד ברמת אבטחה גבוהה, מדי 18 חודשים לפחות כנדרש בתקנות אבטחת מידע.

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. בעל המאגר ידון בממצאיהם של מבדקי החדירה ואם יתגלו במבדקים ליקויים הוא יפעל לתיקונם.

לפי מדיניות ההגנה בצה"ל על מנת לאתר ליקויים ונקודות תורפה בהגנה של מערכות תקשוב, יופעלו צוותי חדירה כחלק מהגנת מערכות תקשוב.

יש שני סוגים של מבדקי חדירה:

1. מבדק תשתית ורשת תקשורת: צה"ל מבצע מבדק חדירה מסוג תשתית ורשת תקשורת אחת לשנתיים.

2. מבדק אפליקטיבי: מבדקי חדירות מבוצעים במערכות ניהוליות החשופות למרשתת.

נמצא כי אף שבמערכת א' ובמערכת ב' שמור מידע ביומטרי רגיש והן מחויבות בביצוע מבדקי חדירה מדי 18 חודשים, לפי תקנה 5(ד) לתקנות אבטחת מידע, לא בוצעו בהן מבדקי חדירה ממועד הקמתן בשנים 2005 - 2006 ועד מועד סיום הביקורת באפריל 2022 (פרק זמן של כ-16 שנה). עקב כך לא ניתן להעריך את מידת עמידות המערכות בפני איומים וחולשות ידועים ולהכין תוכניות להתמודדות עימם. כמו כן, נמצא כי גם במערכת ב' החדשה הנמצאת בשלב בדיקות לפני מבצוע לא בוצעו מבדקי חדירה.

על אכ"א לוודא ביצוע מבדקי חדירה למערכות אמצעי הזיהוי הנדרשים ברמת אבטחה גבוהה, מידי 18 חודשים לפחות כנדרש בתקנות אבטחת מידע.

בדיקות תאימות לתקנות אבטחת מידע

בקרת צה"ל על העמידה בדרישות התקנות

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 ולמנהל המאגר על ממצאיו. תקנות 16(א) ו-16(ב) קובעות כי במאגר מידע שחלה עליו רמת אבטחה בינונית או גבוהה, 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 שמאגר המידע עומד בהוראות התקנות. בדוח הביקורת ידווח המבקר על התאמת אמצעי האבטחה לנוהל האבטחה ולתקנות אבטחת מידע, יזהה ליקויים ויציע אמצעים דרושים לתיקון המצב.

נמצא כי אין בידי אכ"א תוכנית לבקרה שוטפת על העמידה של מאגרי אמצעי הזיהוי בדרישות תקנות אבטחת מידע, וכן לא בוצעו ביקורות בנושאים אלו. עוד נמצא כי פקודות המטכ"ל בנושא הגנת הפרטיות[15] לא עודכנו ממועד כתיבתן בשנת 1996 (פרק זמן של 26 שנים), לכן אינן מתייחסות לתקנות אבטחת מידע שפורסמו בשנת 2017.

בתשובת צה"ל נמסר כי במסגרת שיתוף הפעולה בינו ובין הרשות להגנת הפרטיות, עדכון פקודת המטכ"ל החל בשנת 2021 ונכון ליוני 2022 הוא נמצא בשלבי טיוטה.

15 פקודת מטכ"ל 30.0413: "הגנת הפרטיות ויישומה במאגר המידע הצה"לי".

נוכח רגישות המאגרים של אמצעי הזיהוי, על אכ"א להכין תוכנית לבקרה שוטפת על מידת העמידה של המאגרים בתקנות אבטחת מידע ולוודא את ביצועה אחת לשנתיים או במסגרת סקר סיכונים. עוד מומלץ כי אכ"א בשיתוף אגף התקשוב יפעלו להשלמת עדכון פקודות המטכ"ל בנושא הגנת הפרטיות.

ממשקי עבודה מול הרשות להגנת הפרטיות

הרשות להגנת הפרטיות היא רגולטור כלל-משקי, המופקד על הרגולציה, לרבות על אכיפה מינהלית ופלילית, ביחס לכלל מאגרי המידע האישי בישראל, בגופים פרטיים וציבוריים כאחד, בהתאם להוראות חוק הגנת הפרטיות ותקנותיו. לנוכח מספרם הרב של הגופים המפוקחים מחד גיסא ומגבלת המשאבים מאידך גיסא, תוכניות האכיפה והפיקוח של הרשות מבוססות ברובן על ניהול סיכונים ותיעדוף. בקביעת תוכנית אכיפה, המתבססת על תוכנית העבודה השנתית ומדיניות הרשות הכוללת, מובאים בחשבון פרמטרים שונים, ובין היתר, מידת ההשפעה הרוחבית של פעילות האכיפה, מתן עדיפות לטיפול בגופים המחזיקים במידע רגיש בהיקף נרחב, ומתן קדימות לנושאים רגישים.

בפגישה שקיים משרד מבקר המדינה במרץ 2022 עם הנהלת הרשות להגנת הפרטיות נאמר כי במהלך שנת 2021 זיהתה הרשות כי גוף גדול כמו צה"ל, מחזיק במאגרי מידע בעלי חשיבות רבה מבחינת הרשות, ובהתאם לכך החלה הרשות בהליך הסדרה רוחבי של הגנת הפרטיות בצה"ל, בשיתוף גורמים בכירים באכ"א: במאי 2021 התקיימה פגישה ראשונה של צוות ההנהלה של הרשות להגנת הפרטיות עם צה"ל (רמ"ח תכנון וארגון וממונת הגנת הפרטיות באכ"א), ובמהלכה סוכם כי תגובש תוכנית עבודה כוללת שתיתן מענה על נושאים שונים ובהם: מינוי ממונה הגנת הפרטיות ביחידות השונות, הסברה פנים-צה"לית בנושא חיזוק תפיסת הגנת הפרטיות בצה"ל, הכללת נושא הגנת הפרטיות בין שאר הנושאים שעליהם חלה הביקורת שמבצע אכ"א ותיקון פקודות מטכ"ל. במרץ 2022 נערכה פגישת המשך ובה הוצגה תוכנית העבודה.

לרשות להגנת הפרטיות נתונה סמכות לבצע הליכי פיקוח ואכיפה במאגרי המידע של צה"ל, וזאת בכפוף להוראת סעיף 10 (ה1)(2) לחוק הגנת הפרטיות, המחייבת תיאום עם הגורם המפוקח לפני כניסה למתקן צבאי. במסגרת הצעת חוק הגנת הפרטיות (תיקון מס' 14), התשפ"ב-2022, אשר נכון למועד סיום הביקורת באפריל 2022 נידונה בוועדת החוקה, חוק ומשפט של הכנסת בהכנה לקריאה שנייה ושלישית, קיים הסדר מקיף בנוגע לאופן קיום הליכי פיקוח בגופים ביטחוניים, ובכלל זה בצה"ל. בין היתר, ההסדר הנכלל בהצעת החוק מטיל חובה למנות מפקח פרטיות פנימי בגופים הביטחוניים, לרבות צה"ל, אשר יפקח על קיום הוראות חוק הגנת הפרטיות בגוף הביטחוני וידווח לרשות בהתאם לכך. בפגישה של הרשות להגנת הפרטיות עם צוות הביקורת נאמר כי יכולת האכיפה והפיקוח של הרשות על גוף כמו צה"ל היא מוגבלת, למשל: לרשות אין אפשרות להתלות מאגר מידע שצה"ל מחזיק.

נמצא כי אף שצה"ל מחזיק במאגרי מידע רבים שבהם שמור מידע רגיש ומידע אישי על אזרחים רבים, עד מועד סיום הביקורת באפריל 2022 לא ביצעה הרשות להגנת הפרטיות ביקורות ופעולות פיקוח רוחביות על מאגרי המידע בצה"ל בכלל, ועל מאגרי אמצעי הזיהוי בפרט, כדי לוודא שהמאגרים עומדים בתקנות אבטחת המידע. יצוין כי במאי 2021 קיימה הרשות להגנת הפרטיות פגישת עבודה עם אכ"א לקידום נושא הגנת הפרטיות בצה"ל אולם נושא יכולת ביצוע הפיקוח והאכיפה טרם הוסדר.

מומלץ כי בד בבד עם הליך תיקון החקיקה המתקיים תפעל הרשות להגנת הפרטיות להסדיר את יכולת הפיקוח והאכיפה על מאגרי המידע שברשות צה"ל, ובכללם מאגרי אמצעי הזיהוי. עוד מומלץ כי אכ"א בשיתוף הרשות להגנת הפרטיות יוציאו לפועל את תוכנית העבודה שגובשה כתוצאה מהפגישה במאי 2021 ובכלל זה יקדמו את ההדרכות בצה"ל בנושא עמידה בתקנות אבטחת מידע ויגבשו תכנית להכשרת בעלי תפקיד שיוכלו לשמש מפקחים פנימיים בתוך צה"ל.

בהיעדר בקרה של צה"ל על מידת עמידת מאגרי אמצעי הזיהוי בתקנות אבטחת מידע, בדק משרד מבקר המדינה את מידת עמידתם של המאגרים בסעיפי החוק והתקנות, כפי שיפורט בפרקים הבאים.

להלן תרשים המסכם את מידת עמידת מאגרי אמצעי הזיהוי בסעיפי החוק או התקנות הרלוונטיות:

תרשים 7: **עמידת מאגרי אמצעי הזיהוי בדרישות תקנות אבטחת מידע**

תקנה	נושא	ממצאי הביקורת
2	מסמך הגדרות המאגר	לא קיים
3	ממונה על אבטחת מידע	לא מונה
4	נוהל אבטחה	לא קיים
5	מיפוי מערכות המאגר וביצוע סקר סיכונים	קיים חלקית
6	אבטחה פיזית וסביבתית	קיים חלקית
7	אבטחת מידע בניהול כוח אדם	קיים חלקית
8	ניהול הרשאות גישה	קיים חלקית
9	זיהוי ואימות	קיים חלקית
10	בקרה ותיעוד גישה	קיים חלקית
11	תיעוד של אירועי אבטחה	קיים חלקית
12	התקנים ניידים	קיים
13	ניהול מאובטח ומעודכן של מערכות המאגר	קיים חלקית
14	אבטחת תקשורת	קיים
15	מיקור חוץ	קיים
16	ביקורות תקופתיות	לא קיים

בעיבוד משרד מבקר המדינה.

איסוף מידע והשימוש בו

מינוי מנהל המאגר

תקנות אבטחת מידע מפרטות דרישות שאותן יש ליישם במאגר מידע, ובהן דרישות הנוגעות לתפעול ולתחזוקה של המאגר וכן לביקורות התקופתיות שיש לבצע כדי לוודא שהמאגר מאובטח כנדרש. לפי דברי ההסבר לתקנות: "האחריות הכוללת לעמידה בתקנות היא של בעל מאגר המידע (כלומר הגוף הציבורי או הפרטי שלמטרותיו ולצרכיו המידע נאסף ומעובד) ושל מנהל המאגר (כלומר מנכ"ל הגוף או בכיר אחר שהוא הסמיך לכך)"[16].

בפגישות שקיים צוות הביקורת עם גורמים ביחידות שונות הקשורים למאגרי אמצעי הזיהוי עלה כי אין גורם שהוא מנהל המאגר.

נמצא כי צה"ל (שלפי התקנות הוא בעל מאגר המידע) לא מינה גורם לתפקיד מנהל המאגר הביומטרי כנדרש בתקנות אבטחת מידע ולא הגדיר את תחומי אחריותו וסמכותו בהתאם לתקנות. מומלץ כי צה"ל ימנה מנהל מאגר שהוא קצין בכיר כנדרש בתקנות.

בתשובת צה"ל נמסר כי עד מועד סיום הביקורת באפריל 2022, לא מונה מנהל מאגר מידע צה"לי.

רישום מאגרים

שמירת מידע אישי במאגר, ובפרט מידע ביומטרי, עלולה לגרום לפגיעה בפרטיות. משום כך מוטלות על בעל מאגר ועל מנהל מאגר חובות בנושא אבטחת המידע של המאגר. חובות אלו נקבעו בחוק הגנת הפרטיות ובתקנות שהותקנו מכוחו, והן מחייבות את הארגון להגדיר את מטרות המאגר ואת אופן הטיפול במידע שבו, וכן למנות בעלי תפקידים הקשורים למאגר ולהגדיר את חובותיהם.

סעיף 8(ג) לחוק הגנת הפרטיות מחייב, בתנאים מסוימים, לרשום מאגרי מידע אצל רשם מאגרי המידע. סעיף 9(ב) לחוק מפרט מה תכלול בקשה לרישום, ובכלל זה: זהות בעל המאגר ומנהל המאגר; מטרות הקמת המאגר והמטרות שלהן נועד המידע (אסור להשתמש במידע במאגר עבור מטרות שלא הוגדרו); סוגי המידע שייכללו במאגר.

נוסף על חובת רישום המאגר, תקנה 2 לתקנות אבטחת מידע מחייבת את בעל המאגר להכין "מסמך הגדרות מאגר", ולהגדיר בו מידע חיוני הקשור למידע ולאופן השימוש בו, ובכלל זה: תיאור כללי של פעולות איסוף המידע והשימוש בו; תיאור מטרות השימוש במידע; סוגי המידע הכלולים במאגר; סיכוני אבטחת המידע שהמאגר חשוף אליהם ודרכי ההתמודדות של הארגון

---

16 מסמך "טיוטת תקנות הגנת הפרטיות (אבטחת מידע) התשע"ו-2016"; מכתב משרת המשפטים אל יו"ר ועדת חוקה, חוק ומשפט, טיוטת חוק ודברי הסבר (11.5.16), בחלק המבוא שלפני דברי ההסבר לטיוטת החוק.

עימם; פרטי בעלי התפקיד במאגר - מנהל המאגר וממונה אבטחת המידע (אם מונה בעל תפקיד זה).

באתר מאגרי המידע הממשלתיים שבמרשתת ניתן למצוא את פנקס מאגרי המידע (המאגרים הרשומים אצל רשם מאגרי המידע)[17]. מאגרי אמצעי הזיהוי אינם ברשימה זו. בפגישה עם הרשות להגנת הפרטיות נמסר כי צה"ל לא רשם את המאגרים שברשותו אצל רשם מאגרי המידע.

נמצא כי אף שמאגרי אמצעי הזיהוי שברשות צה"ל מקיימים את התנאים שנקבעו בחוק ולכן חייבים ברישום, צה"ל לא רשם אותם. עוד נמצא כי צה"ל לא גיבש מסמך הגדרות למאגרי אמצעי הזיהוי כנדרש בתקנות אבטחת מידע, הכולל מידע חיוני הקשור למאגרים ולאופן השימוש בהם כמו פירוט הסיכונים העיקריים של פגיעה באבטחת המידע ואופן ההתמודדות מולם.

בתשובת צה"ל נמסר כי למיטב ידיעתם מאגר המידע הצה"לי נרשם ברשם מאגרי המידע בתחילת שנות התשעים של המאה העשרים. לא התקבל מצה"ל מסמך המוכיח זאת.

מומלץ כי צה"ל יכין מסמך הגדרות למאגרי אמצעי הזיהוי כנדרש בתקנות, ויפעל מול הרשות להגנת הפרטיות בנושא רישום המאגרים.

העברת מידע מהמאגר לעמותה א'

נמצא כי במאגרי המידע של עמותה א' נשמר מידע אישי המזוהה עם חיילים, וכי במרשתת יש אינדקציה שעמותה א' מחזיקה במידע רגיש זה.

מומלץ כי צה"ל יבחן להעביר לעמותה א', המחזיקה במאגרי מידע שבהם פרטי חיילים, מזהה אחר במקום המספר האישי.

