כ״ז תמוז תשע״ח
10 ביולי, 2018

לכבי
עו״ד עמית אשכנזי
היועץ המשפטי
מערך הסייבר הלאומי
משרד ראש הממשלה

הנדון: **<u>עמדת ISACA ישראל - תזכיר חוק הגנת הסייבר ומערך הסייבר הלאומי, התשע״ח-2018</u>**

התגברות איומי הסייבר על ישראל מצד גורמים שונים, בין אם מדינות עוינות, תאגידים בינלאומיים ומתחרים עסקיים, מצריכה מענה הגנתי הולם אשר ימנע פגיעה בתשתיות מחשוב ותקשורת המהוות מסד להתנהלות היום-יומית, בין אם במוסדות פיננסיים, תחנות כוח ועוד.

תזכיר חוק הגנת הסייבר, שפורסם על ידי הכנסת ב- 20 ביוני 2018, נועד ״לממש את החלטות הממשלה ומדיניותה בתחום הגנת הסייבר, ובהתאם לכך גם את ההיבטים הקשורים במערך הסייבר הלאומי וסמכויותיו״.

הניתוחים וההמלצות, שהועלו במסמך המצורף, מתייחסים להבנתנו לרבדים המקצועיים המרכזיים בפעילות המערך, לרבות למבנהו הארגוני, תפקידיו ותחומי סמכותו ואחריותו למול רגולטורים אחרים. בהתייחסותנו, התבססנו על תפיסות וגישות מובילות, המקובלות בישראל ובזירה הבינלאומית, ככל אשר היו רלבנטיות.

אנו סבורים, כי תזכיר החוק הינו במידה רבה ״ראשית הצירים״ באשר להגנת הסייבר ברמה הלאומית בכלל ופעילות מערך הסייבר בפרט. נוכח זאת, קיימת חשיבות בשקלא וטריא מעמיקים וראויים אשר ימצאו את האיזון הראוי בנושאים חשובים אלה.

*את כתיבת מסמך העמדה המצורף, הובילו מר **תומר רוזנר**- חבר ISACA ישראל, והשתתפו בהכנתו מר **עידו שגיא**- מזכיר ISACA ישראל ומר **שוקי פלג**- חבר הנהלה ויו״ר הוועדה המקצועית של ISACA ישראל.*

אנו נשמח להמשיך ולסייע בעתיד למערך הסייבר ככל שיידרש.

בברכה,

אסף ויסברג, CISA, CISM, CGEIT, CRISC
נשיא
ISACA ישראל

1. אודות ISACA ישראל

ISACA ישראל הינה עמותה מקצועית הרשומה כמלכ"ר, והמספקת מעטפת מקצועית למקצוענים בתחומי ניהול סיכוני מערכות מידע, הגנה בסייבר ואבטחת מידע, ביקורת מערכות מידע וממשל טכנולוגיות המידע.

ISACA ישראל מסונף לארגון ISACA® – מלכ"ר בינלאומי בו חברים מעל 135,000 אנשי מקצוע הפזורים ב- 188 מדינות בעולם ומאוגדים ב 217 סניפים.

כגוף מקצועי מוביל, מעניק ISACA הסמכות מקצועיות אשר צברו עם השנים הכרה בינלאומית רחבה. הסמכות אלו מעידות על המחזקים בהן, כי הם בעלי ניסיון מעשי וידע תיאורטי רב בתחום הרלבנטי:

