

דוח מבקר המדינה | אדר ב' התשפ"ב | מרץ 2022



תחום הגנת הסייבר

הגנת הסייבר בחברת החשמל לישראל בע"מ



הגנת הסייבר בחברת החשמל לישראל בע"מ

רקע

מרחב הסייבר כולל מחשבים, מערכות ממוכנות ורשתות, תוכנות, מידע ממוחשב, תוכן דיגיטלי, נתוני תעבורה ובקרה. תקיפת סייבר היא רצף הפעולות שמבצע יריב במרחב הסייבר. איומי הסייבר הולכים ומתעצמים עם צמיחתו של מרחב הסייבר, ועלולים להוביל לפגיעה הן בתוך המרחב והן בעולם הפיזי, כגון בתחנות כוח ובפסי ייצור. פגיעות אלה עלולות לגרום לפגיעה כלכלית ואף לפגיעות בגוף ובנפש. בשנים האחרונות מסתמנת עלייה הדרגתית ברמת האיום האמור, במספר האירועים המתרחשים בפועל ובחומרתם, בארץ ובעולם. חברת החשמל לישראל בע"מ (חח"י) מייצרת, מוליכה ומספקת חשמל. החברה מפקדת על כמה מהתשתיות הקריטיות ביותר במדינה. פגיעה במערך התקשוב התומך בתהליכי הייצור, ההשנאה, ההולכה והחלוקה עלולה להשבית תהליכים אלה ולמנוע אספקת חשמל סדירה לפרקי זמן העלולים להיות קריטיים למשק, בייחוד בעיתות חירום.

נתוני מפתח

100

מיליון דולר

גבול כיסוי ביטוח מפני נזקי סייבר של החברה בשנת 2021, בהשתתפות עצמית של מיליוני דולר

527 מיליון ש"ח

ביצוע תקציב IT בחברת החשמל בשנת 2019. בשנת 2018 ביצוע התקציב הסתכם ב-521 מיליון ש"ח

19%

צמצום במצבת העובדים בחטיבת התקשוב בשנים 2015 - 2019



פעולות הביקורת

בחדושים מאי עד דצמבר 2020 בדק משרד מבקר המדינה את הגנת הסייבר בחח"י ואת הפעולות שנקטו חח"י ומערך הסייבר הלאומי (מס"ל) לצורך שיפור הגנת הסייבר על תהליכים ומערכות קריטיים בחברת החשמל. הבדיקות נעשו בחח"י, במס"ל ובמשרד האנרגיה. 🔍

הדוח שבנדון הומצא לראש הממשלה ולעדה לענייני ביקורת המדינה של הכנסת ביום 29/07/2021 והוטל עליו חיסיון עד לדיון בוועדת המשנה של הוועדה לענייני ביקורת המדינה.

מתוקף הסמכות הנתונה למשרד מבקר המדינה בסעיף 17(ג) לחוק מבקר המדינה, התש"ח 1958 [נוסח משולב] ובשים לב לנימוקי הממשלה, לאחר היועצות עם הגופים האמונים על אבטחת המידע הביטחוני ובתיאום עם יו"ר הכנסת, משלא התכנסה ועדת המשנה האמורה, 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 סיום הביקורת האמור לעיל.

תמונת המצב העולה מן הביקורת



אחידות בגורם המנחה ובהנחיה במשק האנרגיה - נמצא כי בהתאם לחלוקת העבודה בין מס"ל למשרד האנרגיה, תחנות כוח שהיו בידי חברת החשמל ונמכרו לגורמים פרטיים הועברו מהנחיית מס"ל להנחיה של משרד האנרגיה, על פי הרגולציה שקבע משרד האנרגיה (שמונחה מקצועית בידי מס"ל). בהשוואה בין הנחיית מס"ל, המנחה את חח"י לבין הנחיות משרד האנרגיה המנחות את הגורמים הפרטיים עלו מספר הבדלים.

הפיקוח והמעקב של מס"ל על ביצוע ההנחיות הניתנות לחברת החשמל - נמצא כי מס"ל לא הסדיר בכללים את האופן שבו חח"י צריכה לדווח לו כדי שיוכל לעקוב אחר ביצוע הנחיותיו ואחר תיקון הליקויים שמצא. נמצא כי מס"ל לא ביצע מעקב ופיקוח מלא בעניין ביצוע כל ההנחיות שנתן, בידי חברת החשמל. בעניין חלק מההנחיות שמס"ל העביר לצוות הביקורת במשרד מבקר המדינה, מס"ל מסר כי לא התקבל מידע על סטטוס ההנחיה בכתב או בעל-פה.

הכנת תוכניות עבודה רב-שנתיות ושנתיות ליישום הנחיות מס"ל (להלן - תוכניות הטמעה) - במועד סיום הביקורת חח"י טרם הגישה תוכנית רב-שנתית. עוד נמצא כי במועד סיום הביקורת תוכניות העבודה השנתיות שחח"י הציגה לשנים 2019 - 2021 אינן כוללות את מלוא הפירוט לגבי אופן יישומן.



ביצוע סקרי סיכונים ומבדקי חדירה - ממסמכי חברת חשמל עולה כי ביולי 2019 היא לא גיבשה תוכנית עבודה רב-שנתית או שנתי לביצוע סקרי סיכונים ומבדקי חדירה. בפועל, עלו פערים בביצוע סקרי סיכונים ומבדקי חדירה. עם זאת, במאי 2020 הכינה חח"י תוכנית עבודה תלת-שנתית לביצוע סקרי סיכונים ומבדקי חדירה.

היפרדות יחידת ניהול המערכת מחברת החשמל במסגרת הרפורמה - במועד סיום הביקורת חח"י לא השלימה תוכנית להפרדת יחידת ניהול המערכת מחח"י בהיבטי סייבר, ולא הגישה למס"ל תוכנית כאמור, וזאת אף שבמועד סיום הביקורת יחידת ניהול המערכת הייתה אמורה לעבור לחברת ניהול המערכת בתחילת יוני 2021.



הקמת מרכז קיברנטי (להלן - המק"ם) - משרד האנרגיה הקים את המרכז הקיברנטי המגזרי (המק"ם), המנטר את כלל תשתיות האנרגיה, מתכלל מידע המתקבל מהן ומשקף תמונת מצב בנושא הגנת סייבר על משק האנרגיה.

בדוח זה נבדקו נושאים נוספים כגון רמת החוסן, מדיניות אבטחה פנים-ארגונית, תוכניות עבודה והטמעה רב-שנתיות ושנתיות, בקורות בהגנת סייבר ובאבטחת מידע והמצאים שוקפו לגורמים הרלבנטיים.

עיקרי המלצות הביקורת

מומלץ כי מס"ל כמאסדר יפעל לאסדרה של סדרי הדיווח והבקרה שלו על חברת החשמל. בכלל זה, מומלץ לקבוע הוראות בדבר הדיווח בכתב שחח"י צריכה למסור לו בעניין אופן ביצוע הנחיותיו, בעניין תיקון ליקויים שנמצאו על ידו או על ידי גורמים אחרים בביקורות חיצוניות או פנימיות, ומהם ההסברים הנדרשים בדיווח. כמו כן, מומלץ כי מס"ל יקבע את המועדים הנדרשים למסירת דיווחים בכתב כאמור, לרבות דיווחים עיתיים ומידיים, ואת הפרטים שחח"י נדרשת למסור בדיווחיה. עוד מומלץ כי מס"ל יפעל לקבל מחח"י מידע באופן סדור לגבי יישום כלל הנחיותיו מהשנים שחלפו וכי מס"ל יבחן הקמת מערך דיווחים ובקורות מקוון לחח"י ולכלל הגופים המונחים על ידו.

מומלץ שהחברה תכין תוכנית עבודה רב-שנתית מפורטת יותר בתחום הסייבר בהתאם להוראת העבודה בנושא, הכוללת את מלוא הפירוט הנדרש. כמו כן, מומלץ שהחברה תכין תוכניות שנתיים מפורטות כאמור.



סיכום

חברת החשמל מופקדת על תשתית לאומית קריטית. פגיעה בשרשרת החשמל עלולה לגרום נזק למשק בכללותו. בדוח נמצאו ליקויים בהגנת הסייבר של חברת החשמל. דוח זה הציג תמונת מצב בנושא הגנת סייבר בחברת חשמל ובפיקוח של של מס"ל על חברת חשמל. בין היתר נמצאו ליקויים במעקב של מס"ל אחר יישום הנחיותיו.



הגנת הסייבר בחברת החשמל לישראל בע"מ

מבוא

מרחב הסייבר הוא המרחב הפיזי והקיברנטי, הכולל מחשבים, מערכות ממוכנות ורשתות, תוכנות, מידע ממוחשב, תוכן דיגיטלי, נתוני תעבורה ובקרה¹. מרחב הסייבר האזרחי בישראל הוא תת מרחב בתוך מרחב הסייבר הישראלי, הכולל² את "כלל הגורמים הממלכתיים והפרטיים במדינת ישראל, למעט הגופים המיוחדים"³

תקיפת סייבר היא רצף הפעולות (חד-פעמי או מתמשך) שמבצע יריב במרחב הסייבר לתכלית קונקרטית - כגון חבלה, איסוף מידע או השפעה תודעתית.

איומי הסייבר הולכים ומתעצמים עם צמיחתו של מרחב הסייבר, הגברת התלות בו ועומק החיבור בינו לבין המרחב הפיזי. איומים אלה עלולים להוביל הן לפגיעה בתוך המרחב (במידע או בתפקוד) והן לפגיעה בעולם הפיזי, כגון: פגיעה במכשור רפואי, במתקני התפלה, בתחנות כוח ובפסי ייצור. פגיעות אלה יכולות לגרום לפגיעה כלכלית ניכרת ואף לפגיעות בגוף ובנפש. בשנים האחרונות מסתמנת עלייה הדרגתית ברמת האיום, במספר האירועים בפועל ובחומרתם, בארץ ובעולם. כך למשל בשנת 2018 היו כ-813 מיליון התקפות סייבר בעולם לעומת כ-309 מיליון בשנת 2014⁴.

בעשור האחרון קיבלה ממשלת ישראל כמה החלטות ממשלה שמטרתן קידום היכולת הלאומית במרחב הסייבר, לצורך שיפור ההתמודדות עם אתגרים אלו⁵.

החוק להסדרת הביטחון בגופים ציבוריים, התשנ"ח-1998 (להלן - החוק להסדרת הביטחון), מסמיר, בין היתר, את מערך הסייבר הלאומי (להלן - מס"ל)⁶ להנחות מהבחינה המקצועית

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

2 מתוך החלטת הממשלה 3611 (7.8.11).

3 בהחלטת הממשלה 3611 (7.8.11), "קידום היכולת הלאומית במרחב הקיברנטי", הוגדרו גופים אלה: "צבא ההגנה לישראל, משטרת ישראל, שירות הביטחון הכללי, המוסד למודיעין ולתפקידים מיוחדים ומערכת הביטחון באמצעות המלמ"ב".

4 www.purplesec.us/resources/cyber-security-ststistics

5 משרד מבקר המדינה, **דוח היערכות גופים חיוניים להגנת הסייבר**, (2019) **דוח שנתי 69**, עמוד 2065.

