דוח מבקר המדינה

ההגנה מפני איומי סייבר על מערכת השליטה והבקרה של פיקוד העורף (שוע"ל)

▪ ניסן התשפ"ה ▪ אפריל 2025

ההגנה מפני איומי סייבר על מערכת השליטה והבקרה של פיקוד העורף (שוע"ל)

מבוא

מדינת ישראל נערכת לקראת אירועי חירום, משברים או אסונות מסוגים שונים בתוך שטח ישראל, העלולים לסכן חיי אדם, לגרום לפגיעה קשה בכל אורחות החיים, בתשתיות לאומיות וביכולות ביטחוניות ולפגוע במידה ניכרת בחוסן הלאומי. על פי הוראת הפיקוד העליון, ייעודו של פיקוד העורף (להלן - פקע"ר) הוא להיות סמכות מקצועית ראשית בנושאי התגוננות אזרחית, חילוץ והצלה, והוא מופקד על שירות ההתגוננות האזרחית. פקע"ר אחראי בין היתר להכנת הרשויות המקומיות לתפקוד רציף בשעת חירום, להכשרתן ולתרגולן, ולניהול ועדות המל"ח המחוזיות[1] באופן שיאפשר את תפקודן הרציף של הרשויות המקומיות בשעת חירום. כמו כן, פקע"ר מפקד על חמ"ל העורף הלאומי ואחראי לגיבוש תמונת מצב לגבי העורף עבור מקבלי ההחלטות, לצורך הכוונת המאמצים לטיפול בעורף.

ניהול המרחב האזרחי בעיתות שגרה וחירום הוא משימה מורכבת, היות שבמרחב זה פועלים גופים רבים, ובהם משרדי ממשלה, רשויות מקומיות גופי תשתית (למשל, חברת החשמל לישראל וחברת נתיבי ישראל) וגופי חילוץ והצלה, ובכללם משטרת ישראל, מגן דוד אדום (להלן - מד"א), כבאות והצלה לישראל ופקע"ר. ניהול יעיל של מרחב זה מחייב יצירת תמונת מצב לאומית אחידה ואמינה לגבי העורף המבוססת על שיתוף מידע בין גופים אלה. בתמונת מצב זו יש כדי לאפשר לגופים אלה לייצר תובנות, לקבל החלטות, לשלוט על הכוחות והגורמים שהם אחראים להם ולבצע עליהם בקרה.

בינואר 2011 החליטה הממשלה[2] על בחינת חלופות למערכת תקשורת ושליטה ארצית לשעת חירום. בהמשך להחלטת ממשלה זו הציג פקע"ר בשנת 2016 למטה לביטחון לאומי (מל"ל) תוכנית לפיתוח מערכת שליטה ובקרה (להלן - שו"ב) לאומית לעורף (להלן - מערכת שוע"ל). מטרת המערכת היא לשמש "מערכת שליטה ובקרה מרכזית המאפשרת את קיום התהליכים המבצעיים הפיקודיים ומשמשת ככלי עזר לקבלת החלטות למפקד ברמות השונות, מדרג השטח ועד לרמה הלאומית. זאת באמצעות מיצוי מאגרי מידע וידע לאומיים וקישוריות לגופים אופרטיביים ומדיניים"[3]. החזון שעמד בבסיס הקמת המערכת היה בניית מערכת מתכללת (אינטגרטיבית) לרשויות המקומיות, לכוחות העורף, למגיבים הראשונים, למשרדי הממשלה, לרשות החירום הלאומית (רח"ל) ולגופי תשתית לאומיים, לצורך עבודה משותפת, גיבוש תמונת מצב אחודה ותמיכה בקבלת החלטות.

מערכת שוע"ל נחלקת לשתי מערכות מידע:

1. **שוע"ל צבאי:** מערכת שו"ב המשמשת את פקע"ר בניהול כוחותיו בעיתות שגרה וחירום, וכן משמשת להעברת מידע חיוני מהכוחות בשטח לרמה הממונה ומהרמה הממונה לכוחות בשטח. כמו כן, המערכת מאפשרת שיתוף מידע עם גופים אחרים המעורבים בפעילויות בעורף, כגון רשויות מקומיות ומשרדי ממשלה, לצורך גיבוש תמונת מצב, קבלת החלטות וניהול המשאבים. במערכת נאסף מידע חיוני ממערכות צבאיות, כגון מערכת "מסר לאומי" המפיצה התרעה על אפשרות לנפילת טילים ורקטות, ומגורמים חיצוניים. המערכת כוללת כלי היתוך מידע[4], כלים אוטומטיים לתמיכה בהחלטות וכלים טכנולוגיים מתקדמים לשיתוף מידע שמביאים לידי ביטוי תובנות ותוצרים ממאגרי המידע. מערכת שוע"ל צבאי החלה לפעול בשנת 2016.

---

1 משק לשעת חירום (מל"ח) - גוף המוקם מכוח פקודת העיריות, המחייבת כל רשות מקומית להכין את היישוב או היישובים שבתחום שיפוטה לשעת חירום ולהפעיל אותו בשעת חירום. מתוך **משרד הפנים, ועדת חירום וביטחון 2018**.

2 החלטה מס' 2699 מ-9.1.11 בנושא "שיפור היערכות העורף למקרי חירום ואסונות וקביעת המקורות התקציביים ליישום החלטה זו".

3 מתוך מסמך פקע"ר בנושא המלצה על מערכת שוע"ל לפרס ביטחון ישראל (15.2.22).

4 תהליך שמטרתו קישור, מציאת התאמה, חיבור והצלבת נתונים (data), מידע (information) וידע (knowledge).

תמונת המצב שמייצרת מערכת שוע"ל כוללת היבטים שונים הקשורים לעורף האזרחי, כגון מספר התושבים שהתפנו מבתיהם, ומספר שיגורי הטילים והרקטות ומקומות נפילתם ותמונת מצב לגבי היכולות המשפיעות על הרציפות התפקודית של כלל המשק, דוגמת יכולות אספקת החשמל והמים.

2. **שוע"ל אזרחי:** מערכת שו"ב עבור הרשויות המקומיות לניהול בעיתות שגרה וחירום. המערכת מספקת תמונת מצב של אירועים, כוחות ומשימות, תוך הנגשת מידע רלוונטי מגורמים מחוץ לרשות המקומית, כגון פקע"ר, ארגונים לשעת חירום ונתיבי ישראל, לצורך ניהול משאבי הרשות המיועדים לטיפול באירועים כאלה. המערכת פועלת על בסיס תשתית מרשתת (אינטרנט) אזרחית, ללא צורך בפריסת תשתיות פיזיות. כדי לעודד את הרשויות המקומיות להשתמש במערכת שוע"ל אזרחי ולהגביר את הרלוונטיות שלה עבורן, פקע"ר מיפה מערכות טכנולוגיות הפועלות ברשויות המקומיות וחיבר חלק מהן למערכת שוע"ל אזרחי. מערכת שוע"ל אזרחי נכנסה לפעילות בשנת 2017, והיא פרוסה כיום ב-251 מ-258 הרשויות המקומיות הקיימות בישראל.

איום הסייבר, שעלול לפגוע בזמינות, ברציפות ובאמינות התקשובית, הוא חלק מאיום הייחוס, והוא מחייב מענה הגנתי בסביבת עבודה טכנולוגית. לפיכך ארגון נדרש להיות בעל יכולת לניטור ניסיונות תקיפה של רשתות ומערכות שלו ולהתרעה עליהן, וכן להחזיק ביכולת למתן מענה הגנתי על המערכות שלו, הרכיבים המרכיבים אותן והתשתיות שלו, כדי למנוע אפשרות לפעילות עוינת, כגון מתקפות שמטרתן להשבית את המערכות ומתקפות אשר מטרתן להביא לדליפת מידע.

אירוע סייבר הוא התרחשות המעידה על פגיעה אפשרית בפעילותו התקינה של נכס סייבר, ושקיים יסוד להניח כי היא נובעת מפעילות מכוונת במרחב הסייבר. לאירוע מסוג זה יכולה להיות השפעה רוחבית (לדוגמה, פגיעה בשרתים רבים ושונים בתוך אותה רשת או פגיעה במקביל בכמה רשתות בארגון) או השפעה ארוכת טווח (למשל על ההתאוששות שיכולה להימשך שבועות עד חודשים).

כדי להתמודד עם איומים בסייבר אימץ מערך הסייבר הלאומי (להלן - מס"ל) מודל[5] הכולל חמישה שלבים ב"מחזור החיים" של הגנת סייבר על מערכות ותשתיות ושילב אותו בתורת ההגנה בסייבר. כמפורט להלן:

1. **זיהוי סיכונים:** מיפוי התהליכים המבצעיים והתשתיות הטכנולוגיות שעליהן נשענים תהליכים אלו; מיפוי משטחי התקיפה[6] אשר עלולים לאפשר לאויב לממש את כוונותיו לפגוע בתהליכים המבצעיים, בהתאם לפערי ההגנה שזוהו.

2. **הגנה מפני הסיכונים:** יישום תוכנית להגנה על המערכות, הרכיבים, התשתיות והתוכנה, בהתאם למדיניות ניהול הסיכונים שהוגדרה בשלב הזיהוי ולתקציב שהוגדר.

3. **איתור אירועי סייבר:** איסוף מידע מהמערכות, הרכיבים, התשתיות והתוכנה באמצעות התרעות (לוגים) על חשד לאירוע בעת זיהוי חריגה מהשגרה.

4. **תגובה:** בעקבות התרעה על חשד לאירוע סייבר, האירוע ינוהל באמצעות כלים טכנולוגיים ונהלים לפי סדר פעולות מוסכם, עד לפתרונו.

5. **התאוששות:** החזרת מערכות המידע ותהליכי העבודה לתפקוד מלא לאחר אירוע סייבר, כדי לאפשר רציפות תפקודית של הארגון.

---

5 המודל מבוסס על פרסומים של חברות התקנים הגדולות והמקובלות בעולם:
(ISO) National Institute of Standarts and Technology (NIST); International Organization for Standardization.

6 כינוי למכלול המרכיבים של מערכות דיגיטליות שכל אחד מהם לחוד או צירוף שלהם זה לזה טומנים בחובם פגיעות מסוימת שתוקף יכול לנצל לטובתו (מתוך מערך הסייבר הלאומי, **מילון מונחי סייבר**).

