



מבקר המדינה

**הגנה בתחום הסייבר:
היבטי אסדרה והגנה
על המידע ומערכות
המחשוב ברפאל מערכות
לחימה מתקדמות בע"מ**

חשון התשפ"ה | נובמבר 2024



הגנה בתחום הסייבר: היבטי אסדרה והגנה על המידע ומערכות המחשוב ברפאל מערכות לחימה מתקדמות בע"מ

מבוא

בהחלטת הממשלה מאוגוסט 2011¹ שעניינה קידום היכולת הלאומית במרחב הקיברנטי (להלן גם - מרחב הסייבר) ושיפור ההתמודדות עם האתגרים הנוכחיים והעתידיים במרחב הקיברנטי הוגדר מרחב הסייבר כמתחם פיזי ולא פיזי, שנוצר או מורכב מחלק מהגורמים האלה או מכולם: מערכות ממוחשבות, רשתות מחשבים ותקשורת, תוכנות, מידע ממוחשב, תוכן שמועבר באופן ממוחשב, נתוני תעבורה ובקרה והמשתמשים בכל אלה.² בהחלטת הממשלה האמורה נקבע כי מרחב הסייבר האזרחי הישראלי כולל את כלל הגורמים הממלכתיים והפרטיים במדינת ישראל, למעט הגופים המיוחדים.³ דהיינו, מרחב הסייבר הישראלי כולל את המרחב האזרחי, הממשלתי והביטחוני.

הפעילות הגוברת במרחב הרשתי מביאה עימה חדשנות טכנולוגית ופיתוחים לאדם ולסביבתו. לצד היתרונות שמאפשרות מערכות ממוחשבות, הן גם יצרו איום חדש ההולך ומתעצם: איום הסייבר. איום זה הוא צירוף של כוונות ויכולות של תקיפה במרחב הסייבר שטרם התממש. איום הסייבר עלול להביא לפגיעה בתוך מרחב הסייבר ובארגונים, ובכלל זה פגיעה ברציפות התפקודית של הארגון, בשלמות ובאמינות של התהליכים העסקיים המתרחשים בו, פגיעה כלכלית ניכרת, פגיעה בחדשנות ובתחרות, ועוד.

אירוע סייבר הוא התרחשות אשר מעידה על פגיעה אפשרית בפעילותה התקינה של מערכת מחשוב. אירועי סייבר עלולים להיגרם בשוגג או במזיד, על ידי גורם פנימי או חיצוני לארגון. אירועים אלו מבוססים על ניצול פגיעויות או חולשות אבטחה במערכות המחשוב של הארגון, העלולים לפגוע בו ברמות חומרה שונות. בשנים האחרונות מסתמנת עלייה הדרגתית ברמת איומי הסייבר וכן במספר האירועים בפועל ובחומרתם, דבר המשבש את פעילותם התקינה של ארגונים בארץ ובעולם.⁴

תקיפת סייבר היא רצף פעולות (חד-פעמי או מתמשך) שמבצע תוקף במרחב הסייבר לתכלית קונקרטית, כגון חבלה, איסוף מידע או השפעה תודעתית. תקיפות סייבר משמשות לפשיעה, טרור, ריגול ולוחמה. בדוח לסיכום שנת 2022 שפרסם מערך הסייבר הלאומי⁵ (להלן - מס"ל) במאי 2023 לגבי הסייבר בישראל נכתב כי בשנת 2022 דווחו למערך 9,108 אירועים על ידי כלל הגורמים במדינה שאומתו כאירועי סייבר. להלן פירוט בתרשים.

1 החלטת הממשלה 3611 "קידום היכולת הלאומית במרחב הקיברנטי" (7.8.11).

2 מרחב הסייבר כולל גם פעילות של גורמים ישראלים בחו"ל.