6 הרשות הלאומית להגנת הסייבר, בעת שפעלה כיחידת סמך עצמאית למשרד ראש הממשלה הוסמכה להיות אחראית לחח"י בעקבות תיקון חקיקה משנת 2016, שבהתאם להחלטת ועדת החוץ והביטחון של הכנסת נקבע כהוראת שעה. ראו: חוק להסדרת הביטחון בגופים ציבוריים (הוראת שעה), התשע"ו - 2016, ס"ח 2579 מאגוסט 2016. צו שהוציא ראש הממשלה מכוח סמכותו על פי התיקון האמור העביר את האחריות מהשב"כ לרשות הלאומית להגנת סייבר החל מ-2017. ראו: צו להסדרת הביטחון בגופים ציבוריים (הוראת שעה) (קצין מוסמך לעניין גוף המנוי בתוספת החמישית לחוק), התשע"ז - 2016. בינתיים הרשות הלאומית להגנת הסייבר אוחדה עם מטה הסייבר הלאומי ליחידת סמך אחת למשרד ראש הממשלה - היא מערך הסייבר הלאומי, ובדצמבר 2018 התקבל תיקון נוסף לחוק לפיו הוראת הפכה להוראת קבע וסמכויות הרשות הלאומית להגנת הסייבר הועברו למערך הסייבר הלאומי תוך הרחבתו.



גופים ציבוריים מסוימים⁷, בהם חברת החשמל לישראל בע"מ (להלן - חח"י, חברת החשמל או החברה), בתחום אבטחת מערכות ממוחשבות חיוניות⁸.

מס"ל משמש גוף מטה במשרד ראש הממשלה, שבין היתר ממליץ על מדיניות לאומית ומקדם את יישומה בתחום הסייבר. מס"ל מנהל, מפעיל ומבצע בהתאם לצורך את כלל מאמצי ההגנה האופרטיביים במישור הלאומי במרחב הסייבר, ובכלל זה מטפל באיומי סייבר ובאירועי סייבר בזמן אמת, מגבש תמונת מצב שוטפת, מרכז מחקר מודיעין ועובד עם הגופים המיוחדים. מס"ל מפעיל מרכז לסיוע בהתמודדות עם איומי סייבר עבור כלל המשק. מס"ל אמון על הנחיית גופים שנקבעו בחוק או על פיו, ובהם חברת החשמל, וכן על הנחיית גופים נוספים במשק בהתאם להחלטות ממשלה, בכפוף להסכמתם.

אחד התרחישים הקיצוניים ביותר של מתקפת סייבר על המשק האזרחי הוא תקיפת תשתיות האנרגיה.

חברת החשמל מייצרת, מוליכה ומספקת חשמל. החברה מופקדת על כמה מהתשתיות החיוניות במדינה, ולפיכך כל פגיעה מהותית בתפקוד חברת החשמל עלולה לגרום לפגיעה בתפקוד המדינה. פגיעה במערך התקשוב התומך בתהליכי הייצור, ההשנאה, ההולכה והחלוקה עלול להשבית לחלוטין תהליכים אלה במישור המקומי, האזורי ואף הארצי ולמנוע אספקת חשמל סדירה לפרקי זמן העלולים להיות קריטיים למשק, בייחוד בעיתות חירום. חברת החשמל מופקדת על כמה מתשתיות מדינה קריטיות (להלן - תמ"ק), הכוללות מערכות ממוחשבות אשר פגיעה בזמינותן, באמינותן, בשלמותן או הפעלתן שלא בהתאם ליעודן עלולות לגרום נזק לתהליך קריטי⁹.

בחברת החשמל פועלות החטיבות האלה: חטיבת הייצור והאנרגיה, חטיבת שירותי רשת, חטיבת פרויקטים הנדסיים, חטיבת התפעול והלוגיסטיקה, חטיבת כספים וכלכלה, חטיבת משאבי אנוש וחטיבת התקשוב. הפעילות של כל החטיבות מבוססת על מערכות מידע שחטיבת התקשוב נותנת להן שירות.

פגיעה בתשתיות משקיות עלולה לגרום להיווצרות גלי נזק בעלי השפעות חמורות ביותר במישור הלאומי. יצוין כי ההנחה הרווחת היא כי מתקפת סייבר על תשתיות אנרגיה במישור המשקי דורשת, ככלל, רמת תחכום גבוהה בשל המורכבות הטכנית של תקיפת בקרים תעשייתיים בשרשרת הייצור האנרגטית¹⁰.

7 "גוף ציבורי" הוגדר בחוק: "כל גוף המנוי בתוספות, ולגבי משרד ממשלתי המנוי בתוספות - לרבות יחידות הסמך שלו".

8 "פעולות לאבטחת מערכות ממוחשבות חיוניות" הוגדרו בחוק: "פעולות הדרושות לשם שמירה על מערכות ממוחשבות, שגוף שהסמיכה הממשלה קבע שהן מערכות ממוחשבות חיוניות, על מידע האגור במערכות אלה ועל מידע מסוג הקשור למערכות אלה, וכן פעולות למניעת פגיעה במערכות או במידע כאמור".

9 תהליך עסקי מרכזי, שהוא תהליך קריטי, הוא סדרת פעילויות המבוצעות על ידי מספר גורמים בארגון (אנשים, מערכות ממוחשבות) על מנת לממש את ייעודו העסקי של הגוף, אשר פגיעה קיברנטית מולו היא בעלת פוטנציאל נזק ברמה המדינית.

10 על פי מסמך נלווה "הערכת השפעות רגולציה", שצורף לתזכיר חוק הגנת הסייבר מיוני 2018.



מחקר משנת 2015¹¹ העריך כי מתקפה נגד אחת ממפעילות רשת החשמל האמריקנית תעלה למשק האמריקני 243 מיליארד דולר בתרחיש ביניים וטריליון דולר בתרחיש קיצון. מחקרים אחרים¹² העריכו את הנזק הישיר הנגרם במישור הלאומי למדינות מערביות בעקבות תקיפות רשת ה-IT¹³ בשיעור של עד 1.6% מהתוצר המקומי הגולמי בשנה. כמו כן, מחקרים העריכו בשנת 2014 את הנזקים הישירים לכל אחת מהחברות בצרפת ובגרמניה בטווח שבין חצי מיליון ל-20 מיליון אירו בשנה.

11 LLOYD's, The insurance implications of a cyber attack on the US power grid, Emerging Risk Report, 2015

12 Enisa, The cost of incidents affecting CIIs, August 2016

13 רשת טכנולוגיית מידע - IT - Information Technology, שהיא טכנולוגיות מחשוב ותקשורת לשם עיבוד וניהול של מידע.



בתרשים 1 להלן מוצגת סקירה של מספר התקפות הסייבר והניסיונות לתקיפות בארץ ובעולם.

תרשים 1: דוגמאות לאירועי סייבר ידועים במתקני תשתית בארץ ובעולם בשנים 2012 - 2020



מנתוני אתר האינטרנט <https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents>

מנתוני חברת החשמל עולה כי בשנת 2014 מספר הניסיונות לתקיפת סייבר¹⁴ של מערכות החברה ברוב חודשי השנה היה 183,000 - 293,000 ביום, וכי בחודשים אוגוסט-ספטמבר חל גידול ניכר במספר ניסיונות תקיפות הסייבר, ומספרן זינק לכ-865,000 בממוצע ביום (ממוצע של

14 תקיפת סייבר היא רצף הפעולות (חד-פעמי או מתמשך) שמבצע יריב במרחב הסייבר לתכלית קונקרטית - כגון חבלה, איסוף מידע או השפעה תודעתית.



כ-36,000 ניסיונות בשעה). עוד עולה מנתוני החברה, כי מספר ניסיונות התקיפה האמיר במידה ניכרת בשנים האחרונות.

פעולות הביקורת

בחודשים מאי-דצמבר 2020 בדק משרד מבקר המדינה את אופן ההיערכות של ח"י להגנת הסייבר בחח"י ואת הפעולות שנקטו חח"י ומס"ל לשיפור הגנת הסייבר על תהליכים ומערכות בחברת החשמל. הבדיקות נעשו בחח"י, במס"ל ובמשרד האנרגיה. בדיקת השלמה בוצעה ברשות החשמל.

הדוח שבנדון הומצא לראש הממשלה ולעדה לענייני ביקורת המדינה של הכנסת ביום 29/07/2021 והוטל עליו חיסיון עד לדיון בוועדת המשנה של הוועדה לענייני ביקורת המדינה.

מתוקף הסמכות הנתונה למשרד מבקר המדינה בסעיף 17(ג) לחוק מבקר המדינה, התשי"ח 1958 [נוסח משולב] ובשים לב לנימוקי הממשלה, לאחר היועצות עם הגופים האמונים על אבטחת המידע הביטחוני ובתיאום עם יו"ר הכנסת, משלא התכנסה ועדת המשנה האמורה, 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 סיום הביקורת האמור לעיל.

מערך המידע והתקשוב בחח"י

מערך המידע והתקשוב בחברה כולל מערכות מידע תפעוליות ייעודיות לניהול שרשרת החשמל (דוגמת מערכת פיקוד ובקרה על מערכת ייצור החשמל), וכן מערכות מידע ניהוליות, לרבות תשתיות התקשורת הארגוניות אשר מנוהלות בחטיבת תקשוב.

חטיבת התקשוב (להלן - החטיבה) עוסקת באפיון, בפיתוח וביישום של מערכות מידע ופתרונות התומכים בתהליכים עסקיים, תפעוליים ומינהליים בחברה. החטיבה פועלת על פי תוכנית תלת-שנתית, אשר בהתבסס עליה נקבעות תוכניות העבודה השנתיות של החטיבה. במסגרת התוכנית הרב-שנתית הוגדרו המהלכים העיקריים של החטיבה בתחומים הבאים: הכשרה ומודעות בנושא אבטחת מידע וסייבר - גיוס והכשרה של עובדים, הגברת המודעות של עובדים לנושא אבטחת מידע וסייבר, ביצוע הסמכות ברשת ה-IT, יישום תקנות הגנת הפרטיות, הקמה, תרגול ותפעול של מערך התגובה לסייבר, ליווי של אבטחת מידע וסייבר במסגרת פרויקטים אסטרטגיים, שיפור והקשחה¹⁵ של תשתיות אבטחת מידע, רשתות ומערכי ניהול, העמקת ניטור של רשתות תקשוב קריטיות במרכז הסייבר הארצי (על מרכז הסייבר הארצי ראו להלן בהמשך פרק זה).

15 הקשחה כוללת ביצוע שינויים בפרמטרים של הפעלה או קונפיגורציה של מערכת המחשוב, אשר מטרתה היא לצמצם את משטח התקיפה במרחב הסייבר. המשטח האמור מייצג את כלל הממשקים שבאמצעותם יריב פוטנציאלי עשוי לבצע תהליך של התערבות לא רצויה במערכת המחשוב, למשל הזנת קלט זדוני.



בשנים 2019 - 2020 חטיבת התקשוב מיפתה את כל מערכות המידע שבחברה, והעלתה כי בחברה יש מערכות מידע רבות, מתוכן מספר מערכות מידע הוגדרו ע"י החברה כקריטיות ביותר. סביבת מערכות המידע של החברה כוללת תחנות עבודה רבות לשימוש המשתמשים ברשת המינהלית של הארגון, מחשבים פיזיים רבים וכן שולחנות עבודה וירטואליים¹⁶.

