דוח מבקר המדינה - סייבר ומערכות מידע |
חשוון התשפ"ד | נובמבר 2024

תעשיות ביטחוניות ממשלתיות

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

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

רקע

בהחלטת הממשלה מאוגוסט 2011[1] נקבע כי מרחב הסייבר האזרחי הישראלי כולל את כלל הגורמים הממלכתיים והפרטיים במדינת ישראל, למעט הגופים המיוחדים[2]. דהיינו, מרחב הסייבר הישראלי כולל את המרחב האזרחי, הממשלתי והביטחוני. הפעילות הגוברת במרחב הרשתי מאפשרת חדשנות טכנולוגית ופיתוחים לאדם ולסביבתו. ואולם לצד היתרונות שמאפשרות מערכות ממוחשבות במרחב הרשתי, הן יצרו גם איום חדש ההולך ומתעצם: איום הסייבר. אירוע סייבר הוא התרחשות אשר מעידה על פגיעה אפשרית בפעילותה התקינה של מערכת מחשוב. רפאל מערכות לחימה מתקדמות בע"מ (רפאל) היא מרכיב משמעותי בבניית עוצמתה הצבאית וחוסנה של המדינה. החברה כפופה בין היתר להוראות חוק החברות הממשלתיות, התשל"ה-1975, והחוק להסדרת הבטחון בגופים ציבוריים, התשנ"ח-1998 (החוק להסדרת הביטחון). הממונה על הביטחון במערכת הביטחון (מלמ"ב) מנחה את מפעלי מערכת הביטחון ומפעלים המייצרים מוצרים עבור מערכת הביטחון[3]. רשות החברות הממשלתיות מפיצה חוזרים לחברות הממשלתיות ולחברות בנות ממשלתיות בנושאים שונים בהתאם לסמכותה בחוק החברות הממשלתיות, התשל"ה-1975, ובכלל זה לגבי ניהול הסיכונים התאגידי.

בשנת 2022 דווחו למערך הסייבר הלאומי (מס"ל) על ידי כלל הגורמים במדינה 9,108 אירועי סייבר. כ-31% מהם נבעו ממתקפות דיוג[4].

1 החלטת הממשלה 3611 (7.8.11).

2 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 הביטחון בגופים ציבוריים, התשנ"ח-1988, וכן ספקים ומפעלים המפתחים או המייצרים ציוד ביטחוני עבורם.

3 מערכת הביטחון - צה"ל ומשרד הביטחון (משהב"ט), לרבות יחידות הסמך שלו.

4 phishing - מתקפת סייבר שבה התוקף מתחזה לגורם אמין כדי להונות אנשים ולגרום להם לחשוף מידע רגיש.

נתוני מפתח

10%

בשנת 2022: התקציב של מחלקת אבטחת טכנולוגיות והגנה בסייבר ברפאל מתוך התקציב בנושא מחשוב של מינהל טכנולוגיות מידע ותהליכים ברפאל

12 שנים

לא יישמו מס"ל ומלמ"ב את החלטת הממשלה בנושא קידום היכולת הלאומית במרחב הקיברנטי, בכל הנוגע לקביעת הסדרים מיוחדים לקידום ההגנה במרחב הסייבר

31%

שיעור אירועי הסייבר מסוג דיוג שדווחו למערך הסייבר הלאומי (מס"ל) בשנת 2022 מתוך כלל אירועי הסייבר

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 ובקרות על אבטחת המידע המיושמות בהן; ומיגון תשתיות מסוימות ברפאל. הביקורת נערכה במלמ"ב וברפאל. בדיקות השלמה נערכו בתעשייה האווירית לישראל בע"מ (התע"א), בחברת החשמל לישראל בע"מ 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].

תמונת המצב העולה מן הביקורת

- **הסדרת יחסי העבודה בין מס"ל למלמ"ב -** 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.

- **סמכויות ההנחיה והפיקוח של מלמ"ב -** 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.