בתשובת צה"ל נמסר כי יהיה נכון לתקף מחדש את ההסכם עם עמותה א' ולזהות את החיילים לפי מספר הזהות, ולא להעביר פרט מזהה שיסמן אותם במאגר כחיילים.

בתשובת עמותה א' נמסר כי אם צה"ל יאשר צירוף חיילים באמצעות מספר זהות, שם מלא ופרטי קשר הנושא יוסדר.

מידע עודף במערכות אמצעי הזיהוי

בעידן הדיגיטלי איסוף מידע ושמירתו במאגרי מידע נתפסים כהליכים הכרחיים. עם זאת, במקרים רבים המידע הנשמר אינו נחוץ או שאינו רלוונטי להשגת המטרה שלשמה הוא נאסף מלכתחילה או מטרות המאגר שבו הוא נשמר.

17 https://data.gov.il/dataset/pinkas

סעיף 2(9) לחוק הגנת הפרטיות קובע כי פגיעה בפרטיות היא, בין היתר: "שימוש בידיעה על ענייניו הפרטיים של אדם... שלא למטרה שלשמה נמסרה" (להלן - עקרון צמידות המטרה).

הרשות להגנת הפרטיות הפיצה לציבור טיוטת מסמך מדיניות, הסוקר את הוראות הדין ומציג את פרשנות הרשות והמלצותיה בנושא צמצום מידע[18]. במסמך הוגדר כי מידע שנשמר במאגר מידע, אשר אינו רלוונטי או אינו נדרש להשגת המטרה שלשמה הוא נאסף או למטרות המאגר שבו הוא נשמר, נחשב כמידע עודף. מידע עודף יכול להיווצר כבר בשלב איסוף המידע הראשוני או להפוך לכזה במהלך שמירתו לאורך זמן במאגרי מידע. גם בית המשפט העליון בשבתו כבית משפט גבוה לצדק קבע כי הטלת מגבלות על איסוף מידע ועל אגירתו באופן אלקטרוני הן חלק אינטגרלי מהזכות לפרטיות[19].

בנוסף על האמור, החזקת מידע עודף במאגרים גורמת לגידול מיותר בעלויות הניהול והתחזוקה של המאגרים.

תקנה 2(ג) לתקנות אבטחת מידע קובעת כי על בעל מאגר מידע לוודא אחת לשנה שהמידע השמור במאגר אינו רב מן הנדרש בהתאם למטרות המאגר.

נמצא כי צה"ל לא בחן אחת לשנה כנדרש בתקנות אם שמור מידע עודף במאגרי אמצעי הזיהוי, וכן נמצא כי במאגרי המידע של מערכות אמצעי הזיהוי (מערכת א' ומערכת ב') שמור מידע עודף.

מומלץ כי צה"ל יבחן אחת לשנה כנדרש בתקנות אם שמור מידע עודף במאגרי אמצעי הזיהוי. עוד מוצע כי במסגרת הבחינה, ככל שימצא מידע שנדרש אולם אין לו הסמכה בדין, צה"ל ידאג להסדרת ההסמכה של מידע זה.

מידע בנוגע לפטורים משירות ולנפטרים

צה"ל מנהל מעקב אחר מקבלי הפטור מחובת שירות צבאי, וזאת באמצעות סימונם כמשתייכים ליחידת "פטורים". כמו כן צה"ל מקבל ממשרד הפנים עדכון תקופתי בדבר מוות של אזרחים כדי לחדול מלזמנם למילואים, ומסמן אותם במאגרי המידע כמשויכים ליחידת "נפטרים".

נמצא כי צה"ל אינו מוחק ממאגרי אמצעי הזיהוי את רשומות המידע, ובפרט את המידע הביומטרי על חיילים אשר הלכו לעולמם (נפטרים) ואשר לא בוצע לגביהם תהליך זיהוי. מכיוון שכבר אין צורך בזיהוים, המידע עליהם אשר נשמר במאגרים הוא מידע עודף ויש למוחקו. יודגש כי מידע ביומטרי על נפטרים עלול לשמש ביתר קלות למטרת התחזות וגנבת זהות, שכן אין מי שיתלונן על השימוש שנעשה במידע זה.

מומלץ כי צה"ל ימחק ממאגרי אמצעי הזיהוי אחת לתקופה את המידע הביומטרי על חיילים שהלכו לעולמם ואשר לא בוצע לגביהם תהליך זיהוי.

18 "צמצום מידע עודף - מסמך מדיניות, טיוטה להערות הציבור", הרשות להגנת הפרטיות (מאי) 2020.

19 בג"ץ 6732/20 **האגודה לזכויות האזרח בישראל נ' הכנסת**, בפסק דינה של השופטת דפנה ברק-ארז, פסקה 12 (פורסם במאגר ממוחשב, 1.3.2021).

בתשובת צה"ל נמסר כי מוסכם שאין צורך בשמירת אמצעי זיהוי של חיילים שנפטרו ולא בוצע לגביהם תהליך זיהוי. כמו כן נמסר כי תבוצע בחינה לגבי עדכניות נתוני הנפטרים במאגרי המידע של צה"ל ולגבי היכולת למחוק מידע זה.

נמצא כי צה"ל אינו מוחק ממאגרי אמצעי הזיהוי את הרשומות של אנשים שקיבלו פטור משירות צבאי, גם לאחר שחולף זמן משחרורם וכבר לא יחזרו מסטטוס "פטור" לסטטוס "משרת מילואים".

הרבנות הצבאית ציינה כי חשוב לה לשמור את אמצעי הזיהוי של חיילים שקיבלו פטור משירות צבאי כדי שיתאפשר לזהותם בהתרחש אסון לאומי, וכי הנושא נבחן במסגרת עבודת המטה (עמ"ט) "הצבי לישראל". בעניין זה ראו פירוט בפרק "שימוש במאגר אמצעי הזיהוי כצורך לאומי".

אם בסיום עמ"ט "הצבי לישראל" יוחלט לשמור את המידע הביומטרי במסגרת ההיערכות לאסון לאומי עתידי, מומלץ להגביל את הגישה של משתמשים לרשומות אלו בזמן שגרה. אם בסיום העמ"ט יוחלט שלא להשתמש במידע הביומטרי באסון לאומי, מומלץ כי צה"ל ימחק ממאגרי אמצעי הזיהוי אחת לתקופה את המידע הביומטרי על חיילים שקיבלו פטור משירות צבאי.

שדות מיותרים ברשומות

השדה "סוג שירות" הוא חלק מרשומת המידע במערכת ב', והוא מכיל מידע על סטטוס השירות של החייל (חובה / חובה בתנאי קבע / קבע / מילואים / פטור / נפטר).

נמצא שנכון למועד סיום הביקורת באפריל 2022 אין שימוש בשדה "סוג שירות", ולכן הוא בבחינת מידע עודף. כמו כן נמצא כי המידע הנשמר בשדה זה אינו מתעדכן, ועקב כך נפגעת שלמות ומהימנות הנתונים במאגר המידע.

מומלץ כי ענף תכלית יבחן אחת לשנה, כנדרש בתקנות אבטחת מידע, את מבנה הרשומות של מערכות אמצעי הזיהוי ויסיר שדות שאין בהם יותר צורך.

מידע ביוגרפי במערכות אמצעי הזיהוי

מידע ביוגרפי הוא מידע שעל פיו ניתן לזהות מי האדם ממידע אחר הנמצא ברשומה שבמאגר. שמירת מידע ביוגרפי במאגר מידע, כשהוא מוצמד למידע ביומטרי, מגדילה את פוטנציאל הנזק במקרה של חדירה למאגר או הדלפה ממנו. לפיכך הממונה על היישומים הביומטריים ממליץ להפריד בין מידע ביומטרי למידע ביוגרפי[20].

במערכת ב' נכללת טבלה ובה שדות של מידע ביוגרפי.

20 מדיניות לאומית ליישומים ביומטריים, סעיף 4.10.2: "עיצוב מערכת ביומטרית ומימושה ייקחו בחשבון את עיקרון הפרדת המידע הביומטרי מהמידע הביוגרפי, לרבות הקישור ביניהם, ככל שניתן".

מומלץ כי צה"ל יוודא שבכל המאגרים הביומטריים שברשותו יישמר רק מזהה של המתגייס, ולא מידע ביוגרפי נוסף.

מתן הודעה למתגייסים

מסירת אמצעי זיהוי בצה"ל היא חובה לפי סעיף 11 לחוק שירות ביטחון [נוסח משולב], התשמ"ו-1986. בתקנות שהותקנו מכוח החוק נקבע כי אמצעי זיהוי לעניין סעיף 11 לחוק הם טביעת אצבעות וצילומי שיניים. בתקנות לא נקבע כי תמונות פנים ודגימות דנ"א (כתמי דם) הם אמצעי זיהוי לעניין החוק, ולפיכך אין חובה למסירתם על פי חוק זה.

על פי סעיף 11 לחוק הגנת הפרטיות: "פניה לאדם, לקבלת מידע לשם החזקתו או שימוש בו במאגר מידע, תלווה בהודעה שיצוינו בה -

1. אם חלה על אותו אדם חובה חוקית למסור את המידע, או שמסירת המידע תלויה ברצונו ובהסכמתו.
2. המטרה אשר לשמה מבוקש המידע.
3. למי יימסר המידע, ומטרות המסירה".

כאמור, בשר"ח נאספים מן המתגייסים אמצעי זיהוי מסוגים שונים, אך חובה חוקית למסירתם קיימת רק לגבי חלק מהם. להלן לוח המסכם את אמצעי הזיהוי שניטלים מהמתגייסים ובו מצוין אם חלה חובה חוקית למסור אותם:

לוח 2: **סוגי אמצעי הזיהוי והאם חובה למסור אותם**

אמצעי הזיהוי	האם יש חובה חוקית למסור את המידע
טביעות אצבעות וכפות ידיים	V
תמונות פנים	X
צילום שיניים - רנטגן	V
צילום שיניים - אופטי	V
כתמי דם (לדנ"א)	X

בעיבוד משרד מבקר המדינה.

בתשובת צה"ל נמסר כי הרבנות הצבאית מייחסת חשיבות רבה להכללת איסוף כתמי דם בתקנות שירות ביטחון (אמצעי זיהוי). מאז יולי 2021 מתקיים מהלך להכללת דגימות דנ"א בתקנות. הטיפול הוא באחריות לשכת הרמטכ"ל, מכיוון שמדובר בעבודה מול דרג מדיני (שר הביטחון).

נמצא כי בשר"ח לא מקבלים המתגייסים הודעה ובה כל המידע הנדרש בחוק בדבר חובתם החוקית למסור כל אחד מאמצעי הזיהוי הביומטריים. כאמור תמונת הפנים מוצגת למתגייסים כחלק מתחנת הרכשת טביעות אצבעות על אף שאינה מופיעה בתקנות ואין חובה בחוק למסור אותה.

יש שלושה נהלים צבאיים העוסקים באופן ביצוע איסוף כתמי הדם:

1. הנוהל הצבאי העוסק בנטילת כתמי דם קובע כך: "...במידה והחייל מסרב מתבצע הסבר נוסף על חשיבות הדגימה על ידי מפקד התחנה. במידה והחייל עומד בסירובו הוא מוחתם על טופס סירוב אשר מאוחסן במערכת".

2. לפי הוראות "נוהל עבודה בתחנת דנ"א": "במקרים בהם מסרב מתגייס לביצוע לקיחת דגימת הדנ"א, יישלח לאחראית המרפאה אשר תפקידה יהיה לתת הסבר מפורט למתגייס אודות דגימת הדנ"א ועל חשיבותה. במידה והמתגייס אינו מוכן לבצע מתן הדגימה לאחר שיחה עם אחראית המרפאה יחתום על טופס סירוב למתן דנ"א אשר ייסרק לתיקיית סרבני דנ"א...".

3. "טופס סירוב לנטילת דנ"א", מנוסח כך: "למרות כל ההסברים שקיבלתי אני עומד על דעתי ומסרב למסור את דגימת דמי למאגר לצורך זיהוי חללים", וכן: "אני מודע לכך שעובדת סירובי תימסר למשפחתי בעת הצורך".

המתגייסים חותמים על הסכמה מדעת לתת את כתמי הדם אשר מודפסת על טופסי ה-FTA. כאמור, מתגייסים שאינם מסכימים למסור את דגימת דמם מוחתמים על טופס המתעד זאת ומנוסח כ"טופס סירוב".

החתמת מתגייסים על "טופס סירוב" כאשר הם לא מסכימים למסור דגימת דם שמלכתחילה אין מוטלת עליהם חובה למסור, עלולה להתפרש אצל המתגייסים באופן שבו כביכול מימוש זכותם לאי הסכמה היא "סרבנות", על כל הקשרי מונח זה בשיח הצבאי.

מומלץ כי צה"ל ינסח מחדש את הטופס המתעד חיילים שבחרו שלא למסור דגימות דם, באופן שאי-ההסכמה לא תשתמע כדבר פסול או שלילי, לדוגמה: "טופס ויתור על מסירת דגימת דם" או "טופס אי-הסכמה למסירת דגימת דם".

בתשובת צה"ל נמסר כי הנושא נבחן, והוסכם שראוי לשנות את כותרת הטופס. במהלך הביקורת נוסף טופס דיגיטלי למערכת ב' החדשה, ושמו עודכן ל"טופס ויתור".

עוד מומלץ כי צה"ל ישלים את הטיפול באסדרת המקור החוקי לנטילת כל אמצעי הזיהוי שהוא סבור כי עליו לאסוף ממתגייסים.

הגנה פיזית

כללי

סעיף 7 לחוק הגנת הפרטיות מגדיר אבטחת מידע כלהלן: "הגנה על שלמות המידע, או הגנה על המידע מפני חשיפה, שימוש או העתקה, והכל ללא רשות כדין". סעיף 17 לחוק קובע כי בעל מאגר מידע, מחזיק במאגר מידע או מנהל מאגר מידע, כל אחד מהם אחראי לאבטחת המידע שבמאגר. לפי תקנה 4 לתקנות אבטחת מידע, נוהל אבטחה של מאגר מידע יכלול הוראות בעניין האבטחה הפיזית והסביבתית של אתרי המאגר. לפיכך חלה על צה"ל ועל מנהל המאגר וממונה האבטחה של המאגר האחריות לטפל גם בהיבט הפיזי של ההגנה על המידע.

שורה של הוראות דין נועדו להפחית את חשיפת המערכות לסיכון של גישה למידע עצמו. לפי תקנה 6(א) לתקנות אבטחת מידע נדרש להבטיח כי תשתיות ומערכות החומרה, וכן רכיבי התקשורת ואבטחת המידע, יישמרו במקום מוגן המונע חדירה וכניסה אליו בלא הרשאה. כמו כן, לפי תקנה 6(ב) בעליו של מאגר שחלה עליו רמת אבטחה בינונית או גבוהה חייב לנקוט אמצעים הן לבקרה על כניסה לאתרים שבהם נמצאות מערכות אלו ועל יציאה מאתרים אלה והן לתיעוד כניסה ויציאה כאמור. תקנה 4(ג)(1) קובעת כי ההוראות בעניין האבטחה הפיזית והסביבתית[21] של אתרים בהם מצויות תשתיות ומערכות חומרה, וכן רכיבי תקשורת ואבטחת מידע, ייכללו במסמך נוהל האבטחה.

מערכות אמצעי הזיהוי כוללות מתקן מחשב מרכזי הנמצא באחריות ממר"ם ובו נמצאים שרתי מערכת א' ומערכת ב'. כמו כן קיימות עמדות קצה ביחידות שונות המקושרות לשרתים אלו באמצעות הרשת. נוסף על אלו יש רכיבים כלל-צה"ליים: רשתות התקשורת ורכיבי אבטחת המידע, שההגנה הפיזית עליהם היא באחריות מצו"ב וממר"ם.