בשנת 2020 בוצע שינוי במבנה הארגוני של חטיבת התקשוב. חח"י מסרה למשרד מבקר המדינה בפברואר 2021 כי השינוי המבני בחטיבת התקשוב נועד לתמוך בשינויים הארגוניים שחלו בחברה בעקבות הרפורמה ובשינויים במשק האנרגיה.

בחברה פועלים כמה גופים בתחום אבטחת מידע וסייבר: מטה סייבר, מחלקת אבטחת מידע וסייבר, מחלקת תקשורת ואבטחת מידע.

נמצא כי בחברה קיימים מספר גופים האמונים על תחום הסייבר בכפיפויות שונות, חלקם כפופים ישירות לסמנכ"ל תקשוב וחלקם כפופים ישירות למנהל אגף מערכות מידע. בביקורת נמצא ליקוי במבנה הארגוני שעלול ליצור לעיתים קונפליקט במשקל הניתן לשיקולים השונים.

משרד מבקר המדינה ממליץ שחח"י תשקול, במסגרת השינוי הארגוני המתבצע בשנים האחרונות בחטיבת התקשוב, לבצע שינויים במטרה למנוע קונפליקט פוטנציאלי כאמור.

חח"י השיבה למשרד מבקר המדינה במאי 2021 (להלן - תשובת חח"י) כי "נושא זה נמצא בטיפול בראשותו של סמנכ"ל תקשוב, הנושא גם דווח למנכ"ל בוועדת היגוי עליונה. הנושא ייסגר במהלך שנה זו, 2021".

מצבת העובדים בחטיבת התקשוב

בשנים 2015 - 2019 צומצמה מצבת העובדים של חטיבת התקשוב בשיעור העולה על הצמצום במצבת העובדים הכללית של החברה באותן שנים שצומצמה מ-12,371 ל-11,391 (צמצום של כ-8%).

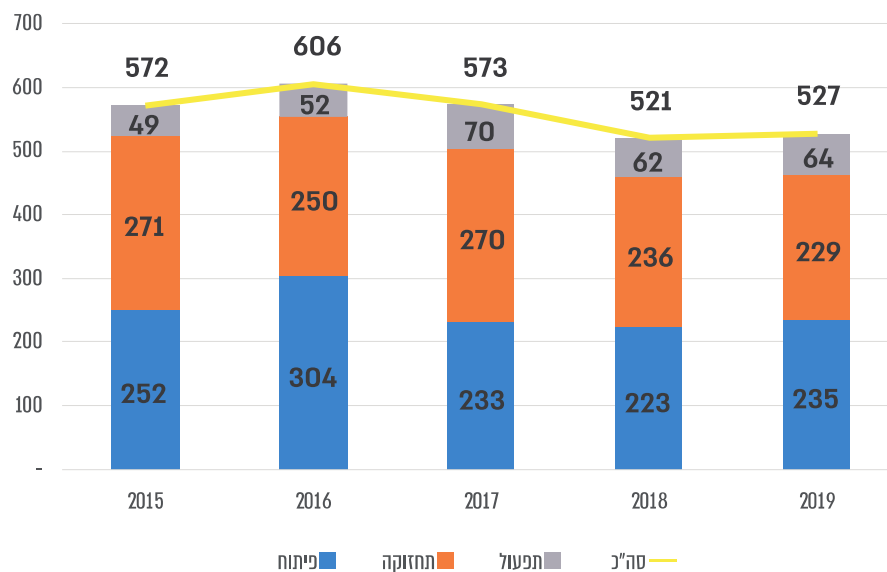
16 בשיטת העבודה הקרויה "שולחן עבודה וירטואלי" (Virtual Desktop Infrastructure) העובד משתמש במכונה וירטואלית שמופעלת משרת מרכזי, ולא במחשב שבעמדת העבודה שלו.



תקציב חטיבת התקשוב

תקציב חטיבת התקשוב (להלן - החטיבה) לשנת 2020 הסתכם בכ-540 מיליון ש"ח, ובשנת 2019 בכ-527 מיליון ש"ח. תרשים 2 מציג את פילוח תקציב החטיבה לפיתוח, תחזוקה ותפעול, בשנים 2015 - 2019.

תרשים 2: פילוח תקציב חטיבת התקשוב, 2015 - 2019 (במיליוני ש"ח)



על פי נתוני חח"י, בעיבוד משרד מבקר המדינה.

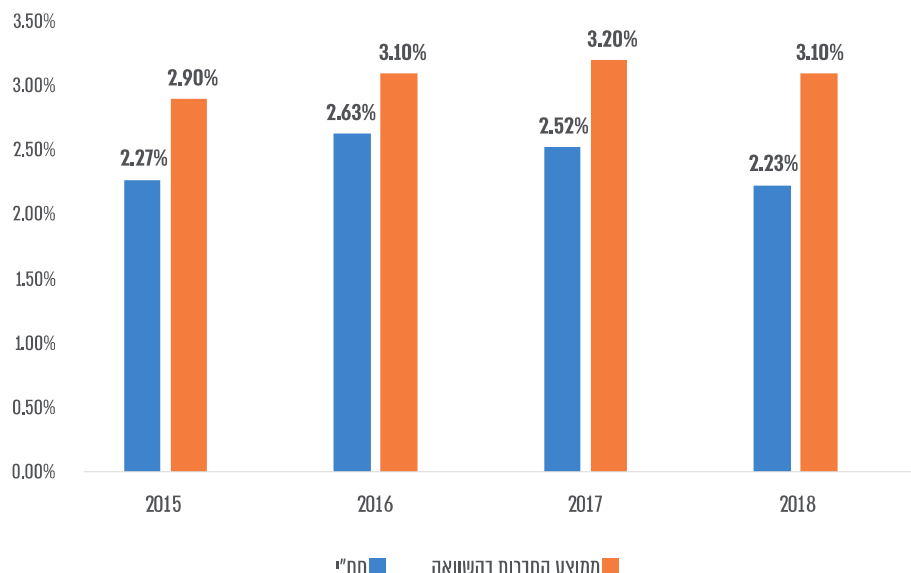
החטיבה מעניקה שירות לשאר החטיבות הפועלות בחברה, על ידי פיתוח ותחזוקה של מערכות לתמיכה בצרכים השונים של החברה, העלאת רמת ההגנה וההיערכות בתחומי הסייבר ואבטחת מידע, ותמיכה תקשורתית בפרויקטים אסטרטגיים של החברה, כדוגמת הרפורמה והשינוי המבני בחברה.

ביצוע תקציב טכנולוגיות המידע בחברה (להלן - IT) בפועל בשנת 2018 הסתכם בכ-513 מיליון ש"ח (מתוך 521 מיליון ש"ח), ושיעורו היה 2.23% מתוך סך הכנסות החברה באותה שנה. מחקר¹⁷ אשר סקר את נתונין של 136 חברות ברחבי העולם אשר מקורות ההכנסה העיקריים שלהן היו שירותי אנרגייה ומים, כגון ייצור, הולכה ואספקה של חשמל, הולכת גז טבעי והולכת מים (להלן - חברות תשתית), העלה כי שיעור הוצאות ה-IT של החברה מסך הכנסותיה קטן משיעור תקציב ה-IT הממוצע של החברות שאליהן הושוותה. תרשים 3 מפרט את שיעור הוצאות ה-IT של החברה מסך הכנסותיה, לעומת שיעור תקציב ה-IT הממוצע של החברות שאליהן הושוותה, בשנים 2015 - 2018.

17 מחקר אשר חח"י מסרה למשרד מבקר המדינה. IT Key Metrics Data 2019: Key Industry Measures: Utilities Analysis, Gartner, December 2018.



תרשים 3: שיעור הוצאות ה-IT של החברה מסך הכנסותיה, לעומת חברות תשתית בעולם, באחוזים, 2015 - 2018.



על פי נתוני חח"י, IT Key Metrics Data 2019: Key Industry Measures: Utilities Analysis, Gartner, December 2018, בעיבוד משרד מבקר המדינה.

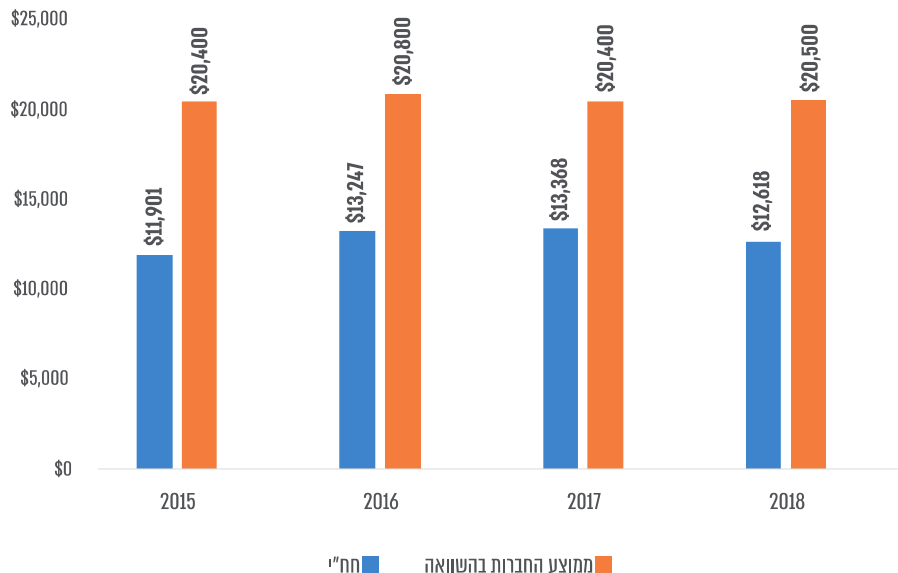
מהתרשים עולה כי בשנת 2018 היה שיעור הוצאות ה-IT הממוצע מתוך סך ההכנסות בקרב חברות תשתית בעולם כ-3.1%, לעומת שיעור של 2.3% בחח"י. על מנת לתת תובנה מדויקת יותר, המחקר חילק את חברות התשתית לחמש תתי-קבוצות על פי מחזור הכנסותיהן¹⁸. מבין החברות שמחזור הכנסותיהן היה 10 - 1 מיליארד דולר בשנת 2018 (מחזור ההכנסות של חח"י בשנה זו הסתכם בכ-6.6 מיליארד דולר), שיעור הוצאות ה-IT הממוצע מתוך סך הכנסותיהן של חברות אלו היה 2.7% באותה שנה, שהוא קרוב יותר לשיעור הוצאות ה-IT של חח"י.

תרשים 4 מפרט את הוצאות ה-IT בחברה פר עובד, לעומת ממוצע החברות שאליהן השוותה, בשנים 2015 - 2018.

18 חברות בעלות מחזור הכנסות: (1) קטן מ-250 מיליון דולר בשנה; (2) בין 250 ל-500 מיליון דולר בשנה; (3) בין 500 מיליון ל-1 מיליארד דולר בשנה; (4) בין 1 ל-10 מיליארד דולר בשנה; (5) יותר מ-10 מיליארד דולר בשנה.



