טיוטת חוק הגנת הסייבר ומערך הסייבר הלאומי (סמכויות לצורך חיזוק הגנת הסייבר) (הוראת שעה), התשפ"א-2021

א. שם החוק המוצע

חוק הגנת הסייבר ומערך הסייבר הלאומי (סמכויות לצורך חיזוק הגנת הסייבר) (הוראת שעה), התשפ"א-2021.

ב. מטרת החוק המוצע

החוק המוצע נועד להקנות למערך הסייבר הלאומי במשרד ראש הממשלה כלים להתמודדות עם סיכוני סייבר לתפקוד התקין של מרחב הסייבר הישראלי ולשירותים חיוניים בו, כהוראת שעה, עד לחקיקת חוק הגנת הסייבר ומערך הסייבר הלאומי.

ג. עיקרי החוק המוצע

טיוטת החוק נועדה להקנות למערך הסייבר הלאומי סמכויות לתת הוראות או לפנות לבית המשפט במקרה של סיכון משמעותי להגנת הסייבר. כיום פועל מערך הסייבר הלאומי מכוח החוק להסדרת הביטחון בגופים ציבורים, התשנ"ח-1998, כלפי הגופי המנויים בתוספת החמישית לחוק בלבד, ואילו מול יתר הגופים במשק פועל המערך בהתאם להחלטות הממשלה בתחום הסייבר, בהסכמה בלבד. זאת, בהתאם להחלטות הממשלה והדין הכללי בהתאם למסגרת משפטית שתואמה עם היועץ המשפטי לממשלה ב"עקרונות ה-CERT הלאומי".[1]

תזכיר חוק הגנת הסייבר ומערך הסייבר הלאומי, התשע"ח-2018 הופץ להערות משרדי הממשלה והציבור ביום 20.06.18, על מנת להסדיר מסגרת משפטית מקיפה לפעילות מערך הסייבר הלאומי להגנת מרחב הסייבר. לאחר קבלת הערות משרדי הממשלה והציבור בוצעה עבודה רבה מאוד להכנת טיוטת חוק. עם זאת, ניתן להעריך, כי לנוכח הרצון לקדם מסגרת משפטית מקיפה, יידרש זמן חקיקתי משמעותי לצורך דיון בחוק וקידומו.

בהקשר זה יצוין כי מרחב הסייבר הלאומי נתון כל העת לאיומים על תפקודו התקין. בשנה האחרונה, עקב התפרצות משבר הקורונה, רמת הסיכון עלתה במידה ניכרת, בין השאר בשל עלייה חדה בהיקף העבודה מרחוק במגזר הציבורי והפרטי, הרחבת הפעילות בזירה הדיגיטלית ותהליכי דיגיטציה מואצים של שירותים ציבוריים ופרטיים.

לנוכח האמור, במסגרת החוק מוצע להסמיך את המערך להנחות ארגון חיוני לבצע פעולות הנדרשות לטובת הגנת הסייבר בארגון כאשר קיימת בו חשיפה קריטית, וכן להסמיכו להנחות ארגונים לבצע פעולות הנדרשות לטובת הגנת הסייבר בעת התרחשות של תקיפת סייבר חמורה בארגון.

---

[1] https://www.gov.il/he/Departments/Policies/principles.

כמו כן, מוצע לקבוע אפשרות לפנות במקרה הצורך בבקשה למתן צו שיפוטי שיאפשר ביצוע פעולות נדרשות להגנה, ובכלל זה להסמיך את המערך לבצע בעצמו פעולות הגנת סייבר אם ארגון מסרב לשתף פעולה.

בנוסף, ועל מנת לאתר סיכונים להגנת הסייבר הלאומית ולסייע לארגונים נתקפים או לארגונים החשופים לתקיפות סייבר הנובעות מחולשות מוכרות הנגישות מרשת האינטרנט, מוצע לאפשר למערך הסייבר לקבל פרטי קשר של ארגונים (בלבד) הקשורים לכתובת IP שבהן מבוצעת התקיפה או נמצאה חולשה המאפשרת ניצול. בהתאם לדין הקיים, שירות הביטחון הכללי מקבל מידע זה מספקיות התקשורת, כחלק מביצוע תפקידיו בתחום הסייבר והגנת הסייבר. על כן לצורך יעילות הפעילות מול גופי התקשורת מוצע כי ברירת המחדל היא כי המערך יקבל מידע זה משירות הביטחון הכללי, המקבל מידע זה בהתאם לייעודו.

על מנת להתמודד עם המצב המשפטי הקיים, ולענות על הצורך המיידי של מערך הסייבר הלאומי בעת הזו, החוק מוצע כהוראת שעה, ואין בו כדי ליתן מענה שלם לצרכי הגנת מרחב הסייבר הישראלי.

ד. <u>השפעת החוק המוצע על החוק הקיים</u>

החוק מוצע כהוראת שעה לשנתיים, וקבועות בו הוראות שמירת דינים מפורטות.