- **CSX-P®** (**CSX Practitioner Certification**) - הינה הסמכה מקיפה ראשונה ויחידה בתחום הסייבר, אשר בודקת את יכולתו של איש המקצוע לבצע מיומנויות סייבר קריטיות בסביבה וירטואלית חיה ומעריכה את היכולת האנליטית של המועמדים לזהות ולפתור בעיות סייבר.
- **CSX-F®** (**Cybersecurity Fundamentals**) – הינה הסמכה בסיסית בתחום הסייבר המשמשת מבוא לעולם זה ומבוססת על היכרות עם המושגים והמסגרת ומגדירה את הסטנדרטים, הקווים המנחים והפרקטיקות של עולם הסייבר.
- **CISM®** (**Certified Information Security Manager**) – מנהל אבטחת מידע מוסמך.
- **CISA®** (**Certified Information Systems Auditor**) – מבקר מערכות מידע מוסמך.
- **CRISC®** (**Certified in Risk and Information Systems Control**) – הסמכה המיועדת לאנשי IT העוסקים בזיהוי, הערכה, ניתוח וניטור של סיכונים, ועיצוב ניתוח ויישום של בקרות.
- **CGEIT®** (**Certified in the Governance of Enterprise IT**) - הסמכה המיועדת לאנשי מקצוע המנהלים, מספקים שירותי ייעוץ או תומכים בממשל ה- IT בארגון .

התייחסות לסעיפי תזכיר החוק

2. משמעות המונח "תקיפות סייבר"

2.1. תזכיר החוק

עמוד 5- *"הביטוי "תקיפת סייבר" נועד לבטא את טווח המעשים של ניצול לרעה של מחשב או מידע ממוחשב באמצעות מחשב."*

2.2. התייחסות ISACA

להבנתנו, המונח כפי שמופיע בתזכיר החוק אינו מכיל את כלל ממדי הסיכון בהיבטי הסייבר. זאת, נוכח העובדה, כי פעולת התקיפה יכולה לנצל לרעה גם רשתות תקשורת, קוד תוכנה וכו', שאינם נכללים תחת ההגדרה *"ניצול לרעה של מחשב או מידע ממוחשב באמצעות מחשב"*.

- כך למשל, הגדרת משרד ההגנה האמריקני ל-Cyber attack הינה כדלקמן:[1]

> 10. **Cyber attack:** A hostile act using computer or related networks or systems, and intended to disrupt and/or destroy an adversary's critical cyber systems, assets, or functions. The intended effects of cyber attack are not necessarily limited to the targeted computer systems or data themselves—for instance, attacks on computer systems which are intended to degrade or destroy infrastructure or C2 capability. A cyber attack may use intermediate delivery vehicles including peripheral devices, electronic transmitters, embedded code, or human operators. The activation or effect of a cyber attack may be widely separated temporally and geographically from the delivery.

- הגדרת ה-NCSC למונח זה הינה:[2]

Malicious attempts to damage, disrupt or gain unauthorized access to computer systems, networks or devices, via cyber means

2.3. המלצות

2.3.1. **אנו ממליצים להרחיב את הגדרת המושג "תקיפות סייבר" כך שיתייחס למוקדי סיכון נוספים.**

[1] http://www.nsci-va.org/CyberReferenceLib/2010-11-joint%20Terminology%20for%20Cyberspace%20Operations.pdf
[2] https://www.ncsc.gov.uk/glossary

3. תפקידי מערך הסייבר הלאומי

3.1. תזכיר החוק

עמוד 14, סעיף 3 מפרט באשר לתפקידי המערך.

3.2. התייחסות ISACA

לראייתנו, נוכח סעיף 2 (ב) המגדיר את ייעוד המערך כ: "הגנת מרחב הסייבר. . .", ראוי להוסיף לרשימת תפקידיו של המערך התייחסות גם לנדבכים הבאים:

3.2.1. <u>תפקידו של המערך בהיבט גיבוש תורה בתחום הסייבר</u>. מחד גיסא, פרסם המערך את תורת ההגנה הלאומית בסייבר (תוה"ג), מאידך גיסא, תזכיר החוק מתייחס באופן מצומצם יחסית לתפקיד של המערך בהיבט התורה. כך, בין היתר, סעיף ו' בעמוד 84 קובע כי:

"החל מסוף שנת 2015 מפתח מערך הסייבר את תורת ההגנה בסייבר לארגון, המהווה בסיס להנחייתו המקצועית של המערך כלפי ארגונים וכלפי רגולטורים."