תרשים 4: הוצאות IT בחברה פר עובד בהשוואה לחברות בעולם, 2015 - 2018 (באלפי דולר)



על פי נתוני חח"י, ועל פי המחקר, IT Key Metrics Data 2019: Key Industry Measures: Utilities Analysis, בעיבוד משרד מבקר המדינה. Gartner, December 2018.

מהתרשים עולה כי החברה הוציאה 12,618 דולר פר עובד בשנת 2018, לעומת 20,500 דולר פר עובד בממוצע בקרב החברות שאליון הושוותה. יצוין כי בקרב חברות שמחזור הכנסותיהן בשנת 2018 היה 1 - 10 מיליארד דולר נמצא כי הוצאות ה-IT היו 19,883 דולר פר עובד. יצוין כי מספר העובדים בחברה בשנה זו היה 11,475, וזאת לעומת מספר ממוצע של 5,100 עובדים בקרב החברות שאליון הושוותה חברת החשמל.

תקציב הסייבר לעומת הביצוע

שיעור ניצול תקציב הסייבר של החברה בין השנים 2015 ועד 2020 נע בין 90% ל-116%.

חח"י מסרה למשרד מבקר המדינה בפברואר 2021 כי עד שנת 2017 תקציבי הגנת הסייבר לא נוהלו במרוכז, וכל חטיבה ביצעה את הפעילות בהתאם ליכולותיה. חח"י הסבירה כי תקציב הסייבר בשנת 2016 היה בהתאם ליכולות של החטיבות ולמידת בשלות הפרויקטים. עוד היא הסבירה כי בשנת 2015 בוצעו רכישות של מערכות ותוכנות, אשר הגדילו את תקציב הסייבר בפיתוח ושימוש את החברה בשנים שלאחר מכן. חח"י השיבה למשרד מבקר המדינה במאי 2021 "שכל אתר מנהל את התקציב שאושר על ידו באופן חטיבתי/אגפי בצורה מפורטת".



ביטוח סייבר

במסגרת התמודדות החברה עם סיכונים, היא נוהגת לבטח את עצמה מפני נזקים שייגרמו לה או לצד שלישי. ציוד התקשוב והמערכות הממוחשבות של החברה, וכן שאר הרכוש התפעולי של החברה, מבטחים במסגרת ביטוח הכולל כיסוי בגין אובדן רווחים בעקבות נזקים לחברה.

בשנים 2014 - 2020 ביטוח סיכונים הסייבר של החברה היה חלק מביטוח הרכוש הכולל של החברה. ביטוח הרכוש הכולל כלל כיסוי לנזקי אש, התפוצצות ושבר מכני בגין אירוע סייבר. גבול הכיסוי בביטוח הרכוש הכולל היה 1 מיליארד דולר. כיוון שפוליסת ביטוח הרכוש הכולל של החברה כללה חריג עבור נזקים לצד שלישי אשר עשויים להיגרם בשל מתקפות סייבר, משנת 2014 החברה רכשה ביטוח מפני נזקים העלולים להיגרם ממתקפת סייבר לצד שלישי כהרחבה¹⁹ לביטוח הרכוש הכולל שלה.

החברה מסרה למשרד מבקר המדינה באפריל 2021 כי "בפוליסת הרכוש שנרכשה לשנת 2021 ... קיים חריג לסייבר, אשר התווסף בשנה האחרונה לכל פוליסות הביטוח בשוק הביטוח הבינ"ל". לפיכך, רכשה החברה ביטוח סייבר לכיסוי נזקי רכוש הנובעים מסייבר שלא במסגרת ביטוח הרכוש הכולל. גבול כיסוי ביטוח זה הוא עד סך של 100 מיליון דולר, והשתתפות העצמית היא בסך של מיליוני דולר.

משרד מבקר המדינה ממליץ לחח"י להמשיך ולבחון מעת לעת את היקף הכיסוי הביטוחי למקרי סייבר בהתאם להיקף ניסיונות התקיפה ולפוטנציאל הנזק מהם.

חח"י השיבה למשרד מבקר המדינה במאי 2021 כי ההמלצה מקובלת עליה וכי הנושא מטופל באופן שוטף.

הכרה תעריפית בעלויות הגנת סייבר

הכנסותיה של חברת החשמל מבוססות על תעריף החשמל שהיא גובה מצרכני החשמל, מתוקף חוק משק החשמל, התשנ"ו-1996 (להלן - החוק, או חוק משק החשמל). החוק מסמיך את רשות החשמל לקבוע את תעריף החשמל ולעדכנו, על בסיס עקרון העלות²⁰, בהתחשב, בין היתר, בסוג השירותים וברמתם. התעריף שקובעת רשות החשמל מתעדכן אחת לכמה שנים.

בפברואר 2021 מסרה חח"י למשרד מבקר המדינה כי אין בתעריף החשמל הנוכחי משום חסם להוצאות הנדרשות בתחום הסייבר.

19 ההרחבה כללה כיסוי ביטוחי עבור הוצאות משפטיות וקנסות בגין הפרת הגנת הפרטיות, עבור נזקים והפסדים הנגרמים מפרצות מידע סודי, מכשל ביטחוני, או מאי-הודעה של החברה לרגולטור הרלוונטי על חשיפה לא מורשית של מידע אישי אשר החברה אחראית להגנה על פרטיותו מתוקף חוק. יצוין כי הרחבה זו לא כללה, בין היתר, כיסוי ביטוחי בגין הפסדים שעלולים להיגרם מפעולות מלחמה וטרור (למעט טרור סייבר), מפגיעות בגוף ומנזק לרכוש או מהחרמת מערכות המחשוב של החברה על ידי גורמים ממשלתיים.

20 עקרון העלות על פי החוק, משמעותו, שהמחיר של כל שירות ישקף את העלות שלו בלבד וזאת בתוספת שיעור תשואה נאות על ההון.



אסדרה ופיקוח

סמכויות הנחיה

בתחום הסייבר במדינת ישראל גופים השייכים למערכת הביטחון, כגון צבא ומשטרה, מנחים את עצמם; מתקנים רגישים ותעשיות ביטחוניות מונחים בידי הממונה על הביטחון במשרד הביטחון; גופים המופקדים על תשתיות קריטיות, מונחים בידי מס"ל או השב"כ. בין התשתיות הקריטיות נכללות תשתיות הגז, האנרגיה, החשמל, המים, התחבורה ותשתיות תקשורת; משרדי ממשלה מונחים לגבי הפעילות הממשלתית הפנימית על ידי היחידה להגנת הסייבר בממשלה (להלן - יה"ב)²¹; המגזר העסקי ברובו אינו מונחה, מחוץ מאשר גופים כגון הבנקים, חברות אחרות הפעילות בשוק ההון, מפעלי אנרגיה ומוסדות בריאות המונחים על ידי רגולטור מגזרי.

החוק להסדרת הביטחון קובע סמכויות ואחריות לאבטחה פיזית, לאבטחת מידע ולאבטחת מערכות מחשוב חיוניות של גופים ציבוריים כהגדרתם בחוק. בין גופים אלה נכללים גופי ממשלה וגופים בבעלות פרטית, ובהם חח"י. על פי החוק, עד אפריל 2017 האחריות להנחיה בנושא אבטחת מערכות ממוחשבות חיוניות של חח"י הייתה בידי שירות הביטחון הכללי (להלן - שב"כ). בדצמבר 2018 תוקן החוק, ובכלל זה נקבע בו כי האחריות להנחיה בנושא מערכות ממוחשבות חיוניות של חלק מהגופים, ובהם חח"י, היא בידי מערך הסייבר הלאומי (להלן - מס"ל), שהוקם על פי החלטת ממשלה²² (ראו להלן). בתקופת הביניים האחריות בנושא לגבי חח"י הייתה של הרשות הלאומית להגנת הסייבר.

בשנת 2011 החליטה הממשלה²³, בין היתר, על הקמת מטה קיברנטי לאומי (להלן - המטה או מטה הסייבר) במשרד ראש הממשלה, שבין תפקידיו לייעץ לממשלה ולוועדותיה בנושא הסייבר, לרכז את עבודתן בנושא זה ולתת לראש הממשלה ולממשלה המלצות בנושא מדיניות הסייבר הלאומית.

בהחלטת ממשלה משנת 2015²⁴ (להלן - החלטה 2444) נקבע כי תוקם רשות לאומית להגנת הסייבר (להלן - רשות הסייבר או הרשות) במשרד ראש הממשלה, שייעודה הגנת מרחב הסייבר, ותפקידיה העיקריים הם ניהול, הפעלה וביצוע של שלל מאמצי ההגנה האופרטיביים במישור הלאומי במרחב הסייבר; הפעלת מרכז לסיוע בהתמודדות עם איומי סייבר²⁵ הנוגעים לכלל המשק; עיצוב, יישום והטמעה של תורה לאומית להגנת סייבר. עוד החליטה הממשלה על הקמת מס"ל, אשר יכלול את הרשות והמטה כשתי יחידות סמך עצמאיות למשרד ראש הממשלה. באותה החלטה גם קבעה הממשלה כי יש "להטיל על המטה להציג... מתווה להעברת שטח הפעולה בתחום פעולות לאבטחת מערכות ממוחשבות חיוניות... משירות

21 יה"ב הוקמה על פי החלטת ממשלה 2443 מ-15.2.15, ותפקידיה הם, בין היתר, הכוונה והנחיה בהיבטי הגנת הסייבר, לרבות הגדרת המדיניות ודרישות האסדרה, ליווי מקצועי שוטף ומענה על פניות מקצועיות, בהתאם למאפיינים של הגופים אשר הפעילות נוגעת להם בנושאים שחל עליהם החוק להסדרת הביטחון בגופים ציבוריים ובנושאים שחל עליהם חוק הגנת הפרטיות תתבצע ההנחיה בתיאום עם הגורם המוסמך לפי חוקים אלה.

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

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

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

25 המרכז הארצי לניהול אירועי סייבר (CERT - Computer Emergency Response Team).



הביטחון הכללי לרשות"; וכי יש להטיל על המטה ועל הלשכה המשפטית במשרד ראש הממשלה בשיתוף עם משרד המשפטים להכין את תזכיר חוק הגנת הסייבר.

בסוף שנת 2017, בהתאם להחלטת הממשלה 3270²⁶, מוזגו מטה הסייבר הלאומי והרשות הלאומית להגנת הסייבר ליחידה אחת: מערך הסייבר הלאומי הוא מס"ל.

ביוני 2018 הופץ בקרב הציבור תזכיר חוק הגנת הסייבר, לקבלת הערותיו ותגובותיו בנושא. ממסמכי מס"ל²⁷ עולה כי "בעקבות ההערות בוצעה עבודת הטמעה והפנמה של ההערות ובוצעו סבבי דיונים עם גורמים שונים... ונערכה עבודה משמעותית לטובת קידום הכנת תזכיר החוק לפורמט 'הצעות חוק'". עלה כי בסיום תקופת הביקורת מס"ל ומשרד המשפטים טרם הניחו הצעת חוק על שולחן הכנסת.