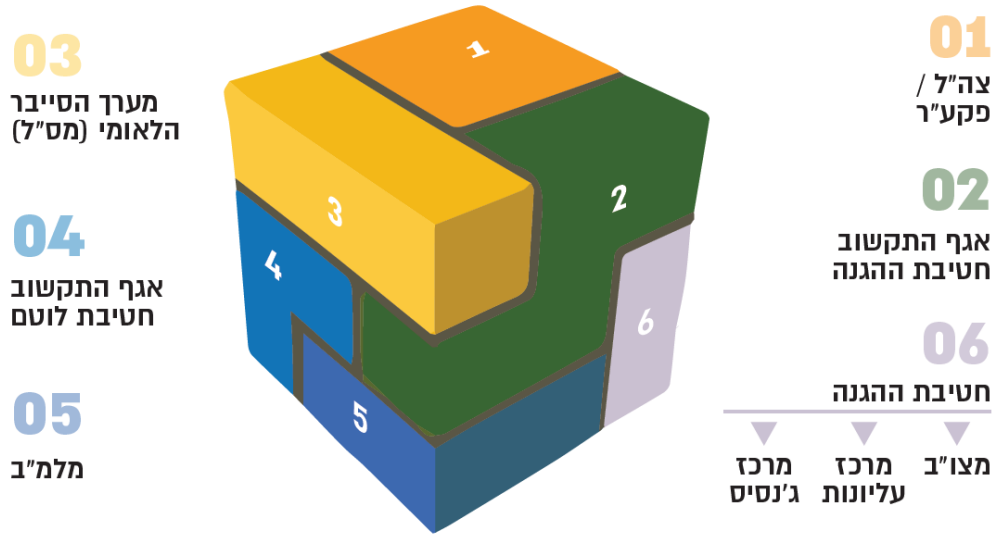
בינואר 2023 אישר מפקד הקשר והאלקטרוניקה הפיקודי בפקע"ר (להלן - מקשא"פ פקע"ר) את תפיסת ההגנה בסייבר של פקע"ר[7]. בנוגע לאיומי הסייבר על מערכות התקשוב של פקע"ר, ובהן מערכת השו"ב שעליה נסמכים תהליכים מבצעיים, צוין בתפיסה כי "האתגר הוא הגנה על מרחב תקיפה אזרחי רחב והתמודדות עם פוטנציאל נזק גבוה".

פקע"ר מנטר את כלל הרשתות והמערכות שבאחריותו. במסגרת זו טיפל פקע"ר ב-2,469 התרעות על אירועי סייבר מינואר עד מאי 2023.

לשם מימוש משימותיו והגשמת ייעודו נדרש פקע"ר לזמינות גבוהה, ונדרשת רציפות פעילותן של מערכותיו ושל רשתות התקשוב שלו. על כן נדרש פקע"ר לפעול להגנה מפני פגיעה בזמינות הרשת שלו, מערכותיו, היישומים שהוא משתמש בהם והמידע האגור בהם; להגנה על התהליכים המבצעיים מבוססי הרשת; להגנה מפני דליפת מידע; ולהגנה מפני פגיעה באמינות הנתונים האגורים ברשת או המוצגים למשתמשים.

בהגנה על המערכות והרשתות של פקע"ר מעורבים כמה גופים.

תרשים 1: **גופי הגנה בסייבר במרחב פקע"ר**[8]



על פי נתוני פקע"ר, בעיבוד משרד מבקר המדינה.

1. אגף התקשוב וההגנה בסייבר (להלן - אגף התקשוב), שהוא אגף במטה הכללי (להלן - מטכ"ל), אחראי בצה"ל לניהול ההגנה בסייבר של הרשתות הצבאיות הפועלות במרחב הצבאי ובמרחב האזרחי, ועל בניין הכוח בתחום הסייבר והפעלתו. אגף התקשוב נושא באחריות כללית ובאחריות אסדרתית (רגולטורית) כלפי כל גופי הצבא בנושאים הקשורים בהגנת הסייבר. לצורך מימוש אחריותו ניתנו לאגף סמכויות רבות, ובהן אפיון, הגדרה, אסדרה, ומימוש של מענה ההגנה בסייבר לגבי כל יכולות צה"ל, לרבות אלו המופעלות עבור צה"ל על ידי גורמים אזרחיים באמצעות התקשרויות של משרד הביטחון. כמו כן ניתנה לאגף סמכות לקביעת מדיניות ההגנה בסייבר בצה"ל. אגף התקשוב אחראי גם להגדרת תרחיש הייחוס להגנה, בשיתוף הזרועות, ולביצוע ביקורות מטכ"ליות לשם בחינת מימוש ההנחיות להגנת הרשתות.

אגף התקשוב מממש את ייעודו באמצעות כמה גופים הפועלים במסגרתו, כמפורט להלן:

7 המסמך אושר לראשונה במאי 2022 ועודכן בינואר 2023.

8 שירות הביטחון הכללי (שב"כ) אינו מעורב בפעילות מערכת שוע"ל, אלא במערכות אחרות של פקע"ר.

א. חטיבת לוטם - חטיבה להתעצמות טכנולוגית מבצעית באגף התקשוב, האחראית לעיצוב מרחב הלוחמה הרשתי בצה"ל. החטיבה שותפה לביצוע פעולות הגנה בממ"ד הסייבר ואחראית לזמינות ולרציפות של התהליכים המבצעיים, כדי לאפשר את חופש הפעולה הצה"לי. בחטיבה זו פועל ענף תוכנית התקשוב לעורף, האחראי לפיתוח תוכנית התקשוב לעורף[9], שמערכת שוע"ל צבאי היא חלק ממנה. גורם בענף[10] משמש קציין פרויקט שוע"ל צבאי (ראו בהרחבה בהמשך).

ב. חטיבת הספקטרום[11] וההגנה בסייבר (להלן - חטיבת ההגנה בסייבר)[12] היא סמכות מקצועית עליונה בצה"ל בתחומי ההגנה בסייבר. לחטיבת ההגנה בסייבר יש כמה תפקידים, ובהם לגבש תפיסת הגנה מטכ"לית בסייבר עבור כלל צה"ל; לשאת באחריות מטכ"לית להגנה בסייבר על תהליכים ומאמצים מבצעיים מבוססי רשת; לקבוע ולהטמיע תקן להגנת גופי הסייבר בצה"ל ולשימור הכשירות ההגנתית של גופים אלה. תחת חטיבת ההגנה בסייבר פועלים כמה מרכזים, ובהם:

(1) מרכז צופן וביטחון (להלן - מצו"ב), שייעודו להיות סמכות מקצועית עליונה ולפתח יכולות ומענה בתחום הצופן וההגנה בסייבר בנוגע למערכות תקשוב ואמצעי לחימה עבור צה"ל.

(2) מרכז עליונות, שאחראי להובלה, עיצוב ומימוש של המערכה בממד הסייבר, להגנת תהליכים מבצעיים ונכסים של צה"ל מבוססי רשת ולסיכול איומי סייבר בכלל מרחבי הפעולה, לצורך השגת חופש פעולה ועליונות מבצעית קיברנטית.

(3) מרכז ג'נסיס, שאחראי להובלת שגרת ההגנה הצה"לית בסייבר.

2. פקע"ר מפעיל מערך הגנת סייבר עצמאי שאחראי, בסיוע אגף התקשוב והמערך לביטחון המידע בצה"ל (להלן - מחב"ם), להגנת הרשתות הצבאיות, היישומים והאתרים שבתחום אחריותו ולמימוש מדיניות ההגנה בסייבר כפי שהיא מוגדרת על ידי אגף המבצעים במטכ"ל, אגף התקשוב ומחב"ם.

פקע"ר מממש את אחריותו בתחום הסייבר באמצעות מקשא"פ פקע"ר. תחת מקשא"פ פקע"ר פועלים גדוד התקשוב ענבר, הכולל את פלוגת הסייבר המשמשת בין היתר גוף הניטור של פקע"ר; וענף התרעה וטכנולוגיה (להלן - ענף התרעה), האחראי לניהול פרויקטים טכנולוגיים, ובהם מערכת שוע"ל. בענף התרעה פועלים ראש מדור (להלן - רמ"ד) פיתוח שו"ב, המשמש גם קציין האמל"ח של מערכת שוע"ל[13], וראש מדור סייבר.

3. מס"ל הוא גוף ממלכתי, מבצעי וטכנולוגי האמון על הגנת מרחב הסייבר הלאומי. מס"ל פועל מתוקף החלטות ממשלה[14] והיה מעורב במתן אישורי הגנת סייבר למערכת שוע"ל אזרחי בשלבי הפעלתה הראשונים. מיוני 2023 מס"ל מספק שירותי ניטור מסוימים למערכת שוע"ל אזרחי.

4. הממונה על הביטחון במשרד הביטחון (להלן - מלמ"ב) הוא אגף במשרד הביטחון המגן על הסודות והנכסים הביטחוניים של משרד הביטחון. תפקידיו הם בין היתר קביעת מדיניות אבטחה, תורה מקצועית ונהלים ויישום כל אלה ב"גופים המונחים", כהגדרתם בחוק להסדרת הביטחון בגופים ציבוריים, התשנ"ח-1998.

---

9 תוכנית התקשוב לעורף היא אחת משש תוכניות מרכזיות ביחידת מעוף, שהיא יחידת חוד טכנולוגית הפועלת בחטיבת לוטם. התוכנית נועדה לפיתוח מערכות ההתרעה הלאומיות של מדינת ישראל ולפיתוח מערכות שו"ב לפקע"ר (מתוך אתר צה"ל במרשתת).

10 ראש תחום השו"ב הלאומי, דיגיטל ואגם העורף.

11 הספקטרום האלקטרומגנטי הוא תווך הכולל את התפלגות אורכי הגל או התדרים של כל סוגי הקרינה האלקטרומגנטית, כגון קרינה קוסמית, קרינת גמא, קרינת רנטגן, קרינת על-סגול, קרינה נראית, קרינה תת- אדומה, גלי מיקרו וגלי רדיו.

12 יצוין כי פקודת הארגון של חטיבת ההגנה בסייבר טרם אושרה, ואין לחטיבת ההגנה בסייבר פקודת ארגון מאושרת.

13 קציין האמל"ח מייצג את הגוף המבצעי (אג"מי) ונושא באחריות כוללת לפרויקט (מתוך מילון מושגים בסיסי לניהול פרויקט שע"פ נוהל 10/1).

14 החלטת הממשלה 3611, "קידום היכולת הלאומית במרחב הקיברנטי" (7.8.11); החלטת הממשלה 2444, "קידום ההיערכות הלאומית להגנת הסייבר" (15.2.15); החלטת הממשלה 2443, "קידום אסדרה לאומית והובלה ממשלתית בהגנת הסייבר" (15.2.15), ומתוקף החוק להסדרת הביטחון בגופים ציבוריים, התשנ"ח-1998.

פעולות הביקורת

הביקורת נעשתה בין נובמבר 2022 ליוני 2023. בדיקות השלמה לביקורת נעשו עד אוגוסט 2023. הביקורת נעשתה בצה"ל: בפקע"ר; באגף התקשוב: בחטיבת ההגנה בסייבר ובלוטם (תוכנית התקשוב לעורף); באגף התכנון; ובמס"ל. בדיקות השלמה נעשו בעיריית חיפה. במסגרת הביקורת נפגש צוות הביקורת עם נציגים של החברה העוסקת בפיתוח של מערכות שוע"ל צבאי ושוע"ל אזרחי, ועם נציגים של חברות המספקות לפקע"ר שירותי ניטור.

ועדת המשנה של הוועדה לענייני ביקורת המדינה של הכנסת החליטה שלא להניח דוח זה במלואו על שולחן הכנסת אלא לפרסם רק חלקים ממנו, לשם שמירה על ביטחון המדינה, בהתאם לסעיף 17 לחוק מבקר המדינה, התשי"ח-1958 [נוסח משולב].