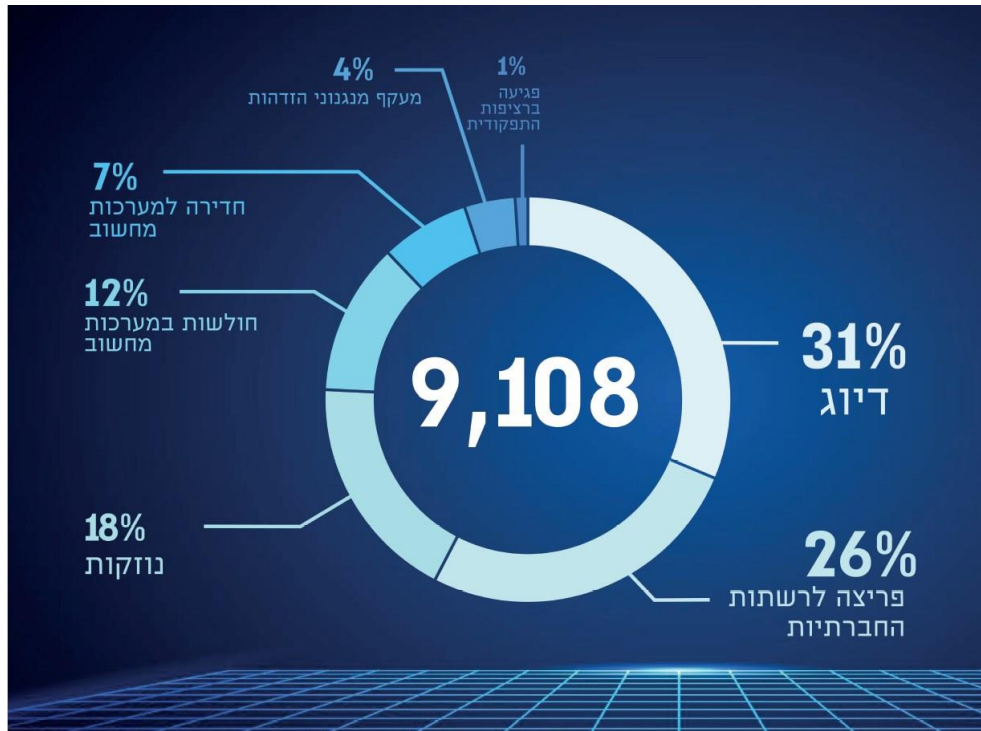
3 בהחלטת הממשלה 3611 (7.8.11) הוגדרו גופים מיוחדים כדלקמן: צה"ל, משטרת ישראל, שירות הביטחון הכללי (שב"כ), המוסד למודיעין ולתפקידים מיוחדים (המוסד) ומערכת הביטחון באמצעות הממונה על הביטחון במערכת הביטחון (מלמ"ב); וכמו כן הוגדרה מערכת הביטחון כדלקמן: הגופים המונחים על ידי מלמ"ב מכוח החוק להסדרת הבטחון בגופים ציבוריים, התשנ"ח-1988, וכן ספקים ומפעלים המפתחים או המייצרים ציוד ביטחוני עבורם.

4 מבקר המדינה, **דוח שנתי של מבקר המדינה בנושא סייבר ומערכות מידע - דצמבר 2022**, "הגנת הסייבר במגזר התחבורה", עמ' 39 - 111.

5 מס"ל הוא גוף ממשלתי האחראי לאבטחת מידע והגנה על מרחב הסייבר הלאומי האזרחי בישראל, למדיניות ישראל במרחב זה, לבניין הכוח הלאומי בסייבר ולקידום וביסוס העוצמה של ישראל בתחום זה.



תרשים 1: אירועי סייבר שדווחו למס"ל מכלל הגורמים במדינה בשנת 2022



על פי דוח מס"ל לסיכום שנת 2022 לגבי הסייבר בישראל (סך האחוזים מסתכם ב-99%), בעיבוד משרד מבקר המדינה.

מהתרשים עולה כי בשנת 2022 דווחו למס"ל 9,108 אירועי סייבר, כ-31% מהם נבעו ממתקפות דיוג⁶.

רפאל היא חברה ממשלתית כהגדרתה בחוק החברות הממשלתיות, התשל"ה-1975 (להלן - חוק החברות הממשלתיות), ובעלות מלאה של המדינה. רפאל מתמחה בפיתוח ובייצור של אמצעי לחימה (להלן - אמלי"ח) ומערכות חימוש והגנה למרחבי האוויר, היבשה, הים והסייבר; בפיתוחים שונים בתחומי התקשוב, איסוף המודיעין ועיבודו והלוחמה ברשת. רפאל כפופה בין היתר להוראות חוק החברות הממשלתיות, החוק להסדרת הבטחון בגופים ציבוריים, התשנ"ח-1998 (להלן - החוק להסדרת הביטחון).

החוק להסדרת הביטחון מסמיך את הממונה על הביטחון במערכת הביטחון (להלן - מלמ"ב) להנחות את מפעלי מערכת הביטחון ומפעלים המייצרים מוצרים עבור מערכת הביטחון (להלן - מפעלי מעהב"ט⁷) שיוגדרו. רשות החברות הממשלתיות הוקמה מכוח הוראות חוק החברות הממשלתיות. בין היתר, בהתאם לסמכותה בחוק, רשות החברות הממשלתיות מטפלת לפי הנחיות הממשלה בעניינים המשותפים לכלל החברות הממשלתיות, מייעצת ומסייעת לחברות הממשלתיות בניהול עסקיהן. כללי רשות החברות הממשלתיות בנושאים שונים הינם תקנות שמתקינים השרים האחראים על החברות. בין היתר רשות החברות מפיצה לחברות הממשלתיות ולחברות הבנות הממשלתיות חוזרים בנושאים שונים.

⁶ מתקפת סייבר שבה התוקף מתחזה לגורם אמין כדי להונות אנשים ולגרום להם לחשוף מידע רגיש (phishing).

⁷ מעהב"ט - צה"ל ומשהב"ט, לרבות יחידות הסמך.