- **תפיסת ההגנה בסייבר במלמ"ב -** 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 תוה"ג 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.

- **ניהול הסיכונים הארגוני ברפאל -** 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 לניהול סיכונים. ואולם הנהלת רפאל לא העלתה לאישור הדירקטוריון את האסטרטגיה והמדיניות האמורות, והדירקטוריון לא אישר אותן. נכון ליולי 2023 מדיניות ניהול הסיכונים לא כללה התייחסות למנגנוני דיווח לגורמים חיצוניים לרפאל. כמו כן 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 -** עלו פערים בתחום זה.

- **ביטוח מפני אירועי סייבר -** ביולי 2023, בעת הביקורת, לחברת החשמל לישראל בע"מ היו שתי פוליסות ביטוח המכסות נזקים לרכוש ותביעות צד ג' בגין אירועי סייבר, ואילו לתעשייה האווירית לישראל בע"מ (התע"א) ולרפאל[5] לא היו פוליסות ביטוח כאמור. רפאל לא רכשה ביטוח מפני אירועי סייבר בעיקר מהסיבות שלהלן: רמת ההגנה על 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

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

לרכוש ביטוח המכסה נזק של עד עשרה מיליוני דולרים בלבד, סכום שאינו מהותי לפעילותה של רפאל.

- **פערי דיווח ברפאל -** רפאל לא דיווחה לדירקטוריון בישיבותיו על כמה אירועי סייבר כנדרש.
- **תחקור אירועי סייבר -** הנהלת רפאל לא תחקרה את ניהול אירועי הסייבר שהתרחשו בשנים 2020 - 2022 בהיבטים מסוימים הנוגעים לתפקוד הנדרש של רפאל.
- **תוכנית מפורטת לניהול אירועי אבטחת מידע -** הוראת מטכ"ם מפברואר 2023 אינה מפרטת את תהליך ההתאוששות מאירוע סייבר מסוים או מפנה לתוכנית מסוימת ואינה כוללת הפניות למסמכים מסוימים.
- **הפקת לקחים מאירועי סייבר מסוימים -** כמה מסמכי תחקור אירועים לא התייחסו להפקת הלקחים הנדרשים.
- **סקרים ומבדקי חדירה -** רפאל לא קבעה את התדירות לביצוע סקרים ומבדקי חדירה הנדרשים. כמו כן, עלו פערים בתחום זה.

עיקרי המלצות הביקורת

- על מס"ל ומלמ"ב לקיים את החלטות הממשלה בכל הנוגע להסדרת שיתוף הפעולה ביניהם באמצעות המנגנונים שנקבעו בהחלטות.
- מומלץ כי מלמ"ב יפעל להסדיר ככל הנדרש את הסמכויות הנדרשות לצורך מימוש ייעודו.
- 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 ולניהול האירועים, תחקורם והפקת הלקחים בנושא.
- על הנהלת רפאל לדווח לדירקטוריון כנדרש לגבי אירועי סייבר.
- 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.
- על הנהלת רפאל לתחקר את ניהול אירועי הסייבר בהתאם לנדרש. על רפאל להשלים את ההוראה בנושא ניהול אירועי אבטחת טכנולוגיות והגנת סייבר במערכות המחשב כנדרש.
- מומלץ כי רפאל תפעל לתיקון הפערים שעלו בתחום הסקרים ומבדקי החדירה.
- על רפאל לפעול לתיקון הליקויים שעלו בדוח זה.

סיכום

רפאל היא מרכיב משמעותי בבניית עוצמתה הצבאית וחוסנה של המדינה. בביקורת עלו ליקויים הנוגעים בין היתר לאי-הסדרת יחסי העבודה בין מערך הסייבר הלאומי (מס"ל) למלמ"ב ולהגנה על המידע ומערכות המחשוב ברפאל. על הנהלת רפאל ודירקטוריון רפאל לפעול לתיקון הליקויים ולוודא בשיתוף מלמ"ב כי רפאל מיישמת את הנחיות מלמ"ב כנדרש.