ה. <u>השפעת החוק המוצע על קבוצות אוכלוסייה מסוימות</u>

לא רלבנטי

ו. <u>השפעת החוק המוצע על תקציב המדינה, על תקנים במשרדי הממשלה ועל ההיבט המנהלי</u>

אין.

ז. <u>הערות משרדי ממשלה וגופים אחרים</u>

טיוטת החוק מבוססת על תזכיר חוק הגנת הסייבר ומערך הסייבר הלאומי, התשע"ח-2018, שפורסם להערות ביום 20.06.2018, לאחר עבודת מטה פנים ממשלתית ממושכת.

כאמור לעיל, הנוסח הנוכחי מוצע כהוראת שעה וממוקד בסמכויות הנדרשות בעת הזו למערך הסייבר, ואינו כולל את כל ההסדרים שהוצעו בתזכיר החוק. בפרט, הנוסח הנוכחי אינו כולל הסדרים משפטיים בתחום האסדרה, קרי פעילות הממשלה בתחום רישוי ופיקוח על פעילות משקית. הצעת החוק הנוכחית גם אינה עוסקת ביחסי מערך הסייבר עם משרדי הממשלה המאסדרים. היבטים אלה, שהוגדרו בהחלטת הממשלה מס' 2443 מיום 15.2.15, ובאו לידי ביטוי בפרק מקיף בתזכיר החוק, אינם כלולים בנוסח הנוכחי. בהתאם לזאת, רבות מההערות של משרדי הממשלה וגופי החברה האזרחית בנושאים אלה, אינן רלבנטיות לנוסח הנוכחי.

באשר להוראות שנכללו בתזכיר בעניין סמכויות לטיפול בתקיפות סייבר, משרדי הממשלה, ובמרכזם משרד המשפטים, הרשות להגנת הפרטיות, וגופי החברה האזרחית העירו כי הן מעלות חששות לפגיעה בזכויות אדם ובמרכזן הזכות לפרטיות. סעיפי הסמכויות המוצעים בטיוטת החוק נוסחו תוך התחשבות בהערות אלה, ונועדו לצמצם ככל הניתן חששות אלה, מבלי לפגוע בפעילות הגנת הסייבר.

מגופי ביטחון אחרים התקבלו הערות ביחס לסמכויות המערך והחשש מפני צמצום סמכויותיהם הקיימות בתחום הגנת הסייבר. בהתאם לזאת, בהנחיית ראש הממשלה, קיים המטה לביטחון לאומי עבודת מטה מקיפה לצורך תיאום נוסח החוק, באופן המוסכם על גופי הביטחון. ההסכמות וההסדרים שהושגו באים לידי ביטוי בנוסח זה.

קידום הטיוטה בתקופה זו נבחן לאור הנחיות בית המשפט העליון והיועץ המשפטי לממשלה בנושא תקופת בחירות, ונמצא כי לנוכח מאפייני ההצעה, המבוססת על עבודת מטה מקיפה שבוצעה בשנים האחרונות, הכוללת גם שיח ציבורי, ולנוכח רמת הסיכון שהתעצם במידה ניכרת בעת הזו, אין מניעה לקדם את הצעת החוק בתקופה זו.

ראש אשכול סייבר במחלקת ייעוץ וחקיקה אישרה כי אין מניעה משפטית לקידום הצעת החוק.

הצעת חוק מטעם הממשלה:

טיוטת חוק הגנת הסייבר ומערך הסייבר הלאומי (סמכויות לצורך חיזוק הגנת הסייבר) (הוראת שעה), התשפ"א-2021

הגדרות 1. בחוק זה -

"אינטרס ציבורי חיוני" – כל אחד מאלה:

(1) מניעת פגיעה חמורה בשלום הציבור;

(2) חיי אדם;

(3) כלכלת המדינה;

(4) הגנה על הסביבה;

(5) בריאות הציבור או בטיחותו;

(6) מניעת אירוע אבטחה חמור במאגר שחלה עליו רמת האבטחה הגבוהה, כהגדרתם בתקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017;

(7) תפקודם התקין של תשתיות, מערכות או שירותים חיוניים;

(8) תפקודו התקין והבטוח של מרחב הסייבר;

"ארגון" – מוסד כהגדרתו בסעיף 35 לפקודת הראיות;

"ארגון שמקיים פעילות חיונית" – ארגון שפעילותו חיונית בשל אחד או יותר מאלה:

(1) הפעילות בעלת מאפיינים ציבוריים הנוגעים לכלל הציבור או לחלק משמעותי ממנו, והיא נדרשת לקיום אספקה חיונית או שירותים חיוניים לציבור, בשגרה או בחירום או למניעת פגיעה חמורה בענף החשוב למשק המדינה;

(2) שירותי הארגון מהווים תשתית מיחשובית או תשתית תקשורת לניהול נכסי המדינה ומשאביה או לצורך המשך פעילותו התקינה של ארגון המנוי בפסקה (1), או של גוף מהגופים המנויים בתוספת החמישית לחוק להסדרת הביטחון;

"בית משפט" – בית המשפט לענינים מינהליים כמשמעותו בסעיף 3 לחוק בתי משפט לענינים מינהליים, התש"ס-2000[2] (להלן – חוק בתי משפט לענינים מינהליים);

"גוף מיוחד" -

(1) צבא ההגנה לישראל;

(2) שירות הביטחון הכללי;

(3) משטרת ישראל;

---

[2] ס"ח התש"ס, עמ' 190.