פעולות הביקורת

בתקופה נובמבר 2022 עד יולי 2023 ביצע משרד מבקר המדינה ביקורת בנושא ההגנה בסייבר בכמה היבטים הנוגעים לאסדרה ולהגנה על מידע ומערכות המחשוב ברפאל. בביקורת נבדקו הנושאים האלה: הסדרת יחסי העבודה בין מס"ל למלמ"ב; סמכויות ההנחיה והפיקוח של מלמ"ב; תפיסת ההגנה בסייבר במלמ"ב; מדיניות אבטחת המידע ברפאל; ניהול הסיכונים הארגוני ברפאל; תוכניות העבודה ותקציב ההגנה בסייבר של רפאל; ההגנה על רשת מחשוב מסוימת ומערכות מידע מסוימות ברפאל ובקורות על אבטחת המידע המיושמות בהן; ומיגון תשתיות מסוימות ברפאל. הביקורת נערכה במלמ"ב וברפאל. בדיקות השלמה נערכו בתעשייה האווירית לישראל בע"מ (להלן - התע"א), בחברת החשמל לישראל בע"מ (להלן - חח"י) ובמס"ל. ועדת המשנה של הוועדה לענייני ביקורת המדינה של הכנסת החליטה שלא להניח על שולחן הכנסת ולא לפרסם נתונים מפרק זה לשם שמירה על ביטחון המדינה ועל יחסי מסחר בין-לאומיים של המדינה, בהתאם לסעיף 17 לחוק מבקר המדינה, התשי"ח-1958 [נוסח משולב].

חלק ראשון: היבטי אסדרה בסייבר

הסדרת יחסי העבודה בין מס"ל למלמ"ב

החלטת הממשלה מאוגוסט 2011: בהחלטת הממשלה מאוגוסט 2011 בעניין קידום היכולת הלאומית במרחב הקיברנטי הוחרגו הגופים המיוחדים, לרבות מלמ"ב, מההחלטה ונקבע כי יחולו עליהם הסדרים מיוחדים הנוגעים לקידום ההגנה על המרחב הקיברנטי ולקידום המחקר והפיתוח בתחום המרחב הקיברנטי כפי שייקבעו בהסכמה ביניהם ובין מטה הסייבר הלאומי⁸ בתוך 120 ימים מיום הקמתו.

בביקורת עלה כי אף שעברו כ-12 שנים ממועד החלטת הממשלה מאוגוסט 2011 בעניין קידום היכולת הלאומית במרחב הקיברנטי, מס"ל ומלמ"ב לא קבעו הסדרים מיוחדים הנוגעים לקידום ההגנה על המרחב הקיברנטי ולקידום המחקר והפיתוח בתחום המרחב הקיברנטי כנדרש בהחלטת הממשלה.

החלטת הממשלה מפברואר 2015: בהחלטת הממשלה מאוגוסט 2011 נקבע כי ראש מטה הסייבר הלאומי יגיש לממשלה הצעה לתפיסת הגנה כוללת על המרחב הקיברנטי, בתיאום עם הגופים המיוחדים, בתוך 120 ימים מיום תחילת פעילות המטה. לאחר כשלוש שנים וחצי, בהמשך להחלטת הממשלה מאוגוסט 2011 ובעיקר לצורך קביעת תפיסת הגנה כוללת על המרחב הקיברנטי שתחליף תפיסה קודמת, החליטה הממשלה בפברואר 2015⁹ בין היתר להקים את הרשות הלאומית להגנת הסייבר (להלן - הרשות).

על מס"ל ומלמ"ב לקיים את החלטות הממשלה בכל הנוגע להסדרת שיתוף הפעולה ביניהם באמצעות המנגנונים שנקבעו בהחלטות אלו.

⁸ מטה הסייבר הלאומי פעל מינואר 2012 עד ינואר 2018. בהחלטת הממשלה 3270 (17.12.17) אוחדו מטה הסייבר הלאומי והרשות הלאומית להגנת הסייבר, שהוקמה על פי החלטת הממשלה 2444 מ-15.2.15 בנושא קידום ההיערכות הלאומית להגנת הסייבר, לגוף אחד - מערך הסייבר הלאומי (מס"ל). בהחלטת הממשלה 3270 נקבע כי יעדי מס"ל, תפקידיו וסמכויותיו יהיו התפקידים של מטה הסייבר הלאומי ושל הרשות הלאומית להגנת הסייבר הקבועים בחוק ובהחלטות הממשלה בנושא ועל פי החלטות שני הגופים.

⁹ החלטת הממשלה 2444 "קידום ההיערכות הלאומית להגנת הסייבר" (15.2.15).



סמכויות ההנחיה והפיקוח של מלמ"ב

סמכויות הנחיה ופיקוח: בחוק להסדרת הביטחון נקבע כי ראש הממשלה רשאי להורות¹⁰, בהסכמת שר הביטחון, כי קצין מוסמך למתן הנחיות כהגדרתו בחוק לעניין הגופים המנויים בסעיפים 2 ו-3 לתוספת הראשונה לחוק, ובהם משרד הביטחון, יהיה מי שמינה ראש מלמ"ב (להלן - נציג מלמ"ב). מלמ"ב פועל בין היתר מתוקף החוק להסדרת הביטחון והצו להסדרת הביטחון.

בחוק להסדרת הביטחון נקבעו סמכויות ההנחיה והפיקוח של נציג מלמ"ב, ולפיהן הוא רשאי לתת הנחיות מקצועיות לגופים המונחים ולאדם שמונה על פי החוק להיות אחראי לארגון פעולות האבטחה ולפיקוח עליהן (להלן - ממונה הביטחון) בגופים אלו, בכל הנוגע לפעולות אבטחת מידע, לרבות הנחיות בעניין בקרה ודיווח. בחוק הוגדר כי פעולות לאבטחת מידע משמען פעולות הדרושות לשם שמירה על מידע מסווג של גוף ציבורי¹¹ או על מידע כאמור המצוי אצלו, וכן פעולות למניעת פגיעה בכל אחד מאלה. עוד נקבע בחוק כי הגופים המונחים וממונה הביטחון ימלאו אחר ההנחיות המקצועיות שניתנו להם, וכי נציג מלמ"ב רשאי לבדוק בגופים אלו אם הם מילאו את הוראות החוק ואת ההנחיות שניתנו להם.