היבטי אסדרה בנושא הגנת הסייבר על מערכת השו"ב של פקע"ר

בפקודה שעוסקת בהגנה בסייבר קבע אגף המבצעים במטכ"ל את ההישגים הנדרשים לגבי הגנה בסייבר, ובהם מניעת חדירה לרשתות במרחב הסייבר הצה"לי[15]; מניעת חדירה לרשתות צה"ל דרך מרחב הסייבר האזרחי[16]; מניעת פגיעה באתרי צה"ל וביישומי צה"ל; מניעת אירועים מביכים לצה"ל במרחב הלבן[17]; הגנה על נכסי צה"ל במרשתת.

בתפיסת ההגנה בסייבר של פקע"ר נקבע כי פקע"ר אחראי באופן מלא להגנת רשתות החיל ומערכות המידע הפועלות בהן, בין שפותחו על ידיו ובין שנרכשו או סופקו מחברה עסקית או מגוף אחר במערכת הביטחון ומופעלות על ידיו. עוד נקבע כי "**ההגנה בסייבר הינה מרכיב קריטי** ביכולת של פיקוד העורף לשמר את הרציפות התקשובית ולהוציא לפועל את משימותיו" (ההדגשה במקור).

בתפיסת ההגנה בסייבר של פקע"ר מצוין כי פקע"ר אמון על הגנת מרחב הסייבר במערכות וברשתות אשר באחריותו, ובמסגרת זו הוא מסייע ומסתייע בפעולות גורמים אחרים שיש להם אחריות להגנת הסייבר במרחב האזרחי והצה"לי.

בתגובתו על טיוטת הדוח מינואר 2024 מסר צה"ל (להלן - תגובת צה"ל) כי הוא רואה חשיבות עליונה בהגנה על כלל המערכות הפועלות בממד הסייבר ומשקיע משאבים רבים כדי לחזק את ההגנה עליהן בשגרה ובחירום. צה"ל ציין כי מלחמת "חרבות ברזל" מביאה לשינויים ולהתפתחויות שונות בתחום איומי הסייבר על מדינת ישראל ועל צה"ל ובפרט על מערכת שוע"ל, וכי הוא פועל ללא הרף לשיפור יכולות ההתמודדות עם האיומים "ומפיק לקחים תוך כדי תנועה".

---

15 מרחב הסייבר הצה"לי, הנקרא גם מרחב כחול, כולל את כל רשתות צה"ל - המסווגות ושאינן מסווגות, המבודלות מרשת המרשתת העולמית ושאינן מבודלות. חלק מנכסי הסייבר של פקע"ר נכללים במרחב זה.

16 מרחב הסייבר האזרחי, הכולל גם את מרחב התכלת, כולל גם גופים ממשלתיים, גופים פרטיים, חברות תקשורת ישראליות ואת כלל משתמשי רשת המרשתת העולמית בישראל. חלק מנכסי הסייבר של פקע"ר נכללים במרחב זה, לרבות מערכת שוע"ל. מרחב התכלת משמש כחיץ בין המרחב הכחול בו מצויות הרשתות הצה"ליות, לבין המרחב הלבן בו מצויה המרשתת העולמית.

17 על פי הפקודה במרחב הלבן מצויה המרשתת העולמית, ופועלות בו מדינות ותעשיות, חלקן באופן לגיטימי המגובה בדין הבין-לאומי וחלקן בניגוד לחוקי הסייבר הבין-לאומיים המתהווים. מדינות הפועלות בניגוד לחוקי הסייבר הבין-לאומיים משמשות כר נרחב לגופים תוקפים.

איום הייחוס[18] ותרחישי ייחוס[19] ותהליך ניהול סיכונים בסייבר

איום הייחוס בתחום הסייבר משמש "כמצפן עבור בניין הכוח והפעלת הכוח בתהליכי הגנה", ומטרתו להכווין את בניין הכוח ואת הפעלת הכוח לטובת שימור העליונות בממד הסייבר במציאות של משאבים מוגבלים וקצב השתנות מהיר. גופי ההגנה ובניין הכוח נדרשים להעמיק ברשתות ובמערכות שבאחריותם, במטרה לבחון כיצד להגן מפני תרחישי התקיפה הנוגעים לתהליכים המבצעיים שבאחריותם.

פקודת מטכ"ל בנושא הגנת מערכות תקשוב והמידע האגור בהן קובעת כי על אגף התקשוב לגבש באופן עיתי את איום הייחוס להגנה בסייבר התקשובי, בהתבסס על הערכת האיום המודיעיני ועל הערכת האיום בסביבה הטכנולוגית, ולהעבירו לאישור אגף תכנון ובניין כוח רב-זרועי (להלן - אג"ת) במטכ"ל.

פקודה להגנה בסייבר קובעת כי אג"ת יגדיר את איום הייחוס להגנה בסייבר, בתיאום עם אגף התקשוב, אגף המודיעין במטכ"ל והזרועות; אגף התקשוב יגדיר את תרחיש הייחוס להגנה בסייבר, בשיתוף הזרועות; והזרועות יגדירו את תרחיש הייחוס למערכות הזרועיות, בתיאום עם אג"ת ואגף התקשוב.

ביולי 2023 מסר ראש ענף ניתוח ארוך טווח באג"ת לצוות הביקורת כי בשנת 2019 גובשה באג"ת טיוטת מסמך איום ייחוס להגנה בסייבר, אך בשל אתגרים בגיבוש התוכנית הרב-שנתית של צה"ל ("תנופה") מסמך זה לא אושר ונותר במעמד של טיוטה. איום הייחוס להגנה בסייבר של אגף התקשוב משנת 2022 תואם את איום הייחוס שבטיוטה האמורה משנת 2019.

על פי פקודת הארגון של חטיבת הספקטרום וההגנה בסייבר (להלן - פק"א חטיבת ההגנה בסייבר), אחד מתפקידי החטיבה בעיתות שגרה, בעיתות חירום ובעת לחימה הוא להגדיר את איום הייחוס הקיברנטי[20] ואת תרחיש הייחוס בסייבר לצה"ל, בתיאום עם אג"ת.

בינואר 2022 פרסמה מחלקת המבצעים של אגף התקשוב וההגנה בסייבר את מסמך איום הייחוס ותרחיש הייחוס בסייבר לשנים 2022 - 2024 (להלן - איום הייחוס ותרחיש הייחוס של אגף התקשוב); המסמך תוקף מחדש בפברואר 2023. במסמך מתואר תהליך העבודה, הכולל ניתוח מודיעיני שבוחן לגבי כל אחד מהשחקנים בזירת הסייבר את יכולות התקיפה שלו, הכוונות שלו, אירועי עבר שמעידים על נכונותו לבצע מתקפות סייבר ורמת הביצוע שלהן, ושעל בסיסו נבנה איום הייחוס. אגף התקשוב גם מבצע ניתוח טכנולוגי לתשתיות טכנולוגיות המשמשות לתהליכים המבצעיים, וכן מנתח את משטחי התקיפה שעלולים לסכן את התהליכים המבצעיים ואת פערי ההגנה המוכרים והעלות להשלמתם. על בסיס הניתוח הטכנולוגי מגבש אגף התקשוב את תרחישי הייחוס. על בסיס השילוב של איום הייחוס ותרחיש הייחוס מגדיר אגף התקשוב תוצר סופי כמיקוד מטכ"לי לכלל צה"ל. המיקוד המטכ"לי כולל את תרחישי התקיפה בסייבר שפוטנציאל הנזק ממימושם הוא הגדול ביותר, ומשמש את כלל צה"ל בתהליכי בניין הכוח במענה לאיומי הסייבר.

על פי איום הייחוס ותרחיש הייחוס של אגף התקשוב, תרחישי התקיפה לפי המיקוד המטכ"לי כוללים גם תרחישים רלוונטיים לפקע"ר.

בתגובתו מסר צה"ל כי איום הייחוס של חטיבת ההגנה בסייבר אינו כולל התייחסות לתרחיש הייחוס ולמערכות פקע"ר.

---

18 איום הייחוס הוא האיום הנגזר ממכלול האיומים האסטרטגיים, הנכללים בהערכת המודיעין כחלק מהערכת המצב בתחום הביטחון הלאומי, והוא האיום המוגדר או המתואר בתסריט הייחוס (על פי מילון צה"ל).

19 על פי מסמך איום הייחוס ותרחיש הייחוס בסייבר לשנים 2022 - 2024, תרחיש ייחוס מגדיר בהתאם לנושא ובהתאם למסמך איום הייחוס את הפרמטרים האלה: תכלית ההגנה; התשתית הרלוונטית; התרחיש הראשי, המציין את הנזק הצפוי מהתרחשות אירוע סייבר; התרחיש המשני; וכן את המתודולוגיה שנבחרה לניתוח תרחיש הייחוס, לשם בניין הכוח.

20 קיברנטי משמעו סייבר.

איום הייחוס של חטיבת ההגנה, שהיא הסמכות המקצועית העליונה בצה"ל בתחומי ההגנה בסייבר ואחראית לקבוע את תרחיש הייחוס בסייבר לכלל צה"ל, אמנם אינו מכוון במפורש למערכות פקע"ר, אולם תרחישי התקיפה שגיבשה חטיבת ההגנה רלוונטיים לכלל צה"ל, לרבות התרחישים הנוגעים למרחב הסייבר האזרחי. לפיכך מומלץ שפקע"ר יראה בתרחיש הייחוס שפרסם אגף התקשוב מסמך מנחה.

בפקודת מטכ"ל בנושא "הגנה בסב"ר" (להלן - פ"מ הגנה בסייבר) נקבע כי על סמך איום הייחוס ותרחיש הייחוס שגיבש אגף התקשוב, יגבש כל גוף שיש לו יחידת סייבר איום ייחוס ותרחיש ייחוס למערכות שבאחריותו.

על פי תפיסת ההגנה בסייבר של פקע"ר, במסגרת אחריותו של פקע"ר לבניין הכוח ולהפעלתו עליו לבצע ניהול סיכונים ולהגדיר את איום הייחוס על תשתיות טכנולוגיות שבאחריותו. בתפיסת ההגנה בסייבר של פקע"ר נקבע כי הכנת איום הייחוס לבניין הכוח נדרשת כדי לבנות את יכולות פקע"ר להתמודדות מול איומים עתידיים, והכנת איום הייחוס להפעלת הכוח נדרשת כדי לספק מענה להתמודדות עם איומים הקיימים היום. עוד נקבע כי איום הייחוס משקלל בתוכו סבירות להתממשות האיומים, חומרתם והנחות יסוד לגבי המענה שיינתן והאיום השיורי.

בתפיסת ההגנה בסייבר של פקע"ר נקבע כי על בסיס איום הייחוס (מיקוד מטכ"לי) יש לבצע תהליך זיהוי ומיפוי של נכסים קריטיים להגנה, על פי חשיבות התהליכים המבצעיים והאופרטיביים של פקע"ר, ומערכת שוע"ל צבאי היא מהמרכזיים שבנכסים אלה.