(4) המוסד למודיעין ולתפקידים מיוחדים;

(5) מערכת הביטחון, הממונה על הביטחון במערכת הביטחון במשרד הביטחון והגופים המנויים בצו שר הביטחון לפי החוק להסדרת הביטחון;

"גורם אחראי" – עובד בכיר במערך הסייבר הלאומי שמינה ראש המערך להפעיל סמכויות לפי סעיף 2;

"הגנת סייבר" – פעולות להגנה על מחשב, על חומר מחשב השמור בו ועל תקשורת הנתונים אליו וממנו מפני תקיפת סייבר, ובכלל זה פעולות לאיתורה, היערכות לה, מניעתה, או טיפול בה וצמצום הנזקים הנגרמים ממנה, במהלכה או לאחריה;

"חולשה" – נקודת תורפה במחשב או בחומר מחשב אשר ניתן לנצלה כדי לבצע תקיפת סייבר נגד אותו מחשב או חומר מחשב.

"חשיפה קריטית" – חולשה שיוצרת סיכון לתקיפת סייבר חמורה או לתקיפת סייבר בהיקף נרחב, בשים לב לאחד או יותר מאלה:

(1) מאפייניה הטכנולוגיים של החולשה;

(2) קיומן של שיטות ואמצעים לנצל את החולשה לתקיפת סייבר או למנוע ניצול שלה לתקיפת סייבר;

(3) שכיחותה של החולשה;

"חומר מחשב", "מחשב", "שפה קריאת מחשב" ו-"תוכנה" – כהגדרתם בחוק המחשבים;

"חוק הגנת הפרטיות" – חוק הגנת הפרטיות, התשמ"א-1981[3];

"חוק להסדרת הביטחון" – חוק להסדרת הביטחון בגופים ציבוריים, התשנ"ח-1998[4];

"חוק המחשבים" – חוק המחשבים, התשנ"ה-1995[5];

"חוק התקשורת" – חוק התקשורת (בזק ושידורים), התשמ"ב-1982[6];

"מידע בעל ערך הגנתי" – מידע טכני שיש בו כדי לסייע להגנת הסייבר, ובכלל זה מידע כמפורט להלן:

---

[3] ס"ח התשמ"א, עמ' 128.
[4] ס"ח התשנ"ח, עמ' 348.
[5] ס"ח התשנ"ה, עמ' 366.
[6] ס"ח התשמ"ב, עמ' 218.

(1) מידע על שיטות תקיפת סייבר;

(2) חולשות ודרכי הטיפול בהן;

(3) מאפיינים טכנולוגיים של תקיפת סייבר, ובכלל זה כתובת המחשב שממנו בוצעה התקיפה או של המחשב שנתקף;

(4) נתונים בשפה קריאת מחשב המעידים על תבנית תקיפת סייבר;

"מידע מוגן פרטיות" – מידע כהגדרתו בסעיף 7 לחוק הגנת הפרטיות וכן ידיעות על ענייניו הפרטיים של אדם אף אם אינן בגדר מידע כאמור;

"המערך" או "מערך הסייבר הלאומי" – כהגדרתו בחוק להסדרת הביטחון;

"נציג מוסמך", של ארגון – העובד האחראי על הגנת הסייבר בארגון או עובד אחר הכפוף ישירות למנהל הארגון, שהמנהל הסמיכו לעניין חוק זה, ואם לא הוסמך עובד כאמור – המנהל;

"עובד מוסמך" – עובד מערך הסייבר הלאומי שמונה לפי סעיף 3;

עובד השירות – עובד בכיר בשירות הביטחון הכללי שמינה ראש השירות להפעיל סמכויות לפי סעיפים 9 ו-10.

"פעולות הגנת סייבר" – פעולות במחשב שהן אחת מאלה:

(1) מתן הוראות למחשב בשפה קריאת מחשב;

(2) בחינה של חומר מחשב או תקשורת נתונים ובכלל זה סריקה ממוכנת שלהם לצורך איתור מידע בעל ערך הגנתי;

(3) העתקה של חומר מחשב או תקשורת נתונים לצורך ביצוע הפעולה המנויה בפסקה (2);

(4) דיווח על איתור מידע בעל ערך הגנתי למערך הסייבר הלאומי;

(5) התקנת מחשב או תוכנה במחשב של ארגון לשם ביצוע הפעולות המנויות בפסקאות (1) עד (4);

"פקודת הראיות" – פקודת הראיות [נוסח חדש], התשל"א-1971[7];

"ראש המערך" – מי שמופקד על ניהול מערך הסייבר הלאומי ועל ביצוע תפקידיו.