לפי מתודולוגיה מקובלת להגנה על גופים שהם תשתיות מדינה קריטיות, הגנה פיזית היא: "אמצעי האבטחה הדרושים למניעת נגישות פיזית של גורם לא מורשה לרשומה או לרכיב ממוחשב". בסעיף 9 של "הנחיית מסגרת להגנת הסייבר בממשלה" (להלן - הנחיית יה"ב 5.2) מובאת רשימה של בקרות שנועדו לאפשר הגנה פיזית מפני גישה לא מורשית: הן ברמת האתר כולו, הן ברמת האזורים הרגישים בתוך האתר והן ברמת סביבת העבודה. ההנחה היא כי תוקף יחפש את החוליה החלשה ביותר מבחינת פרצות במערכת ההגנות ומשם ינסה לפגוע. "אתר", לצורך העניין, הוא כל היחידה שבה נמצאות תשתיות ומערכות הקשורות למאגרי אמצעי הזיהוי; "אזור רגיש" הוא המקום - המבנה או החדר בתוך האתר - שבו נמצאים רכיבי המחשוב והתקשורת; ו"סביבת העבודה" היא עמדות המחשב שבאמצעותן יש גישה למערכות.

נמצא כי צה"ל לא גיבש נוהל אבטחה פיזית ייעודי למערכות אמצעי הזיהוי כנדרש בתקנה 4 לתקנות אבטחת מידע, זאת אף ששמור בהן מידע ביומטרי, אישי ורגיש החייב ברמת אבטחה גבוהה.

על צה"ל לפעול לכתיבת נוהל אבטחה פיזית, כנדרש בתקנות.

21 המונח "אבטחה סביבתית" נוגע לשמירה על סביבת המערכות מפני נזקים כגון נזקי אש ומים.

בתשובת צה"ל נכתב כי נוהל האבטחה הפיזית בהיבט ביטחון המידע ייקבע בהתאם להגדרת הסיווג המרבי של מערכות אמצעי הזיהוי.

משרד מבקר המדינה בדק בתחום ההגנה הפיזית את הנושאים שלהלן ביחידה א': הגנה פיזית ובקרה על הכניסות והיציאות, הגנת סביבת העבודה והגנה סביבתית.

בביקורת משרד מבקר המדינה הועלו פערים בנושאים האמורים אשר הוצגו לגופים המבוקרים במאי 2022 לצורך ביצוע פעולות תיקון נדרשות.

הדרכת עובדים בנושא אבטחת רשומות והגברת מודעותם לנושא

תקנה 7 לתקנות אבטחת מידע קובעת כי לא ייתן בעל מאגר גישה למידע המצוי במאגר אלא אם כן נקט באמצעים סבירים המקובלים בהליכי מיון עובדים ושיבוצם, כדי לברר שאין חשש כי בעל ההרשאה אינו מתאים לקבלת גישה למידע המצוי במאגר. על מנת ליישם תקנה זו נדרש לוודא כי העובדים מודעים לנושאי פרטיות ואבטחת מידע.

בפקודת מטכ"ל 21.0123 בנושא אבטחת רשומות במערכות תקשוב נקבע, בסעיף שכותרתו "שינון הפקודה, הכשרה והדרכה", כלהלן: "פקודה זו והוראות מקצועיות משלימות... ישוננו בכל תחום שיש בו עיסוק במחשב האישי וברשומותיו". לצורך יישום הפקודה יש לקיים הדרכה ייעודית בנושאי אבטחת רשומות מידע לכל משתמשי המערכות של אמצעי הזיהוי.

גם בקווים המנחים של המדיניות הלאומית ליישומים ביומטריים יש הנחיות בנושא זה:

1. סעיף 4.11.1 - על הנהלת הגוף לוודא כי קיימת מודעות לנושא הגנת הפרטיות וכבוד האדם בקרב הגורמים בגוף העוסקים ביישומים הביומטריים או במידע הביומטרי.
2. סעיף 4.11.2 - על הנהלת הגוף לוודא קיום פעילויות הדרכה לגורמים הנ"ל, שמטרתן הטמעת תחושת המחויבות לנושא הגנת הפרטיות וכבוד האדם.

בפגישות עם גורמים ביחידות שונות הקשורות למערכות אמצעי הזיהוי רוכז מידע באשר לפעולות שננקטו לצורך הדרכה והעלאת המודעות בנושאי הגנת הפרטיות ואבטחת מידע. להלן הפירוט:

1. באכ"א לא הוכנה ליחידות השונות שיש להן זיקה למערכות אמצעי הזיהוי תוכנית הדרכות בנושאי הגנת הפרטיות. כאמור, בשנת 2021 החלו אכ"א והרשות להגנת הפרטיות לקדם תוכנית עבודה להדרכה בנושא הגנת הפרטיות ולהכשרת ממוני הגנת הפרטיות ביחידות.
2. במיטב מתקיימת הדרכה סדירה לחיילי היחידה בנושאי מודעות להגנת הסייבר ואבטחת מידע, אך נמצאו פערים הקשורים בביצוע תרגילים.
3. מהרבנות הצבאית נמסר כי הדרכות בנושאי ביטחון מידע מתקיימות על פי המתחייב בפקודות הצבא כחלק מתהליך קליטה ביחידה (תחנה ב"טופס טיולים נכנס") ובהדרכות עיתיות, כמו כן מתבצעים באופן שוטף תדריכים בנושא חובת השמירה על חסיון מידע אישי.

4. מפקד מעבדת טביעות האצבע ציין כי הוא הוציא הוראות פנימיות לחיילי המעבדה, ובכלל זה הוראות האוסרות על הכנסת מכשירים סלולריים לאזור עמדות העבודה.

נמצא כי גורמים העוסקים במערכות אמצעי הזיהוי שמכילות מידע פרטי ורגיש, אשר לפי תקנות אבטחת מידע רמת האבטחה שלהן נדרשת להיות גבוהה, לא עוברים הדרכה מובנית בנושאי הגנת הפרטיות והגנת הסייבר וכן לא מתרגלים אותה.

מומלץ כי חטיבת ההגנה האחראית לביטחון מערכות המידע, בשיתוף עם מחלקת ביטחון המידע, יקיימו פעולות הדרכה שישולבו עם תרגולים מעת לעת בנושאים הקשורים בהגנת הפרטיות, באבטחת מידע ורשומות מידע ממוחשבות, וזאת בהתאם לסיכום בין אכ"א לרשות להגנת הפרטיות. את פעולות ההדרכה והתרגול הללו יש להעביר לכלל בעלי ההרשאות למערכות אמצעי הזיהוי בצה"ל אשר מכילות מידע רגיש או מסווג.

הגנה לוגית

בהנחיית המסגרת להגנת הסייבר בממשלה 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 נכתב 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.

משרד מבקר המדינה בדק בתחום ההגנה הלוגית את הנושאים שלהלן: הזדהות; הרשאות גישה; סקר בקרת גישה; בקרה על ביצוע פעולות לא מורשות; מנגנוני הצפנה; בקרה שוטפת לצורך תהליכי הגנה על יישומים.

בביקורת משרד מבקר המדינה הועלו פערים בנושאים האמורים אשר הוצגו לגופים המבוקרים במאי 2022 לצורך ביצוע פעולות תיקון נדרשות.

שינויים מבוקרים

מדיניות ההגנה של צה"ל קובעת כי שינויים ושיפורים (להלן - שו"ש) במערכות התקשוב יבוצעו רק לאחר קבלת אישור ועדת הגנת מערכות תקשוב.

רע"ן תכלית מסר לצוות הביקורת כי אישורים כאלו נדרשים רק כאשר מתבצע שינוי מהותי ולפי שיקול דעתו של קצין הפרויקט. לפני כל הכנסת עדכון תוכנה לרשת מבוצעת סריקה של המידע במערכת שפותחה על ידי מצו"ב הסורקת את עדכון התוכנה לאיתור איומים שונים.

נמצא כי שו"שים פותחו במערכת ב' החדשה ובמערכת ג', בהם שדרוג תשתיות טכנולוגיות שבוצע במערכת ב' החדשה, מבלי שהתקבל אישור מיחידת ההגנה בסייבר כנדרש במדיניות ההגנה.

מומלץ כי ועדת האמל"ח תבחן את השינויים המתוכננים במערכות אמצעי הזיהוי ואת הצורך שלהם בקבלת אישור יחידת ההגנה ובמיוחד ביחס לשדרוג של השרתים במערכת א' הצפוי להתחיל ביולי 2022 ולהסתיים במאי 2023.

מיקור חוץ

לפי תקנה 15 לתקנות אבטחת מידע בעל מאגר המתקשר עם גורם חיצוני לצורך קבלת שירות הכרוך במתן גישה למאגר יקבע במפורש בהסכם עם הגורם החיצוני, בין השאר, את חובתו של הגורם החיצוני להחתים את בעלי ההרשאות שלו על התחייבות לשמור על סודיות המידע, להשתמש במידע רק לפי האמור בהסכם וליישם את אמצעי האבטחה הקבועים בהסכם.

מערכת א' היא מוצר מדף שצה"ל רוכש מספק בחו"ל (להלן - חברה א'). הזמנת הרכש מחברה א' היא עבור המוצר ועבור שירותי תמיכה טכנית. חברה ב' מספקת את התמיכה הטכנית ללקוחות חברה א' בישראל, הגישה שלהם למערכות היא רק מתוך בסיס צה"ל ולא מתאפשרת גישה מרחוק.

בשלבי סיום הביקורת ביוני 2022 הושלם תהליך ההסמכה של חברה ב' על ידי הממונה על הביטחון במערכת הביטחון (מלמ"ב) אשר במסגרתה עברו עובדי חברה ב' הליך של סיווג בטחוני כדי שיוכלו לקבל משתמש "חזק" במערכות צה"ל ולבצע את הפעולות ללא ליווי של מנהל רשת באופן שבו כל הפעולות שלהם במערכות יהיו מנוטרות ומתועדות.

משרד מבקר המדינה מציין לחיוב את הפעולות שנקט צה"ל במהלך הביקורת כדי לוודא שיש לחברה ב' המספקת תמיכה טכנית למערכת א', גישה מאובטחת למערכות אמצעי הזיהוי ואת הפעולות שנקט כדי לבקר גישה זו.

המשכיות עסקית

תוכנית להמשכיות עסקית

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

באירוע מתמשך ומרובה נפגעים כמלחמה, תהליך איסוף אמצעי הזיהוי, ניהולם והשימוש בהם בצה"ל הופך לקריטי ומחייב תפקוד וזמינות מלאים של התהליך. מנגד עלול אירוע כזה לפגוע ביכולתו של צה"ל לבצע את התהליכים העסקיים העיקריים הקשורים באמצעי הזיהוי - איסוף

האמצעים וזיהוי החללים. נוכח זאת מוטל על צה"ל להבטיח יכולת להמשכיות עסקית בעת חירום.

הנחיה 1.3.06 של ראש רשות התקשוב הממשלתי בנושא "היערכות להמשכיות עסקית ותפקודית בשעת חירום" (להלן - הנחיה בנושא המשכיות עסקית) מגדירה תוכנית המשכיות עסקית (BCP[22]) כך: "תכנית פעולה מקיפה, הקובעת נהלים ומערכות הדרושים כדי לשמר את המשכיות פעילות המשרד במצב חירום ולשקמה במידת הצורך"[23]. ההנחיה מפרטת את תהליך קבלת ההחלטות ואת ההיערכות הנדרשת למקרה של התממשות איום אשר עלול לגרום נזק לתפקוד הארגון והשבתה חלקית או מלאה של שירותים ותהליכים עסקיים ותפקודיים. רשימת עקרונות דומה, שיאפשרו המשך פעילות של המערכות החיוניות בעת חירום, מובאת גם בהנחיית יה"ב 5.2.

פיתוח תכנית המשכיות עסקית נחלק לשלבים העיקריים האלו:

1. ניתוח התהליכים הרלוונטיים והגדרה של השלבים החיוניים בכל תהליך אשר נדרש כי ימשיכו לפעול 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 מכל שלב בתהליך בהתרחש אירוע חירום ופרק הזמן הנדרש להחזרת הפעילות בהיקף האמור מרגע קרות האירוע.

ב. יעד אחזור הנתונים (RPO) - היקף אובדן המידע שצה"ל מוכן להכיל בהתרחש אירוע חירום[24].

4. הכנת תוכנית התאוששות מאסון (להלן - DRP) - אוסף התהליכים שעל הארגון לבצע כדי לחזור לכשירות בקרות אירוע, בהלימה ליעדי ההתאוששות שהארגון הגדיר בתוכנית ההמשכיות העסקית. במסגרת פיתוח התוכנית יש לוודא כי ליחידות הרלוונטיות מוקצים משאבים ותשומות שיאפשרו זאת.

עפ"י הנחיית יה"ב 5.2, ארגון נדרש לתרגל את התוכנית שלו להמשכיות עסקית בתדירות קבועה ולפחות אחת לחמש שנים. על פי הנחיית ראש רשות התקשוב מטרת התרגול היא לבחון את מערך השיקום ואת יכולת ההתאוששות מאסון שהוגדרה בתכנית ה-BCP, ובכלל זה את מידת העמידה ביעדים. בסיום התרגול על הארגון לבצע הליך של הפקת לקחים והיזון חוזר ולתקף את תוכנית ההמשכיות העסקית.

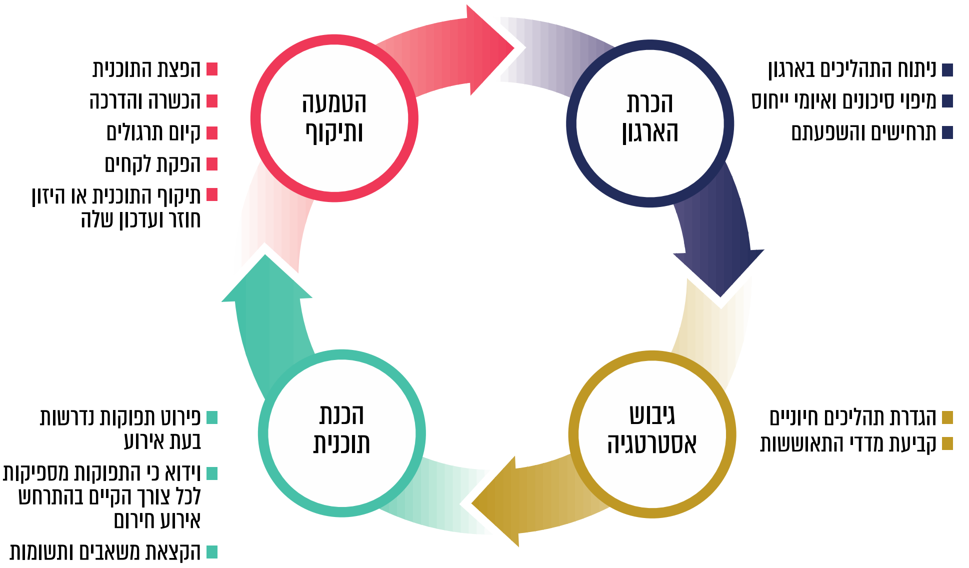
---

22 Business Continuity Plan.

23 הנחיה מ-18.11.20, סעיף 4.14. המונח אינו נוגע לפעולות ההצלה הראשוניות המתבצעות בהתרחש האירוע, אלא להתכוננות לקראתו ולהיערכות להשגת יכולת התאוששות מהירה לאחריו.

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

תרשים 8: **תהליך הטמעת תוכנית המשכיות עסקית**



בעיבוד משרד מבקר המדינה.