לראייתנו, נוכח העובדה כי אחד מתפקידיו המרכזיים של המערך כפי שמוגדר בסעיף 3. (1) הינו: "לנהל, להפעיל ולבצע בהתאם לצורך את מאמצי ההגנה הלאומיים", ראוי להגדירו כמי שמגדיר את התורה בתחום הגנה הסייבר ומפקח על הטמעתה וביצועה; זאת, בדומה להגדרת תכולת תפקיד של קצין חיל ראשי בצה"ל, שהינו הסמכות המקצועית העליונה בתחומו, כמו גם הגורם שמגדיר את תורת הלחימה החיילית ומפקח על הטמעתה וביצועה.[3]

3.2.2. <u>תפקידו של המערך באשר לאסדרת ההסמכות המקצועיות בתחומים הרלבנטיים</u>. מסמך "מדיניות אסדרת מקצועות הגנת הסייבר במדינת ישראל", שפורסם על ידי מטה הסייבר הלאומי ב- 31 לדצמבר 2015,[4] דן, בין השאר, בהסמכות הנדרשות על מנת להיות מוכר כעוסק בכל אחד מהתחומים. עוד מתייחס מסמך האסדרה ל"דור המדבר", שהינם אנשי מקצוע העוסקים בתחום הגנת הסייבר בהיקף נרחב במשך 4 שנים לפחות.

הסניף הישראלי של ISACA, התייחס לנושא במסגרת "מסמך עמדה בנושא שילוב 'דור המדבר' באסדרת מקצועות הסייבר", אשר הועבר למערך הסייבר ביום 19 באוגוסט 2016.

לתפיסתנו, תזכיר החוק מהווה פלטפורמה ראויה להתייחסות לאסדרת המקצועות, בעיקר בשל התובנות הרבות שהצטברו במערך נוכח העיסוק בנושא מזה כשנתיים.

---

[3] "הוראת הפיקוד העליון (הפ"ע) 1.0104, "קציני חיל ראשיים".

[4] http://www.pmo.gov.il/SiteCollectionDocuments/cyber/hagana.pdf

3.2.3. <u>תפקידו של המערך בהיבט מודעות להגנת סייבר</u>. זאת, נוכח העובדה כי תקיפות מנצלות במידה רבה גם את הממד האנושי (Social Engineering לסוגיו), ועל כן ההתמודדות עימן מהווה מרכיב מהותי בכל האמור להגנת סייבר. להבנתנו, תפקיד זה נובע מסעיף 42 (1) בתזכיר החוק, המנחה כדלקמן:

"העלאת העמידות והחוסן של ארגונים במגזרי המשק לתקיפות סייבר, בין היתר באמצעות הנחייתם להיערכות ושמירה על כשירות מתאימה להתמודדות עם איומי סייבר ותקיפות סייבר."

3.3. המלצות

3.3.1. אנו ממליצים להוסיף לתפקידי המערך התייחסות לתפקידו כגורם המגדיר את התורה בתחום הגנת הסייבר ומפקח על הטמעתה וביצועה.

3.3.2. אנו ממליצים לכלול במסגרת תזכיר החוק את העקרונות המנחים באשר לאסדרת מקצועות הסייבר, לרבות הכרה בהסמכות בינלאומיות רלבנטיות.

3.3.3. אנו ממליצים להוסיף לתפקידי המערך התייחסות לתפקידו בהיבטי מודעות להגנת הסייבר, הן ברמת יעד ארגוני – הגברת מודעות לנושא, והן ברמת פעילויות קונקרטיות- ייזום קמפיינים ברמה הלאומית, אכוונת הנושא בקרב ארגונים ועוד.

4. מינוי מפקח פרטיות במערך

4.1. תזכיר החוק

מקומות שונים בתזכיר, לרבות:

4.1.1. עמ' 16-17, סעיפים 10-12.

4.1.2. עמוד 18, סעיף 14(א)(3).

4.1.3. עמוד 27, סעיף 38.