משרד מבקר המדינה בחן את האופן שבו פקע"ר ממלא את תפקידו בזיהוי ומיפוי של נכסים קריטיים להגנה בהתאם למסמך איום הייחוס ותרחיש הייחוס של אגף התקשוב, ובהתאם לתפיסת ההגנה בסייבר שהגדיר לעצמו. כמו כן בחן משרד מבקר המדינה את האופן שבו פקע"ר מנהל את הסיכונים שבהפעלת רשתות התקשוב שברשותו, להלן הפירוט:

מדיוני הערכת מצב סייבר שקיים פקע"ר בין פעמיים לשלוש פעמים בשנה[21] בשנים 2021 - 2023 עולה כי פקע"ר מיפה את הנכסים הטכנולוגיים שברשותו, ובכלל זה את מערכת שוע"ל צבאי ושוע"ל אזרחי, אולם במיפוי זה לא התייחס לכלל ההיבטים. עוד עלה כי נכון לרבעון הראשון לשנת 2023, פקע"ר זיהה פערי אבטחה הנוגעים בין היתר למערכת שוע"ל צבאי. נוסף על כך, בהערכות המצב לא נעשה ניתוח של משמעות האיומים, חומרתם וההסתברות להתממשותם.

באפריל 2023 מסרה רמ"ד סייבר בפקע"ר לצוות הביקורת כי פקע"ר לא הגדיר תרחישי ייחוס בסייבר. בעניין זה מסר מקשא"פ פקע"ר ביוני 2023 לצוות הביקורת כי אין לפקע"ר המשאבים הנדרשים לעיסוק בנושאים שונים בתחום הגנת הסייבר, ובהם עולם בניין הכוח והכנת תרחישי ייחוס.

יצוין כי ביוני 2022 קיימו נציגי מבקר מערכת הביטחון דיון עם נציגי מערך הסייבר בפקע"ר, במסגרת ביקורת בנושא "הגנה וחוסן הרשתות המבצעיות המאפשרות את היכולת המבצעית" שביצע מבקר מערכת הביטחון בפקע"ר. כבר בדיון זה צוין כי המשמעות של היעדר תרחישי ייחוס היא שאנשי פקע"ר אינם יודעים להעריך לאילו איומים קיים מענה, ומה היא רמת איכותו. עוד צוין בדיון כי תכנון פעילות הניטור אינו מבוסס על תרחישי ייחוס, ולא ניתן לבחון את רמת המענה שנותן גוף הניטור לתרחישי ייחוס מוגדרים.

בביקורת עלה כי פקע"ר לא הגדיר תרחישי ייחוס בסייבר, לא ביצע זיהוי וניתוח של סוגי האיומים ולא קיים הליך סדור של ניהול הסיכונים. כך, אף שזיהה פערי אבטחה הנוגעים בין היתר למערכת שוע"ל צבאי, פקע"ר לא ניתח את משמעות האיומים, את חומרתם ואת ההסתברות להתממשותם. זאת שלא בהלימה לפקודת המטכ"ל שקובעת כי כל גוף שיש לו יחידת סייבר יכין איום ייחוס ותרחיש ייחוס למערכות שבאחריותו, בהתאם למתודולוגיה המפורטת במסמך איום הייחוס ותרחיש הייחוס של אגף התקשוב ולקביעת פקע"ר בתפיסת ההגנה שגיבש. כמו כן, כפי שנמסר מאג"ת מסמך איום ייחוס להגנה בסייבר, בשל אתגרים בגיבוש התוכנית הרב-שנתית של צה"ל ("תנופה"), לא אושר, ונותר במעמד של טיוטה.

[21] ראו בהרחבה בהמשך בנוגע לדיוני הערכת מצב סייבר.

בתגובתו מסר צה"ל כי פקע"ר מבצע מיקוד ותיעדוף לגבי ההגנה על הנכסים והגנת המשימות המבצעיות, באישור מקשא"פ ומפקד פקע"ר. עוד מסר צה"ל כי הליך ניהול הסיכונים מתבצע בפרויקטים החדשים של פקע"ר שלא נבחנו בביקורת.

על פקע"ר להשלים את תהליך ניהול הסיכונים ולגבש תרחישי ייחוס בסייבר בהלימה לאיומים הממוקדים העדכניים הנשקפים למערכות פקע"ר. על פי זאת על פקע"ר לבנות תוכנית לבניין הכוח הכוללת בניית מערכי בקרה וניטור, לצורך מענה הגנה מיטבי מפני איומי הסייבר.

מומלץ כי חטיבת ההגנה בסייבר, מתוקף אחריותה המטכ"לית להגנה בסייבר על תהליכים ומאמצים מבצעיים, תוודא כי פקע"ר מבצע תהליך מלא של ניהול סיכונים, ובכלל זה מגדיר תרחישי ייחוס לבניין הכוח.

צה"ל מסר בתגובתו כי כיום חטיבת ההגנה מתמקדת ברשתות צה"ל שאינן חוצות פרימטר (רשתות מסווגות). צה"ל הוסיף כי חטיבת ההגנה, מתוקף תפקידה כמתכללת תחום הסייבר, תגבש בתיאום עם פקע"ר תרחיש ייחוס, על פי איומי הייחוס.

ועדות ניהול הגנה וביצוע בקרה בתחום ההגנה בסייבר

ועדה מטכ"לית להגנה בסייבר

הוראת קבע 3.013 של אגף התקשוב בנושא "ועדות הגנת מערכות התקשוב" (להלן - הוראת קבע 3.013) קובעת את תפקידיה וסמכויותיה של ועדת הגנת מערכות התקשוב המטכ"לית, ובכלל זה לאשר דרישות ומענה הגנה בנוגע למערכות התקשוב בצה"ל ולבצע בקרה ופיקוח על מימוש הדרישות.

בפ"מ הגנה בסייבר נקבעו הקריטריונים להבאת פרויקטי תקשוב לדיון לפני ועדת הגנה מטכ"לית, ובהם פרויקטים המכילים קישוריות בין מערכות תקשוב בצה"ל לגורמים מחוצה לו ומערכות עם טכנולוגיה חדשה.

עוד נקבע בהוראה כי קצין האמל"ח של הפרויקט יעביר בקשה לוועדת ההגנה המטכ"לית לאישור מענה ההגנה בשלב ייזום המערכת, בשלב הפיתוח ולפני הפעלת המערכת (להלן - מבצוע המערכת), וגם במקרה של שינויים ושיפורים במערכת. כמו כן נקבע כי פעילות הוועדה תתועד בסיכומים רשמיים.

גם בתפיסת ההגנה בסייבר של פקע"ר נקבע כי ועדת הגנה מטכ"לית, שבראשה עומד ראש חטיבת הגנה, תבצע בקרה ופיקוח בעניין דרישות ההגנה בסייבר ומימושן[22]. משרד מבקר המדינה בחן את פעילות ועדת ההגנה המטכ"לית בנוגע למערכות שוע"ל, ולהלן הממצאים:

שוע"ל אזרחי

למערכת שוע"ל אזרחי יש ממשקים עם חברות חיצוניות. לפיכך מערכת שוע"ל אזרחי עומדת בקריטריונים לדיון בוועדת הגנה מטכ"לית. בשנת 2015, במהלך הפיתוח של מערכת שוע"ל אזרחי, דנה ועדת הגנה מטכ"לית במערכת. פקע"ר החל בפריסת המערכת ברשויות המקומיות בשנת 2017 ובשנים 2018 ו-2019 בחן מס"ל את מענה ההגנה על שוע"ל אזרחי ואישר את פריסתה ברשויות המקומיות.

ביוני 2023 מסר מקשא"פ פקע"ר לצוות הביקורת כי מערכת שוע"ל אזרחי לא נדונה לפני ועדת הגנה מטכ"לית.

בביקורת עלה כי משנת 2015 מערכת שוע"ל אזרחי לא נדונה בוועדת הגנה מטכ"לית, אף שמבצוע המערכת היה בשנת 2017, וזאת שלא בהתאם להוראות אגף התקשוב ולפקודת מטכ"ל להגנה בסייבר הקובעות כי יש לקיים

[22] הוועדות יתכנסו בכל רבעון ועל פי הצורך.

דיון בוועדת הגנה מטכ"לית לגבי המערכת לאחר הפיתוח ולפני המבצוע. אי-דיון כאמור בוועדת הגנה פוגע בבקרה ובפיקוח על הגדרת דרישות ההגנה של מערכת שוע"ל אזרחי, ועלול לחשוף אותה לאיומי סייבר.

בתגובתו מסר צה"ל כי מערכת שוע"ל אזרחי נדונה בוועדת הגנה סדורה במס"ל, ומענה ההגנה אושר. עוד ציין צה"ל בתגובתו כי חטיבת ההגנה היא הגוף המנחה היחיד של פקע"ר, וכי גופים אחרים, ובכללם מס"ל, נועדו רק לביסוס שיתופי פעולה וקיום התייעצויות, ואינם בגדר גורמים מנחים.

כפי שנקבע בהוראות, על פקע"ר ואגף התקשוב לוודא את קיומם של דיונים בוועדות ההגנה המטכ"ליות לשם אישור מענה ההגנה בשלב הייזום של מערכת התקשוב, בשלב פיתוחה, בעת מבצוע המערכת ובעת הכנסת שינויים ושיפורים בה.

שוע"ל צבאי

מערכת שוע"ל צבאי החלה לפעול כמערכת מבצעית בשנת 2016. למערכת יש ממשקים עם גורמים מחוץ לצה"ל. על פי הוראת קבע 3.013 ופ"מ הגנה בסייבר, מערכת זו הייתה צריכה להידון בוועדת הגנה מטכ"לית.

במאי 2023 מסרה רמ"ד תכנון וארגון (להלן - תוא"ר) בחטיבת ההגנה בסייבר לצוות הביקורת כי לא התכנסה ועדת הגנה מטכ"לית בנוגע למערכת שוע"ל צבאי.

ביולי 2023 מסר מקשא"פ פקע"ר לצוות הביקורת כי לא התקיימו דיונים של ועדות הגנה מטכ"ליות בנוגע למערכת שוע"ל צבאי.

צה"ל מסר בתגובתו כי גרסת שוע"ל צבאי הנוכחית היא נגזרת של הגרסה הראשונה של שוע"ל צבאי (שוע"ל 1) שאושרה על ידי ועדת הגנה מטכ"לית. עם זאת, כאמור לפקע"ר אין מסמכים המעידים על התכנסותה של ועדת הגנה מטכ"לית לדיון בנושא ענן פקע"ר ומערכת שוע"ל צבאי.

בביקורת עלה כי לפקע"ר ולחטיבת ההגנה אין מסמכים הנוגעים לדיוני ועדת ההגנה המטכ"לית בעניין הגרסה הראשונה של מערכת שוע"ל צבאי ואישורה. עוד עלה כי לאחר עדכוני גרסאות במערכת שוע"ל צבאי, ובכלל זה מעבר לענן, לא התקיים דיון של ועדת הגנה מטכ"לית במערכת שוע"ל צבאי, וזאת שלא בהתאם להוראת אגף התקשוב שקובעת כי על ועדת הגנה מטכ"לית לאשר את דרישות ההגנה ומענה ההגנה בנוגע למערכות התקשוב בצה"ל ולבצע בקרה ופיקוח על מימוש הדרישות. קיום דיון של ועדת הגנה מטכ"לית בשלבים הנדרשים נועד להבטיח את קיומו של מענה הגנה מיטבי.