"תבנית תקיפת סייבר" – סדרת פעולות במחשב של ארגון המבוצעת במסגרת הכנות לתקיפת סייבר או במסגרת תקיפת סייבר;

[7] דיני מדינת ישראל, נוסח חדש 18, עמ' 421.

"תקיפת סייבר" – פעולה המבוצעת בחומר מחשב שנועדה לפגוע במחשב, בחומר מחשב המאוחסן בו, בתקשורת הנתונים מהמחשב או אליו או גישה לחומר מחשב או לתקשורת נתונים בלא הרשאה;

"תקיפת סייבר חמורה" – תקיפת סייבר שמתקיים לגביה אחד מאלה:

(1) התקיפה עלולה לגרום לפגיעה ממשית באינטרס ציבורי חיוני;

(2) יש יסוד סביר להניח שהתקיפה תגרום לפגיעה ממשית באינטרס ציבורי חיוני לנוכח חומרת הסכנה להתפשטותה למחשבים אחרים ולפגיעה נרחבת בהם או במידע השמור בהם;

(3) התקיפה אותרה בארגון שמקיים פעילות חיונית או שיש יסוד סביר להניח שהיא מכוונת כלפי ארגון כאמור או כלפי גוף המנוי בתוספת החמישית לחוק להסדרת הביטחון;

(4) יש יסוד סביר להניח שהתקיפה נועדה לפגוע בביטחון הלאומי של המדינה.

"תקשורת נתונים" – מעבר של חומר מחשב ממחשב אחד למחשב אחר באמצעות התקשרות או התחברות של מחשב עם מחשב אחר.

גורם אחראי

2. ראש המערך ימנה עובד בכיר מעובדי המערך לגורם אחראי לעניין חוק זה.

עובד מוסמך

3. (א) ראש המערך ימנה עובד מעובדי המערך לעובד מוסמך לעניין חוק זה, ובלבד שמתקיימים לגביו כל אלה:

(1) הוא לא הורשע בעבירה שמפאת מהותה, חומרתה או נסיבותיה אין הוא ראוי, לדעת ראש המערך, להיות עובד מוסמך;

(2) הוא קיבל הכשרה מתאימה בתחום הסמכויות שיהיו נתונות לו לפי חוק זה, כפי שהורה ראש המערך;

(3) הוא עומד בתנאי כשירות נוספים שקבע ראש הממשלה, אם קבע.

(ב) עובד מוסמך לא יעשה שימוש בסמכויות הנתונות לו לפי סעיף 6 אלא בעת מילוי תפקידו ובהתקיים שני אלה:

(1) הוא נושא באופן גלוי תג המזהה אותו ואת תפקידו;

(2) יש בידו תעודה החתומה בידי ראש המערך, המעידה על תפקידו ועל סמכויותיו של עובד מוסמך, שאותה יציג על פי דרישה.

הנחיות מקצועיות להיערכות לתקיפת סייבר

4. (א) גורם אחראי רשאי לתת לארגון ולנציג מוסמך שלו הנחיות מקצועיות להיערכות לתקיפת סייבר, ובכלל זה להורות לארגון לבצע פעולות הגנת סייבר, אם היה לו יסוד סביר להניח כי התקיימו כל אלה, ולאחר שהודיע על כך לארגון ונתן לו הזדמנות להשמיע טענותיו:

(1) הארגון מקיים פעילות חיונית;

(2) בארגון קיימת חשיפה קריטית והארגון אינו נוקט בפעולות לטיפול בה;

(3) תקיפת סייבר נגד הארגון עלולה לגרום לפגיעה ממשית באינטרס ציבורי חיוני;

(ב) הנחיות מקצועיות לפי סעיף זה יכללו את המועד להשלמת ביצוען.

(ג) ארגון שקיבל מגורם אחראי הנחיות מקצועיות יבצען בהקדם, בתוך התקופה שנקבעה, וידווח לו על כך באופן שקבע הגורם האחראי.

הנחיות מקצועיות למניעת תקיפת סייבר חמורה

5. (א) גורם אחראי רשאי לתת לארגון ולנציג מוסמך שלו הנחיות מקצועיות למניעת תקיפת סייבר חמורה, ובכלל זה להורות לארגון לבצע פעולות הגנת סייבר, אם היה לו יסוד סביר להניח כי התקיימו כל אלה, ולאחר שהודיע על כך לארגון ונתן לו הזדמנות להשמיע טענותיו:

(1) מתרחשת או עומדת להתרחש תקיפת סייבר חמורה בארגון;

(2) הארגון אינו נוקט בפעולות הנדרשות להתמודדות עם התקיפה ולמניעת פגיעה באינטרס ציבורי חיוני כתוצאה מהתקיפה;

(ב) הוראות סעיפים 4(ב) ו-(ג) יחולו גם על הנחיות מקצועיות לפי סעיף זה.