תזכיר החוק המוצע נועד לממש את החלטות הממשלה ומדיניותה בתחום הגנת הסייבר, ובהתאם לכך גם את ההיבטים הקשורים במערך הסייבר הלאומי וסמכויותיו²⁸. מס"ל פרסם באתר האינטרנט שלו²⁹ כי תפקידיו על פי תקציר תזכיר חוק הגנת הסייבר הם:

1. לנהל, להפעיל ולבצע בהתאם לצורך את מאמצי ההגנה הלאומיים האופרטיביים מפני תקיפות סייבר.
2. לקדם את יכולת ההתמודדות של ישראל עם תקיפות סייבר.
3. לקדם מדיניות ומובילות ישראליות בתחום הסייבר בהתאם למדיניות הממשלה ולהחלטותיה.
4. לקדם שיתופי פעולה בתחום הסייבר במישור הבין-לאומי ולגבש הסכמי שיתוף פעולה בתחום הסייבר.
5. לייעץ לממשלה ולוועדותיה בתחום הסייבר.
6. לבצע כל תפקיד אחר בתחום הגנת הסייבר שיקבע ראש הממשלה.

בדוח מבקר המדינה בנושא "היערכות גופים חיוניים להגנת הסייבר" מפברואר 2019 (להלן - הדוח הקודם)³⁰ נכתב כי "במועד סיום הביקורת"³¹, כשלוש שנים לאחר קבלתה של החלטת הממשלה, ועל אף החשיבות הלאומית שבהסדרת ההגנה על המרחב האזרחי, טרם הושלמו התהליכים הנדרשים לגיבוש נוסח חוק הסייבר, וכן לא הוסדרו בהחלטות הממשלה 2443 ו-2444 היבטים תפעוליים בעבודת עובדי מס"ל מול הגופים שהוא מנחה. עוד העיר מבקר המדינה כי היעדר מקור נורמטיבי לסמכות עובדי המערך עלול להקשות את שיתוף הפעולה עם

26 החלטת הממשלה 3270 (17.2.17), "איחוד יחידות מערך הסייבר הלאומי".

27 אתר המרשתת של מערך הסייבר הלאומי, עדכון מ-5.7.20 של ההודעה שפורסמה ב-12.7.18.

28 תזכיר חוק הגנת הסייבר ומערך הסייבר הלאומי, התש"ע - 2018.

29 הודעה בנושא "תקציר תזכיר בנושא חוק הגנת הסייבר", פורסמה באתר המרשתת של מערך הסייבר הלאומי ביולי 2020.

30 משרד מבקר המדינה, **דוח היערכות גופים חיוניים להגנת הסייבר**, (2019) דוח שנתי 69, עמ' 2070-2071.

31 יולי 2018.



הגופים ולגרום להימנעותם של עובדי המערך מביצוע פעולות מסוימות... עקב חוסר בהירות בעניין תחומי הסמכות.

במועד סיום ביקורת זו, כחמש שנים לאחר שהתקבלה החלטת הממשלה 2444 וכשנתיים לאחר שהופץ תזכיר החוק, טרם הושלמו התהליכים הנדרשים לגיבוש נוסח חוק הסייבר.

משרד מבקר המדינה ממליץ למס"ל ולמשרד המשפטים להשלים את התהליכים הנדרשים לגיבוש טיוטת חוק הגנת הסייבר כפי שנקבע בהחלטת הממשלה 2444, ולאסדר את כל הסמכויות הנדרשות כדי שמס"ל יוכל להשיג את המטרה שלשמה הוקם.

משרד המשפטים השיב למשרד מבקר המדינה באפריל 2021 כי "עקב התפזרות הכנסת החל מדצמבר 2018 ולנוכח משבר הקורונה... לא ניתן היה להביא את הטיוטה לווועדת שרים לחקיקה". עוד השיב המשרד כי הוא "רתום לסייע להשלמת המהלך החקיקתי כך שניתן יהיה להסדיר משפטית את הפעילות השלטונית להגנת הסייבר על מנת שיעמדו לרשות המדינה כלים מגוונים ואפקטיביים להתמודדות עם איומי סייבר בממשלה ובמשק האזרחי".

מס"ל השיב למשרד מבקר המדינה כי הוא "ממשיך לקדם מול כלל הגורמים הרלבנטיים חקיקת סייבר על מנת להעלות את רמת הגנת הסייבר במשק הישראלי".

הנחיה במשק האנרגיה

בעשור האחרון החל תהליך הפרטה של תשתיות אנרגיה ומים, ובמסגרתו מוקמים מתקני תשתית פרטיים בתחומים אלה, כגון תחנות כוח לייצור חשמל ומתקנים להתפלת מי ים. פגיעה במערכות חיוניות במתקנים אלה עלולה לגרום בין היתר לפגיעה בחיי אדם ולנזקים כלכליים.

על פי חוק משק החשמל, ייצור חשמל בהספק של יותר מ-16 מגה-ואט מותנה בקבלת רישיון לייצור חשמל מרשות החשמל³² במשרד האנרגיה. על פי החוק, הרשות רשאית לתת רישיון, בין היתר, לייצור חשמל, ולקבוע בו תנאים וכן להגביל או שלא להגביל את תקופת תחולתו. הרישיון יכול, בין היתר, את הגבלת תחולתו, אם זו אכן הוגבלה, וכן את הכללים והחובות החלים על בעל הרישיון לפי חוק זה.

בהחלטת ממשלה 2443 משנת 2015 נקבע, בין היתר, כי יחידות להכוונה מקצועית מגזרית בתחום הגנת הסייבר במשרדי הממשלה יפעלו להכוונה והנחיה מקצועית בתחום הגנת הסייבר "בהתאם לסמכויות הרגולציה המופעלות על המשרד הממשלתי או במסגרתו", ובהנחייה מקצועית של הרשות הלאומית להגנת הסייבר³³. מתוקף החלטה זו והחלטות ממשלה נוספות (ראו לעיל) הנוגעות לפעילות ההגנה והאסדרה במרחב הסייבר של מדינת ישראל, מונחים מתקני התשתיות הפרטיים. מתקנים אלו, הכוללים את יצרני החשמל הפרטיים (להלן - יח"פ)

32 לצורך ייצור חשמל בהיקף של יותר מ-100 מגה-ואט נדרש בין היתר אישור שר האנרגיה.

33 הרשות הלאומית להגנת הסייבר אוחדה עם מטה הסייבר הלאומי ליחידת סמך אחת המשרד ראש הממשלה - היא מערך הסייבר הלאומי, החלטת ממשלה מס' 3270 מיום 17.12.2017 בנושא איחוד יחידות מערך הסייבר הלאומי (ראו לעיל בפרק זה).



מונחים על ידי מערך החירום, הביטחון, המידע והסייבר במשרד האנרגיה (להלן - אגף חירום וביטחון במשרד האנרגיה). ההנחיה כוללת הגנה בתחום הסייבר והתמודדות עם אירועי סייבר.

ביוני 2020 פרסמה מועצת רשות החשמל עדכון³⁴ הכולל דרישה מיזם פרטי המקים תחנת כוח ברשת המתח הגבוה (בהספק של 630 קילו-ואט עד 16 מגה-ואט) לעמוד בדרישות משרד האנרגיה בנושאי אבטחה פיזית וחמושה ואבטחת סייבר כתנאי לחיבור לרשת החשמל. כדי לעמוד בדרישה זו, עליו לפנות לאגף חירום וביטחון במשרד האנרגיה כדי לקבל אישור לכך שהוא עומד בדרישות הסייבר בשלב הסנכרון לרשת החשמל. מתקן שאינו עומד בדרישות המשרד לא יחובר לרשת החשמל.

אגף חירום וביטחון במשרד האנרגיה הוציא הנחיה להתמודדות עם אירועי סייבר ושמירה על רציפות תפקודית של משק האנרגיה והמים במדינת ישראל. הנוהל כולל עקרונות, נהלים ובקרה בכל הנוגע לתכנון ולביצוע של אבטחה ומיגון של מערכות מחשוב חיוניות משלב הייזום, דרך שלב ההקמה וכלה בשלבי תפעול ותחזוקת השוטפת של הגוף המונחה. הנוהל חל על כל גוף מונחה אשר על פי דין או על פי תנאי הרישוי שלו כפוף להנחיה אבטחתית או ביטחונית של משרד האנרגיה.

משרד האנרגיה מסר למשרד מבקר המדינה בפברואר 2021 כי יחידת הסייבר המגזרית הפועלת במערך, מלווה את היח"פ משלב הייזום, דרך שלב ההקמה ולכל אורך חיי הפעלתו המסחרית, וכי ההנחיות ואמצעי הסייבר מוטמעים במיזם כבר בשלבי המוקדמים, באופן שמתקן המקבל את אישור ההפעלה מדי משרד האנרגיה עומד במלוא דרישות הגנת הסייבר ודרישות האבטחה הפיזית. לאחר הפעלתו המסחרית של המתקן מתקיימת הנחיה שוטפת לחיזוק, לשימור ולתחזוקה של ההגנה, וכן תרגול וביקורת סייבר.

כמו כן, משרד האנרגיה הקים מרכז קיברנטי מגזרי (להלן - מק"ם) לניטור כלל תשתיות האנרגיה הלאומיות והפרטיות. המק"ם מנטר גם גופי תמ"ק המונחים על ידי מס"ל.

המק"ם פועל החל מספטמבר 2016, ובמועד סיום הביקורת היו מחוברים אליו מתקנים ממגזרי תשתיות האנרגיה.

משרד מבקר המדינה רואה בחיוב את העובדה כי משרד האנרגיה הקים את המק"ם, המנטר את כלל תשתיות האנרגיה, מתכלל מידע המתקבל מהן ומשקף תמונת מצב בנושא הגנת סייבר על משק האנרגיה.

במשק החשמל קיימים שני גופי רגולציה בתחום הסייבר המנחים את הגורמים הנמצאים תחת אחריותם.

בהשוואה בין הנחיות שני הגופים האמורים נמצאו מספר הבדלים.

34 אמת מידה 4.35 על פי סעיף 30 לחוק משק החשמל התשנ"ו - 1996 בין תפקידי הרשות: "קביעת אמות מידה לרמה, לטיב ולאיכות השירות שנותן בעל רישיון ספק שירות חיוני לצרכן, לבעל רישיון הספקה, ליצרן חשמל, ליצרן חשמל פרטי, לבעל רישיון אגירה או לבעל רישיון ספק שירות חיוני אחר (להלן אמות מידה) ופיקוח על מילוי חובותיו על פי אמות המידה".



מומלץ כי הגופים הרלוונטיים ובהם שני גופי הרגולציה יבחנו הגדרתן של הנחיות אחידות עבור כלל הגורמים המונחים על ידם.

אחד הגופים הרגולטוריים השיב למשרד מבקר המדינה במאי 2021 כי הוא כתב נוהל בין היתר בהתאם לתקינה מקובלת ומשלב בין היתר הנחיות חופפות להנחיותיו של הרגולטור האחר וכי הוא מתעדכן באופן שוטף

הגוף הרגולטורי השני השיב למשרד מבקר המדינה כי בינו לבין הגוף הרגולטורי האחר מתקיימים קשרי עבודה שוטפים.