על אגף התקשוב לדאוג לכינוס ועדת הגנה מטכ"לית ולתעד את דיוניה, כדי לממש את אחריותו כלפי פקע"ר בנושאים הקשורים בהגנת הסייבר. במסגרת זו עליו לבחון את הבקרה והפיקוח על מענה ההגנה לפרויקטים להקמת מערכות תקשוב שיש להן ממשקים עם מערכות מחשוב חיצוניות לצה"ל, בשלבי חייהן השונים בכלל וטרם מבצוען בפרט. כל זאת כדי להבטיח מענה הגנתי מיטבי ולצמצם את סיכוני הסייבר.

על פקע"ר וכן על לוטם שבאגף התקשוב לוודא במסגרת אחריותם כי כל חריגה ממענה ההגנה של מערכת שוע"ל צבאי תעלה לדיון לפני ועדת הגנה מטכ"לית, כדי להבטיח שהחריגה אינה חושפת את המערכת לסיכונים לא מחושבים.

בתגובתו על טיוטת הדוח מסר צה"ל כי ההמלצה תיבחן.

ועדת היגוי וועדות הערכת מצב בסייבר

על פי תפיסת ההגנה בסייבר של פקע"ר, ועדת היגוי להגנה בסייבר היא פורום ניהולי בראשות ראש מטה הפיקוד הכולל נציגים שעוסקים בהגנת המרחב הקיברנטי, ובהם נציגים של אגף המבצעים, של גופי הפעלת הכוח[23], של גופי בניין הכוח[24] ושל המודיעין. ועדה זו עוסקת בנושאים האלה: אישור האסטרטגיה והגדרת המדיניות וההכוונה (דירקטיבה) של פקע"ר בנושא ההגנה בסייבר; מעקב אחרי תוכנית העבודה השנתית והרב-שנתית של פקע"ר בנוגע להגנה בסייבר; קבלת דיווח על אירועי סייבר; קבלת סקירה של מודיעין רלוונטי; קבלת סקירה לגבי מצב ההגנה של מערכות פקע"ר; פיקוח על תהליך ניהול סיכונים; עמידה בתקנים בין-לאומיים; ותשתית לשיתופי פעולה עם גופי ביטחון לאומיים במרחב הקיברנטי. הבסיס לסדר היום של הוועדה יהיה תמונת המצב במרחב הקיברנטי, הכוללת את תמונת המצב של כוחותינו ושל האויב, היבטי מודיעין ופרויקטי בניין כוח. עוד נקבע בתפיסת ההגנה בסייבר של פקע"ר כי ועדה זו תתכנס לפחות אחת לחצי שנה.

במאי 2023 מסרה רמ"ד סייבר בפקע"ר לצוות הביקורת כי ועדות בנושא הערכות מצב הסייבר הן למעשה ועדות ההיגוי להגנה בסייבר, וכי לא התקיימו בנפרד דיוני ועדות היגוי סייבר.

על פי תפיסת ההגנה בסייבר של פקע"ר, נוסף על התכנסותן של ועדות ההיגוי, יש לקיים דיונים בנושא הערכות מצב הסייבר, שבהם יוצג מדד החוסן של מערכות התקשוב בפקע"ר, וזאת כחלק מתהליכי הניהול והבקרה הנוגעים למצב ההגנה בסייבר במערכות וברשתות של הפיקוד. עוד נקבע כי דיונים בנושא הערכות מצב הסייבר יתקיימו בתדירות שלהלן:

1. אחת לחודש - בראשות ראש ענף (להלן - רע"ן) התרעה.
2. אחת לחודשיים - בראשות מקשא"פ העורף (פקע"ר).
3. אחת לרבעון - בראשות ראש מטה הפיקוד ואלוף הפיקוד.

בשנים 2021 - 2023 התקיימו שמונה דיונים בנושא הערכות מצב הסייבר. צוות הביקורת בחן את המצגות וחומרי הרקע שהוצגו בדיונים האמורים ואת סיכומי הדיונים, ולהלן הפרטים:

1. בתקופה זו לא התקיימו הערכות מצב חודשיות בראשות רע"ן התרעה.
2. התקיימו שני דיוני הערכות מצב בראשות מקשא"פ פקע"ר - דיון אחד בינואר 2022 ודיון שני בינואר 2023.
3. התקיימו שישה דיוני הערכות מצב בראשות מפקד פקע"ר או בראשות ראשת מטה פקע"ר[25].
4. אף דיון לא כלל התייחסות לפיקוח על תהליך ניהול הסיכונים.
5. אף דיון לא כלל התייחסות לאישור האסטרטגיה והגדרת ההכוונה (הדירקטיבה) של פקע"ר בנושא ההגנה בסייבר.
6. אף דיון לא כלל התייחסות לתמונת המצב של כוחותינו ושל האויב.
7. באף דיון לא הוצגה תמונת מצב עדכנית ומפורטת של מדד החוסן, כפי שנקבע בתפיסת ההגנה בסייבר של פקע"ר.

בביקורת עלה כי דיוני פקע"ר בנושא הערכות מצב הסייבר לא התקיימו בתדירות שנקבעה בתפיסת ההגנה בסייבר של הפיקוד, כך למשל המקשא"פ קיים בשנים 2022 ו-2023 שני דיוני הערכות מצב במקום שש הערכות מצב כנדרש. כמו כן, דיוני הערכות המצב, שהיו חלופיים לדיוני ועדת היגוי להגנה בסייבר, לא כללו התייחסות לחלק מהנושאים שבהם ועדה זו אמורה לעסוק, ובכלל זה התייחסות לפיקוח על תהליך ניהול הסיכונים או לאישור האסטרטגיה והגדרת ההכוונה (הדירקטיבה) של פקע"ר בנושא ההגנה בסייבר. לפיכך הם אינם

---

23 מקשא"פ פקע"ר הוא הרמה הממונה על גופי הפעלת הכוח.

24 בניין כוח להגנה מפני איומי סייבר כולל גיבוש תורת לחימה בנושא, הצטיידות, הכשרה, ארגון ותכנון סדר הכוחות.

25 באפריל 2021, באוקטובר 2021, בינואר 2022, במרץ 2022, ביולי 2022 ובאוגוסט 2022.

ממלאים במלואם את תפקידי ועדת ההיגוי להגנה בסייבר כפי שנקבעו בתפיסת ההגנה בסייבר של פקע"ר. אי-קיומם של דיונים אלו לצד קיום דיונים חסרים פוגעים בהכוונה הפיקודית בתחום ההגנה בסייבר בפקע"ר.

על פקע"ר לקיים את דיוני ועדות ההיגוי להגנה בסייבר בתדירות שקבע בתפיסת ההגנה ולהעלות בדיונים את כלל הנושאים כפי שנדרש בתפיסה, כדי להכווין את בניין הכוח והפעלתו בתחום הגנת הסייבר.

תמונת המצב של מדד החוסן של מערכות פקע"ר שנדרש להציג בדיוני הערכות מצב הסייבר צריכה להיות עדכנית ולשקף נתונים בנוגע לרמת המוגנות של מערכות המחשב ורשתות המחשב בפקע"ר. על פי תפיסת ההגנה בסייבר של פקע"ר, על תמונת המצב כאמור לכלול שלושה מרכיבים מרכזיים וקריטריונים למדידת ההישגים בהם:

1. תהליכי שגרת הגנה הנוגעים למענה ההגנה על פרויקטים (הכולל ביצוע מבדק חדירות ובקרה על תיקון ליקויים שעלו מסקרים ובדיקות), לעדכוני פק"לי[26] הגנה בסייבר, לעדכניות מערכות שונות, לביצוע ביקורות סייבר אצל ספקים, לבקרת תהליכי הלבנה ולמצב עדכוני אבטחה.

2. תהליכי הכשרת כוח אדם, תרגולו ואיוש משרות, ובכלל זה בדיקת הכשירות המקצועית של אנשי מערך ההגנה בסייבר בפקע"ר, ביצוע הכשרות והשתלמויות, ביצוע חפיפה בכניסה לתפקיד, השתתפות באימונים ותרגילים, עמידה בתקן ותגבור כוח האדם המקצועי באמצעות יועצים.

3. הטמעה של כלי הגנה מוגדרים.

צוות הביקורת בחן טבלאות ממאי ומיוני 2023 המייצגות את רמת החוסן והמוגנות של מערכת שוע"ל אזרחי ושל מערכות נוספות. בטבלאות אלה יש התייחסות לחלק מהקריטריונים בממד תהליכי שגרת הגנה[27] ולחלק מהקריטריונים בממד כלי הגנה. אין כל התייחסות לממד הבוחן את הכשירות המקצועית של מערך ההגנה בסייבר בפקע"ר.

ביולי 2023 מסר מקשא"פ פקע"ר לצוות הביקורת כי מדד החוסן מצוי בתהליך גיבוש, ועדיין אינו נמדד באופן שוטף. עוד מסר מקשא"פ פקע"ר כי טבלת רמת המוגנות מתייחסת לחלק מהממדים, ורמת הפירוט בה נמוכה יותר.

פקע"ר טרם סיים לגבש את מדד החוסן, ומשכך גם אין לפקע"ר תמונת מצב עדכנית של מדד החוסן, כנדרש בתפיסת ההגנה בסייבר של פקע"ר, ועקב כך לא ניתן לקבל תמונת מצב מלאה בנוגע לרמת המוגנות של מערכות התקשוב בפיקוד, ובהן שוע"ל צבאי ושוע"ל אזרחי. היעדר תמונת מצב מלאה עלול לפגוע ביכולת של פקע"ר לאתר את נקודות התורפה שלו ולהכווין את מאמציו בתחום הגנת הסייבר בהתאם.

בתגובתו מסר צה"ל כי ענף הגנה בענן שהקים מצו"ב החל את פעילותו לאחרונה, ובכלל זה יזם פעולות להעלאת רמת החוסן של סביבת הענן. צה"ל הוסיף כי במסגרת עיצוב המדיניות מצו"ב יקבע ויעדכן מדדים וכלי מדידה שיציגו את רמת החוסן באופן רחב, וכי רמת החוסן תבוקר בתהליכים עיתיים במסגרת הערכות המצב.

על פקע"ר לסיים את גיבוש מדד החוסן בשיתוף עם מצו"ב, וכן למדוד את חוסן כלל מערכות המידע שלו, בסביבת הענן ובסביבות אחרות, באמצעות מדד החוסן, כנדרש בתפיסת ההגנה שלו, ולהציג מדד זה בדיוני הערכות מצב הסייבר. זאת כדי להבטיח את קיומם של תהליכי פיקוח ובקרה על פעילות ההגנה בסייבר.

בתגובתו מסר צה"ל כי ההמלצה תיבחן.

---

[26] פקודות קבע לקרב.