4.2. התייחסות ISACA

אנו מברכים על ההתייחסות לנושא ומתן חשיבות לפרטיות הנתונים והמידע הקיימים והנאספים במסגרת המערך. זאת, בין היתר על ידי מינוי מפקח פרטיות, דיווח על אירועים חריגים בהיבט זה במסגרת הוועדה המפקחת על מערך הסייבר הלאומי, כמו גם הגשת דיווח שנתי לראש הממשלה על פעילות המערך בהתאם להוראות החוק, כמפורט בסעיפים המופיעים לעיל.

5. הגדרת תחומי סמכות ואחריות, ויחסי גומלין בין המערך לבין רשויות מאסדרות

5.1. תזכיר החוק

5.1.1. עמוד 21, סעיפים 20-21, מנחים באשר לסמכות המערך לדרוש חומרים בהיבטי תקיפת סייבר.

5.1.2. עמוד 30 סעיף 47 מתייחס לנושא של רשות מאסדרת, המוגדרת כ*"רשת או ממונה שנתונות לו סמכויות בדין להסדרת פעילות בתחומים משקיים המופיעים בתוספת השנייה"*. התוספת השנייה מתייחסת לתחומים הבאים:

- שירותים פיננסיים;
- שירותי בריאות ורפואה;
- תחבורה, תחבורה ציבורית, תובלה, תעופה, ושייט;
- הגנת הסביבה;
- ייצור אנרגיה והולכתה;
- מים וביוב;
- שירותי דואר ותקשורת, שירותי בזק ושידורים מסחריים

5.2. התייחסות ISACA

להבנתנו, סעיף זה כללי מדי, ואינו מגדיר באופן ברור את גבולות הגזרה בין המערך לבין רשויות מאסדרות אחרות במדינת ישראל, כפי שבאים לידי ביטוי, בין היתר, בחפיפה בתחומי סמכות ואחריות~~ת~~ דוגמת אלה המופיעים בטבלה להלן:

	קריטריון	מערך הסייבר הלאומי תזכיר הצעת חוק הגנת הסייבר ומערך הסייבר הלאומי התשע"ח 2018	רשות הגנת הפרטיות חוק הגנת הפרטיות, התשמ"א 1981[5]	רשות שוק ההון, ביטוח וחסכון חוק הפיקוח על שירותים פיננסיים, התשמ"א 1981[6]	המפקח על הבנקים פקודת הבנקאות 1941[7]
.1	חפיפה בסמכויות ביצוע בין המערך לבין רשויות מאסדרות	"3. (1) לנהל, להפעיל ולבצע בהתאם לצורך את **מאמצי ההגנה הלאומיים האופרטיביים כנגד תקיפות סייבר**."	"10. (ד) שר המשפטים, באישור ועדת החוקה חוק ומשפט של הכנסת, יקים בצו, יחידת פיקוח שתפקח על מאגרי המידע, **רישומם ואבטחת המידע בהם**; גודלה של היחידה יותאם לצורכי הפיקוח."	"1ג. (א) תפקידי הרשות הם: (1) **הגנה ושמירה על עניינים** של המבוטחים, העמיתים ולקוחות הגופים המפוקחים. (2) **הבטחת היציבות** והניהול התקין של הגופים המפוקחים."	"5. (א) הנגיד רשאי למנות מפקח על הבנקים (להלן - המפקח), ומשנתמנה יהיה עובד בנק ישראל ובידיו יהיו **הפיקוח הכללי והביקורת** על כל תאגיד בנקאי. . ."
.2	חפיפה בהגדרת הסמכות לדרישת מידע ומסמכים	"20. עובד מוסמך רשאי לדרוש מכל ארגון הנוגע בדבר **למסור לו כל ידיעה או מסמך, ובכלל זה עותק של חומר מחשב,** הנדרשים לצורך איתור תקיפת הסייבר, התמודדות עמה או מניעתה."	"10. (ה1) לצורך ביצוע תפקידיו רשאי מפקח – (1) לדרוש מכל אדם הנוגע בדבר **למסור לו ידיעות ומסמכים המתייחסים למאגר מידע**."	"49. (ג) לשם פיקוח על ביצוע ההוראות לפי חוק זה, רשאי הממונה או מוסמך פיקוח, לאחר שהזדהה לפי סעיף 49ה – (1) לדרוש מכל אדם הנוגע בדבר **למסור לו כל ידיעה או מסמך** הנוגעים לעסקי אדם שחוק זה חל עליו או הנוגעים להפרה לפי חוק זה."	"5. תהא לו (למפקח על הבנקים) או לבאים מטעמו הסמכות לדרוש מתאגיד בנקאי וכן מדירקטור, מעובד או מרואה החשבון של תאגיד בנקאי, **למסור לו ידיעות ומסמכים** שבידיהם הנוגעים לעסקי התאגיד הבנקאי וכל תאגיד שבשליטתו, או **לאפשר לו לעיין בכל מסמך כאמור,** להעתיקו או לצלמו; **נדרשה ידיעה המאוחסנת במחשב, תומצא הידיעה בדרך שתידרש.**"
.3	חפיפה בהגדרת הסמכות לתפיסת חומרים	"23. (א) עובד מוסמך **רשאי לתפוס חפץ** שיש לו יסוד סביר להניח שיש בו מידע בעל ערך אבטחתי, שבדיקתו המידית נדרשת לצורך איתור תקיפת הסייבר, התמודדות עמה או מניעתה."	"10. (ה1) לצורך ביצוע תפקידיו רשאי מפקח – (2) **להיכנס למקום. . . לערוך בו חיפוש ולתפוס חפץ,** אם שוכנע כי הדבר דרוש לשם הבטחת ביצוע חוק זה וכדי למנוע עבירה על הוראותיו."	"49ג. לשם פיקוח על ביצוע ההוראות לפי חוק זה, רשאי הממונה או מוסמך פיקוח, לאחר שהזדהה לפי סעיף 49ה – (2) להיכנס למקום שאינו משמש בית מגורים בלבד אשר יש לו יסוד להניח כי פועל בו מבטח או סוכן ביטוח, ולדרוש כי ימסרו לו כל ידיעה או מסמך הנוגעים לפעילותו כאמור; **ואולם אין לתפוס מסמך לפי פסקה זו אם ניתן להסתפק בהעתק ממנו**. . . "	"5. (ג) שר המשטרה רשאי להסמיך כל עובד מעובדי בנק ישראל, המוסמך על פי סעיף קטן (א) לבוא מטעמו של המפקח, לערוך חקירות בעניין עבירות על פקודה זו. . . עובד שהוסמך כאמור יהיו לו **כל הסמכויות הנתונות לקצין משטרה בדרגת מפקח ומעלה**."

[5] https://www.knesset.gov.il/review/data/heb/law/kns9_privacy.pdf
[6] https://www.nevo.co.il/law_word/Law01/p194_001.doc
[7] https://www.boi.org.il/he/BankingSupervision/BankingLegislation/DocLib/103.pdf

5.3. המלצות

5.3.1. אנו ממליצים להגדיר באופן מובחן יותר את יחסי הגומלין בין המערך לבין רגולטורים אחרים בעלי תחומי סמכות ואחריות בהיבטי סייבר בתחומם, הן בשגרה והן בעקבות התרחשות אירוע סייבר, לרבות בכל האמור לבאים:

- **הנחייה מקצועית שוטפת של רשויות מאסדרות;**
- **דרישת מידע ומסמכים;**
- **תפיסת חומרים;**

זאת, בעיקר נוכח הצורך לוודא כי תהליך הטיפול באירועי סייבר מבוצע באופן האפקטיבי ביותר.