הנחיית סייבר בישראל לעומת מדינות אחרות

במדינות המערב מקודמת מדיניות הגנת סייבר לאומית. בשנת 2015 המליץ ה-OECD למדינות הארגון לגבש מדיניות הגנת סייבר הכוללת התמודדות עם הסיכונים במרחב הדיגיטלי³⁵. בשנת 2016 נקבעה באיחוד האירופי (התקף ממאי 2018) דירקטיבה³⁶ המחייבת את החברות באיחוד לגבש מדיניות הגנת סייבר, לקבוע את אופן האסדרה של תשתיות קריטיות ולהקים מרכז טיפול לאומי באירועי סייבר. בדוח הפורום הכלכלי העולמי לשנת 2018 נקבע כי סיכון הסייבר הוא אחד מחמשת הסיכונים הגדולים בעולם³⁷ והומלץ להגביר את ההיערכות לאירועי סייבר.

<http://www.oecd.org/sti/ieconomy/digital-security-risk-managment.pdf> 35

<https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive> 36

<https://www.weforum.org/reports/the-global-risks-report-2018> 37



הנחיית סייבר בחברת החשמל

הפיקוח על ביצוע ההנחיות הניתנות לחברת החשמל

על פי סעיף 15 לחוק להסדרת הביטחון, מס"ל רשאי לגבי הגופים שבאחריותו "להיכנס בכל עת לגוף ציבורי כדי לבדוק אם מולאו ביחס אליו ההוראות לפי חוק זה וההנחיות שניתנו על פיו".

על פי הנחיות מס"ל, הנחיית הגופים המונחים על ידי מס"ל יכולה להתבצע בשלוש תצורות אפשריות: הנחיה ישירה, הנחיה עקיפה והסכם שיתוף פעולה. בתצורת הנחיה ישירה מס"ל מקיים קשרי עבודה ישירים עם הגוף המונחה, והמשרד הממשלתי הרגולטורי של הגוף המונחה מתעדכן ומתואם על פי צורך; ולעומת זאת בתצורת הנחיה עקיפה חלק מקשרי העבודה מתקיימים מול המשרד הממשלתי הרגולטורי הממונה על הגוף המונחה.

נמצא כי מס"ל לא הסדיר בכללים את האופן שבו חח"י צריכה לדווח לו כדי שיוכל לעקוב אחר ביצוע הנחיותיו ואחר תיקון הליקויים שמצא.

משרד מבקר המדינה בחן את הפיקוח בפועל של מס"ל על יישום כמחצית מההנחיות שמסר מס"ל לחח"י בשנים 2018 - 2020 ושנמסרו למשרד מבקר המדינה במהלך תקופת הביקורת.

עולה כי מס"ל לא ביצע מעקב ופיקוח מלא בעניין ביצוע כל הנחיותיו בידי חברת החשמל וכי לגבי חלק מתוך ההנחיות, מס"ל מסר לצוות הביקורת במשרד מבקר המדינה כי לא התקבל מידע על סטטוס ההנחיה בכתב או בעל-פה.

יצוין כי חח"י גיבשה את הוראת העבודה "מודל תהליכי עבודה בין חברת חשמל למערך הסייבר הלאומי" (להלן - ההוראה), התקפה ממרץ 2020, כשנתיים לאחר שמס"ל החל להנחות אותה. ההוראה עודכנה ביוני 2020 ובנואר 2021. בהוראה צוין בין היתר כי אחת לשבוע או שבועיים יתקיים מפגש עבודה בין מס"ל למטה הסייבר בחח"י; בכל מפגש ירוכזו הנושאים שלשני הגורמים חשוב לדון בהם וכן יתבצע מעקב שוטף אחר סטטוס יישום ההחלטות.

חח"י השיבה למשרד מבקר המדינה כי היא מגישה "באופן שוטף סטטוס יישום הנחיות מס"ל", וכי "מתקיימות פגישות שוטפות ברמה שבועית לטובת דיווחים בין שני הצדדים". עוד היא השיבה כי הפערים ביישום חלק מההנחיות נמצאים בבדיקה מול מס"ל, וחלק מההנחיות האחרות לטענת חח"י היא עדכנה את מס"ל.

מס"ל השיב למשרד מבקר המדינה כי "האחריות על ביצוע ההנחיה והדיווח לאגף תמ"ק [במס"ל] מוטלת קודם כל על הגוף עצמו. על רקע היכרותו של אגף תמ"ק עם מאפייני הגוף, הוא נמנע בדרך כלל, מלקבוע סד זמנים נוקשה למימוש ההנחיה, אלא עוקב באופן עתי אחר ביצועה בפרק זמן סביר".

יצוין כי על אף הפגישות כאמור בין הצדדים והקשר השוטף המתקיים בין חח"י לבין מס"ל, יש פער בין סטטוס יישום ההנחיות על פי מסמכי חח"י לבין זה הידוע למס"ל, כפי שעולה ממסמכיו.



בהוראה שגיבשה חח"י יחד עם מס"ל לא נקבעו סדרי הדיווח של חח"י בכתב למס"ל, לרבות קביעת לוחות זמנים להגשת דיווח זה.

על מנת למנוע את הפער בין סטטוס יישום ההנחיות על ידי חח"י בפועל לבין זה הידוע למס"ל, מומלץ כי מס"ל כמאסדר יפעל לאסדרה של סדרי הדיווח והבקרה שלו על חברת החשמל. בכלל זה, מומלץ לקבוע הוראות בדבר הדיווח בכתב שחח"י צריכה למסור לו בעניין אופן ביצוע הנחיותיו, בעניין תיקון ליקויים שנמצאו על ידו או על ידי גורמים אחרים בביקורות חיצוניות או פנימיות, ומהם ההסברים הנדרשים בדיווח. כמו כן, מומלץ כי מס"ל יקבע את המועדים הנדרשים למסירת דיווחים בכתב כאמור, לרבות דיווחים עיתיים ומידיים, ואת הפרטים שחח"י נדרשת למסור בדיווחיה.

עוד מומלץ כי מס"ל יפעל לקבל מחח"י מידע באופן סדור לגבי יישום כלל הנחיותיו מהשנים שחלפו.

משרד מבקר המדינה ממליץ למס"ל להקים מערכת ממוחשבת להזנת כלל ההנחיות לגופים המונחים הכוללת התראות על סטטוס תיקון הליקויים, אשר תשמש לו ככלי בקרה על ביצוע הנחיותיו.

מס"ל השיב למשרד מבקר המדינה ביוני 2021 (להלן - תשובת מס"ל) כי הוא "מקבל את נקודת המבט של צוות המבקר אודות חשיבות "פירמול" התקשורת עם חח"י... עם זאת... מאפייני פעילות אגף תמ"ק, כפי שמבוצעים מחייבים התאמה של שיטה רגולטורית זו למול כלים אחרים כדי להשיג את התוצאה הרצויה - אפקטיביות והנעה לפעולה מהירה של הארגון, ולדעתו פירמול נהלים הינו אמצעי ולא מטרה בפני עצמה".

עוד השיב המס"ל כי "הליכי ההנחיה הישירים בין אגף תמ"ק לארגונים המנויים בתוספת לחוק להסדרת הבטחון מתאפיינים בקשר שוטף ורציף בין המנחה לגוף המונחה (באמצעות ממונה התמ"ק), ופגישות עבודה עתיות ביניהם שבסופן יוצא סיכום דיון" עם זאת, "בימים אלו החלה להיערך באגף תמ"ק [במס"ל] עבודת מטה אודות יצירת קובץ הנחיות והאחדת תהליכים בין האגף לגופים המונחים, ובכוונת האגף לבחון במסגרת עבודת מטה זו גם את הצורך לגבש נהלים ברורים ואחידים למימוש הפיקוח והבקרה על הגופים כמתואר בדוח [ביקורת זה], לרבות עיגון הדברים בכתב תוך קביעת לוחות זמנים ברורים ומוגדרים".

לפי ההנחיות המקצועיות, על גופי התמ"ק לכלול תוכנית לצמצום פערים ולהטמעת המענה האבטחתי.

במהלך הביקורת עלו פערים מסוימים בעמידת חח"י בחלק מן ההנחיות.

יצוין כי תוך כדי ביצוע הביקורת נקטה חח"י בפעולות על מנת לצמצם ולבטל פערים אלו.

כמו כן, לאחר מועד סיום הביקורת, במאי 2021, מסרה חח"י למשרד מבקר המדינה תוכנית עבודה רב-שנתית ובה יעדים לעמידה בהנחיות.



לנוכח החשיבות של תשתיות החברה מבחינת כלל פעילות המשק, מומלץ שחח"י תשלים יישומה של התוכנית תוך קביעת אבני דרך ולוחות זמנים ותדווח עליהם למס"ל.

מדיניות אבטחה פנים-ארגונית

עפ"י ההנחיות הרגולטוריות, על ארגון להגדיר, בין היתר, את הסדרת הסמכויות בהיבטי הגנת הסייבר ואת התמיכה הניהולית.

ועדת היגוי עליונה הגנת מרחב הסייבר ואבטחת מידע (להלן - ועדת היגוי עליונה לסייבר) - בראשות מנכ"ל החברה. לצד ועדה זו פועלות ועדות נוספות. ועדת ההיגוי העליונה מגבשת היבטים בתחום הסייבר הוועדה מתכנסת אחת לשנה.

ועדת ההיגוי העליונה להגנת הסייבר ולאבטחת מידע התכנסה פעם אחת בכל אחת מהשנים 2019 ו-2020. בדיוני הוועדה הוצגו: סיכום הפעילות השנתית בנושאי הסייבר ואבטחת מידע בחברה, עיקרי תוכנית העבודה לאותה שנה ותקציב הסייבר בחברה לאותה שנה.

הוועדה קבעה בין היתר כי עד למועד מסוים תושג עמידה ביעד מסוים אולם הוועדה לא דנה בצורך לקבוע תוכנית עבודה רב-שנתית לגבי יעדים נוספים.

נהלים פנימיים

נמצא כי חלק מנוהלי החברה שנדרשים במסמכי מס"ל בנושא הגנת הסייבר נכתבו בתקופת הביקורת בשנת 2020. יצוין כי גם מסמך מדיניות הגנת הסייבר של החברה נכתב והושלם בשנת 2020.

מומלץ כי החברה תבדוק בשיתוף מס"ל אילו נהלים נוספים נדרשים לה ותכין תוכנית עבודה להכנתם.

חח"י השיבה למשרד מבקר המדינה כי הנושא מטופל ומיושם באופן שוטף עם מס"ל.

תוכניות שנתיות ורב-שנתיות

עפ"י ההנחיות הרגולטוריות, על חח"י להגדיר תוכנית רב-שנתית. כמו כן, ההנחיות קובעות, בין היתר, כי יש להציג את התוכנית לוועדת ההיגוי ולעדכנה בהתאם לעדכונים.

בהוראת עבודה של החברה בנושא תוכנית עבודה ובקורות להגנת הסייבר ואבטחת מידע, צוין כי תוכנית עבודה שנתית או רב-שנתית, בקרה, סקרים וביקורת הם כלי ניהול חיוניים לתכנון פעילות החברה בתחום הגנת הסייבר ואבטחת המידע, להצבת יעדים ולצמצום פערים, תוך הקצאת משאבים יעילה.

במועד סיום הביקורת, דצמבר 2020, חח"י טרם הגישה תוכנית רב-שנתית.