[27] בממד שגרת ההגנה יש לבדוק מענה הגנה לפרויקטים, ובכלל זה ביצוע מבדק חדירות ובקרת תיקון ליקויים שעלו בסקרים ובבדיקות בטבלאות יש התייחסות לקיומו של מענה הגנה עדכני, ללא התייחסות לביצוע מבדקים ולתיקון ליקויים. כמו כן לא נבדקו ביצוע ביקורות סייבר אצל ספקים, ביצוע בקרת תהליכי הלבנה ועדכוני פק"לי הגנה בסייבר.

ועדות הגנה פיקודיות

על פי תפיסת ההגנה בסייבר של פקע"ר, ועדת הגנה פיקודית בסייבר בראשות מקשא"פ פקע"ר היא תת-ועדה של ועדת ההיגוי, וייעודה הוא לבחון ולאשר את היבטי ההגנה בסייבר בפרויקטים לאורך מחזור חייהם ולאשר תקניות הגנתית למערכת. במסגרת תפקידה זה הוועדה עוסקת בבחינת מענה ההגנה הניתן לפרויקט פנים-זרועי בהתאם לתקן המטכ"לי[28], לאיום הייחוס ולניתוח האיומים; בחינת מענה הגנה למערכות פקע"ר שהן בעלות קישור למערכות חיצוניות, כוועדה מקדימה לוועדה מטכ"לית; פיקוח ובקרה על יישום מענה לדרישות ההגנה בפרויקט; הנחיות לטיפול בפערים; ואישור תקניות הגנתית למערכת. בוועדה יש חברים קבועים[29], ומשתתפים בה נציגים נוספים בהתאם לצורך[30]. הוועדה מתכנסת בהתאם למחזור חיי הפרויקטים הרלוונטיים, ולפחות אחת לרבעון.

על פי תפיסת ההגנה בסייבר של פקע"ר, בוועדות ההגנה הפיקודיות יוצגו לגבי הפרויקטים הנדונים ניתוח האיומים, דרישות ההגנה, מענה ההגנה הטכנולוגי והתהליכי, הפערים והחלופות.

ביולי 2023 מסר מקשא"פ פקע"ר לצוות הביקורת כי פקע"ר כינס ועדת הגנה פיקודית לדיון במערכת שוע"ל צבאי בשנת 2018, אולם אין מסמכים המעידים על כך. עוד מסר מקשא"פ פקע"ר כי מערכת שוע"ל צבאי עלתה לענן במחצית שנת 2021, ללא כינוס ועדת הגנה לפרויקט. לגבי מערכת שוע"ל אזרחי מסר מקשא"פ פקע"ר כי לא דנו בה ועדות הגנה פיקודיות, וכי ועדות ההגנה שהתכנסו בעניינה היו של מס"ל.

בינואר 2023 כינס מקשא"פ פקע"ר ועדת הגנה פיקודית לדיון בעניין מערכת שוע"ל צבאי. הדיון התמקד בעיקר בהעמקה במערכת זו. בסיום דיון הוועדה קבע מקשא"פ פקע"ר שיש לקיים עוד דיון בוועדה לקראת מבצוע גרסה נוספת של שוע"ל צבאי.

בביקורת עלה כי שלא בהתאם לתפיסת ההגנה בסייבר של פקע"ר, מקשא"פ לא כינס ועדות הגנה פיקודיות כסדרן הן לגבי מערכת שוע"ל צבאי והן לגבי מערכת שוע"ל אזרחי. לגבי כינוס של ועדה אחת בנוגע לשוע"ל צבאי ב-2018, עלה כי אין מסמכים המעידים על כך. מאז כונסה ועדת הגנה אחת בראשות המקאש"פ, וזאת ובמהלך הביקורת, בינואר 2023, במקום ארבע ועדות (לפחות) בשנה. מצב זה מעיד על חוסר סדר ארגוני העלול לפגוע בבקרה על הגנת מערכות התקשוב בפקע"ר, ובכללן שוע"ל, ופגיעה בזיכרון הארגוני.

על פקע"ר להקפיד על כינוסן של ועדות ההגנה הפיקודיות כסדרן, בהתאם לתפיסת ההגנה בסייבר של הפיקוד, כדי לטייב את תהליכי הבקרה על תכנון מענה ההגנה ועל מימושו. עוד מומלץ כי פקע"ר יתעד את חומר הרקע המוגש לוועדות ואת סיכומיהן, כדי להבטיח זיכרון ארגוני ורציפות תהליכית.

בתגובתו מסר צה"ל כי ההמלצה תיבחן.

<u>קביעת אמות מידה (סטנדרטים) להגנה הנדרשת מחברות אזרחיות</u>

בהתאמה לפקודות על אגף התקשוב להגדיר את המענה המבצעי הנדרש להגנה בסייבר בכלל המרחבים, ובכלל זה את מדיניות התקשורת עם חברות אזרחיות בתחום זה, בתיאום עם מחב"ם.

בהתאם לפק"א חטיבת ההגנה בסייבר, על חטיבת ההגנה בסייבר לקבוע את סטנדרט ההגנה בסייבר הנדרש מחברות אזרחיות המתקשרות עם צה"ל, בתיאום עם משרד הביטחון. הסטנדרט כולל לדוגמה את רכיבי ההגנה הנדרשים ברשתות שבהן מתבצע הפיתוח של מערכות, לחובת הדיווח על אירוע סייבר שהתרחש אצל חברה מתקשרת כאמור ולביצוע ביקורות ומבדקים.

---

28 על פי קביעת אגף התקשוב בנושא סייבר.

29 רע"ן התרעה (יו"ר הוועדה), רמ"ד סייבר (מזכיר הוועדה), מ"פ סייבר מהגדוד, רמ"ד הנדסת תוכנית העורף מלוטם וקצין ביטחון מידע בפקע"ר.

30 קצין אמל"ח רלוונטי, קצין פרויקט (קפ"ט) רלוונטי, נציגי תעשייה, נציג חטיבת ההגנה בסייבר וכד'.

על פי מסמכי מס״ל בשנים האחרונות חל גידול ניכר במספר תקיפות הסייבר על ארגונים ובעוצמתן, והמקור של חלק מתקיפות אלו הוא בשרשרת האספקה[31] של הגוף המותקף. כדי לצמצם את סיכוני הסייבר יש צורך בהגדרת תהליכי עבודה מאובטחים וביישום והטמעה של בקרות.

מס״ל פרסם באוגוסט 2020 מסמך בנושא הגנת סייבר לשרשרת האספקה, ובו מפורטים תהליכי העבודה והפעולות הנדרשים להגנה מפני איום הקשור לשרשרת האספקה. הנושאים שצוינו במסמך זה הם בין היתר מדיניות הערכת סיכונים וכתיבת נוהל עבודה שיאושרו על ידי ההנהלה פעם בשנה, ניהול מחזור חיים של התקשרויות, סיום תהליך התקשרות עם ספק וביצוע הערכת מוגנות של ספק.

בנובמבר 2022 פרסם מלמ״ב - שמנחה חברות אזרחיות שנותנות שירותים למערכת הביטחון, ובהן גם חברות שנותנות שירותים לפקע״ר - נוהל לדיווח ולטיפול בפעולות מתוכננות, אירועים חריגים ותקלות[32]. הנוהל מגדיר בין היתר את עקרונות הדיווח על אירועים חריגים והטיפול בהם. בנוהל נקבע כי כל אירוע ביטחוני, ובכלל זה אירוע סייבר הקשור לשרשרת האספקה, ידווח למלמ״ב בתוך שעתיים לכל היותר מגילוי האירוע. כמו כן מפרט הנוהל את סדר הפעולות להתמודדות עם אירוע מסוג זה.

בתפיסת ההגנה בסייבר של פקע״ר צוין כי הימצאות מערכות פקע״ר במרחב הציבורי, האזרחי או המסחרי מרחיבה במידה ניכרת את פוטנציאל התקיפה בתחום הסייבר, והאתגר שנוצר הוא התמודדות עם נקודות כשל פוטנציאליות רבות עקב קשרים עם חברות אזרחיות.

בנובמבר 2022 ובאפריל 2023 מסרה רמ״ד סייבר בפקע״ר לצוות הביקורת כי חטיבת ההגנה בסייבר לא הנחתה את פקע״ר לגבי מערכת שוע״ל אזרחי בכל הנוגע לתנאי ההתקשרות בהיבטי הגנת סייבר עם חברות וארגונים אזרחיים שנותנים שירותים לפקע״ר או שיש למערכות שלהם ממשק עם המערכת. על כן פקע״ר קובע באופן עצמאי את הדרישות שהוא מציב לאותם ארגונים וחברות.

במאי 2023 מסרה מפקדת מרכז עליונות בחטיבת ההגנה בסייבר לצוות הביקורת כי בחוזים עם חברות אזרחיות אין סעיף המחייב אותן בהגנת סייבר, מאחר שהחוזים נערכו בשנים שקדמו לנושא הגנת הסייבר. עוד מסרה מפקדת מרכז עליונות כי חטיבת ההגנה בסייבר פועלת עם מלמ״ב לשילוב סעיף הנוגע להגנת סייבר בנספח הביטחון לחוזה, אך ציינה כי סעיף זה אינו בהכרח נבדק ומאושר על ידי חטיבת ההגנה בסייבר.

נמצא כי החברות שמונחות על ידי מלמ״ב הן רק חלק מהחברות האזרחיות שלהן יש ממשקים עם מערכת שוע״ל[33].

ביולי 2023 מסר מקשא״פ פקע״ר לצוות הביקורת את הדברים האלה:

1. לארבע משמונה[34] חברות פרטיות שאינן מונחות על ידי מלמ״ב ויש להן ממשק עם מערכת שוע״ל אזרחי, אין מסמך או נוהל התקשרות המסדירים את ההתחייבויות של הצדדים המעורבים בממשק עם פקע״ר.

2. לגבי ארבע החברות שיש להן מסמכי התקשרות עם פקע״ר, בפקע״ר מתועד רק מסמך התקשרות אחד (להלן - מסמך ההתקשרות המתועד).

---

31 שרשרת אספקה כוללת את כלל הארגונים, כוח האדם, הפעילויות, המידע והמשאבים המעורבים באספקת מוצר או שירות. יוצא אפוא כי המערכות המקושרות לשוע״ל אזרחי ולשוע״ל צבאי ומעורבות בתמונת המצב שהמערכות מייצרות עבור פקע״ר ועבור הרשויות המקומיות הן חלק משרשרת האספקה.

32 נוהל מס׳ 0714.

33 לדוגמה, חברות ה-CRM שנותנות שירותים לרשויות המקומיות ויש להן ממשק עם מערכת שוע״ל אזרחי אינן מונחות על ידי מלמ״ב.

34 ארבע חברות - CRM.

3. לפקע"ר אין מסמכי התקשרות או נוהל המסדירים את ההתחייבויות של הצדדים המעורבים בממשק של מערכת שוע"ל צבאי עם מערכות משטרת ישראל ומד"א, ובכלל זה בנושאים הקשורים להגנת הסייבר.

מבחינה של מסמך ההתקשרות המתועד עלה כי הוא אינו כולל פרק אבטחת מידע, ואין בו סעיפים שפורטו בתפיסת ההגנה בסייבר בנוגע לנושא הגנת הסייבר. כמו כן, אין בחוזה ההתקשרות התייחסות ליכולות הניטור של החברה ולחובתה לעדכן את פקע"ר על אירועי אבטחת מידע שיתרחשו ברשתות ובמערכות שלה.