צו שיפוטי לביצוע פעולות הגנת סייבר

6. (א) בית המשפט רשאי, לבקשת גורם אחראי, להתיר בצו לעובד מוסמך לבצע פעולות הגנת סייבר שיפורטו בבקשה או ליתן כל הוראה אחרת בנוגע לביצוען של פעולות כאמור (להלן – צו), אם שוכנע כי הפעולות נדרשות למניעת פגיעה באינטרס ציבורי חיוני, ובלבד שהתקיים אחד מאלה:

(1) הארגון נדרש לבצע הנחיות מקצועיות בהתאם לסעיף 4 או 5 ולא מילא אחר ההנחיות שניתנו תוך פרק הזמן שנדרש לעשות כן;

(2) לא ניתן להשיג את תכלית הפעולות המבוקשות בצו באמצעות הנחיות מקצועיות בלבד לביצוע פעולות אלה בידי הארגון או מי מטעמו.

(ב) לצורך ביצוע פעולות הגנת סייבר לפי סעיף קטן (א) בית המשפט רשאי להתיר גם כניסה למקום ותפיסת חפץ כמשמעותו בפקודת סדר הדין הפלילי (מעצר וחיפוש) [נוסח חדש], תשכ"ט-1969;

(ג) צו לפי סעיף זה יעמוד בתוקפו למשך התקופה שתיקבע בו ובלבד שלא תעלה על 90 יום, ויהא ניתן להאריכה בהתאם לבקשה שתוגש לפי סעיף זה;

(ד) סבר בית המשפט כי ארגון לא מילא אחר הנחיות מקצועיות במלואן או בחלקן ולא הייתה סיבה מוצדקת להתנהלותו, יחייבו בהוצאות לאלתר לטובת אוצר המדינה, זולת אם מצא טעמים מיוחדים שלא לעשות כן.

(ה) שר המשפטים רשאי לקבוע בתקנות סדרי דין לעניין הליכים לפי סעיף זה.

הגנה על פרטיות

7. (א) בפעולות לפי חוק זה לא יאסוף המערך מידע מוגן פרטיות אלא אם כן המידע הוא מידע בעל ערך הגנתי כמפורט בפסקאות (3) ו-(4) להגדרת מידע בעל ערך הגנתי, או בהתקיים אחד מאלה:

(1) האיסוף מותר לפי דין;

(2) בית המשפט אישר את האיסוף מנימוקים מיוחדים שיירשמו אם שוכנע, לאחר ששקל את מידת הפגיעה הנובעת מכך לפרטיותו של אדם, כי הדבר נדרש כדי להגן על אינטרס ציבורי חיוני.

(ב) לא יעשה אדם שימוש במידע מוגן פרטיות שהתקבל או שנאסף לפי חוק זה אלא למטרת הגנת הסייבר, או לאחר שהתקבל אישור בית המשפט לכך בהתאם לסעיף 7(א)(2), בשינויים המחויבים.

(ג) לא יעביר אדם מידע מוגן פרטיות שהתקבל או שנאסף לפי חוק זה אלא לצרכי הגנת הסייבר ולגוף ציבורי כהגדרתו בפסקה (1) להגדרה "גוף ציבורי" בסעיף 23 לחוק הגנת הפרטיות, ואולם המערך רשאי להעביר מידע מוגן פרטיות גם לארגון, אם מדובר במידע בעל ערך הגנתי כהגדרתו בפסקאות (3) ו-(4) ככל שהדבר נדרש לצרכי הגנת הסייבר.

(ד) מידע מוגן פרטיות שהתקבל או שנאסף לפי חוק זה יימחק עם תום הצורך בו.

(ה) לא יהיה בסעיף זה כדי למנוע העברת מידע שהתקבל או שנאסף לפי חוק זה לגוף מיוחד בהתאם לסמכויותיו לפי כל דין, פרט להעברת מידע לפי פרק ד' לחוק הגנת הפרטיות.

שיקולים לקבלת החלטות לפי סעיפים 4 עד 6

8. בהחלטה לפי סעיפים 4 או 5, או במתן צו לפי סעיף 6, ישקול הגורם האחראי או בית המשפט, לפי העניין, בין השאר, את כל אלה:

(א) מאפייני הארגון ומידת הסיכון לאינטרס ציבורי חיוני כתוצאה מתקיפת סייבר נגדו;

(ב) התאמת הפעולה המבוקשת לאיתור התקיפה, להיערכות לה, לטיפול בה או למניעתה;

(ג) היכולת להשיג את תכלית הפעולה באמצעות אדם בעל ידע ומומחיות מטעם הארגון.