נמצא כי בניגוד לנורמות מקובלות בתחום, צה"ל לא פיתח לתהליך אמצעי הזיהוי תוכנית המשכיות עסקית שמכסה את כל התהליכים הקשורים לאמצעי הזיהוי ואת כל היחידות המעורבות בתהליכים אלו, ולא הגדיר מהם החלקים בתהליך שהם קריטיים לאירוע חירום. עוד נמצא כי צה"ל לא ביצע תרגול הפעלה במתכונת חירום של כל המערך הנדרש לזיהוי חלל. במצב זה חשוף צה"ל לסיכונים שיגרמו להתאוששות ממושכת, כגון: פגיעה או השבתה באמצעי ההרכשה שרכישתם המחודשת צפויה לארוך תקופה של כמה חודשים.

בתשובת צה"ל נמסר כי על מתקנים פיזיים לעמוד בתקן רציפות התפקוד בצה"ל בהתאם לרמת החיוניות שנקבעה עבורם. באשר לקיום תרגולים, בהתאם לגרף האימונים הצה"לי נעשים תרגולים של תרחישים המדמים פגיעה ברציפות התפקודית של מתקן פיזי או של תהליך עסקי מסוים.

משרד מבקר המדינה מציין כי תקן רציפות התפקוד בצה"ל מתייחס למתקנים פיזיים ואינו מתייחס לתהליך השלם של אמצעי הזיהוי המורכב מתהליכי משנה אשר מערבים כמה יחידות וכמה מתקנים פיזיים.

מומלץ כי צה"ל יגבש תוכנית התאוששות עסקית לתהליך אמצעי הזיהוי ובמסגרתה יבחן את מכלול התהליכים, הסיכונים וההשלכה של התממשותם, ויגדיר את רמת המענה שניתן לכל סיכון. עוד מומלץ כי צה"ל יערוך באופן עיתי תרגולי חירום כך שיכוסו כל התהליכים הקשורים לאמצעי הזיהוי וכל היחידות המעורבות בתהליכים אלו.

תהליך ההרכשה ויתר התהליכים הנוגעים לזיהוי חלל מתבצעים בכמה יחידות בצה"ל. להלן תפורט היערכות היחידות לאירוע המצריך הפעלה של תוכנית להמשכיות עסקית.

יחידות שחר וממר"ם

גיבוי של הנתונים ושל סביבת המערכת[25] הוא שלב חיוני בתהליך המשכיות תפקודית. נמצא כי המידע שקיים במאגרי המידע משוכפל מיד לאתר חלופי, וכן כי צה"ל מגבה מידע זה באופן סדיר.

נוסף על ביצוע הגיבוי, נודעת חשיבות לביצוע תרגולים עיתיים לאחזור המידע מאתר הגיבוי. מטרת התרגולים היא לוודא כי ידוע היכן (באיזה אתר, באיזו מדיה) שמור המידע המגובה וכי המידע המגובה הוא בר-אחזור תוך עמידה ביעד אחזור הנתונים[26].

נמצא כי יחידת ממר"ם, בניגוד למקובל בתחום, לא ביצעה תרגולים עיתיים של אחזור המידע מגיבויים כדי לבדוק את תקינות הגיבויים ואת העמידה ביעד אחזור הנתונים. תרגול זה לא בוצע היות והוא מצריך ביצוע תהליכים מקדימים ובהם הקמה של סביבה נפרדת שאליה יבוצע השחזור, כדי שלא לפגוע בנתונים העדכניים הקיימים.

נוכח החשיבות שיש לבדיקת תקינות ואיכות הגיבויים, מומלץ כי אחת לתקופה יבוצע תרגול של אחזור מלא מגיבוי, כולל ביצוע תהליכים מקדימים.

מערכות אמצעי הזיהוי בעלות יכולת שרידות, לכן בהתרחש אירוע המשפיע על ההמשכיות העסקית קיימת אפשרות להמשיך את הפעילות.

בתשובת צה"ל נמסר כי על מנת לאפשר רציפות תפקודית (המשכיות עסקית) במערכות מידע, כאשר למשתמשי הקצה קיימים אתרים חלופיים, אפשר להמשיך לפעול מאתרים אלו.

נמצא כי לגבי אתרים חלופיים שנקבעו מראש, צה"ל לא וידא כי המערכות נגישות באופן קבוע גם מאתרים אלו. עוד נמצא כי לגבי מערכות שאינן מחייבות עבודה באתר חלופי מסוים, למשל: מערכת א', צה"ל לא הגדיר דרישות ומדדי התאוששות לביצוע המעבר לגישה אליהן מעמדת מחשב אחרת ברשת הצה"לית, ונדרשות פעולות מסוימות כדי שמשתמשי הקצה יוכלו לקבל גישה למערכות אלו מעמדה אחרת.

מומלץ כי עבור אתרים חלופיים שהוגדרו מראש, יסדירו יחידת שחר בשיתוף קצין האמל"ח והמשתמש המבצעי גישה קבועה של המשתמשים למערכות אמצעי הזיהוי. עבור משתמשים שיידרשו להיכנס למערכות מכל עמדת מחשב ברשת הצה"לית, מומלץ כי יחידת ממר"ם תפרסם נוהל DR מפורט עבור התחברות חלופית של משתמשי הקצה למערכות אמצעי הזיהוי. עוד מומלץ לתרגל באופן עיתי את המשתמשים המבצעיים בעבודה מאתרים חלופיים או מעמדות מחשב אחרות.

25 הנחיית ראש רשות התקשוב, סעיף 6.3.2.

26 הנחיית ראש רשות התקשוב, סעיף 6.3.3.

יחידת מיטב

יחידת מיטב מבצעת כאמור את תהליך ההרכשה בשר"ח בבסיס הקליטה והמיון שבתל השומר. בחלק מתחנות ההרכשה יש ציוד ייעודי כמו מכונות רנטגן וחומרה ייעודית. עלות חלק מהמכונות שקיימות בתחנות ההרכשה נאמדת במאות אלפי ש"ח לכל מכונה, לכן כל מצאי הציוד הייעודי שקיים בצה"ל משמש אותו לפעילות השוטפת בשר"ח, וצה"ל אינו מנהל מלאי של מכשירים נוספים במקום אחר. תהליכי הרכש של ציוד זה צפויים לארוך חודשים רבים.

נמצא כי בעת אירוע חירום, תקלה הנוגעת להפעלת השר"ח או כל מניעה אחרת להפעלתו עלולה לעצור את תהליך ההרכשה של אמצעי הזיהוי. בשל תהליך הרכש הממושך של המכונות המשמשות להרכשה ובשל היעדר ניהול מלאי, ההשבתה עד להפעלה מחודשת של התהליך עלולה לארוך כמה חודשים.

עוד נמצא כי גם תקלה משביתה בציוד בעת שגרה תגרום לפגיעה ניכרת בביצוע ההרכשות ולהיעדר אפשרות להפעיל את העמדה התקולה במשך חודשים רבים[27]. כמו כן, לצה"ל אין הסכמים עם גופים אחרים המחזיקים בציוד דומה שיכולים לסייע בעת אירוע חירום.

לדברי ראש ענף קליטה ולוגיסטיקה במיטב (להלן - רע"ן קו"ל), עצירת תהליך ההרכשה למשך כמה חודשים אינה בעייתית שכן המתגייסים החדשים ממילא נמצאים בהכשרה בתקופה זו ואינם צפויים להשתתף בלוחמה. כמו כן, לדבריו לא נחתמו הסכמים עם גופים אחרים המחזיקים ציוד דומה מפני שאסור לחבר לרשת הצה"לית ציוד שהיה מחובר לרשתות אזרחיות בגורמים אזרחיים, וזאת מטעמי אבטחת מידע.

השלמת הרכשת אמצעי זיהוי מתבצעת רק בין מחזורי גיוס ובקצב נמוך, לכן אם יושבת תהליך ההרכשה צפוי כי איסוף אמצעי הזיהוי יושלם זמן רב לאחר סיום ההשבתה. לדוגמה, עקב מגיפת הקורונה לא נאספו במשך כשנה אמצעי זיהוי של חלל הפה, וביחידת מיטב העריכו כי השלמת איסופם של אמצעי הזיהוי צפויה להימשך לפחות שנתיים.

מומלץ כי במסגרת גיבוש תוכנית ההתאוששות העסקית ופיתוח תוכנית DRP יבחן צה"ל את מכלול הסיכונים ואת ההשלכה של התממשותם, כגון קצב ההשלמה האיטי של איסוף אמצעי הזיהוי במקרה של השבתה ממושכת, ויגדיר את רמת המענה שניתן לכל סיכון.

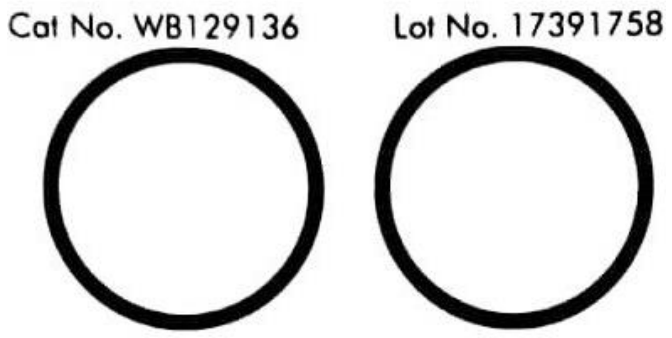
אוסף כתמי הדם

אחד מאמצעי הזיהוי שמוסרים המתגייסים בשרשרת החיול הוא כתמי דם. כתמים אלו נשמרים על גבי כרטיסי FTA [28] בעלי שני אזורי דגימה. כשיש צורך בזיהוי חלל, אפשר לפענח מכל אחד מאזורי הדגימה בנפרד פרופיל גנומי. הכרטיסים נשמרים באוסף כתמי הדם.

27 ראו בפרק בנושא שלמות המידע פירוט לגבי היכולת לבצע השלמות של הרכשות.

28 https://www.sigmaaldrich.com/IL/en/product/sigma/whawb120205.

תמונה 1: **דוגמה לנייר FTA שבו שומרים את כתמי הדם**[29]



המקור: חלק מטופס FTA של צה"ל.

בדיון שהתקיים בדצמבר 2015 כחלק מפרויקט העברת מחנה ג' נקבע כי יש צורך לקיים ניתוח משלים של צורכי הרבנות הראשית, בדגש על מאגר ומעבדות הדנ"א, כדי לייצר יתירות.

נמצא כי אף שבכל כרטיס FTA יש כפילות של המידע (שני כתמי דם), האוסף הפיזי של כתמי הדם נשמר במקום יחיד וצה"ל לא יצר יתירות על ידי חלוקה של שני כתמי הדם שבכל דגימה באוסף לשני מקומות פיזיים שונים. נוכח זאת בעת אירוע של פגיעה בארכיון צה"ל יש סיכון לאובדן מלא של המידע או למניעת הגישה אליו.

מומלץ כי צה"ל יבחן את הצורך בחלוקת אוסף כתמי הדם לשני מקומות כדי להפחית את הסיכון האמור.

בתשובת צה"ל נמסר כי בעקבות הביקורת עלה למודעות הצורך בכפילות של אוסף כתמי הדם, וכי הנושא עלה לדיון בראשות רח"ט לוגיסטיקה בנושא הדרישות לפרויקט "אופק רחב"[30].

שלמות המידע הביומטרי ויעילות תהליכי העבודה

חוק הגנת הפרטיות, התשמ"א-1981[31] מגדיר שלמות מידע כך: "זהות הנתונים במאגר מידע למקור שממנו נשאבו, בלא ששונו, נמסרו או הושמדו ללא רשות כדין".

29 Cat No. - מספר קטלוגי של הפריט; Lot No. - מספר אצווה בייצור.

30 מחנה רב-יחידתי חדש שאליו יועברו יחידת מיטב ואוסף כתמי הדם.

31 חוק הגנת הפרטיות התשמ"א-1981, פרק ב' בחוק, סעיף 7.

לפי ההגדרות שבתקנות אבטחת מידע[32], אירוע אבטחה חמור הוא אירוע שבו נגרמה פגיעה כלשהי בשלמות המידע במאגר מידע שחלה עליו רמת אבטחה גבוהה, או בשלמות המידע לגבי חלק מהותי ממאגר שחלה עליו רמת אבטחה בינונית.

סעיף 11 לחוק שירות הביטחון מחייב כל מתגייס להתייצב במקום ובזמן שנקבעו בצו לשם מתן אמצעי זיהוי. אמצעי הזיהוי הנדרשים הוגדרו בתקנות שירות הביטחון ובפק"א.

להלן יוצגו כמה נושאים הנוגעים להיבטי שלמות המידע ולייעול תהליכי עבודה שעלו בביקורת:

שלמות אמצעי הזיהוי במאגר זיהוי חללים

חוסרים באמצעי הזיהוי במאגרי המידע לזיהוי חללים יכולים להיווצר במהלך תהליך ההרכשה מהסיבות המפורטות להלן. בכל אותם המקרים המתגייס יידרש לבצע הרכשה חוזרת:

1. השבתת עמדות הקצה להרכשת אמצעי הזיהוי - ההשבתה עשויה להיגרם במהלך תקופת משבר אפידמיולוגי כמו בתקופת הקורונה, בשל היעדר אישור של בטיחות העמדה כמו אישור בטיחות קרינה (בצילומי שיניים), ובשל תקלות טכניות שאינן מאפשרות את העברת המידע מעמדת ההרכשה למאגר המידע (טביעות אצבע).

2. מגבלות בריאותיות - מגבלות המונעות מהמתגייס לבצע את ההרכשה כמו היריון או מוגבלות פיזית.

3. איכות הרכשה לא מספקת - מקרים שבהם רק לאחר שהמתגייס יצא ממתחם השר"ח נמצא כי איכות אמצעי הזיהוי שהורכש לו לא הייתה מספקת.

השלמת אמצעי הזיהוי יכולה להתבצע רק בין מחזורי הגיוס, שכן במהלכם התחנות פועלות במסגרת העבודה השוטפת. יחידת מיטב מקצה כ-60 ימים בשנה לביצוע הרכשות חוזרות ומעבירה את המועדים האלו למקמש"ר - ענף תורה והדרכה, כדי שתזמן את החיילים המשרתים בשירות סדיר או בשירות קבע שיש חוסר באמצעי הזיהוי שלהם. ניתנת עדיפות להשלמת אמצעי זיהוי ללוחמים. כמו כן, ניתנת עדיפות להשלמת טביעת אצבע על פני שאר אמצעי הזיהוי.