בחוק להסדרת הביטחון משנת 1998 לא הוקנו למלמ"ב סמכויות ברורות בכל הנוגע לביצוע פעילות טכנולוגית אופרטיבית, ולא הוקנתה למלמ"ב סמכות הנחיה מקצועית לגבי רשתות מסוימות.

מומלץ כי מלמ"ב יפעל להסדיר ככל הנדרש את הסמכויות הנדרשות לצורך מימוש ייעודו.

תפיסת ההגנה בסייבר במלמ"ב

בביקורת עלה כי תורת ההגנה בסייבר שהכינה חטיבת תורה והגנה (תוה"ג) ביחידה הטכנולוגית במלמ"ב אינה כוללת תקן למרכז ניטור של ארגון, על אף היותו של מרכז ניטור כזה אחד ממרכיבי ההגנה החשובים ביותר של ארגון. כמו כן, חטיבת תורה והגנה (תוה"ג) לא פרסמה לגופים המונחים הנחיה לגבי היערכות הנדרשת לניהול אירוע סייבר ולגבי ניהול האירוע עצמו.

מומלץ כי היחידה הטכנולוגית במלמ"ב תפעל להשלים את תורת ההגנה בסייבר, ובכלל זה להכין את התקן למרכז הניטור ואת ההנחיות הנדרשות לגבי היערכות לניהול אירועי סייבר ולגבי ניהול האירועים, תחקורם והפקת הלקחים בנושא.

¹⁰ בנובמבר 2022 מסרו נציגי מלמ"ב למשרד מבקר המדינה בעל פה כי ראש הממשלה אריאל שרון ז"ל הורה זאת בהתאם לאמור בחוק, אולם לא נמצאו במלמ"ב מסמכים בנוגע לקביעה האמורה.

¹¹ כל גוף המנוי באחת מהתוספות לחוק, ולגבי משרד ממשלתי המנוי באחת מהתוספות - לרבות יחידות הסמך שלו.



חלק שני: הגנה על המידע ומערכות המחשוב ברפאל מערכות לחימה מתקדמות בע"מ

ניהול הסיכונים הארגוני ברפאל

אסטרטגיית הסיכון ומדיניות ניהול הסיכונים: במאי 2023, בעת הביקורת, כשלוש שנים וחצי לאחר פרסום חוזר רשות החברות הממשלתיות בנושא ניהול סיכונים תאגידי מינואר 2020, אישרה הוועדה הארגונית לניהול סיכונים ברפאל מסמך אסטרטגיית סיכון כוללת לחברה ומדיניות ניהול הסיכונים. ואולם הנהלת רפאל לא העלתה לאישור הדירקטוריון את האסטרטגיה והמדיניות האמורות, והדירקטוריון לא אישר אותן. כן עלה בביקורת כי נכון ליולי 2023 מדיניות ניהול הסיכונים לא כללה התייחסות למנגנוני דיווח לגורמים חיצוניים לרפאל.

עוד עלה בביקורת כי רפאל לא דיווחה לרשות החברות הממשלתיות כנדרש ממנה. כל זאת שלא בהתאם לאמור בחוזר רשות החברות הממשלתיות לגבי ניהול סיכונים תאגידי מינואר 2020.

מיגון פיזי של תשתיות מסוימות

בביקורת עלו פערים בתחום המיגון הפיזי של תשתיות מסוימות.

ביטוח מפני אירועי סייבר

משרד מבקר המדינה בדק את נושא רכישת פוליסות ביטוח מפני אירועי סייבר ברפאל, וערך השוואה בנושא בין מצב הדברים ברפאל למצב בתע"א ובחח"י.

ביטוח סייבר בחח"י: לחח"י יש פוליסת ביטוח "רכוש" לתקופה יוני 2022 - דצמבר 2023, המכסה נזקים פיזיים לרכוש בגין אירוע סייבר בסכום של עד 100 מיליוני דולרים; ופוליסת "חבולות כלליות" לתקופה יולי 2022 - יוני 2023, המכסה תביעות של צד ג' בגין נזקי גוף ורכוש הנובעים מאירוע סייבר בהתאם לתנאי הפוליסה. עם זאת, לחח"י אין פוליסת ביטוח סייבר ייעודית המכסה נזקים, כגון תשלום דמי כופרה, אובדן נתונים ופגיעה במוניטין.

בקרות מקרה ביטוח על חח"י לספק למבטחים או למי מטעמם מידע ולאפשר להם לבצע בדיקה של מערכות המידע של חח"י.

בינואר 2023 מסרה חח"י למשרד מבקר המדינה כי היא בוחנת בין היתר את האפשרות לרכוש ביטוח נוסף בתחום הסייבר בהתאם לתנאי הפוליסה, לרבות הכיסויים הניתנים, ובהתחשב בשיקולי עלות תועלת.