כמו כן, על פי הפרוטוקולים של ועדת ההיגוי העליונה, במועד סיום הביקורת תוכנית עבודה רב-שנתית כאמור טרם הוצגה לוועדה.

עוד נמצא כי במועד סיום הביקורת, תוכניות העבודה השנתיות שח"י הציגה לשנים 2021-2019 אינן כוללות את מלוא הפירוט לגבי אופן יישומן.

משרד מבקר המדינה ממליץ שהחברה תכין תוכנית עבודה רב-שנתית מפורטת יותר בתחום הסייבר בהתאם להוראת העבודה בנושא, הכוללת את מלוא הפירוט הנדרש. כמו כן, מומלץ שהחברה תכין תוכניות שנתיות מפורטות כאמור.

עוד המליץ משרד מבקר המדינה כי תוכניות העבודה השנתיות והרב-שנתית כאמור תוצגנה לגורמים הרלבנטיים ותעודכנה כפי שנדרש.

ח"י השיבה למשרד מבקר המדינה כי לאחר מועד סיום הביקורת, בפברואר וביוני 2021, היא הציגה לגורמים הרלבנטיים את תוכנית העבודה השנתית לשנת 2021. עוד היא השיבה כי "תוכנית עבודה רב שנתית ושנתית הוצגה" במאי 2021. בנוסף היא השיבה כי תוכניות העבודה השנתיות מוצגות ונדונות עם הגורמים הרלבנטיים באופן שוטף. כמו כן, ציינה ח"י כי היא "רואה חשיבות רבה בתוכנית עבודה שנתית ורב שנתית".

בקורות בהגנת סייבר ובאבטחת מידע

דרישות הגנת סייבר בהתקשרויות מסוימות

בהנחיות מס"ל יש פרק העוסק בשרשרת האספקה. מטרת הפרק היא קביעת הנחיות לגבי הסדרי האבטחה הנדרשים בקרב ספקי הגופים המונחים, על מנת לאפשר אבטחה של נכסי המידע המסווגים ושל רכיבי המערכות הקריטיות, אשר גורמים חיצוניים מפקדים על תחזוקתם, מפעולם, התקנתם, ניהולם ואספקתם.

על פי מסמך מדיניות הגנת הסייבר ואבטחת המידע של ח"י, אחריות כוללת של מנהל כל פרויקט מטעם ח"י היא בין היתר להגדיר את אופן היישום של כל דרישות אבטחת המידע לפרויקט במסגרת כל מחזור החיים של הפרויקט, החל בשלב התכנון, דרך הפיתוח וכלה בשלב התחזוקה השוטפת של התשתית, ולפקח על יישומן של דרישות אלה.

בהנחיות הרגולטוריות ובהוראות ח"י מפורטים כללים הנוגעים לדרישות אבטחת המידע בהתקשרויות מסוימות.

משרד מבקר המדינה בדק את יישום הכללים האמורים באחת מהתקשרויות ח"י.

נמצא כי באחת העסקאות חברת חשמל לא ביצעה את כל הפעולות שהיה עליה לבצע לפי הכללים

בין היתר נמצא כי אחד המסמכים נחתם ע"י עובדת ח"י בתפקיד מסוים ולא ע"י מורשי החתימה של החברה.



עד מועד סיום הביקורת טרם הסתיים התהליך וטרם נקבע מענה מספיק לכל הפערים. משרד מבקר המדינה ממליץ למס"ל ולחח"י לפעול להשלמת כלל הפעולות הנדרשות כדי לעמוד בדרישות הסייבר.

חח"י השיבה למשרד מבקר המדינה כי המלצה זו מקובלת עליה וכי היא גם פועלת לפיה.

משרד מבקר המדינה מציין כי היה ראוי שהמסמך, בפרט בעסקה בהיקף כספי משמעותי, ייחתם בהתאם לנהלי החברה ע"י מורשי החתימה, ככל שאר מסמכי ההסכם, לאחר ביצוע הבקורות הנדרשות.

מומלץ שהחברה תבחן עם מס"ל כיצד ניתן למנוע את הישנותם של הליקויים שנמצאו בהליך חתימת המסמך, וכי תוודא מול מס"ל שהבקורות בתהליך יהיו מקובלות עליו ויאושרו על ידו.

סקרי סיכונים ומבדקי חדירה

החוק להסדרת הביטחון³⁸ מסמיך את מס"ל לתת הנחיות מקצועיות לגופים שהוא מנחה, ובהם חח"י, בכל הנוגע לפעולות אבטחה, לרבות בעניין בקרה ודיווח. כאמור, מס"ל מנחה את חח"י בתצורת הנחיה ישירה, באמצעות הנחיות ונהלים, טיפול באירועים, משוב, הזרמת מידע ודיווחים, ניתוח איומים והתאמת המענה, בקרה (ביקורות, תרגילים, מעקב הנחיות), הדרכה והכשרה.

על פי ההנחיות הרגולטוריות, יש לבצע סקר סיכונים עבור תהליכים מסויימים אחת לתקופה.

כמו כן מנחות ההנחיות הרגולטוריות לבצע מבדק חדירה אחת לתקופה מסוימת. מטרת מבדק החדירה היא לבחון את היכולת לפגיעה בזמינותה, באמינותה, בשלמותה או בהפעלתה של המערכת.

ממסמכי החברה מפברואר 2020³⁹ עולה כי נכון ליולי 2019, לחטיבת התקשוב בחברה לא היה מסמך מדיניות כתוב או נוהל או הוראת עבודה בנושא ביצוע סקרי סיכונים ומבדקי חדירה. מסמך מדיניות הגנת הסייבר ואבטחת מידע הוכן ואושר במאי 2020 (להלן - מסמך המדיניות)⁴⁰.

במסמך המדיניות הוגדרו תכנון פעילות סקרי הסיכונים ומבדקי החדירה לפי דרישות הרגולציה השונות.

ממסמכי חברת חשמל עולה כי ביולי 2019 היא לא גיבשה תוכנית עבודה רב-שנתית או שנתי לביצוע סקרי סיכונים ומבדקי חדירה. בפועל, עלו פערים בביצוע סקרי סיכונים ומבדקי חדירה עד יולי 2019.

38 סעיף 10 לחוק.

39 חברת החשמל, דוח ביקורת פנימי

40 מסמך המדיניות תקף מיוני 2020.



במאי 2020 הכינה חח"י תוכנית עבודה בנושא מבדק סיכונים או חדירה תלת-שנתית לשנים 2020 - 2023. חח"י השיבה למשרד מבקר המדינה כי באותה שנה "הוקצו משאבים נוספים לקידום פעילות זו". הועלה כי בשנת 2020 ביצעו חח"י ומס"ל מבדקים כאמור.

עלו פערים בתוכנית העבודה להכנה ויישום של סקרי סיכונים ומבדקי חדירה. מומלץ כי חברת חשמל תשלים הכנת תוכניות עבודה לביצוע סקרי סיכונים ומבדקי חדירה בכלל מערכותיה ותפעל ליישומה ולמעקב אחר תיקון הליקויים שיעלו.

חח"י השיבה למשרד מבקר המדינה כי במאי 2020 החברה אישרה נוהל ביצוע סקרי סיכונים ומבדקי חדירה בתשתיות התקשוב, ובשנת 2020 היא השלימה סקרי סיכונים לכל היישומים בתחומים מסויימים וכי באותה שנה הוקמה ועדת היגוי ייעודית ברשות סמנכ"ל תקשוב לצורך מעקב ובקרה על פעילות זו. עוד השיבה החברה, כי במאי 2021 הכינה חח"י תוכנית עבודה תלת-שנתית עדכנית לנושא זה.

סקרי סיכונים שביצע מס"ל בחח"י בשנים האחרונות

משרד מבקר המדינה בחן מספר סקרי סיכונים שביצע מס"ל בחח"י בשנים האחרונות ואת אופן יישום המלצות מס"ל על ידי חח"י.

מבחינה זו עלה כי עבור מספר סקרים נמצאה חוסר התאמה בדבר תיקון הליקויים שהעלה הסקר, בין הדיווח שהמציאה חח"י לביקורת לבין הדיווח שהיה בידי מס"ל. משרד מבקר המדינה ממליץ למס"ל בשיתוף עם חח"י להשלים מתכונת מעקב ודיווח אחר תיקון הליקויים.

מנגנוני בקרה

ההנחיות הרגולטוריות והוראות החברה קובעות כללים באשר למנגנוני הבקרה השונים שעל החברה ליישם ובאשר לתהליכי העבודה השונים הקשורים לתחום הגנת הסייבר.

עלה כי עבור חלק ממנגנוני הבקרה ותהליכי העבודה שנבדקו בביקורת, החברה אינה עומדת באופן מלא בכלל ההנחיות הרגולטוריות והוראות החברה. יצוין כי החברה מסרה למשרד מבקר המדינה כי התהליכים השונים שנועדו ליישום ההנחיות וההוראות הרלוונטיות הושלמו או שנמצאים בפעילות לצורך השלמתם. משרד מבקר המדינה מציין כי על החברה לעמוד בהנחיות ובהוראות הרלוונטיות. כמו כן, מומלץ כי מס"ל יעקוב אחר סטטוס ביצוע הנחיותיו.



היערכות לתגובה על אירועי סייבר ולהתאוששות מהם

כושר התאוששות של העסק (business resilience) משמעו יכולתו של הארגון להסתגל להפרעות ואירועים על מנת לשמור על רציפות בפעילותו ולהגן על נכסיו.

על פי הנחיות מס"ל תהליך קריטי הוא סדרת פעילויות המבוצעות על ידי מספר גורמים בארגון (אנשים, מערכות ממוחשבות) על מנת לממש את יעודו העסקי של הגוף אשר פגיעה קיברנטית מולו היא בעלת פוטנציאל נזק ברמה המדינית; מערכת קריטית הוגדרה כמערכת ממוחשבת אשר פגיעה בזמינותה, אמינותה, שלמותה או הפעלתה שלא בהתאם לייעודה עלול לגרום לנזק לתהליך הקריטי בהתאם לתבחינים שהוגדרו על ידי מערך הסייבר הלאומי..

חח"י הגדירה את המושג "נכס מידע" כמאגר נתונים, או כל צבר של נתונים או מידע, המשמש במערכות טכנולוגיות המידע.

יצוין כי מהמידע שחברת חשמל מסרה למשרד מבקר המדינה עולה כי יש בחברה מערכות מידע רבות, חלקן הוגדרו ע"י החברה כקריטיות ביותר.

משרד מבקר המדינה ממליץ כי מס"ל יאסדר בנוהל את חובתה של חח"י למסור לו תמונת מצב, ובכלל זה יקבע בנוהל את הפרטים שעל חח"י למסור לו ובאילו מועדים עליה למסור לו עדכונים לשם בחינתו ואישורו כנדרש.