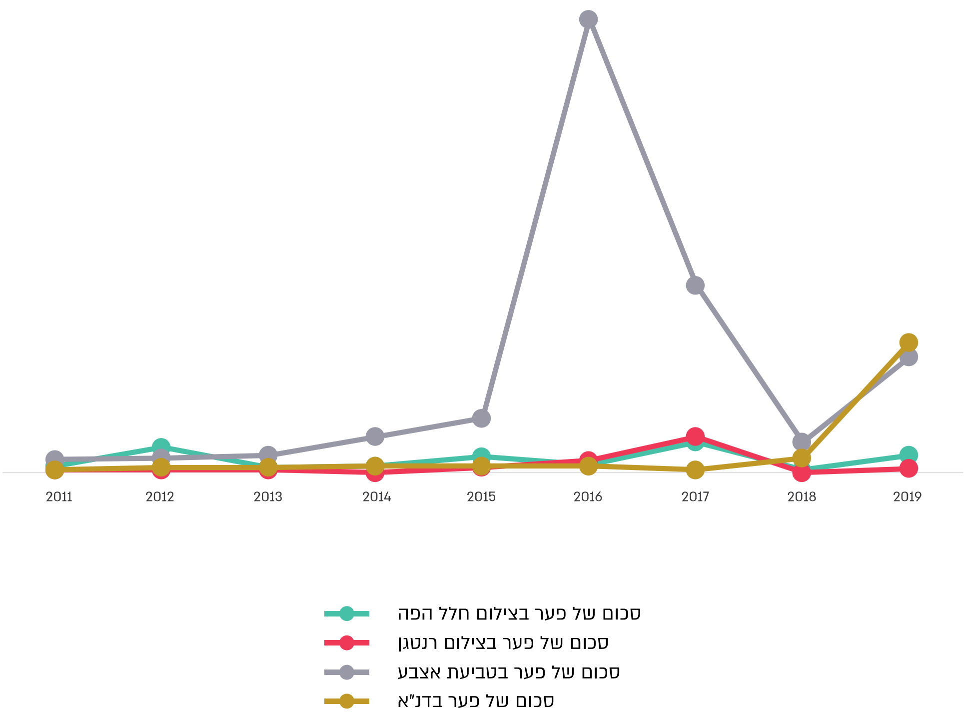
> בתחילת התפשטות נגיף הקורונה, החל ממרץ 2020 ועד אפריל 2021, לא בוצעו צילומי חלל פה של חיילים בשל החשש להעברת הנגיף בתהליך הבדיקה. עקב כך לא בוצע צילום חלל פה של כמה עשרות אלפים מהחיילים בעת הגיוס, ונדרש לזמנם למיטב כדי להשלים את נטילת אמצעי הזיהוי. נכון לאוגוסט 2021, השלימו את נטילת אמצעי הזיהוי כמה אלפי חיילים (5%) בלבד, ולהערכת מיטב תידרש עוד כשנה וחצי עד להשלמת נטילת אמצעי זיהוי זה.

בניסיון להדביק את קצב השלמת הפערים הועלתה במקמש"ר יוזמה להפעלת תחנה ניידת להרכשת אמצעי זיהוי מהלוחמים בשטח. הושלם פיילוט ראשון שיצא לדרך בתקופה שבין הגיוסים (פברואר-מרץ 2022) עם עמדות הרכשה שהושאלו מהשר"ח, למעט עמדת צילומי חלל

32 תקנה 1 לתקנות אבטחת מידע- פרק הגדרות, הגדרת "אירוע אבטחה חמור".

פה שאינה מתאימה לשימוש כעמדה ניידת. צה"ל מסר כי החל בתהליך רכש של מצלמה ייעודית לטובת התחנה הניידת.

תרשים 9: **אמצעי זיהוי חסרים לפי שנים וסוג אמצעי**



על פי נתונים שהתקבלו ממערכת ב', בעיבוד משרד מבקר המדינה.

נמצא כי מאגר הנתונים הביומטריים של צה"ל המכיל מאות אלפי רשומות אינו שלם. במאגר קיימות כמה מאות אלפי רשומות של משרתי חובה וקבע שנכון למועד סיום הביקורת באפריל 2022, חסרים בהם אמצעי הזיהוי האלו: 0.5% מטביעות האצבע, 6.6% מתצלומי הרנטגן, 32.8% מתצלומי חלל הפה ו-3.8% מדגימות הדנ"א. עוד נמצא כי יש חוסרים של מאות טביעות אצבע של חיילים שהתגייסו בשנים 2016 ו-2017 ושל כמה אלפי תצלומי שיניים עבור אנשי קבע שהתגייסו בין השנים 1994 - 2004. כמו כן, נמצאו חוסרים באמצעי זיהוי של מתגייסים מלפני עשר שנים ומעלה. נמצא כי ל-1 מכל 87 משרתים פעילים יש רק אמצעי זיהוי אחד, דבר שמעלה חשש ליכולת הזיהוי שלהם.

עוד נמצא, כי אם עמדת הרכשה מושבתת לפרק זמן של מחזור גיוס אחד, ההשלמה של אמצעי זיהוי עלולה להימשך כ-6 חודשים (אף שבפרק זמן זה החיילים נמצאים בתקופת הכשרה, עדיין תיתכן פגיעה גם בבסיסים עורפיים בשעת חירום). לנוכח חוסרים אלו יש חשש שתפגע פעולת הזיהוי של חללים בעת הצורך.

מומלץ כי אכ"א יגביר את פעולתו לצמצום הפערים בהרכשת אמצעי הזיהוי החסרים, תוך תיעדוף ההשלמות לפי אופי שירותם של החיילים (שירות קרבי, רמות סיכון וכיו"ב), סוג אמצעי הזיהוי (טביעות אצבע) ומספר הפעמים שנקראו להשלמה. במסגרת המאמץ לצמצום הפערים מומלץ לקדם את היוזמה להפעלת תחנה ניידת להרכשת אמצעי זיהוי, בכלל זה תצלומי שיניים.

שמירת מידע מחוץ למערכות המידע לזיהוי חללים

על פי התוספת הראשונה לתקנות אבטחת מידע, על מאגר מידע הכולל מידע על צנעת חייו האישיים של אדם וכן על מידע רפואי של אדם חלה רמת אבטחה בינונית. כאמור, תקנות אבטחת מידע מפרטות כיצד על הארגון להגן על מידע זה.

בביקורת נמצא כי מידע שמור מחוץ למערכות המידע ובכלל זה מידע על צנעת חייו האישיים של האדם וכן מידע רפואי. להלן דוגמאות:

1. **מתגייסים עם מוגבלויות רפואיות או פיזיות:** לפי הנוהל הקיים בשר"ח, מתגייס אשר בשל מגבלה רפואית או פיזית אינו יכול לבצע הרכשה של אמצעי זיהוי, כמו מתגייסת בהריון, אינו נדרש לבצע את ההרכשה. במערכת ב' אין חיווי על כך שאמצעי הזיהוי לא נלקח מסיבות רפואיות, ולכן מצוין במערכת ב' כי יש חוסר באמצעי זה.

נמצא כי במערכת ב' לא נשמר חיווי על מתגייסים שאינם יכולים לבצע את ההרכשה עקב מוגבלות רפואית או פיזית, ולכן חיילים אלו מזומנים לבצע הרכשה חוזרת אף שלעיתים במועד החדש הם לא יוכלו לבצעה.

מומלץ כי מיטב תוסיף דרישה לשו"ש במערכת ב' החדשה שיאפשר לציין מדוע לא ניתן לבצע את ההרכשה. באופן זה יוזמנו להשלמות אמצעי הזיהוי רק החיילים שאפשר להרכיש מהם את האמצעים באותו המועד.

בתשובת צה"ל נמסר כי במערכת ב' החדשה, שנכון ליוני 2022 נמצאת בשלבי קבלה, פותחה היכולת לתעד סיבת אי הרכשה עקב מגבלה רפואית.

2. **מתגייסים המסרבים למסור דגימות דם:** מתגייס המסרב למסור דגימת דם נדרש לחתום על טופס סירוב. בסוף יום הגיוס סורקים את הטפסים של המתגייסים שחתמו על סירוב לתיקייה ברשת ומעבירים אותם בדואר האלקטרוני למנהל אוסף כתמי הדם. המידע נשמר מחוץ למערכת. בקליטת הדגימות באוסף כתמי הדם מסמנים את מי שסרב במערכת ב'.

נמצא כי טופסי הסירוב להרכשת כתמי דם לא נשמרים במערכת ב' ועקב כך לא ניתן יהיה לאחזר אותם בקלות במידת הצורך. כמו כן, יש חוסר יעילות בכך שרק עם הגעת הדגימות לאוסף כתמי הדם נדרש להזין במערכת את פרטי מי שסרב, אף שהסירוב היה כבר בשר"ח.

מומלץ כי יחידת מיט"ב תוסיף למערכת ב' החדשה שו"ש שיאפשר את קליטת טופסי הסירוב ואת סימון מי שסרב להרכשת כתמי דם במערכת ב' כבר בתהליך ההרכשה בשר"ח.

בתשובת צה"ל נמסר כי במערכת ב' החדשה, שנכון ליוני 2022 נמצאת בשלבי קבלה, פותחה היכולת לתעד את אי-ההסכמה למסירת מידע על ידי המתגייס ולהחתים אותו בצורה דיגיטלית.

ניהול מערכות אמצעי הזיהוי

רקע

מחזור חיי מערכת מידע כולל שלבים שונים, ומקובל להפריד בין שני השלבים האלו: מערכות בהקמה ומערכות בתחזוקה. שלב הקמת המערכת נחלק לכמה תתי-שלבים: ייזום, איסוף דרישות, אפיון, פיתוח, בדיקות, מבצע והרצה. שלב תחזוקת המערכת הוא השלב שבו לקוחות המערכת משתמשים בה וצוות הפרויקט מבצע עדכונים ושיפורים במערכת בהתאם לתקלות ולדרישות חדשות.

מתודולוגיה לניהול פרויקטים

נוהל מפת"ח הוא נוהל מסגרת לטיפול כולל בתחום המחשוב בארגון - הן בכל אחת ממערכות המידע בנפרד, הן במישור הארגון כולו. הנוהל נקבע בהחלטת הממשלה[33] משנת 1991 כנוהל אחיד מחייב לפיתוח ולתחזוקה של כל מערכות המידע הממשלתיות. בהחלטת ממשלה[34] משנת 2014 בוטלה ההחלטה האמורה בנוגע לנוהל מפת"ח והוטל על רשות התקשוב הממשלתי לגבש מתודולוגיה לניהול מחזור החיים של מערכות מידע ולניהול יעיל של פרויקטים, תשתיות ותהליכים בתחום התקשוב, ולהעמיד לרשות אגפי מערכות המידע כלים מתקדמים ליישומה.

בהנחיה של רשות התקשוב מאפריל 2020 בנושא "מסגרת מתודולוגיית תקשוב ממשלתית" (להלן - הנחיות מסגרת מתודולוגיה) הגדירה הרשות מתודולוגיה סדורה באופן זה: "מתודולוגיה מוכרת או מתודולוגיית תקשוב ממשלתית או מתודולוגיה שפותחה ע"י המשרד ובתנאי שמתייחסת ומכילה פתרונות להיבטים הניהוליים, הכלכליים והטכנולוגיים ולהיבטי הלקוחות של מערכות המידע והטכנולוגיות הדיגיטליות של יחידות התקשוב". כמו כן לפי ההנחיה, מתודולוגיה

33 החלטת ממשלה מספר 1981 מיום 28.10.1991 בנושא נוהל מפתח.

34 החלטת ממשלה מספר 2097 מיום 10.10.2014 בנושא "הרחבת תחומי פעילות התקשוב הממשלתי, עידוד חדשנות במגזר הציבורי וקידום המיום הלאומי ישראל דיגיטלית"

סדורה כוללת נושאי חובה ובכללם: בהיבט הניהולי - תכנון הביצוע ומעקב אחריו, ניהול סיכונים, ניהול משאבים; בהיבט הכלכלי - בקרה על עלויות הפרויקט ואמידתן; בהיבט הטכנולוגי - תיעוד, איכות ובקרה של התוצרים ושל הנתונים; בהיבט העובדים: שימור ושיתוף של ידע ארגוני.

יש שתי מתודולוגיות מרכזיות מקובלות בתחום ניהול מערכות וטכנולוגיות המידע:

1. שיטת "מפל המים" (Waterfall): שיטה ובה השלבים השונים במחזור חיי הפרויקט מנוהלים באופן סדרתי. לפי שיטה זו, בכל שלב במחזור החיים יש מסמך מפורט המגדיר מה נדרש באותו שלב. למשל: מסמך אפיון - מפרט את התהליכים העסקיים שהמערכת תתמוך בהם, ואת המסכים והשדות במערכת. על מסמך האפיון חותם הלקוח, כדי לוודא שתכולת המערכת מתאימה לצרכיו; מסמך בדיקות - מפרט את תרחישי הבדיקה; מסמך בדיקות קבלה מתאר את התרחישים שיבדוק הלקוח לפני מבצוע המערכת.

2. השיטה "הזמישה"[35] (Agile): שיטה גמישה יותר מבחינת שלבי מחזור החיים של המוצר, הדוגלת במסירת תוצרים ללקוח לעיתים תכופות תוך שיתוף פעולה הדוק עם הלקוח לאורך כל שלבי הפרויקט כדי להגדיר בכל שלב את הדרישות הנוספות.

בצה"ל קיים נוהל פיתוח אמל"ח 10/01 לניהול פרויקטים גדולים - טכנולוגיים ושאינם טכנולוגיים שעודכן לאחרונה בנובמבר 2016.

בפגישות שהתקיימו עם צוות הביקורת ב-20.1.22 ובתשובת צה"ל נמסר כי מערכת ג' שלב א' נוהלה לפי שיטת "מפל המים" וכי פרויקט השלמות שלב א' של המערכת יעבור לצורת ניהול לפי השיטה "הזמישה" כדי לשפר את איכות המוצר, להפחית סיכונים באמצעות פיתוח ובדיקה במחזורים קצרים, וכמו כן כדי להתמודד עם תחלופת כוח אדם שקיימת בצה"ל כל שנתיים-שלוש. עוד נמסר כי מערכת ב' החדשה מנוהלת לפי השיטה "הזמישה".

נמצא כי המתודולוגיה לניהול פרויקטים בצה"ל (הק"א 10/1) שפרסם אגף תכנון אינה ייעודית לניהול פרויקטי מערכות מידע ועקב כך איננה כוללת התייחסות מפורטת לנושאי חובה שנדרשים במתודולוגיות מקובלות לניהול פרויקטי מערכות מידע. כמו כן, המתודולוגיה אינה כוללת כלי עזר שיסייעו לגופים ביישומה: תקנים, קווים מנחים, נוהלי עבודה ותבניות אחידים בתחום ניהול הפרויקטים. עקב כך, כל גוף מנהל את הפרויקט שלו בהתאם לנוהלי עבודה, תבניות וכלי עבודה שגיבש. עוד נמצא כי המתודולוגיה לא כוללת התייחסות לניהול פרויקטים לפי השיטה הזמישה אף שצה"ל מפתח מערכות לפי מתודולוגיה זו, למשל: מערכת ב' החדשה.

בתשובת צה"ל נמסר כי צה"ל הבין שנוהל 10/1 אינו נותן מענה לפיתוח מערכות טכנולוגיות בשיטה "הזמישה" ועל כן הוגדר על ידי מנהלת הטרנספורמציה הדיגיטלית באגף התקשוב בשיתוף אגף התכנון נוהל עדכני בשם 10/6 שבו הדרישות ליישום הפרויקט עדכני לשיטה הזמישה ולתהליכי העבודה בצה"ל. בימים אלו אכ"א בשיתוף מנהלת הטרנספורמציה הדיגיטלית ואגף תכנון החלו להניע פרויקטים ראשיים בעולם התוכנה לפי נוהל 10/6.

35 הלחם של המילים "זריז" ו"גמיש"

מומלץ כי אכ"א יפעל בשיתוף אגף תכנון לעדכון הנהלים הרלוונטיים לניהול פרויקטי מערכות מידע (10/01 ו-10/6), באופן שיכללו התייחסות מפורטת לנושאי החובה הנדרשים במתודולוגיות מקובלות לניהול פרויקטי מערכות מידע ולהתאמת המתודולוגיה לניהול פרויקטים בשיטה "הזמישה". עוד מומלץ כי יגובשו כלי עזר ליישום המתודולוגיה ותבחן הקמת גוף תומך לניהול פרויקטים (כמו PMO) שייתן מענה לצורך זה.