ביטוח סייבר בתע"א: בנובמבר 2021 קיימה ועדה בראשות המשנה למנכ"ל לאסטרטגיה, חדשנות וטרנספורמציה דיון בנושא ההתמודדות עם איומי הסייבר. בדיון צוין בין היתר כי לתע"א הייתה באותו מועד פוליסת ביטוח המכסה נזק בגין אירוע סייבר בסכום של עד 10 מיליוני דולרים; כי הפוליסה אינה יעילה מכיוון שנזק בסכום של עד 10 מיליוני דולרים אינו נזק מהותי לתע"א; וכי רכישת פוליסה המכסה נזק כאמור בסכום של יותר מ-10 מיליוני דולרים מייקרת מאוד את עלות הרכישה ומחייבת מסירת מידע לחברת הביטוח, אולם מסיבות ביטחוניות לא ניתן למסור מידע למבטח.

משנת 2016 הייתה לתע"א פוליסת ביטוח המכסה נזק בגין אירוע סייבר ובתקופה ינואר 2021 - פברואר 2022 הפוליסה כיסתה נזק כאמור בסכום של עד עשרה מיליוני דולרים. ממרץ 2022 לא



חידשה התע"א את הפוליסה. בפברואר 2023 מסרה הנהלת התע"א לוועדת הביקורת של הדירקטוריון כי התע"א לא חידשה את פוליסת הביטוח, בגלל הכיסוי המצומצם שיש לפוליסה והעלות הגבוהה של רכישתה.

בתגובה על ממצאי הביקורת מנובמבר 2023 מסרה התע"א כי ההנהלה והדירקטוריון מתמקדים בניהול סיכון הסייבר, לרבות בחינת תוכניות להפחתתו וקבלת דיווחים שוטפים; כי פוליסת ביטוח אינה משמשת להפחתת הסיכון אלא לפיצוי כספי בגינו; כי עקב "כשל שוק" עולמי לא ניתן היה לרכוש פוליסת ביטוח בהיקף כיסוי נאות במרץ 2022; וכי הדירקטוריון וועדותיו דנו בנושא לפחות שלוש פעמים בשנת 2023.

ביטוח סייבר ברפאל: בפוליסה הביטוח לכיסוי "נזקי רכוש ועסקים" שרכשה רפאל לתקופה ספטמבר 2022 - אוגוסט 2023 קיימת החרגה לנזקים בגין אירוע סייבר. לפי הפוליסה האמורה, הרכוש, לרבות ציוד התקשוב והמערכות הממוחשבות, אינו מבוטח מפני נזק הנובע מאירוע סייבר. עם זאת, הציוד והמערכות כאמור מבוטחים בגין אירוע סייבר שמקורו בטעות או במחדל¹².

בישיבת ועדת הביקורת שהתקיימה ביולי 2020 בנושא ביטוח ברפאל צוין כי רפאל נמצאת לקראת סיומה של עבודת מטה בנושא ביטוח סייבר, וכי המנכ"ל הנחה להציג לפני הדירקטוריון את מסקנותיה של עבודת המטה. בדיון בראשות מנכ"ל רפאל שהתקיים באוקטובר 2020 בנושא סיכויי סייבר וביטוח סייבר הוצגה מצגת לגבי עבודת המטה האמורה. במצגת צוין בין היתר כי התקבלו שלוש הצעות מחיר לביטוח מפני סיכויי סייבר; כי פעילות רפאל להגנה על הסייבר צמצמה את האיום המרכזי של דלף מידע ביטחוני ועסקי; כי פרמיית הביטוח גבוהה, לעומת התקבולים שיתקבלו מחברת הביטוח בגין אירוע סייבר; כי לא יהיה ניתן לתבוע מחברת הביטוח פיצוי בגין פגיעה בתפוקה או במחזור המכירות; כי לא ניתן לחשוף מידע מסווג לפני חברת הביטוח בעקבות נזק בגין אירוע סייבר, ומגבלה זו מקשה לממש את ביטוח הסייבר בקרות אירוע; וכי ניתן לרכוש ביטוח המכסה נזק של עד 10 מיליוני דולרים בלבד. יצוין כי סכום זה אינו מהותי לפעילותה של רפאל: בשנת 2022 מחזור המכירות שלה היה כ-3.3 מיליארד דולר¹³ והרווח התפעולי שלה היה כ-160 מיליון דולר. בעבודת המטה הומלץ לא לרכוש ביטוח סייבר והמנכ"ל סיכם בדיון כי הוא מקבל את ההמלצה.

על אף הודעת רפאל לוועדת הביקורת ביולי 2020 כי מנכ"ל רפאל הנחה להביא לפני הדירקטוריון את מסקנות עבודת המטה לגבי ביטוח מפני אירועי סייבר, בביקורת עלה כי רק בנובמבר 2021, כשנה לאחר שהנהלת רפאל סיימה להכין את עבודת המטה באוקטובר 2020 וכשנה לאחר שמנכ"ל רפאל החליט שרפאל לא תרכוש ביטוח בנושא, הציגה הנהלת רפאל לפני הדירקטוריון את תוצרי עבודת המטה ומסקנותיה.