6. סמכות המערך לדרוש מידע בהיבטי סייבר

6.1. תזכיר החוק

עמוד 21, סעיף 20, מנחה באשר לסמכות המערך לדרוש חומרים בהיבטי תקיפת סייבר: *"עובד מוסמך רשאי לדרוש מכל ארגון הנוגע בדבר למסור לו כל ידיעה או מסמך, ובכלל זה עותק של חומר מחשב, הנדרשים לצורך איתור תקיפת הסייבר, התמודדות עמה או מניעתה."*

6.2. התייחסות ISACA

להבנתנו, סעיף זה כללי מדי, ואינו מתייחס לשני היבטים משמעותיים:

6.2.1. <u>מה נכלל תחת ההגדרה של "כל ארגון"</u>. יוזכר כי בעמוד 18, סעיף 20 בתזכיר החוק מפורטים הארגונים הנכללים במסגרת מערך הגילוי והזיהוי. האם אלה הארגונים מהם רשאי עובד המערך לדרוש ידיעה או מסמך או שמא מדובר בארגונים נוספים?

6.2.2. <u>מהו אופן ההגנה על המידע הנמסר על ידי גורם כלשהו למערך</u>? תזכיר החוק מפרט רבות באשר לשמירה על פרטיות המידע, לרבות מינוי מפקח על פרטיות (עמוד 16, סעיף 10), עיצוב לפרטיות והגנה על מידע מוגן (עמוד 27, סעיף 38). עם זאת, תזכיר החוק אינו מתייחס לצורך בהגנה על מידע המגיע למערך בכל האמור לשמירה על חיסיון מידע נוכח דרישות רגולטוריות או מסחריות ונוכח התחייבויות חוזיות ו/או אחרות של אותו גורם שמסר את המידע, העלולות להיות מופרות, למשל, חוזים והתחייבויות למול גורמים ישראליים ו/או זרים.

להלן מספר תרחישים אפשריים בהיבט זה שראוי לתת עליהם את הדעת:

- מידע הנמסר למערך על ידי גוף פיננסי ישראלי ומכיל התייחסות לבעלי חשבונות אמריקניים; מידע מסוג זה אודות בעלי חשבונות אמריקניים בגופים פיננסיים ישראליים אמור להיות מועבר לרשות המסים בישראל ומשם לשלטונות האמריקניים במסגרת הסכם ה-FATCA. סעיף 7 בהסכם זה קובע מפורשות כדלקמן[8]:

"כל המידע המוחלף לפי הסכם זה (FATCA) יהיה כפוף לסודיות ולהגנות אחרות לפי הוראות האמנה, כולל ההוראות המגבילות את השימוש במידע שהוחלף. יראו מידע שהוחלף לפי הסכם זה כסודי וניתן יהיה לגלותו רק לאדם או לרשות (כולל בתי משפט וגופים מנהליים) המעורבים בשומה, בגבייה או במינהל, באכיפה או בהעמדה לדין, או בהכרעה בערעורים ביחס למסים המתוארים בסעיף 1 לאמנה, או בפיקוח על פעולות כאמור. . . **לא ניתן להעביר את המידע לכל אדם, ישות, רשות או סמכות שיפוט אחרים**."

[8] http://mof.gov.il/chiefecon/internationaltaxation/informationreplacementagreements/documents/fatca_agreement-heb.pdf

מסמך עמדה בנושא תזכיר חוק הגנת הסייבר ומערך הסייבר הלאומי

- מידע הנמסר למערך על ידי תעשייה בטחונית ישראלית, ונוגע לפרויקט המבוצע במשותף עם חברה בטחונית זרה, במסגרתו נעשה שימוש במידע שהוא קניין רוחני של אותה חברה זרה.

6.3. המלצות

6.3.1. אנו ממליצים להבהיר באופן מפורש מהו "כל ארגון".

6.3.2. אנו ממליצים לקבוע את מדרג הציות המחייב ארגונים, ביחס לדרישות חוק הסייבר אל מול דרישות חוק ורגולציה אחרות החלות על ארגונים, תוך איזון בין הדרישות הרגולטוריות השונות וצרכי הארגונים.