הק"א 10/1 מגדירה את מסמכי היסוד הנדרשים בכל שלב בפרויקט למשל: בשלב הייזום - הגדרת הדרישה המבצעית, בשלב האיפיון - מסמך אפיון טכני, בשלב הפיתוח - גיבוש תוכנית פיתוח (להלן - תוכניות עבודה), בקרה על הפרויקט, ניהול סיכונים.

נמצא כי במערכות אמצעי הזיהוי אין מסמכי יסוד או תוצרים הנדרשים בתהליכי עבודה לפי מתודולוגיות מקובלות לניהול פרויקטי מערכות מידע ולפי הק"א 10/1. ללא מסמכי יסוד ותוצרי ביניים אלו נשקף סיכון שהמערכות שמפותחות אינן תואמות לדרישות המשתמשים. להלן דוגמאות:

1. מסמכי דרישות - למערכת ב' החדשה אין מסמך דרישות מבצעיות כנדרש בהק"א 10/1 אלא קיימת מצגת עם רשימה כללית של תכולות שלא קיבלה את אישור הלקוח.

2. תוצרי ביניים - מערכת ב' החדשה מפותחת לפי השיטה הזמישה, שבה אמור הלקוח לקבל תוצרים לעיתים תכופות, אולם במשך תשעה חודשים מתחילת הקמת המערכת ביולי 2021 לא נמסרו ללקוח יחידות של המערכת ולא בוצעו מבדקים בשיתוף הלקוח.

מומלץ כי מקמש"ר תנהל את מערכות אמצעי הזיהוי בהתאם למתודולוגיות מקובלות לניהול פרויקטי מערכות מידע, ובהתאם להק"א 10/1, ותגבש את מסמכי העבודה הנדרשים לפי מתודולוגיות אלו.

מנהל הפרויקט

בפרויקטים טכנולוגיים בזרועות השונות בצה"ל מקובל כי מנהל הפרויקט הוא גוף אמצעי לחימה (להלן - אמל"ח). בהקשר של מערכות אמצעי הזיהוי גוף האמל"ח הוא אכ"א. מאז הקמתן של מערכות הזיהוי הועבר הניהול שלהן בין כמה גופים באכ"א, עד שבינואר 2021 עברו לניהול אגף מערכות מידע ודיגיטל במקמש"ר.

במסגרת תפקידו כמנהל הפרויקט, אחראי מקמש"ר בין היתר להגדרת הדרישות, האפיון וניהול הפרויקט ממועד הקמתו ועד הטמעתו. ענף אד"ם באכ"א אחראי להיבטי האסטרטגיה וכן לתוכניות העבודה ולתקציבים בראייה של כלל המערכות באכ"א, וכן הוא אחראי למאגרי המידע באכ"א. ענף תכלית, כאמור, הוא הגוף הטכנולוגי שאחראי לתהליכי הפיתוח של המערכות.

לפי PMBoK[36], מדדי ההצלחה של פרויקט מערכות מידע הם עמידה בפרמטרים האלו: משאבים (עלות), זמן ותכולה. תפקיד מנהל הפרויקט הוא להביא את המערכת לשלב המבצוע בהצלחה, תוך עמידה בלוחות הזמנים, בתקציב, בתכולה ובאיכות שהוגדרו ולשביעות רצון הלקוחות.

בפגישה שהתקיימה בין צוות הביקורת לנציגי מקמש"ר ב-20.1.22 נאמר כי מערכות אמצעי הזיהוי הועברו למקמש"ר בינואר 2021 אולם רק במהלך יוני 2021 הם נכנסו לניהול המערכות בפועל, בהובלה של מטה אכ"א. ניהול מערכת ג' התמקד בבדיקות המערכת לצורך החלטה אם למבצע את המערכת. עוד נאמר כי בנוגע למערכת ב' החדשה עדיין לא החל מקמש"ר לנהל את הפרויקט, והוא מעורב רק בנושא רכש המצלמות החדשות אשר אמורות להתחבר למערכת זו. במהלך תקופה זו, המשתמשים במערכות עומדים בקשר ישיר עם צוות הפיתוח של המערכות בענף תכלית.

נמצא כי מערכות אמצעי הזיהוי לא נוהלו לפי מתודולוגיות מקובלות לניהול פרויקטים, ובכלל זה נמצאו פערים בנושאים האלו, אשר מנהל הפרויקט אחראי להם: הכנת תוכניות עבודה ומעקב אחר ביצוען, ניהול ושיתוף של הלקוח, העלאת הפרויקטים לדיון בישיבות של ועדות היגוי, ניהול סיכונים, ניהול שינויים וניהול תקלות (ראו פירוט בהמשך).

עוד נמצא כי פרויקט מערכת ב' החדשה, שהחל ביוני 2021 ונכון ליוני 2022 נמצא בשלב מבדקי קבלה, התנהל ללא מנהל פרויקט האחראי לבחון את מידת העמידה שלה ביעדים של לוחות זמנים, תכולה ומשאבים ותוך הבטחת שביעות רצונו של הלקוח מהמערכת.

בתשובת צה"ל נמסר כי שלב הפיתוח של מערכת ב' החדשה לא נוהל על ידי קצין האמל"ח, מכיוון שהפרויקט הוגדר כשדרוג טכנולוגי ללא שינוי של הצורך המבצעי, הגם שבוצע בו מספר מצומצם של שו"שים.

משרד מבקר המדינה מעיר כי שדרוג טכנולוגי במהותו נושא את כל הנדבכים המחייבים ניהול פרויקט.

על אכ"א לגבש תוכנית מסודרת להגדרת תחומי אחריותו של מקמש"ר כמנהל הפרויקט של מערכות אמצעי הזיהוי, לקראת השלבים הבאים בפיתוח המערכות ולפעול ליישומה לפי מתודולוגיות מקובלות.

תוכנית העבודה השנתית של מערכות אמצעי הזיהוי

תוכנית עבודה לפרויקט להקמת מערכת מידע צריכה להתבסס על חמישה עקרונות יסוד היוצרים תשתית מתודולוגית מוסכמת[37]: (א) הגדרת הפעילויות שיש לבצע בכל שלבי מחזור החיים של המערכת כדי להפיק את תוצריה; (ב) קביעת רצף הפעילויות, למשל איזו פעילות

36 Project Management Body of Knowledge, ארגון ניהול פרויקטים PMI.

37 הארגון העולמי לניהול פרויקטים (PMI) מפרסם משנת 1983 ומעדכן מדי כמה שנים מדריך הסוקר את תהליכי ניהול הפרויקטים, לרבות פירוט של חמשת העקרונות האמורים.

יכולה להתחיל רק בסיום פעילות אחרת; (ג) הערכת המשאבים הנדרשים לביצוע כל פעילות; (ד) הערכת משך הפעילויות; (ה) הכנת לוחות זמנים כוללים לפיתוח המערכת בהתבסס על תאריכי ההתחלה והסיום שנקבעו לכל פעילות. לוח הזמנים הראשוני לפיתוח מערכת מאושר במסמך הייזום ומכונה "תוכנית בסיס".

הק"א 10/1 מנחה כי לכל פרויקט תהיה תוכנית פיתוח ופעולות שונות ופרטניות המתאימות לאופי הפרויקט, לסוגו, לסיכונים בו וכו'. ההוראה גם מנחה כי בשלב הקליטה וההטמעה על המשתמש לגבש, בתיאום הגוף האמל"חי והגוף הטכנולוגי, תוכנית ראשונית לקליטה ולהטמעה של האמצעי.

בתוכניות העבודה השנתיות של ענף תכלית יש אבני דרך המציינות מועדי מבצוע של מערכות אמצעי הזיהוי לשנים 2019 - 2022. בתוכנית העבודה 2020 מופיעה אבן דרך סיום פיתוח מערכת ג' ברבעון השני. בתכנית העבודה לשנת 2021 מופיעה אבן דרך מבצוע מערכת ג' ברבעון 1 שבוצעה בפועל ברבעון 4.

נמצא כי מקמש"ר לא הכין תוכנית עבודה מפורטת להקמת מערכות אמצעי הזיהוי כנדרש לפי מתודולוגית מקובלות לניהול פרויקטים ובהק"א 10/1, לרבות מערכת ב' החדשה הנמצאת לקראת שלבי מבצוע ומערכת ג' שמובצעה. בהיעדר תוכנית עבודה מפורטת הכוללת את רשימת הפעילויות והערכת משך הזמן שלהם, נבצר ממקמש"ר לבחון אם הפרויקט מתנהל בהתאם לתכנון ועומד בלוחות הזמנים ובדרישות הנוגעות לתכולה ולהעריך מחדש את לוחות הזמנים כתוצאה מעיכובים בפרויקט. זאת ועוד, בהיעדר תוכנית עבודה מפורטת נבצר מהמשתמשים להכין "מפת דרכים" (Roadmap) עדכנית של יכולות המערכת לטווח הבינוני והארוך.

על מקמש"ר בשיתוף הרבנות וענף תכלית לגבש תוכנית עבודה לביצוע השלמות שלב א' למערכת ג' אשר תכלול את כל הפעילויות המתוכננות, את הערכת המשאבים הנדרשים ואת משך הפעילויות וכן עליו להכין לוחות זמנים כוללים.

לפי הנחיית רשות התקשוב מתודולוגיה סדורה לניהול פרויקטים צריכה לכלול נושאי חובה כמו מעקב ביצוע, צומתי החלטה ונקודות בקרה לאורך חיי הפרויקט, ניהול תהליך חריגות בפרויקט וניהול משאבים - קיבולת וניצול.

נמצא כי הקמת שתי המערכות החדשות התעכבה וחרגה מלוחות הזמנים שנקבעו, כמפורט להלן:

1. **מערכת ג':** פיתוח המערכת החל במחצית הראשונה של שנת 2018 והסתיים ביוני 2020. באוגוסט 2020 התקיים סבב בדיקות שבסופו נקבע כי המערכת אינה נותנת מענה לצרכים המבצעיים. עד יוני 2021 התקיימו כמה דיונים בפערים מקצועיים שעלו בין האפיון והפיתוח לבין הצורך המבצעי, וזאת לשם קבלת החלטה אם למבצע את המערכת או לגרוט אותה. באוקטובר 2021 התקבלה החלטה למבצע את המערכת. מבצוע המערכת בדצמבר 2021 כלל את התכולות שאופיינו ודרכים לעקיפת חלק מהפערים שנדרשו לצורך המבצעי. פיתוח נוסף ושינויים מהותיים של תהליכים במערכת יתאפשרו רק מהרבעון השלישי של שנת 2022 בשל היעדר כוח אדם.

2. **מערכת ב' החדשה:** מבצוע המערכת אמור היה להתקיים בסוף שנת 2021, אולם הוא נדחה למרץ 2022 ולאחר מכן ליוני 2022, ונכון ליולי 2022 טרם הושלם כיוון שמפתחי המערכת תועדפו לטפל במערכות אחרות.

נמצא כי נוצר עיכוב של כשנה בלוחות הזמנים להקמת מערכת ג' וכן עיכוב צפוי של כחצי שנה בלוחות הזמנים להקמת מערכת ב' החדשה, אולם עיכובים אלו והסיבות להן לא הוצגו לפני לקוחות המערכת ולפני ועדות ההיגוי כדי לקבל את אישורם לעיכוב או כדי לטפל בהסדרתם. זאת ועוד, במועד סיום הביקורת באפריל 2022, לא נקבע מועד למסירת מערכת ג' עם השלמות לשלב א'.

מומלץ כי ענף תכלית ישלים את מבצוע מערכת ב' החדשה והשלמות שלב א' של מערכת ג' בהתאם ללוחות זמנים שיקבעו וכי מקמש"ר יבצע בקרה על עמידה בלוחות זמנים אלו.

ניהול לקוח

אחד המדדים להצלחת פרויקט הוא שביעות רצון הלקוח. לפי הנחיית רשות התקשוב, חלק מנושאי החובה שאמורים להיכלל במתודולוגיה סדורה לניהול פרויקטים נוגעים בהיבטי לקוח כמו וידוא שהלקוח קיבל את התכולה הרצויה והנדרשת לו ושיתוף הלקוח בכל שלבי הפרויקט. כדי לוודא שדרישות הלקוח מיושמות, נדרשת מעורבותו בכמה שלבים של הפרויקט: אישור הדרישות, חתימה על מסמך אפיון, בדיקות קבלה (בדיקות שמבצע הלקוח לפני מבצוע המערכת כדי לוודא שהיא עומדת בדרישותיו).

הק"א 10/1 מנחה כי כחלק מבקרת פרויקט, יבצע קצין הפרויקט, על בסיס מסמך תכולת העבודה, סקרים בהתאם לצורך (סקר דרישות מערכת, סקר תיכון ראשוני, סקר תיכון קריטי ועוד). בסקרים אלו ישתתפו גם קצין האמל"ח ונציגי המשתמש.

בדיון שהתקיים בנוגע למבצוע מערכת ג' העלה קצין האמל"ח כי בסיום הפרויקט זוהה כי חלק מהתהליכים במערכת לא אופיינו, ולכן היו פערים במערכת מול הצורך המבצעי. לאחר ניתוח של כלל הפערים הקיימים במערכת, הועלו 62 שו"שים: 16 מהם הוגדרו קריטיים, שבעה מ-16 השו"שים (44%) הקריטיים טופלו על ידי צוות הפיתוח. עלה כי חלק מהשו"שים נוגעים לשינויים מהותיים בתהליכים שאופיינו במערכת ולכן לא יכלו לקבל מענה מיידי. עוד עלה כי האיפיון של מערכת ג' היה מכוון עבור מצב חירום שהוא מורכב יותר ולכן עלה הצורך לייצר גרסה פשוטה יותר של התהליך עבור משתמש בשגרה.

כאמור, ענף תכלית העלה את הדרישות של מערכת ב' החדשה במצגת ולא במסמך דרישות מפורט, וזאת בלי שהלקוח אישר אותן.

נמצא כי המערכות החדשות - מערכת ב' החדשה ומערכת ג' - פותחו ללא שיתוף הלקוח לאורך כל מחזור חיי הפרויקט. למשל, לא התבצעו סקרים בשיתוף נציג המשתמש כנדרש בהק"א 10/1 לבדיקת יישום הדרישות ביחס לאפיון המערכת ולא בוצעו בדיקות מדורגות בשיתוף הלקוח. נוכח זאת, בשלב מבצוע מערכת ג' הועלה כי ישנם תהליכים עיקריים שלא אופיינו אשר היה אפשר לאפיין אותם בשלב מוקדם יותר במחזור החיים אם הלקוח היה שותף בתהליך. במערכת ב' החדשה לא בוצעו בדיקות בשיתוף הלקוח עד לסיום הפיתוח במשך כשנה.

בתשובת צה"ל נמסר כי להערכתו המקור לפערים מסוג זה הוא התמשכות הפרויקט משלב האפיון ועד לשלב המבצוע, והעבודה בשיטה לא זמישה. בהתאם לכך הוחלט שהמשך הפיתוח משנת 2022 יבוצע בשיטה הזמישה, על מנת לספק מענה רלוונטי ומהיר לצרכים המבצעיים.

מומלץ כי אכ"א יגדיר במסגרת המתודולוגיה הסדורה לניהול פרויקטים את השלבים במחזור חיי הפרויקט שבהם נדרשת מעורבות של הלקוח ונדרש אישורו לכך שהמערכת מפותחת בהתאם לדרישותיו. למשל שלב איסוף הדרישות וביצוע מבדקי קבלה לתוצרי ביניים לפני מבצוע המערכת. עוד מומלץ כי אכ"א יפעל להטמעת הדרישות של הלקוחות - הרבנות הצבאית ומיטב - במערכות אמצעי הזיהוי לאורך כל מחזור חיי הפרויקט.