קבלת מידע מספק גישה לאינטרנט או מעובד שירות הביטחון הכללי

9. (א) גורם אחראי רשאי לקבל מספק גישה לאינטרנט או מעובד השירות מידע על אודות זהותו של לקוח ופרטי התקשרות עמו, אם בהתאם למידע המצוי בידיו קיימת חשיפה קריטית במחשבי הלקוח, תקיפת סייבר או תקיפת סייבר חמורה;

(ב) ספק גישה לאינטרנט או עובד השירות שקיבל דרישה כאמור יעביר את המידע לנציג מערך הסייבר הלאומי בהקדם האפשרי ולא יאוחר מ-72 שעות מקבלת הפנייה.

(ג) המידע ישמש לצורך יצירת קשר עם הלקוח ולצורכי הגנת הסייבר בלבד.

(ד) על אף האמור בסעיף קטן (א) גורם אחראי לא יפנה לקבלת מידע מספק גישה לאינטרנט כאמור בסעיף זה אלא לאחר שראש הממשלה או מי שהוסמך על ידו לעניין זה התיר זאת בכתב, בין ככלל או לתקופה, בהתאם לתנאי ההיתר, ובין במקרה מסוים.

(ה) ראש שירות הביטחון הכללי יקבל דיווח על הפנייה לראש הממשלה לפי סעיף קטן (ד).

(ו) אין באמור בסעיף קטן (ד) כדי לגרוע מחובתו של ספק גישה לאינטרנט להעביר מידע כאמור בסעיף קטן (א) אם קיבל פנייה מגורם אחראי.

(ז) בסעיף זה –

"ספק גישה לאינטרנט" – מי שקיבל רישיון לפי חוק התקשורת, או מי שפועל מכוח היתר כללי לפיו הנותן שירות גישה לאינטרנט כהגדרתו בחוק התקשורת, לרבות בעל רישיון כללי למתן שירותי רדיו טלפון נייד ובעל רישיון רדיו טלפון נייד ברשת אחרת, הנותנים שירות כאמור באמצעות ציוד קצה נייד;

"פרטי התקשרות" של לקוח – שם, מען, מספר טלפון ודואר אלקטרוני;

"לקוח" – למעט יחיד.

הסמכת עובד שירות הביטחון הכללי לטיפול בתקיפת סייבר חמורה

10. (א) הסמכויות המוקנות לגורם אחראי לפי סעיפים 5 ו-6 יוקנו גם לעובד השירות לשם מילוי תפקידי השירות הקבועים בסעיף 7(ב)(1) לחוק שירות הביטחון הכללי, התשס"ב-2002.

(ב) שימוש בסמכויות האמורות על ידי עובד השירות ייעשה על-פי היתר מאת ראש השירות לאחר ששוכנע כי הדבר דרוש לצורך מניעת תקיפת סייבר חמורה או התמודדות איתה בארגון באירוע נתון.

(ג) ראש השירות ידווח לראש הממשלה או למי שהוסמך על ידו לעניין זה על היתרים שניתנו לפי סעיף קטן (ב). הדיווח יימסר גם לראש המערך.

שמירת דינים

11. (א) אין בהוראות חוק זה כדי לגרוע מסמכות הנתונה למערך הסייבר הלאומי לפי דין;

(ב) אין בחוק זה כדי לפגוע בייעוד הגופים המיוחדים או לגרוע מסמכות הנתונה להם לפי דין, ובכלל זה בתחום הגנת הסייבר.

הסדרים הסכמיים בתחום הגנת הסייבר

12. אין באמור בהוראות חוק זה כדי למנוע הסדרה של פעולות לעניין הגנת הסייבר באמצעות הסכמים, ובכלל זה במסגרת הסכמים שבין הגופים המיוחדים או משרד הביטחון לבין ספקיהם.

תוקף

13. חוק זה יעמוד בתוקפו שנתיים מיום פרסומו.

תחולה

14. (א) חוק זה לא יחול על הגופים המיוחדים ועל גוף ציבורי המנוי בסעיפים (2) ו-(3) לתוספת הראשונה לחוק להסדרת הביטחון או בתוספת הרביעית לחוק להסדרת הביטחון; חוק זה לא יחול על ספקים הקשורים בהסכמים כאמור בסעיף 12, המקיימים פעילות החשופה לאיומי סייבר אשר פגיעה בהם עלולה לפגוע בביטחון המדינה ואשר הוסכם בין הממונה על הביטחון במערכת הביטחון לבין מערך הסייבר הלאומי כי ביצוע הפעולות להגנת הסייבר לפי סעיפים אלה תמומש באמצעות הסכמים כאמור בסעיף 12.

(ב) במקרה של מחלוקת לעניין סעיף זה יכריע ראש המטה לביטחון לאומי לפי חוק המטה לביטחון לאומי, תשס"ח-2008.[8]

ביצוע

15. ראש הממשלה ממונה על ביצוע הוראות חוק זה.