בביקורת עלה כי אגף התקשוב וחטיבת ההגנה בסייבר אינם מממשים את אחריותם בהתאם לפקודות בנוגע לקביעת סטנדרט להגנה בסייבר לחברות אזרחיות שלהן יש התקשרות עם צה"ל ובעיגון הסטנדרט בחוזה עם חברות אלה.

בתגובתו על טיוטת הדוח מינואר 2024 מסר מלמ"ב כי הפיץ שני מסמכים הנוגעים להנחיות מחייבות של צה"ל לחברות שרשרת אספקה: (א) מסמך "מדיניות ביטחון להתקשרות חוזית עם חברות שרשרת אספקה ישראלית" (הופץ בספטמבר 2021). מטרתו של מסמך זה היא להגדיר את מדיניות מלמ"ב בעניין התקשרות הגופים המונחים עם ספקים ונותני שירותים ביטחוניים שונים, על ידי הגדרת קווים מנחים ועקרונות להתקשרות של הגוף המונחה עם הספק. זאת, באופן שישרת את האינטרס הביטחוני ויאפשר למערך הביטחון של הגוף המונחה לבצע אכיפה ולממש את אחריותו וסמכותו הביטחונית; (ב) נוהל 2000/004 (מ-1.11.22) שמטרתו להגדיר את מרחב הסמכות והאחריות של כלל הגופים המעורבים בטיפול הביטחוני בחברות שרשרת האספקה. הנוהל קובע שמלמ"ב הוא הגוף המנחה, צה"ל הוא הגוף הדורש, והגוף המיישם (חברת שרשרת האספקה) הוא הגוף המונחה.

עוד מסר מלמ"ב כי נוכח כמה אירועים שבהם עלה קושי לממש את הסמכות שלו לגבי חברות ונותני שירותים, בשל היעדר חוזים או בשל התקשרויות קודמות, ביולי 2022 רוענן ונשלח שוב נוהל מלמ"ב המעודכן בנושא "דרישות ביטחון בהתקשרות חוזית עם חברות שרשרת האספקה".

על אגף התקשוב וחטיבת ההגנה בסייבר, בשיתוף פקע"ר, לקבוע את סטנדרט ההגנה בסייבר הנדרש מחברות אזרחיות שיש להן התקשרות עם פקע"ר, בהתאם לפקודות החלות עליהן ובהתאם להנחיות מלמ"ב. במסגרת זו על חטיבת ההגנה בסייבר לוודא כי סטנדרט ההגנה כולל את כל הנושאים הנדרשים, דוגמת דיווחים על אירועי סייבר בהתאם להנחיות מלמ"ב.

על פקע"ר לעגן את ההתקשרויות עם חברות וארגונים שאיתן יש לו קשר במסמך מסדר או בנוהל מתואם. על פקע"ר לכלול במסמך או בנוהל התייחסות להגנות סייבר על פי הנחיית חטיבת ההגנה בסייבר, בהתאם לתפיסת ההגנה בסייבר של פקע"ר ועל פי הנהוג בישראל ובעולם, כפי שעלה גם מהנחיות מס"ל, ובהתאם למסמך ההנחיות ומדיניות שהפיץ מלמ"ב בספטמבר 2021.

בתגובתו מסר צה"ל כי בשנת 2023 כלל פקע"ר סעיפי הגנה בסייבר בכל חוזי התחזוקה החדשים עם חברות, במסגרת הארכת החוזה עימן. נוסף על כך נכתב נספח הגנה ייעודי למערכות כחלק מחתימה על חוזה חדש.

<u>מדדי כשירות להגנה בסייבר</u>

על פי הוראת פיקוד עליון (הפ"ע) אגף התקשוב, בסמכות אגף התקשוב לקבוע מדדים לכשירות בנושאים שבאחריותו, לבחון את העמידה במדדים אלו ולבצע את הנדרש לשמירת הכשירות.

גם בהפ"ע פקע"ר נקבע כי בסמכות פקע"ר לקבוע מדדים לכשירות בנושאים שבאחריותו, לבחון את העמידה בהם ולבצע את הנדרש לשמירת הכשירות.

בתפיסת ההגנה בסייבר של פקע"ר נקבע כי תפיסה זו תהווה בסיס לבניית הכשירות המבצעית של פקע"ר בנוגע להגנה בסייבר. כמו כן נקבע בתפיסה כי גופי הפעלת הכוח של מערך ההגנה בסייבר, גופי הניהול ותחזוקה של

הרשת וגופי הניטור ההגנתי נדרשים לשמור על כשירות מבצעית גבוהה. התפיסה אינה מפרטת את המדדים לכשירות ואת המשמעות של כשירות מבצעית גבוהה.

באפריל 2023 מסרה רמ"ד סייבר בפקע"ר לצוות הביקורת כי פקע"ר לא קבע הגדרות לכשירות מבצעית בסייבר. ביוני 2023 מסר מקשא"פ פקע"ר בעניין זה כי הוא אינו מכיר הגדרות למדדי כשירות להגנה בסייבר.

ביולי 2023 מסרה רמ"ד מוגנות רשתית במחלקת מבצעים שבחטיבת ההגנה בסייבר כי השיטה הקיימת למדידת הכשירות המבצעית בסייבר נועדה לרשתות מבודלות[35], ומיושמת בנוגע לרשתות הליבה שהן קריטיות לתהליכים מבצעיים. רמ"ד מוגנות רשתית הוסיפה כי המדור עוסק כעת בגיבוש שיטה למדידת הכשירות במרחב הציבורי, ובמסגרת זו גובשה טיוטה של תקן מוגנות רשתית למרחב כחול. רמ"ד מוגנות רשתית ציינה כי הבקרה של ענף חוסן מבוצעת על בסיס בדיקות חוסן וכחלק מהערכות מצב עיתיות המובלות על ידי חטיבת ההגנה בסייבר והמתקיימות עם גופי ההגנה בזרועות ובפיקודים, על בסיס הנתונים המתקבלים מהם.

בביקורת עלה כי נכון למועד סיום הביקורת, אגף התקשוב לא הגדיר מדדי כשירות מבצעית להגנה בסייבר הרלוונטיים לרשתות שאינן מבודלות, ובהן מערכות שוע"ל צבאי ושוע"ל אזרחי. עוד עלה כי פקע"ר לא הגדיר מדדי כשירות להגנה בסייבר למערכות ולרשתות שבאחריותו ולמערך שהוא מפעיל. היעדר הגדרה כאמור עלול לפגוע במוגנות המערכות מול איומי הסייבר.

מומלץ כי אגף התקשוב, מתוקף היותו המאסדר של נושא ההגנה בסייבר בצה"ל, יגדיר באמצעות חטיבת ההגנה בסייבר מדדי כשירות להגנה בסייבר בנוגע לכלל הרשתות ולמערכי הסייבר בזרועות ובפיקודים, ויפעל למדידתם. זאת כדי לאתר חולשות בהגנה בסייבר, לבצע בקרה על כשירות המערך וכדי לתת לגופים בצה"ל את היכולת לבדוק את עצמם על פי מדדים אלה ולהשתפר. עוד מומלץ כי פקע"ר יגזור ממדדים אלה את המדדים הרלוונטיים למערך ההגנה בסייבר של פקע"ר, יקבע שיטה להערכתם ויפעל למימושה בפועל.

☆

מכוח אחריותו של אגף התקשוב כמאסדר בתחום הגנת הסייבר, עליו לוודא היערכות ומוכנות של פקע"ר להתמודד עם איומי סייבר. במסגרת זו על אגף התקשוב באמצעות חטיבת ההגנה בסייבר להנחות את פקע"ר ולסייע לו בבניית מערכי הגנה מפני איומי סייבר על הרשתות שעליהן הוא מופקד, בהתאם למיקוד המטכ"לי ולאיום הייחוס ותרחיש הייחוס. וזאת בין היתר באמצעות קיום דיונים בוועדות ההגנה שבאחריותו, קביעת סטנדרט ההגנה הנדרש מחברות אזרחיות שמחוברות לשוע"ל אזרחי ולשוע"ל צבאי והגדרת מדדי כשירות רלוונטיים.

משרד מבקר המדינה ממליץ לפקע"ר ולחטיבת ההגנה בסייבר להסדיר את קשרי הגומלין ביניהם, וכן להגדיר את מחויבותה ומעורבותה של חטיבת ההגנה בסייבר בנוגע להגנה על מערכות פקע"ר, כחלק ממימוש האחריות האסדרתית שלה.

בתגובתו מסר צה"ל כי ההמלצה תיבחן.

[35] הכוונה לרשתות שאינן מחוברות למרשתת או לרשת חיצונית כלשהי.

מערכת שוע״ל צבאי

נבדקו היבטים שונים הנוגעים למערכת והועלו ליקויים והמלצות.

<u>תקינה</u>

בביקורת עלה כי פקע״ר אינו מכיר את תקן צה״ל למערכות מידע, אף שהוא תקן מחייב.

בתגובתו על טיוטת הדוח מינואר 2024 מסר צה״ל כי תקן צה״ל למערכות מידע אינו רלוונטי לפקע״ר.

מומלץ כי חטיבת ההגנה ופקע״ר יבחנו שנית את הצורך באימוץ תקן צה״ל למערכות מידע בפקע״ר.

צה״ל מסר בתגובתו כי ההמלצה תיבחן.

ניטור מערכות שוע״ל אזרחי וצבאי

החשש ההולך וגובר מפני תקיפות של רשתות תקשוב (להלן - אירועי סייבר) העלולות לגרום לפגיעה בתפקוד הרשתות מחייב הגנה על הרשתות. זאת, בין היתר, באמצעות איתור אירועי סייבר והיכולת להגיב על האירועים ולהתמודד עימם עד לביטול הסכנה וחזרה לפעילות שגרתית של הרשתות. לשם כך נדרש לנטר את פעילות המערכות והרשתות, לזהות פעילות חריגה שעלולה להעיד על ניסיונות לתקיפה של הרשתות ומערכות הארגון ולהתריע עליה למרכז שליטה שתפקידו לחסום את התוקף.

בתפיסת ההגנה בסייבר של פקע״ר נקבע כי מאמץ הניטור הוא מאמץ רציף הנמשך 365 יום בשנה בעיתות שגרה ובלחימה, וכי ההישג הנדרש ממנו הוא גילוי מוקדם של התוקף לפני שהשלים את התקיפה. הנחת העבודה היא שחרף מאמצי המניעה, אויב נחוש יצליח לחדור למערכי ההגנה, או שהתוקף כבר חדר לרשת. לפי התפיסה ״**גוף הניטור ההגנתי [של פקע״ר] הינו גוף מבצעי הנדרש להתנהלות מבצעית**״ (ההדגשה במקור).