ועדות היגוי

ועדת היגוי היא ועדה בראשות נציג בכיר של היחידה העסקית וחבריה הם נציג בכיר של יחידת התקשוב, חברי מנהלת הפרויקט ונציגי המשתמשים העיקריים.

תפקיד הוועדה לבצע בקרה על התקדמות הפרויקט ועל תוצריו העיקריים, לקבוע אם לאשר אבני דרך ולקבל החלטות בנושאים עקרוניים, כגון החלטה בדבר המשך פרויקט או שינוי סדר העדיפויות.

בפרויקטי אמל"ח בצה"ל אשר נמצאים בפיתוח נוהגים לכנס שתי ועדות היגוי:

1. **ועדת אמל"ח**: בהשתתפות המשתמש המוביל, מדור הטמעה (בשלבים הרלוונטיים בפרויקט) וגופי פיתוח. אחת לחודש הוועדה מקיימת ישיבות כדי לדון בכל הפרויקטים, ובתקופות שלקראת מבצוע ישיבותיה מתקיימות בתדירות גבוהה יותר.
2. **ועדת היגוי ניהולית**: אחראית לקבוע אם לאשר דרישות מבצעיות, וכן היא אחראית לבצע בקרה על הפרויקט מבחינת לוח הזמנים, תכולה ומשאבים. הוועדה פועלת בראשות רמ"ט הרבנות. בפגישה עם צוות הביקורת שהתקיימה ב-16.1.22 נמסר כי הרבנות אינה רואה עצמה אחראית למערכת ב' החדשה.

בפגישה שהתקיימה ב- 20.1.22 עם רע"ן מערכות מידע ודיגיטל במקמש"ר נמסר כי היא בשלב של הכרת מערכות אמצעי הזיהוי, וכי בעתיד היא מתכננת לקיים דיון סטטוס אחת לחודש בהשתתפות נציגים מהרבנות ועם גוף הפיתוח בנוגע לשיפורים ולשינויים בפרויקטים בתחזוקה

וכן בנוגע לסטטוס הפיתוח של מערכת ב' החדשה. בפגישה שהתקיימה עם הרבנות בינואר 2022 נמסר כי אינה המשתמש המוביל של מערכת ב'.

נמצא כי אף שמבצוע מערכת ב' החדשה נדחה מדצמבר 2021 למרץ 2022 ואח"כ ליוני 2022, פרויקט זה לא נידון בוועדת אמל"ח ובוועדת ההיגוי הניהולית. עוד נמצא כי נכון למועד סיום הביקורת באפריל 2022 לא הוגדר מיהו המשתמש המוביל של מערכת ב', ולכן הפרויקט נותר ללא מנהל פרויקט וללא ועדת היגוי שאחראית לבקר את התקדמות הפרויקט ואת תוצריו.

בתשובת צה"ל נמסר כי המשתמש המוביל במערכת ב' הוא ענף זו"ק, שכן הייעוד של המערכת הוא סיוע בתהליך זיהוי חלל.

מומלץ כי ועדת אמל"ח תתכנס באופן עיתי כדי לעקוב אחר התקדמות פיתוח מערכות אמצעי הזיהוי. כמו כן, על אכ"א להגדיר לרבנות את מחויבותה בתור המשתמש המוביל של מערכת ב' ובכלל זה את הובלת ועדות ההיגוי הניהוליות.

ביוני 2021 התקיים דיון בראשות רע"ן אד"ם לקבלת החלטה אם למבצע או לגרוט את מערכת ג'. בדיון הוחלט על המשך מבצוע של הפרויקט תוך הכנת תכנית עבודה להתמודדות עם הפערים שהועלו, ובכללם: חלוקה בין השו"שים שיטופלו בטווח הקצר-הבינוני לבין אלו שיטופלו בטווח הבינוני-הארוך וכן תגבור הצוות בשני תוכניתנים.

נמצא כי ועדת אמל"ח דנה בפרויקט הקמת מערכת ג' לפני מבצועו, בשלב מתקדם שבו הועלו פערים משמעותיים שהצריכו קבלת החלטה אם לגרוט אותו. עוד נמצא, כי ועדות היגוי שהתכנסו בנושא מערכת ג' לא עקבו אחר ביצוע החלטותיהן. למשל, למרות שבסיכום הדיון שהתקיים בעניין מבצוע מערכת ג' ביוני 2021 הוטלה משימה על רע"ן אד"ם לתגבר באופן מיידי את צוות הפיתוח בשני תוכניתנים נוסף על שני התוכניתנים הקיימים, במועד סיום הביקורת באפריל 2022 צוות הפיתוח כלל שלושה מתכנתים במקום ארבעה.

מומלץ כי ועדת אמל"ח תתכנס לעיתים תכופות יותר לקראת מבצוע השלבים הבאים של מערכת ג', כדי לוודא את העמידה בלוחות הזמנים ובתכולות הנדרשות וכדי לוודא שננקטו צעדים לצמצום פערים משמעותיים שנמצאו בתהליך המבצוע.

ניהול סיכונים

ניהול סיכונים הוא אחד מנושאי החובה בכל מתודולוגיה סדורה לפי רשות התקשוב. לפי הנחיית הרשות בנושא עקרונות לניהול סיכוני תקשוב במשרדי ממשלה[38], המידע והטכנולוגיה התומכים בניהול המשרדים הם משאבים חיוניים וקריטיים להנעה ולהצלחה של התהליכים והפעילויות הממשלתיות, ועל כן ניהול סיכוני תקשוב הוא מרכיב חשוב הן בניהול אגף מערכות מידע

38 הנחיה 1.3.01 התקפה מ-1.11.18.

ממשלתי והן בניהול הסיכונים התפעוליים של משרדי ממשלה. שימוש במתודולוגיה אחידה יאפשר למנהלי מערכות מידע לאתר, מההיבט של ניהול הסיכונים, כשלים הנוגעים למגוון תהליכים, כגון ניהול פרויקטים ותחזוקת מערכות ותשתיות. בהתאם לכך יוכלו מנהלי מערכות המידע לתעדף את הטיפול בסיכונים על פי חשיבותם, לפעול למזעור הסיכונים ולהקצות את המשאבים הקיימים באופן אפקטיבי.

הק"א 10/1 מנחה כי הגוף האמל"חי, בשיתוף עם הגוף הטכנולוגי, יבצע ניהול סיכונים שוטף לפרויקט, לתקופה שמשלב הפיתוח ועד לסיום הפרויקט. קצין האמל"ח אחראי לכתיבת תוכנית ניהול סיכונים לפרויקט ולעדכונה מפעם לפעם על פי הצורך והתקדמות הפרויקט.

אחד מסוגי הסיכונים אותם יש לנהל הוא הסיכון התפעולי ובכלל זה תחזוקת מערכות ובמיוחד מערכות עם טכנולוגיות מיושנות. שימוש בטכנולוגיות מיושנות נחשב כסיכון, מהסיבות האלו:

1. ככל שחולף הזמן צפויות להתרחש יותר תקלות במערכות שבהן הטכנולוגיות מיושנות, ולכן עלויות ביצוע התחזוקה בהן יגדלו.

2. קשה למצוא מתכנתים הבקיאים בטכנולוגיות אלה, והדבר מגדיל את עלויות הפיתוח של המערכות שבהן הן מותקנות (עדכונים, תיקונים, שו"שים).

3. טכנולוגיות מיושנות חשופות יותר לסיכוני אבטחה, ומספר העדכונים שלהן פוחת.

להלן דוגמאות לסיכונים שקיימים במערכות אמצעי הזיהוי:

1. **מערכת ב':** החל מאוגוסט 2021 ועד מועד סיום הביקורת באפריל 2022 מושבתות שתיים מתוך ארבע עמדות הקצה של צילום חלל הפה (50%) כתוצאה משימוש בציוד ישן בעמדות הקצה והפסקת תמיכת ספק הציוד אשר גרמו לכך שאי אפשר להשיג עבורם חלקי חילוף.

מהרבנות הצבאית נמסר כי בתחילת ינואר 2022 הסתיים האפיון לרכש של מצלמות ייעודיות לחלל הפה אשר יפיקו תצלומים באיכות גבוהה יותר תוך התאמה לציוד קצה מדגמים שונים. יצוין כי נכון ליולי 2022 תהליך הרכש של המצלמות טרם הושלם, וההטמעה שלהן מותנית במבצוע של ב' החדשה, שנמצאת בשלב מבחני קבלה.

מומלץ כי קמש"ר יוודא השלמת רכש המצלמות ושילובן במערכת ב' החדשה כך שכל ארבע עמדות הקצה של צילום חלל הפה יפעלו.

בתשובת צה"ל נמסר כי רכש המצלמות החדשות לא מעכב את היכולת למבצע את מערכת ב' וכי לאחר מבצוע המערכת אפשר יהיה לשלב מצלמות זמניות עד להשלמת הרכש.

2. **איכות צילום חלל הפה:** בביקורות שביצע מדור זיהוי רפואי בשנים 2018 ו-2019 נמצא כי כ-95% מתצלומי השיניים של חלל הפה הקיימים במאגר אמצעי הזיהוי הם באיכות שאינה מספקת (יצוין כי מתצלומים אלו עדיין אפשר לקבל מידע כלשהו).

ממועד ביצוע הביקורות של מדור זיהוי רפואי ועד מועד סיום הביקורת באפריל 2022 (כ-4 שנים) איכות ההרכשה הירודה של תצלומי השיניים לא טופלה.

בתשובת צה"ל נמסר כי הבעיה באיכות התצלומים נובעת מפער בהכשרה ובניסיון של מפעילי העמדה. נכון להיום החיילים שמפעילים את העמדות לא הוכשרו בקורס ייעודי ולא הוסמכו למקצוע "מתעד אמצעי זיהוי", ולעיתים עקב מחסור בכוח אדם אף נעשה שימוש בחיילים שהתחלופה שלהם גבוהה במיוחד. בשל כך ענף זו"ק העלה דרישה למקמש"ר לשפר את ההכשרה של מפעילי עמדות צילום חלל הפה ולצמצם את תחלופת מפעילי העמדות.

מומלץ כי מקמש"ר יפעל לצמצום הסיכונים שקיימים במערכות אמצעי הזיהוי, למשל: יפעל לשיפור האיכות של תצלומי השיניים באמצעות קידום ההכשרות של מפעילי עמדות צילום חלל הפה וצמצום תחלופת כוח האדם בעמדות אלו.

3. **עדכניות תצלומי השיניים:** תצלומי השיניים במערכת ב' משקפים את מצב השיניים של החייל במועד גיוסו. מיטב לא מבצעת מידי תקופה צילומים חוזרים (רנטגן וחלל הפה) לשם עדכון התמונות עקב שינויים המתרחשים בחלוף הזמן (סתימות, חורים בשיניים, הצבע משתנה ואף המיקום עקב יישור שיניים או תזוזה טבעית). ממדור רפואי ברבנות נמסר כי לרופאי השיניים שעוסקים בזיהוי דנטלי יש אפשרות להתחבר לערכת ד' ולצפות בתצלומי רנטגן עדכניים שנעשו לחייל לאורך שירותו לשם השוואה של תצלומי שיניים עדכניים.

בסיכום דיון שהתקיים באוקטובר 2021 בנושא אמצעי זיהוי הוגדרה משימה לטווח הקצר לסנכרן בין הנתונים שבמערכת ב' למערכת ד'.

מומלץ כי אכ"א תקדם את סנכרון המידע של תצלומי השיניים בין מערכת ד' למערכת ב' על מנת שהמידע במערכות אמצעי הזיהוי יוכל לשמש לצורך זיהוי חלל ללא הצורך בגישה למערכת נוספת.

נמצא כי מקמש"ר לא הכין תוכנית לניהול סיכונים הקשורים למערכות אמצעי הזיהוי כנדרש במתודולוגיות מקובלות ובהק"א 10/1 ולא פעל להפחתתם או למניעתם.

מומלץ כי מקמש"ר יבצע מיפוי עיתי של כל הסיכונים הקשורים למערכות אמצעי הזיהוי ויטפל בהם בהתאם לתוכנית סדורה, זאת לפני התממשותם.

ניהול שינויים

מתודולוגיית ניהול פרויקטים מגדירה תהליך מוסדר של ישיבות עיתיות עם הלקוח לשם איסוף דרישות לשינויים ושיפורים במערכת (להלן - ועדת שינויים) ומתבצע מעקב אחר יישומן. התהליך

נדרש במיוחד במערכות שנמצאות בשלבי תחזוקה היות שבמערכות אלו עיקר הפעילות נוגעת לשינויים המתבקשים מלקוחות המערכת.

להלן כמה דוגמאות לבקשות לשינויים שהתבקשו במערכת ב' החדשה אך לא תועדו במסמך דרישות ולא התווספו למסמך האפיון של המערכת:

1. בקשה להוספת דוח על מספר דגימות כתמי הדם שנאספו במיטב, אשר ישמש עבור הרבנות תעודת משלוח ויאפשר השוואה בין מספר הדגימות שנאספו ממיטב ובין מספר הדגימות שהגיעו לאוסף כתמי הדם.

2. חתימה דיגיטלית של חייל המסרב למסור כתם דם בתחנה בשר"ח. החתימה תתבצע במערכת ב', והדבר יחסוך שימוש בטפסים מנייר וביצוע תהליכי סריקה.

נמצא כי קצין האמל"ח לא ניהל תהליך לניהול השינויים והשיפורים המבוקשים במערכת א' ובמערכת ב', שנמצאות בשלבי תחזוקה, כפי שמוגדר במתודולוגיות ניהול פרויקטים מקובלות. עוד נמצא כי בקשות לשינויים במערכת ב' לא תועדו במערכת ממוחשבת נגישה ללקוח. כתוצאה מכך, מענה לבקשות לשינויים במערכת ב' ניתן רק בעת שדרוג תשתיתי של המערכת, כ-15 שנים לאחר מועד הפעלתה.

מומלץ כי כל דרישה לשו"ש במערכות אמצעי הזיהוי תתועד במערכת ממוחשבת המנהלת את המשימות לביצוע, וכי ינוהל תהליך סדור של שינויים ושיפורים שבמסגרתו ידונו הדרישות ויוחלט אם לטפל בהן ובמסגרת איזו חבילת מסירה. עוד מומלץ לשלב את השו"שים שהוחלט לבצע במסמך האפיון באופן שהוא יכיל מידע עדכני של המערכות.

ניהול תקלות

שביעות הרצון של לקוחות המערכת תלויה, בין היתר, באופן הטיפול בתקלות במערכת. בעולם ניהול הפרויקטים מקובל שלרשות המשתמש עומדת מערכת שבה הוא מדווח על תקלות. מנהל הפרויקט מסווג כל תקלה לפי רמת חומרתה, והוא מחליט עם הלקוח באיזו מהדורה או יחידת מסירה היא תתוקן. למערכת כאלו יש גם יכולת לבדוק אינדיקטורים לביצועים (KPI) כמו זמן ממוצע לפתרון תקלה.

בצה"ל יש כמה גופי תמיכה במערכות מידע לפי תחומי תוכן כמו תוב"מ, שאחראי לתמיכה בסגלי המשא"ן בצה"ל ולבקרה עליהם. לגופים אלו מועברות בקשות לטיפול בתקלות באמצעות מערכת לניהול קשרי לקוחות. במקרה הצורך, גופים אלו מעבירים את הטיפול בתקלות לגוף הפיתוח. גופים אלו אינם תומכים במערכות אמצעי הזיהוי.

נמצא כי במערכות אמצעי הזיהוי התגלו תקלות אשר לא תועדו ולא טופלו או שטופלו זמן רב לאחר מועד הגילוי שלהן.