תיקון חוק בתי משפט לעניינים מנהליים

16. בתקופת תוקפו של חוק זה יקראו את חוק בתי משפט לעניינים מינהליים, התש"ס-2000, כך שבתוספת הראשונה, אחרי פרט 62, יבוא:

"62. חוק סמכויות לצורך חיזוק הגנת הסייבר הלאומית (הוראת שעה), התש"ף-2020."

דברי הסבר

בהתאם למסגרת המשפטית שלפיה פועל המערך כיום, אין בידיו כלי משפטי ישיר לחייב ארגון לפעול לצורך נקיטת פעולות להגנה מפני תקיפות סייבר, או לצמצם חשיפה הנובעת מאיומי סייבר לאינטרסים חיוניים הנובעים מפעילותו של הארגון. פעילות המערך נעשית בתיאום עם גופי הביטחון השונים האחראים על ההגנה על ביטחון המדינה, ובהתאם לסמכויות הנתונות לגופים אלה.

בהקשר זה יצוין כי מרחב הסייבר הלאומי נתון כל העת לאיומים על תפקודו התקין. בשנה האחרונה עקב התפרצות משבר הקורונה, רמת הסיכון עלתה במידה ניכרת, בין השאר בשל עלייה חדה בהיקף העבודה מרחוק במגזר הציבורי והפרטי, הרחבת הפעילות בזירה הדיגיטלית ותהליכי דיגיטציה מואצים של שירותים ציבוריים ופרטיים. הרחבת הקישוריות באמצעות מרחב הסייבר הרחיבה את "שטח הפנים" הדיגיטלי להגנה, ואת מגוון השירותים החיוניים. לצד זאת, קבוצות תקיפה מדינתיות וגורמי פשיעה מנצלים את המשבר למימוש תקיפות סייבר של מגוון יעדים, בארץ ובעולם, מתוך כוונה לפגוע ברציפות התפקודית של גופים וארגונים בישראל, ובכלל זה באמצעות הזלגת מידע רגיש ושיבושו.

התממשות סיכונים אלו עלולה להוביל לפגיעה במרחב הסייבר, לפגיעה במרחב הפיסי, לפגיעה תפקודית משקית, ואף לפגיעה בחיי אדם.

[8] פורסם ס"ח תשס"ח מס' 2178 מיום 7.8.2008 עמ' 833) ה"ח הממשלה תשס"ח מס' 343 עמ' 230.

סעיף 1

ההגדרות המוצעות עוסקות בשני תחומי תוכן – הגנת הסייבר, וההגנה על אינטרסים ציבורים חיוניים.

ההגדרה "אינטרס ציבורי חיוני" – הגדרה זו נועדה למנות את הערכים שההגנה עליהם נמצאים בבסיס הפעילות והייעוד של מערך הסייבר הלאומי. האינטרסים הציבוריים החיוניים הנזכרים בהגדרה הם נקודת מוצא להפעלת סמכויות המערך המוצעות בחוק, אולם הפעלת הסמכות בפועל מחייבת קיום תנאים נוספים המוגדרים בסעיפים המהותיים. המונח "אינטרס ציבורי חיוני" צריך להיבחן בתוך הקשר ובהתאם לאינטרס הספציפי הנדון. בנוסף, בסעיף 1 להחלטת הממשלה מס' 2444 מיום 15.02.15 בנושא "קידום ההיערכות הלאומית להגנת הסייבר" קבעה הממשלה כי "ההגנה על תפקודו התקין והבטוח של מרחב הסייבר מהווה יעד ביטחוני לאומי חיוני של המדינה ואינטרס ממלכתי חיוני לביטחונה הלאומי". קביעה זו נכונה ביתר שאת כיום לנוכח התרחבות השימוש והתלות בטכנולוגיית מידע ותקשורת לפעילות כלכלית וחברתית. בנוסף, בעת משבר הקורונה התרחשה "טרנספורמציה דיגיטלית" מואצת שבמסגרתה שירותים חיוניים ופעילות עסקית עברו להתבסס על פעילות באמצעים מקוונים במרחב הסייבר. תפקודו התקין של מרחב הסייבר, אם כן, הוא חלק מהאינטרסים הלאומיים החיוניים.

ההגדרה "ארגון שפעילותו חיונית" – הגדרה זו נועדה להבהיר את סמכותו של המערך בכל הנוגע למתן הנחיות מקצועיות לביצוע פעולות הגנת סייבר לפי סעיף 4 לחוק, לגופים שמבצעים פעילות חיונית ושתקיפת סייבר נגדם עלולה לגרום לפגיעה ממשית באינטרס ציבורי חיוני. ההגדרה מוסיפה ומציעה אמות מידה לבחינה מהי פעילותו חיונית, תוך התמקדות במאפיינים כגון החשיבות של הפעילות לכלל הציבור או לחלק משמעותי ממנו, קיום אספקה סדירה של מוצרים ושירותים, או מניעת פגיעה בענף חשוב למשק המדינה . תנאים אלה יש לפרש לפי הקשר ובנסיבות העניין, בשים לב לחשיבות השירות.
כמו כן מוצע לקבוע כי ארגונים שמספקים שירותי מחשוב ותקשורת למדינה ומוסדותיה ולארגונים חיוניים אחרים ייחשבו כארגונים שמבצעים פעילות חיונית. זאת על רקע התובנה המצטברת כי תשתיות מחשוב ותקשורת מהוות כר לתקיפות סייבר משום שהן מאפשרות לתוקף נגישות לארגונים רבים באמצעות תקיפה מוצלחת אחת. תקיפות אלה הפכו נפוצות מאוד והן ידועות כ"תקיפה באמצעות שרשרת האספקה".