בישיבת ועדת הביקורת שהתקיימה בנובמבר 2021 ובישיבת הדירקטוריון שהתקיימה בדצמבר 2022 בנושא מערך הביטוח השנתי ברפאל, צוינו מסקנות הנהלת רפאל ולפיהן פוליסת ביטוח מפני אירועי סייבר אינה נותנת מענה לסיכונים העומדים לפני רפאל והועלו נימוקים לאי-רכישת פוליסה כאמור. ועדת הביקורת והדירקטוריון אישרו את מערך הביטוח השנתי, ללא ביטוח מפני אירועי סייבר.

מהמתואר לעיל עולה כי ביולי 2023, בעת הביקורת, לחח"י היו שתי פוליסות ביטוח המכסות נזקים לרכוש ותביעות צד ג' בגין אירועי סייבר, ואילו לתע"א ולרפאל¹⁴ לא היו פוליסות ביטוח כאמור. רפאל לא רכשה ביטוח מפני אירועי סייבר בעיקר מהסיבות שלהלן: רמת ההגנה על

¹² בפוליסת הביטוח לא פורט סכום הביטוח האמור.

¹³ חושב לפי שער חליפין 3.52 שקל לדולר ל-31.12.22.

¹⁴ למעט ציוד תקשוב ומערכות ממוחשבות ברפאל המבוטחות בגין אירוע סייבר שמקורו בטעות או במחדל.



הסייבר ברפאל גבוהה; רכישת הביטוח אינה יעילה כלכלית; לא יהיה ניתן לתבוע מחברת הביטוח פיצוי בגין פגיעה בתפוקה או במחזור המכירות; לא ניתן לחשוף מידע מסווג לחברת הביטוח בעקבות נזק בגין אירוע סייבר, ומגבלה זו מקשה לממש את הביטוח בקרות אירוע; וניתן לרכוש ביטוח המכסה נזק של עד עשרה מיליוני דולרים בלבד, סכום שאינו מהותי לפעילותה של רפאל.

מומלץ כי הנהלת רפאל תמשיך לבחון מפעם לפעם את כדאיות הרכישה של ביטוח ייעודי מפני אירועי סייבר בהתחשב בכמות ניסיונות התקיפה, בפוטנציאל הנזק מהם ובכיסויי הביטוח האפשריים בשוק. עוד מומלץ כי מלמ"ב יבחן את הצורך במתן סיווג ביטחוני לגורמים מסוימים בחברות ביטוח כדי לאפשר לגופים המונחים לרכוש ביטוח ייעודי מפני אירועי סייבר ככל הנדרש.

בתגובה על ממצאי הביקורת מאוקטובר 2023 מסרה רפאל כי תבחן את כדאיות הרכישה בעוד שנה וחצי, וככל שתחליט להמשיך לא לרכוש ביטוח ייעודי מפני אירועי סייבר אזי היא תבחן את הנושא שוב כל שלוש שנים. כמו כן, בתגובה על ממצאי הביקורת מנובמבר 2023 מסרה התע"א כי התוצאות של תקיפת סייבר על חח"י אינן דומות במהותן לתוצאות של תקיפה כאמור על חברות ביטחוניות, לרבות התע"א.

התקציב להגנת טכנולוגיות המידע ברפאל

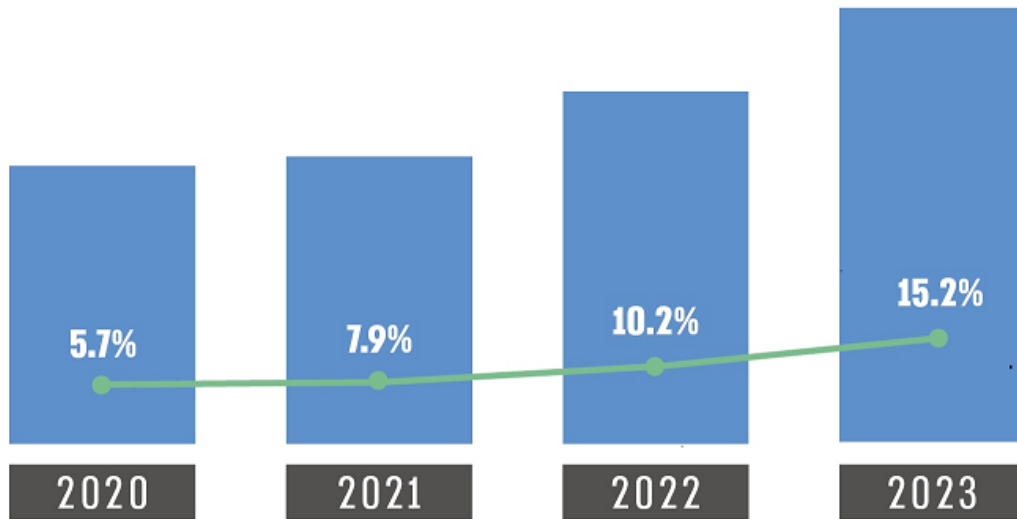
להלן בתרשים מובאים נתונים לגבי התקציב של מינהל טכנולוגיות מידע ותהליכים ברפאל (להלן - מטכ"ם) ותקציב מחלקת אבטחת טכנולוגיות והגנת סייבר לנושאי מחשוב¹⁵ בשנים 2020 - 2023.¹⁶

¹⁵ תקציב תפעולי לנושאי מחשוב, תקציב עבור עובדי חוץ לגבי טכנולוגיות המידע ותקציב השקעות המחשוב של מטכ"ם.