להלן דוגמאות לתקלות שתוקנו רק זמן רב לאחר מועד הגילוי שלהן:

1. השבתה של מחצית העמדות לצילום חלל פה בתהליך עקב חוסר אפשרות להחליף את סוג ציוד ההיקפי במערכת ב'. לתקלה זו לא ניתן פתרון מערכתי בצורה של תיקון או שו"ש במשך שנה מאז שנפתחה באוגוסט 2021 אלא היא צפויה להיות מתוקנת רק במסגרת השדרוג למערכת ב' החדשה ביוני 2022.

2. במקרים של תקלת Timeout בתקשורת של מערכת א' מול מערכת לניהול התחנות במיטב, כשלא מגיע חיווי על כך שלא בוצעה הרכשה, נמחקות הרשומות המקומיות למרות שלא נרשמו לבסיס הנתונים. הבעיה דווחה בסיכום גיוס נובמבר 2018 ותוקנה רק בשלבי סיום כתיבת הביקורת במאי 2022 באמצעות שינוי של הגדרות המערכת (ללא פיתוח).

לקוחות המערכת, כמו מפקד מעבדת טביעות האצבע, מנהלים את התקלות באופן עצמאי ופונים בדואר האלקטרוני או בטלפון ליחידת תכלית, וזו פונה לספק.

נמצא כי גופי התמיכה הצה"ליים אינם תומכים במערכות אמצעי הזיהוי כך שבפועל אין גורם שמנהל את הפניות והתקלות כמקובל. כמו כן, התקלות אינן מנוהלות במערכת ממוחשבת לניהול תקלות. בהעדר ניהול ממוחשב ושיטתי, מקמש"ר, המנהל את מערכות אמצעי הזיהוי, אינו יכול לבחון אילו תקלות פתוחות קיימות בכל מערכת, אינו יכול לסווג את מידת החומרה ומידת הדחיפות של הטיפול בתקלות, וכן אינו יכול לוודא שהן מוסדרות בתוך פרק זמן סביר.

מומלץ כי מקמש"ר יסדיר את ניהול התקלות במערכות אמצעי הזיהוי במערכת ממוחשבת על ידי גוף תמיכה צה"לי מוסדר.

בענף השירותים מקובל שנותן שירות מתחייב לזמן אספקת השירות ולטיב השירות בהסכם SLA. הסכם מסוג זה אמור לעסוק, בין היתר, בנושאים אלה: הזמינות של השירות והתחייבות לתיקון תקלות, המומחיות הנדרשת מנותני התמיכה, "הקו החם" למתן השירות, הזמינות באתר הלקוח, הישיבות התקופתיות שמתקיימות לצורכי מעקב אחר הטיפול בתקלות אצל הלקוח וסיווג התקלות.

נמצא כי הסכם השירות (SLA) בין צה"ל לבין ספק התוכנה של מערכת טביעות האצבע אינו מיושם אף שעלותו השנתית היא בהיקף של כ-700,000 ש"ח. למשל, לא מתקיימת ישיבה דו-שבועית בהשתתפות איש התמיכה מטעם הספק והמטה לצורכי מעקב אחר הטיפול בתקלות, וכמו כן הספק לא שולח דוחות חודשיים המפרטים את מידת ההתקדמות בטיפול בתקלות.

להלן כמה דוגמאות לסעיפים בהסכם שמסתמן כי הם עלולים לא לספק מענה הולם:

1. צה"ל רשאי לבקש מספק התוכנה של מערכת טביעות האצבע תמיכה מעבר לשעות העבודה רק עד שש פעמים בשנה, גם אם מדובר בתקלות קריטיות.
2. תיקון תקלה המצריך תיקון קבוע בקוד המערכת יבוצע בתוך ארבעה חודשים.
3. עבודות תחזוקה באתרים יתבצעו למשך יומיים בשבוע לכל היותר.

בפגישה שהתקיימה עם רע"ן תכלית עלה כי אף שהסכם השירות אינו מסדיר זאת, ניסיון העבר מלמד שבזמן אמת נציג של הספק מגיע בהתראה קצרה כדי לפתור את הבעיות, וכי לא התגלו בשטח בעיות שלא טופלו בזמן סביר.

בתשובת צה"ל נמסר כי ההסכם המקורי מול חברה א' הוא בתוקף עד ינואר 2028, והזמנות התחזוקה עד לסוף תקופה זו ממומשות על פי תנאי המכרז משנת 2014 בו זכתה החברה, ללא משא ומתן מחודש, שכן מדובר במימוש אופציה בעקבות המכרז.

מומלץ כי אכ"א יבחן האם הסכם השרות מול חברה א' נותן מענה הולם לצרכי המשתמשים בהתרחש אירוע רב-נפגעים, כמו לחימה, ובו יידרש שימוש מוגבר במערכת. כמו כן, מומלץ כי אכ"א יפעל ליישום הסכם השירות ובכלל זה יקיים ישיבות עיתיות עם הספק כדי לעקוב אחר אופן הטיפול בתקלות ואחר הוספת השינויים למערכת. על אכ"א לוודא שהדיווחים על התקלות יבוצעו במערכת ממוחשבת שתהיה נגישה לו, כדי שיוכל לנתח את הנתונים ולבצע מעקב אחר קצב הטיפול בתקלות באופן שיאפשר בחינה כמותית (KPI) של מדדי שירות.

שימוש במאגר אמצעי הזיהוי כצורך לאומי

במדינת ישראל קיימת סבירות להתרחשות אירוע רב-נפגעים (להלן - אר"ן), לרבות מלחמה, אסונות טבע כמו רעידות אדמה, תאונות קשות, דליקות ענק, התפרצות מגפות, אירועי טרור ופליטת חומרים רעילים. אירועים כאלו עלולים לגבות חללים רבים שיהיה קשה לזהותם.

לזיהוי חללים עלולות להיות תוצאות חמורות מהבחינה המשפטית, ההלכתית והרגשית הן עבור משפחות החללים והן עבור כלל הציבור. כמו כן נדרשת עבודה מורכבת של צוותים מגופים שונים וגיבוש תוכנית לאומית לזיהוי חללים בעת אסון ותרגול עיתי שלה כדי להיערך מבעוד מועד לתרחיש זה.

להלן יפורטו הגופים העוסקים בטיפול בחללים בעת אר"ן:

1. **רשות החירום הלאומית (להלן - רח"ל):** פועלת במסגרת משרד הביטחון כדי לסייע לשר לממש את אחריות-העל לטיפול בעורף בכל מצבי החרום. תפקידיה של רח"ל כוללים בין היתר: גיבוש תפיסות הפעלה בנוגע למצבי חירום שונים בעורף; ריכוז עבודות מטה לקביעת ההיערכות והמענה הנדרשים של גופים שונים ושל משרדי ממשלה הפועלים בעורף במצבי חירום שונים; הכנת הצעות חקיקה בנושא העורף; תיאום בין משרדי הממשלה הפועלים בעורף במצבי חירום שונים.

2. **הרשות לפינוי, לסעד ולטיפול בחללים בשעת חרום (להלן - פס"ח):** פועלת במסגרת המינהל לשירותי חירום במשרד הפנים ואחראית לטיפול בחללים בשעת חירום.

3. **פיקוד העורף (להלן - פקע"ר):** מארגן ומנהל את פעילות ההתגוננות האזרחית ומשמש גם בעל הסמכות המקצועית הראשית בנושאי חילוץ והצלה ובכלל זה איסוף חללים ונתוני הזיהוי שלהם בזירת האירוע. פקע"ר אוסף את הנתונים ומעביר אותם לתחנת רישום חללים.

4. **משטרת ישראל (להלן - מ"י):** המדור לזיהוי חללים, בהנחייתה המקצועית של המעבדה לזיהוי פלילי (להלן - מז"פ), אחראי לאיסוף אמצעי הזיהוי ובהם טביעות אצבע, תצלומי פנים ותצלומי שיניים, ועל ניתוח הנתונים שאספו חוקרי הזירה. מ"י היא זו שחולטת את הזיהוי הסופי.

5. **המרכז הלאומי לרפואה משפטית:** פועל במסגרת משרד הבריאות ואחראי לתהליכי הזיהוי המדעי[39] של חללים בעיתות שגרה וחרום בתחומים שעליהם הוא מופקד: זיהוי באמצעות דימות, סימנים רפואיים וזיהוי בדנ"א. ההשוואה של דגימת דנ"א שניטלה מהחלל נעשית אל מול דגימת ייחוס משני סוגים שונים: דגימות דנ"א שנלקחו מקרובי משפחה או דגימה עצמית של האלמוני בעל הזהות המשוערת, בין מול חפץ אישי ובין מול מאגר הדנ"א הפלילי שברשות מ"י (ההשוואה מול המאגר הפלילי נעשית על ידי מ"י).

בשנת 2019 פורסם מאמר שסוקר את נושא השימוש בטביעות אצבע לזיהוי קורבנות אסון (Disaster Victim Identification - DVI)[40]. המאמר מציג מקרה מבחן של אסון בין-לאומי - התרסקות של מטוס בטיסה MH17 לאינדונזיה, והוא מציע השוואה בזמן אמת למאגרים ביומטריים שאינם ציבוריים המכילים טביעות AM, כדי לאפשר זיהוי מהיר ואמין יותר. למשל, במקרה המבחן האמור נעשה שימוש בטביעות אצבע שהוטבעו בדרכונים ההולנדיים, אם אלו היו זמינים ובמצב ראוי לאחזור המידע. כמו כן, נעשה שימוש בבסיס הנתונים הביומטרי הלאומי של אינדונזיה[41] וכן בבסיס הנתונים של מחלקת ביטחון המדינה של ארה"ב שהכיל טביעות של יותר מ-200 מיליון נוסעים מכל העולם שביקרו אי פעם בארה"ב. כמו כן נעשו ניסיונות לחיפוש במערכות AFIS כמו זו שבשימוש המשטרה ההולנדית, וכדי להתגבר על הבעיה החוקית שבעניין התאימו את השלבים השונים שבפעולת המערכת כדי שלא ייחשף מידע שאיננו נדרש לתהליך.

בפגישה עם נציגי הרבנות הצבאית נמסר כי גורמים אזרחיים יכולים לקבל מידע מתוך המאגרים של מערכות אמצעי הזיהוי בצה"ל רק מכוחו של צו שופט ולאחר אישור הפרקליטות הצבאית. בהתרחש אירוע רב-נפגעים הליך כזה לא נותן מענה לדרישה המבצעית.

נמצא כי לא הוסדר השימוש במאנ"ח "מרכז הצבי" של הרבנות הצבאית בהתרחש אר"ן מעורב של אזרחים וחיילים. כמו כן, אף שצה"ל מחזיק במאגר ובו מאות אלפי רשומות של אזרחים וחיילים הכולל אמצעי זיהוי ייחודיים כדוגמת טביעות עשר אצבעות וכן כפות ידיים, לא הושלמה הבחינה של אפשרות השימוש במאגרי אמצעי הזיהוי המוחזקים בצה"ל לצורך זיהוי חללים בהתרחש אר"ן.

בתשובת צה"ל נמסר כי בסוף מרץ 2022 החלה עבודת מטה (עמ"ט הצבי לישראל) בהשתתפות הרבנות הצבאית, משרד הפנים ומ"י לצורך התאמת "מרכז הצבי" לטיפול בחללים אזרחיים באר"ן. העמ"ט מגדיר כהנחת עבודה כי השימוש במרכז הצבי למתן מענה (זיהוי וטיפול) בחללים אזרחיים באר"ן הוא בעת שגרה שבה אין מעורבות של חללים צבאיים. בהתרחש אירוע מעורב,

39 זיהוי באמצעות בחינת נתונים פיזיולוגיים ולא על פי מראה.

40 Digital capture of fingerprints in a disaster victim identification setting: a review and case study, Bryan T. Johnson and John A.J.M Riemen; FORENSIC SCIENCES RESEARCH, 2019, VOL 4, NO 4, 293-302 https://doi.org/10.1080/20961790.2018.1521327

41 משנת 2012 אינדונזיה נחשבת למדינה המתקדמת ביותר מבחינת הזיהוי האלקטרוני, ובין היתר היא ביצעה הרכשת זיהוי ביומטרי מכל האזרחים.

אזרחי וצבאי, תינתן החלטה "אד-הוק". לפי עמ"ט הצבי לישראל הפעילות במרכז תבוצע באחריותה ובפיקודה של מ"י. באוקטובר 2022 מתוכנן מבצוע מרכז הצבי כתר"ח לאומי במסגרת תרגיל ההתגוננות הלאומי. ברשימת המאמצים של העמ"ט מוזכרים הנושאים האלה: הגדרת אופן ביצוע תהליך הזיהוי, הגדרת הסינרגיה בין הגופים, התאמת תשתיות ומערכות מידע והסדרה משפטית לשימוש ביכולות צה"ל עבור אזרחים.

בתשובת פס"ח שהתקבלה ביוני 2022 נמסר כי היכולת להתמודד עם נושא החללים מחייבת מעורבות של משרדי ממשלה וגופים אחרים, שכל אחד נושא באחריות לטיפול בעולם התוכן שלו, ולכן משרד הפנים פועל בשיתוף רח"ל להביא לכך שהמטלות השונות יעוגנו בתשתית נורמטיבית.

מומלץ כי רח"ל בשיתוף פס"ח יבחנו את המענה הקיים ואת המענה הדרוש לנושא זיהוי חללים בהתרחש אר"ן, יסדירו את חלוקת האחריות בין הגופים השונים ויפעלו לקידום השימוש ב"מרכז הצבי" כתחנת ריכוז חללים לאומית באר"ן. במסגרת זו מומלץ לבחון את ההיתכנות של הסתייעות במאגר של צה"ל ובמאגרים אחרים לשם זיהוי חללים בהתרחש אר"ן. מומלץ כי הנושא ייבחן בשיתוף נציגי הרשות להגנת הפרטיות, נציגי צה"ל (אכ"א והרבנות הצבאית) ונציגי הפרקליטות הצבאית.

לנוכח המלצת הביקורת הנחה ראש רח"ל להוביל עבודת מטה עם הגורמים הרלוונטיים לבחון את היתכנות ההסתייעות במאגר צה"ל ובמאגרים אחרים לצורך זיהוי חללים באר"ן.

סיכום

צה"ל מנהל מערכות מידע של אמצעי זיהוי שמטרתן לזהות חללים. מדובר במערכות שבאמצעותן מנוהלים מאגרי מידע ביומטריים הכוללים מידע רפואי, אישי ורגיש, ולכן נדרש כי רמת האבטחה של המאגרים תהיה גבוהה לפי תקנות אבטחת מידע.

ממצאיו של דוח זה משקפים פערים משמעותיים באבטחת המידע המצוי במערכות רגישות אלו, וכן הם מעידים על אי-קיום חלק מתקנות אבטחת מידע ועל אי-יישום דרישות שנכללו במסמכי מדיניות הגנת סייבר. מצב זה יוצר סיכון לפגיעה באמינות (שלמות), בזמינות ובסודיות של המידע שבמאגרים.

הדוח כולל ממצאים נוספים הנוגעים להליכי תפעול וניהול של מערכות המידע של אמצעי הזיהוי. בין היתר נמצא כי מערכות המידע אינן מנוהלות ביעילות ולפי מתודולוגיה סדורה לניהול פרויקטי מערכות מידע, ועקב כך יש חשש שמערכות אמצעי הזיהוי לא יוכלו למלא את ייעודן. כמו כן נמצא כי מנהל הפרויקט לא הכין תוכניות עבודה למערכות אמצעי הזיהוי ולא וידא שהקמתן וניהולן של המערכות עומדים ביעדים המקובלים של תכולה, לוחות זמנים, עלויות ושביעות רצון הלקוח.

על ראש אכ"א לפעול לתיקון הליקויים ולבחון את ההמלצות שבדוח זה.