תהליכים קריטיים בחח"י

בחח"י יש נוהל פנימי להמשכיות עסקית ובין המטרות שהוגדרו בו: מיסוד מהלך קבוע בחברה לאיתור התהליכים הקריטיים בעיתות שגרה וחירום והסדרה של הכנת תוכניות המשכיות לתהליכים הקריטיים, קביעת שיטת ההפעלה של תוכניות המשכיות עסקית והטמעתן בחטיבות העסקיות של החברה, תוך בחינה תקופתית של התהליכים הקריטיים. תהליך קריטי הוגדר בנוהל כתהליך חיוני שחייב לפעול ברציפות בכל מצב כדי לאפשר לחברה לתפקד כ"עסק חי" ובכלל זה תהליכים תפעוליים ותקשוביים. המשכיות עסקית הוגדרה בנוהל כשימור התהליכים הקריטיים של החברה להבטחת רציפות תפקודית ותפעולית המאפשרת את קיומו של הארגון כ"עסק חי" בתחומים הקריטיים לרבות התחום התפעולי, הלוגיסטי, התקשובי, הפיננסי והארגוני. על פי הנוהל, תוכנית המשכיות עסקית היא תוכנית סדורה, מוכנה מראש, עבור תהליך קריטי שאישר מנהל אגף או סמנכ"ל (להלן - בעל תהליך).

ממסמכי חח"י מינואר 2020 עולה כי בשנים 2009 - 2014 נבדקו וזוהו בחח"י תהליכים קריטיים. עוד עולה ממסמך של חח"י ממרץ 2020 כי בחח"י מופו תהליכים עסקיים מהותיים של החברה, וכי הוכנו תוכניות המשכיות עסקית עבור חלקם.

חח"י מסרה למשרד מבקר המדינה בינואר 2021 כי בשנת 2020 מחלקת ניהול סיכונים שלה קיימה שיחות עם בעלי תהליכים בנושא המשכיות העסקית, קבעה דגשים ונתנה הנחיות בנושא, וכי גם מחלקת ניהול סיכונים תבחן בשנת 2021 את תוכניות המשכיות העסקית, אשר



עודכנו, בין היתר, בהתאם להנחיות ניהול הסיכונים וקיבלו את אישורם של בעלי התהליכים, כדי שיתקיים תהליך מתמשך של בחינה ושיפור מתמיד.

עפ"י מסמך שמסר מס"ל למשרד מבקר המדינה, נכון לדצמבר 2020, עבור אחד מהתהליכים קיימת תוכנית המשכיות שאינה מלאה.

משרד מבקר המדינה ממליץ לחח"י לפעול להשלמת תוכנית ההמשכיות עבור התהליך המסוים.

לאחר מועד סיום הביקורת, חח"י מסרה כי עדכנה את תוכנית ההמשכיות עבור התהליך המסוים.

תגובה לאירועים

ההנחיות הרגולטוריות מנחות בדבר היערכות לאירועי חירום ולטיפול בהם.

עלה כי לפי תוכנית העבודה של החברה, בסוף שנת 2021 מתוכננות להסתיים פעולות נדרשות הנוגעות לצוותי התגובה ובמועד סיום הביקורת טרם נקבעו לוחות זמנים לפעילויות המשך.

משרד מבקר המדינה ממליץ לחח"י לקבוע לוחות זמנים לפעילויות המשך.

חח"י השיבה למשרד מבקר המדינה כי מתוכנן דיון לפעילות ההמשך.

משרד מבקר המדינה בדק את הכשרתם של גורמי מקצוע מסוימים בתחום הסייבר.

בינואר 2021 חח"י מסרה למשרד מבקר המדינה, כי אין מסמך שקובע את הדרישות מגורמי המקצוע האמורים ביחס לפעילויות הנוגעות לתחום עיסוקם וההכשרה הנדרשת. כמו כן מסרה החברה כי נושאים אלו יעוגנו במסמך מדיניות החברה.

משרד מבקר המדינה ממליץ למס"ל לקבוע בכתב הנחיות מפורשות ומפורטות לגבי ההכשרות הנדרשות לגורמים רלוונטיים ולהנחות את חח"י לגבי דיווחים בכתב על ביצוען. על חח"י לפעול בהתאם להנחיות שיינתנו על ידי המס"ל.

תרגילים

על פי הנחיות מס"ל, יש לבצע תרגילי אבטחה כדי לבחון בפועל את אופן הפעולה של העובדים, גורמי התפעול וגורמי האבטחה בגוף.

עוד נקבע בהנחיות כי יש לבצע בחינת כשירות עיתית של תפקוד חברי הצוות אשר תכלול תרגול בפועל של טיפול באירוע תוך שימוש בכלים הטכנולוגיים ושיטות הפעולה הרלוונטיות. בסיום התרגיל יש לבצע תחקיר והפקת לקחים, לתעדם במסמך ולשלוח אותו למס"ל.



עלה כי בשנים 2015-2019 בוצעו מספר תרגילים, חלקם היו תרגילים מתודיים, חלקם היו מעשיים, וחלקם שילבו גם אירועים מעשיים.

חח"י השיבה למשרד מבקר המדינה כי בשנת 2020 התקיימו תרגילים נוספים וכי "תוכנית עבודה שנתית מהווה תוכנית עבודה מחזורית"

מומלץ שחח"י תגבש תוכנית רב שנתית המפרטת נושאים לתרגילי סייבר בהנחיית מס"ל ובשיתוף עימו וכי בתרגילים ישולבו היבטים מעשיים אשר ילוו בתהליכי סיכום והפקת לקחים מתועדים.

סיווג מסמכים

על פי הנחיות מס"ל והוראות אבטחת מידע יש לסווג מסמכים מסווגים. בביקורת נמצא כי חח"י אינה מקפידה לציין על המסמכים שהיא ציינה בפני משרד מבקר המדינה שהם מסווגים את סיווגם. הדבר עלול לגרום לכך שגורם שאינו ער לסיווג המסמך, בין שהוא חיצוני לחברה ובין שהוא פנימי, ינהג בו כאילו לא היה מסווג.

על חח"י לציין את רמת הסיווג של מסמכים מסווגים. מומלץ כי החברה תגבש נוהל המחייב את עובדיה לסווג כל מסמך לפי סיווגו הביטחוני, לפרסמו, לפעול להטמעתו ולעקוב אחר יישומו של נוהל סיווג והגנה על מידע הקיים בחברה.

חח"י השיבה כי קיים נוהל סיווג והגנה על מידע משנת 2008, וכי במהלך תקופת הביקורת ולאחריה החברה פעלה לעידכנו. בבדיקת מעקב הודיעה חברת חשמל ביולי 2021 כי הנוהל המעודכן נמצא בשלבי אישור וחתימה. כמו כן השיבה חח"י כי "הופצו 4 מידעונים מעודכנים לכלל עובדי החברה" בשנת 2020 ובשנת 2021 הופצו עד יולי 2021 שני מידעונים נוספים. עוד היא מסרה כי "נושא סיווג והגנה על המידע מהווה חלק מתכנית העבודה הרב שנתית והשנתית בנושא מודעות אבטחת מידע והגנת סייבר של החברה". ביולי 2021 השיבה חח"י כי לאחר סיום הביקורת, בשנת 2021, היא הכינה לומדה בנושא סיווג והגנה על מידע שטרם קיבלה את אישור וועדת נהלים בחברה, וכי לאחר קבלת האישורים הלומדה תופץ בקרב עובדי חח"י.

היפרדות יחידת ניהול המערכת מחברת חשמל במסגרת הרפורמה

בסעיף 3(א) של החלטת הממשלה מיוני 2018 נקבע כי פעילות יחידת ניהול המערכת, יחידת תכנון ופיתוח טכנולוגיות (להלן - תפ"ט)⁴¹ והיחידה לסטטיסטיקה ושווקים יועברו מחח"י לחברה

41 אגף תכנון ופיתוח טכנולוגי (תפ"ט) בחח"י כפוף ישירות למנכ"ל החברה, ואחראי על תכנון ופיתוח של מערכת החשמל, בין היתר, באמצעות בחינה וקביעה של טכנולוגיות; תכניות פיתוח במקטעי הייצור, ההולכה וההשנאה; קידום תשתיות וניהול התכנון הפיזי והסביבתי; ניטור ביצועים ומצב של המערכת (הנדסי וסביבתי); ביצוע מחקרים יישומיים לשיפור ביצועי המערכת; ניהול מידע וידע; ורשיו.



ממשלתית נפרדת - חברת ניהול המערכת בע"מ (להלן - החברה לניהול המערכת או חנ"ם) אשר הוקמה בהתאם להחלטת הממשלה מ-30.6.08.

ב-1.12.20 הוקמה חברת ניהול המערכת, אשר פעילותה כוללת תכנון, פיתוח וניהול של משק החשמל בישראל. בסוף שנת 2020 הועברו יחידות תפ"ט וסטטיסטיקה מחנ"י לחנ"ם, יחידת ניהול המערכת אמורה לעבור לחנ"ם עד יוני 2021⁴².

במועד סיום הביקורת חנ"י לא השלימה תוכנית להפרדת הינ"ם מחנ"י בהיבטי סייבר, ולא הגישה למס"ל תוכנית כאמור, וזאת אף שינ"ם אמורה לעבור לחנ"ם עד יוני 2021.

חנ"י השיבה למשרד מבקר המדינה כי עדכנה את מס"ל על כך ש"נושא ההפרדות מינ"מ נמצא בטיפול שוטף ואינו מסוכם סופית בין 2 הגורמים ולפיכך לא הוגשה ת"ע [תוכנית עבודה] למס"ל בנושא זה". עוד השיבה החברה כי "ברמת הפרדת המערכות והתשתיות נבנתה ת"ע [תוכנית עבודה] מסודרת עד ליציאת חנ"ם".

משרד מבקר המדינה ממליץ כי חנ"י תשלים הכנת תוכנית עבודה כתובה.

חנ"י השיבה למשרד מבקר המדינה כי במסגרת תוכנית ההפרדה בין יחידת ניהול המערכת לחנ"י הנושא יטופל ברבעון השלישי לשנת 2021.

42 זאת בהתאם לצו משק החשמל (דחיית מועד מתן רישיון לניהול המערכת), התש"ף-2019.



סיכום

חברת החשמל מופקדת על תשתית קריטית. פגיעה בשרשרת החשמל עלולה לגרום נזק למשק בכללותו. דוח זה הציג תמונת מצב בנושא הגנת סייבר בחברת חשמל ובפיקוח של מס"ל על חברת חשמל.

משרד מבקר המדינה העלה בין היתר כי לא היה בידי מס"ל מידע מלא שאפשר ללמוד ממנו אם חח"י יישמה את כל הנחיותיו ותיקנה את כל הליקויים שעמד עליהם. מס"ל גם לא אסדר את חובתה של חח"י למסור לו דיווחים בכתב, ואת המועדים, הנושאים והפרטים הנדרשים בדיווחים. עוד נמצא כי במועד סיום הביקורת לא כל הנחיות מס"ל יושמו. כן עלה כי במועד סיום הביקורת טרם נערכה חח"י מבחינת הגנת סייבר לכל הנדרש לצורך ביצוע הרפורמה במשק החשמל שנקבעה ביוני 2018.

על חברת החשמל להמשיך לפעול בתיאום עם מס"ל לשיפור הגנת הסייבר על מערכות המידע בשרשרת החשמל וכן להיערך כנדרש לביצוע תהליך הרפורמה בהיבטי הגנת סייבר ובכללו העברת תחנות הכוח, הינ"ם ותפ"ט.