¹⁶ תקציב מחלקת אבטחת טכנולוגיות והגנת סייבר נועד לפעילות בתחום מערכות הגנה ייעודיות בלבד.



תרשים 2 : השיעור של תקציב מחלקת אבטחת טכנולוגיות והגנת סייבר מתוך תקציב מטכ"ם לנושאי מחשוב בשנים 2020 - 2023



■ תקציב מטכ"ם לנושאי מחשוב ■ תקציב מחלקת אבטחת טכנולוגיות והגנת סייבר לנושאי מחשוב

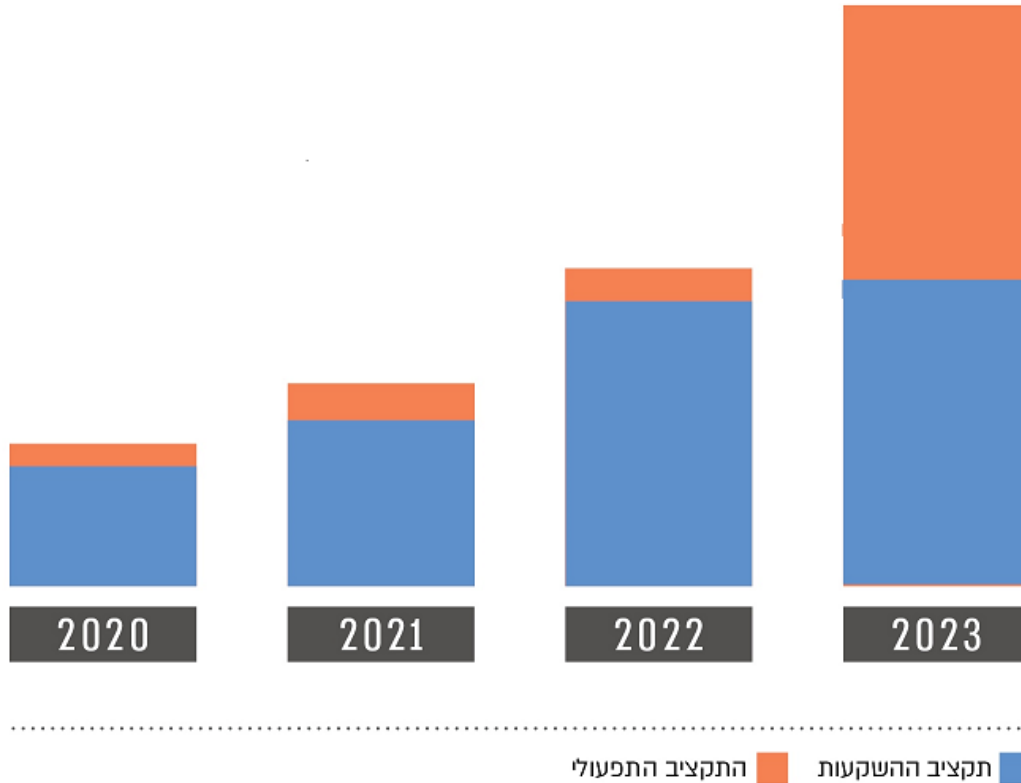
על פי נתוני רפאל, בעיבוד משרד מבקר המדינה.

נמצא כי בשנים 2020 - 2023 גדל תקציב מחלקת אבטחת טכנולוגיות והגנת סייבר פי כארבעה, וכי שיעורו של תקציב המחלקה מתוך תקציב מטכ"ם גדל פי כ-2.7 מ-5.7% ל-15.2%. יצוין כי בשנים 2020 - 2022 ניצלה מטכ"ם כ-99% מהתקציב ואילו שיעור ניצול תקציב מחלקת אבטחת טכנולוגיות והגנת סייבר היה 108%.

להלן בתרשים נתונים על תקציב מחלקת אבטחת טכנולוגיות והגנת סייבר בשנים 2020 - 2023, בחלוקה לתקציב התפעולי ולתקציב ההשקעות בצידוד, במבנים, במערכות ובשילוב טכנולוגיות חדשות להגנה בסייבר.



תרשים 3 : מגמת הגידול של תקציב מחלקת אבטחת טכנולוגיות והגנת סייבר בשנים 2020 - 2023, לנושאי מחשוב, בחלוקה לתקציב התפעולי ולתקציב ההשקעות



על פי נתוני רפאל, בעיבוד משרד מבקר המדינה.

נמצא כי בשנים 2020 - 2023 גדל תקציב ההשקעות של מחלקת אבטחת טכנולוגיות והגנת סייבר פי 2.6, וכי בשנת 2023 גדל התקציב התפעולי של המחלקה פי תשע לעומת שנת 2022. ממשמכי רפאל עולה כי עיקר הגידול בתקציב ההשקעות בשנים 2020 - 2023 נבע משילוב טכנולוגיות חדשות למתן מענה לאיומים שונים.