7. מינוי עובד או יועץ ביחידת הכוונה מגזרית ברשות מאסדרת

7.1. תזכיר החוק

עמודים 31-32, סעיפים 53 (א) ו-53 (ד), מנחים כדלקמן:

(א) *"לצורך מימוש האמור בחוק זה תהיה ברשות מאסדרת יחידת הכוונה להגנת סייבר".*

(ד) *"לא ימונה עובד או יועץ בתחום הגנת הסייבר ליחידת הכוונה מגזרית אלא בהסכמת האחראי במערך".*

7.2. התייחסות ISACA

סעיף 53 (ד) חל, ככל הנראה, על היקף לא מבוטל הן של עובדים והן של יועצים. להבנתנו, הדבר עלול ליצור צוואר בקבוק של שבועות ואף חודשים כתוצאה מהצורך לאשר פרטנית כל עובד ויועץ בתחום הגנת סייבר ברשות מאסדרת.

לחומרה, הדבר עלול להוביל להאטה ואף עצירה של פעילויות הגנת הסייבר המתקיימות כיום באותן רשויות מאסדרות ובגופים הכפופים אליהן.

7.3. המלצות

7.3.1. אנו ממליצים כי המערך יגבש קריטריונים לגיוס כוח אדם לסוגיו ליחידות ההכוונה המגזריות, אשר מחד גיסא יאפשרו למערך להכתיב סטנדרטים מקצועיים הולמים, ומאידך גיסא, יאפשרו לרשויות המאסדרות לפעול באופן עצמאי תוך שמירה על הרף המקצועי המתאים.
בהתאם לסעיף 23 (ד) במסמך "מדיניות אסדרת מקצועות הגנת הסייבר במדינת ישראל"[9], ראוי כי קריטריונים אלו יתייחסו להשכלה, הכשרה והסמכה קודמת, לרבות הסמכות בינלאומיות רלבנטיות.

[9] http://www.pmo.gov.il/SiteCollectionDocuments/cyber/hagana.pdf

מסמך עמדה בנושא תזכיר חוק הגנת הסייבר ומערך הסייבר הלאומי

8. צורך במבקר פנימי למערך הסייבר הלאומי

8.1. תזכיר החוק

אין כל התייחסות בתזכיר החוק לצורך במינוי מבקר פנימי למערך.

8.2. התייחסות ISACA

כפועל יוצא מהיותו יחידת סמך במשרד ראש הממשלה, מערך הסייבר הלאומי הינו גוף מבוקר על ידי מבקר המדינה בהתאם להנחיות סעיף 9 חוק מבקר המדינה התשי"ח (1958)[10].

בנוסף, מערך הסייבר הינו גוף מבוקר על ידי מבקר פנימי בהתאם לסעיף 2 (א) בחוק הביקורת הפנימית התשנ"ב (1992) הקובע כי[11]:

"בכל גוף ציבורי תקוים ביקורת פנימית על ידי מבקר פנימי."

יצוין כי סעיף 2 (ב) בחוק הביקורת הפנימית מנחה כי:

"שר הממונה על משרד ממשרדי הממשלה רשאי לקבוע כי מי שרשאי למנות מבקר פנימי באותו משרד **רשאי למנות מבקר פנימי לגוף או ליחידה באותו משרד שאינם כפופים למנהל הכללי של המשרד**, ולקבוע, במידת הצורך, את סדרי התיאום בין המבקרים הפנימיים שבמשרד."

להבנתנו, נוכח היקף הפעילות הצפוי של המערך, לצד מהותיות תפקידיו ורגישותם, ראוי כי תזכיר החוק יכלול התייחסות למינוי מבקר פנימי למערך.

מינוי מבקר פנימי למערך ראוי משלושה טעמים מרכזיים:

8.2.1. היותו של המערך גוף לאומי בעל היקף פעילות נרחב.

8.2.2. נוכח האופי הרגיש של פעילות המערך המצריך גורם ייעודי.

8.2.3. הקפדתו של המערך בהיבטי ממשל תאגידי, שקיפות וחוקיות פעולותיו.

8.3. המלצות

8.3.1. אנו ממליצים להגדיר במסגרת החוק פונקציה של מבקר פנימי במערך.

[10] http://www.mevaker.gov.il/he/Laws/DocLib/mevakerLaw2015-tikun-48.pdf?AspxAutoDetectCookieSupport=1
[11] https://www.nevo.co.il/Law_Word/law01/041_001.doc