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:

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 משבתות 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 ליכולת 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.