בתגובה על ממצאי הביקורת מאוקטובר 2023 מסרה רפאל כי במסגרת הכנת התקציב השנתי שלה היא שוקלת שיקולים רבים, לרבות פוטנציאל הנזק בגין אירועי סייבר, וכי היא הגדילה את תקציב ההגנת הסייבר בהתאם.

מומלץ כי הנהלת רפאל תמשיך לבחון מדי שנה בשנה את גודל התקציב הנדרש להגנת הסייבר בהתייחס לפוטנציאל הנזק, למחזור המכירות השנתי ולרווח התפעולי השנתי שלה.

פערי דיווח ברפאל

בביקורת עלה כי רפאל לא דיווחה לדירקטוריון בישיבותיו על כמה אירועי סייבר כנדרש.

על הנהלת רפאל לדווח לדירקטוריון כנדרש לגבי אירועי סייבר.

בביקורת עלה כי חטיבת תורה והגנה (תוה"ג) במלמ"ב לא פרסמה לגופים המונחים, הנחיה לגבי ההיערכות הנדרשת לניהול אירוע סייבר ולגבי ניהול האירוע עצמו, הנוגעת לנושאים, כגון תהליכי ניטור, זיהוי אירוע סייבר, תגובה עליו, התאוששות ממנו, תחקורו, הפקת לקחים ממנו,



תרגול אירועי סייבר, הגורמים הפנימיים המשתתפים בניהול אירוע סייבר והממשקים ביניהם, והפעילויות הנדרשות של הגוף המונחה מול גורמים חיצוניים. מומלץ כי חטיבת תורה והגנה (תוה"ג) במלמ"ב תפרסם לגופים המונחים הנחיה לגבי היערכות הנדרשת לניהול אירוע סייבר והנחיה לגבי ניהול אירוע כזה.

תחקור אירועי סייבר: בביקורת עלה כי הנהלת רפאל לא תחקרה את ניהול אירועי הסייבר שהתרחשו בשנים 2020 - 2022 בהיבטים מסוימים הנוגעים לתפקוד הנדרש של רפאל.

על הנהלת רפאל לתחקר את ניהול אירועי הסייבר בהתאם לנדרש.

תוכנית מפורטת לניהול אירועי אבטחת מידע: בביקורת עלה כי הוראת מטכ"ם מפברואר 2023 אינה מפרטת את תהליך ההתאוששות מאירוע סייבר מסוים או מפנה לתוכנית מסוימת ואינה כוללת הפניות למסמכים מסוימים.

על רפאל להשלים את ההוראה בנושא ניהול אירועי אבטחת טכנולוגיות והגנת סייבר במערכות המחשב, כנדרש.

הפקת לקחים מאירועי סייבר מסוימים

בביקורת עלה כי בכל הנוגע לביצוע תהליך הפקת לקחים, כמה מסמכי תחקור אירועים לא התייחסו להפקת הלקחים הנדרשים.

מומלץ כי במסגרת תהליך הפקת לקחים מאירועי סייבר תכלול רפאל המלצות להגברת מודעות העובדים להתקפות סייבר מסוג מסוים.

סקרים ומבדקי חדירה

בביקורת עלה כי רפאל לא קבעה את התדירות לביצוע סקרים ומבדקי חדירה הנדרשים. כמו כן, עלו פערים בתחום זה.

על רפאל לקבוע את תדירות ביצוע הסקרים ומבדקי החדירה. אי-ביצוע הסקרים בתדירות שקבע מלמ"ב עלול לחשוף את מערכות המידע לאיומי סייבר.

עוד מומלץ כי רפאל תפעל לתיקון הפערים.

סיכום

רפאל מערכות לחימה מתקדמות בע"מ היא חברה ממשלתית-ביטחונית המתמחה בפיתוח ובייצור של אמצעי לחימה ומערכות חימוש והגנה למרחבי האוויר, היבשה, הים והסייבר עבור צה"ל ולקוחות זרים, והיא מרכיב משמעותי בבניית עוצמתה הצבאית וחוסנה של המדינה. חדשנות ופיתוח טכנולוגי הביאו עימם יתרונות רבים לאדם ולסביבתו. זאת לצד התגברות איום הסייבר וסיכונים נוספים. מלמ"ב ורפאל נושאים באחריות להיערך ככל הנדרש כדי למנוע חשיפה, שיבוש ופגיעה במידע ובמערכות המחשוב של רפאל עקב מתקפות סייבר.

בביקורת עלו ליקויים הנוגעים בין היתר לאי-הסדרת יחסי העבודה בין מס"ל למלמ"ב ולהגנה על המידע ומערכות המחשוב ברפאל. כך, לא הושלמה ההוראה בנושא הטיפול באירועי סייבר. כמו כן, עלו ליקויים נוספים בהיבטים מסוימים.



הליקויים שעלו בביקורת עלולים להגביר את הסיכון לאירוע סייבר. על הנהלת רפאל ודירקטוריון רפאל לפעול לתיקון הליקויים ולוודא בשיתוף מלמ"ב כי רפאל מיישמת את הנחיות מלמ"ב כנדרש. כמו כן, על מס"ל, והגופים המיוחדים, לרבות מלמ"ב, להסדיר את יחסי העבודה ביניהם כנדרש.



משרד מבקר המדינה
ונציב תלונות הציבור