לצורך ניטור האיומים על רשתות, ארגונים מפעילים מרכז שליטה ובקרה לאיומי סייבר (SOC) או נסמכים על מרכז זה, המשמש מוקד מרכזי אשר מנטר ומאגד את כל פעילות מערכות המידע והתשתיות, ותפקידו לזהות בזמן אמת אירועי סייבר כגון ניסיונות תקיפה של המערכת ופעולות לא מורשות. זיהוי אירוע סייבר מחייב תגובה מהירה בהתאם לסדרי פעולות קבועים מראש, אם על ידי צוות ב-SOC עצמו ואם על ידי צוותי תגובה חיצוניים. לאחר סיום הטיפול באירוע הסייבר צוות ה-SOC מבצע תחקור והסקת מסקנות, וממליץ במידת הצורך על תיקונים נדרשים בתוכנה, בחומרה או בנוהלי העבודה.

תפעול SOC יכול להתבצע על ידי הארגון עצמו שאחראי לניהול, להפעלה ולתחזוקה של כלל משאבי ה-SOC, או באמצעות ספק חיצוני[36] שמספק שירותי אבטחת סייבר, ובכלל זאת שירותי ניטור וניהול של מערכות אבטחה ורכיבים נוספים.

חטיבת ההגנה בסייבר פרסמה במאי 2022 תקן ניטור מטכ״לי הכולל חוקים להטמעה במערכות הניטור בכלל צה״ל. נוסף על כך, חטיבת ההגנה בסייבר מכינה כאמור תקן בנושא מוגנות רשתית במרחב הכחול, ותקן זה שטרם הופץ הוא במעמד טיוטה ונמסר שנידון בו נושא שגרת ניטור.

ביולי 2023 מסר מקשא״פ פקע״ר לצוות הביקורת כי פקע״ר הקים SOC בשנת 2020 כהחלטה עצמאית של גדוד התקשוב, וכי הוא גיבש את המענה על סמך האמצעים והידע שהיו קיימים בגדוד התקשוב בפקע״ר באותה עת, ללא עבודת מטה מקדימה שבמסגרתה נבחנו מודלים שונים להפעלת SOC. עוד מסר כי חטיבת ההגנה בסייבר לא

[36] כגון שירותי SOC מנוהלים (Managed Security Service Provider).

ליוותה את תהליך הקמת ה-SOC ולא נתנה הנחיות לגבי תפיסת הפעלה, נוהלי עבודה, התקנים הנדרשים והיבטים אחרים הקשורים לעבודת ה-SOC. עוד מסר כי הוא אינו מכיר הנחיה צה"לית לגבי ניהול SOC ותפקידיו.

משרד מבקר המדינה מציין לחיוב את פקע"ר על הקמת SOC פקע"ר כהחלטה עצמאית וכמענה לצורך מבצעי להגנת המערכות והרשתות שבאחריותו. עם זאת, בביקורת עלה כי חטיבת ההגנה בסייבר, המשמשת סמכות מקצועית עליונה בצה"ל בנוגע לכל תחומי ההגנה בסייבר לא הנחתה את פקע"ר בהקמת ה-SOC ולא גיבשה נהלים לעבודת ה-SOC ולתפעול של SOC. הפעלת SOC פקע"ר ללא הכוונה וללא עבודת מטה מקדימה עלולה לפגוע ביעילותה של פעילות הניטור וההתמודדות עם אירועי סייבר.

צה"ל מסר בתגובתו כי חטיבת ההגנה מכירה בפקע"ר כגוף בעל יכולות הגנה בסייבר, משבצת בפקע"ר חיילים במקצועות הגנת סייבר וכן מסייעת לפיקוד בשדרוג יכולות הגנת הסייבר הפיקודיות.

מומלץ כי חטיבת ההגנה בסייבר תגבש תפיסת הפעלה ונהלים או פקודות להפעלת SOC פיקודי, וכי פקע"ר יאמץ אותם לצורך טיוב עבודת ה-SOC, שהיא מרכיב משמעותי במשימת מניעתם של אירועי סייבר וההתמודדות עימם.

פקע"ר מבצע ניטור על כלל הרשתות והמערכות שבאחריותו, לרבות מערכת שוע"ל אזרחי ומערכת שוע"ל צבאי, באמצעות ה-SOC שהוא מפעיל. מינואר 2023 ועד סוף מאי 2023 התקבלו ב SOC פקע"ר 2,469 התרעות, מהן 3 התרעות ברמת חומרה גבוהה, 2,100 התרעות ברמת חומרה בינונית ו-366 התרעות ברמת חומרה נמוכה. יצוין כי בתקופה זו SOC פקע"ר טיפל בכל ההתרעות, והן לא גרמו להשבתה של המערכות או השירות. כמו כן, ניסיונות התקיפה שבוצעו לא צלחו.

מנהל SOC פקע"ר מסר לצוות הביקורת ביולי 2023 כי במסגרת פרויקט טיוב הניטור שפקע"ר מבצע בשבועות האחרונים, פקע"ר החל בהטמעת תקן הניטור המטכ"לי של חטיבת ההגנה בסייבר בכלל רשתות פקע"ר.

בביקורת עלה כי עד יולי 2023 לא הטמיע פקע"ר במלואו את תקן הניטור המטכ"לי שקבעה חטיבת ההגנה בסייבר.

בתגובתו מסר צה"ל כי תקן הניטור של חטיבת ההגנה שקיבל מעמד קבע בתחילת 2023 הוא כללי, ורובו אינו רלוונטי למערכות פקע"ר. עוד מסר צה"ל כי פקע"ר הטמיע באופן עצמאי תקן פיקודי שיש בו הוראות ניטור שמתאימות יותר למערכות שברשותו. בתקן הפיקודי מוטמעים החלקים הרלוונטיים מתקן הניטור המטכ"לי של חטיבת ההגנה.

מומלץ כי חטיבת ההגנה תבחן את רלוונטיות תקן הניטור שפרסמה לכלל הגופים המונחים שלה, ואם יעלה הצורך בכך - תעדכן אותו. עוד מומלץ כי פקע"ר יתייעץ עם חטיבת ההגנה, שהיא הגורם המנחה בהיבטי הגנת סייבר, בעניין גיבוש תקן הניטור הפיקודי.

בדיקות חוסן ומבדקי חדירות במערכות שוע"ל אזרחי ושוע"ל צבאי

על פי תפיסת ההגנה בסייבר של פקע"ר יש לבצע מבדקים שונים לבדיקת חוסן מערכות המידע.

צוות הביקורת בחן את דוחות המבדקים ואת המעקב אחר תיקון הליקויים. להלן יוצגו ממצאי הבחינה:

1. במבדקים שבוצעו במערכת שוע"ל אזרחי חזרו ונשנו ליקויים בתחומים דומים.
2. בחלק מהמבדקים לא תועדו הליקויים לצורך מעקב, ועל כן לא ניתן לדעת מהו סטטוס הליקויים.
3. במבדקים שתועדו נמצאו 283 ליקויים. פקע"ר לא ביצע בקרת איכות על תיקון 139 (49%) מהם.
4. פקע"ר מנהל כמה מסמכים למעקב אחר הליקויים שנמצאו במבדקים.

בביקורת עלה כי ליקויים בתחומים דומים חזרו ונשנו בכל המבדקים. עולה מכך שפקע"ר אינו פועל לתיקון מלא של הליקויים שעלו במבדקים. עוד עלה בביקורת כי פקע"ר אינו מתעד באופן מלא את הליקויים שעלו במבדקים ומקיים מעקב חלקי אחר תיקונם. זאת שלא בהתאם לתפיסת ההגנה בסייבר של פקע"ר.

מומלץ כי פקע"ר יבצע מעקב שוטף אחר תיקון הליקויים במערכות שוע"ל צבאי ואזרחי, ובכלל זאת ינהל מסמך אחוד למעקב אחר כלל הליקויים, שיעודכן באופן שוטף, יקבע תאריכי יעד לתיקון הליקויים ויבצע בקרה על תיקונם, וזאת בהתאם לתפיסת ההגנה בסייבר של פקע"ר.

בתגובתו מסר צה"ל כי ההמלצה תיבחן.

מנגנוני בקרה

נבדקו היבטים מסוימים בתחום זה והועלו ליקויים והמלצות.

<u>סיכום</u>

מדינת ישראל נערכת לקראת אירועי חירום, משברים או אסונות מסוגים שונים העלולים לסכן חיי אדם, לגרום לפגיעה קשה ברציפות התפקודית בכל אורחות החיים ולפגום בחוסן הלאומי. לפקע"ר תפקיד מרכזי בטיפול בעורף האזרחי בחירום, ויחד איתו פועלים גופים רבים, ובהם רשויות מקומיות, משרדי ממשלה וגופי חילוץ והצלה. כדי לאפשר שליטה ובקרה על הנעשה בעורף האזרחי פיתח פקע"ר את מערכות שוע"ל (צבאי ואזרחי), שתכליתן לאפשר תהליכים מבצעיים פיקודיים הנוגעים לחילוץ, להצלה ולשמירה על רציפות תפקודית ולספק תמונת מצב אחודה המשמשת כלי עזר למקבלי ההחלטות. הפריסה הרחבה של מערכות השוע"ל בין כלל הגורמים המעורבים בהיערכות לאירועי חירום חושפת את מערכות השוע"ל לסיכונים ולאיומי סייבר, וההגנה מפניהם היא מרכיב קריטי ביכולת של פקע"ר להוציא לפועל את משימותיו.

ממצאי דוח זה מעלים כי הגם שפקע"ר משקיע משאבים רבים בבניית מערכי הגנה בסייבר למערכות שוע"ל, והקים מיוזמתו SOC כמענה לצורך מבצעי להגנת המערכות והרשתות שבאחריותו, קיימים פערים משמעותיים הנוגעים לאופן שבו פקע"ר מנהל את המערכה הזו. בדוח עלו פערים בכל הנוגע לאופן שבו אגף התקשוב ממלא את אחריותו בהיבטי האסדרה, ההנחיה, המעקב והתמיכה במערכי ההגנה בסייבר של פקע"ר. עוד עלה כי פקע"ר אינו מקיים תהליכי ניהול סיכונים ובקרה כנדרש. נוסף על כך מתקיימת בקרה חלקית על תיקון הליקויים שעולים בבדיקות חוסן.

על אגף התקשוב ופקע"ר לפעול במשותף לתיקון הליקויים שעלו בדוח זה כדי לשפר את ההגנה על מערכות שוע"ל צבאי ושוע"ל אזרחי. על אגף התקשוב וחטיבת ההגנה בסייבר לבחון את הצרכים של פקע"ר בתחום הגנת הסייבר ואת מידת התאמתם של המשאבים העומדים לרשותו למימוש פעילות זו. כמו כן, על אגף התקשוב לוודא כי לפקע"ר הידע וההנחיות הנדרשים למימוש אחריותו להגנת המערכות והרשתות שברשותו. על פקע"ר לנתח ולנהל באופן שוטף את סיכוני הסייבר המאיימים על המערכות והרשתות שברשותו, לבצע בקרה על המענה לסיכונים אלו ולשפר את האופן שבו הוא ממלא אחר ההוראות הנדרשות בדגש על מימוש רכיבי הגנה. נוסף על כך, עליו לוודא שעומדים לרשותו כל הכלים הנדרשים כדי להבטיח עבודה סדורה ובטוחה עם חברות אזרחיות.