הגדרות מקצועיות בתחום הגנת הסייבר - כללי

ההגדרה "הגנת סייבר" – המונח "הגנת סייבר" הוגדר באופן רחב על מנת להקיף את

האמצעים הטכנולוגיים המהווים יעד לתקיפה, ובהם מחשב, חומר המחשב (מידע או תוכנה) ותקשורת הנתונים ממנו ואליו. בהתאם לכך, הגדרה זו נועדה לכלול את כל פעולות ההגנה הנדרשות למנוע תקיפה אפשרית או קונקרטית, לפני תקיפה כאמור, במהלכה ולאחריה.

ההגדרה **"חולשה"** – ההגדרה של המונח "חולשה" עוסק במונח המוכר כ-vulnerability, אולם בהקשר של החוק היא רחבה יותר וכוללת גם פגיעויות המהוות נקודות תורפה אשר ניתן לנצלן כדי לבצע תקיפת סייבר. ככלל, חולשה היא למעשה "באג" שמאפשר לגורם זדוני להשתמש במחשב, בחומר מחשב או בתקשורת נתונים בניגוד לאופן הפעולה התקין שלהם, ולבצע בהם שימוש לרעה. מעת שמפורסמת חולשה, מחל מרוץ בין המגנים לתוקפים. המגנים נדרשים להתמודד עם החולשה, בין בהתקנת "טלאי" אבטחה, ובין בהגדרת בקרות מפצות אחרות.
ההגדרה המוצעת של המונח "חולשה" מתייחסת הן לחולשות באמצעי עצמו, למשל חולשה במחשב, בחומר מחשב (ובכלל זה תוכנה) או בפרוטוקול תקשורת, והן לחולשות שנובעות מהתצורה של מערכת המחשבים או מהנהלים הנוגעים להפעלתה.
הגדרות אלה מבוססות על תובנות מקובלות בתחום הגנת הסייבר. בתחום הגנת הסייבר מקובל מסמך ה-CVSS (Common Vulnerability Scoring System)[9] המנוהל בידי ארגון FIRST, ארגון שלא למטרת רווח המאגד ארגוני הגנת סייבר פרטיים וממשלתיים. מטרת מסמך זה לתת כלי לדירוג מאפייני החולשות בתוכנה וחומרתן. בהתאם למסמך זה יש שלושה סוגי מדדים: Base הבוחן את מאפייניה הפנימיים הקבועים של החולשה, Temporal המשקפים את רמת החולשה בזמן נתון, ו – Environmental העוסק במאפייני החולשה ביחס להקשר ארגוני או מגזרי מסויים. ראו עוד בהגדרת "חשיפה קריטית" להלן.
לצד זאת בקהילת האינטרנט ארגון OWASP מקטלג סוגי תקיפות המנצלות חולשות הרלבנטיות לאתרי אינטרנט.[10]

בהקשר של תקיפת סייבר כנגד ארגון, חולשה מהווה פעמים רבות אמצעי להתקנת "ראש גשר" ברשת הארגונית. באמצעות ראש הגשר, מתקין התוקף ברשת הארגון את התוכנות הזדוניות המאפשרות לו שליטה והפעלה מרחוק.[11]
בדרך כלל תוקף המנצל חולשת אבטחה כדי לחדור לארגון, משתמש בה כדי להתקין כלי תקיפה או אמצעי תקיפה נוספים ברשת הארגונית, פעולה הידועה כ"התפשטות רוחבית", ולצדה יצירת ערוץ גישה נוסף שכבר אינו תלוי בחולשה. כך, אם תוקף יצר לעצמו תווך כניסה לארגון, תיקון החולשה בשלב זה כבר לא יהיה מספק מכיוון שהתוקף נמצא בתוך הארגון ואפשרויות הפעולה שלו ברשת הארגונית רחבות יותר.

---

[9] ראו: FIRST, CVSS Common Vulnerability Scoring System version 3.1 User Guide Revision 1, https://www.first.org/cvss/v3-1/cvss-v31-user-guide_r1.pdf

[10] ראו OWASP, Vulnerabilities, What is a vulnerability?, https://owasp.org/www-community/vulnerabilities/

[11] ראו את החיבור: Lockheed Martin, Intelligence Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intursion Kill chains, https://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf

"חשיפה קריטית" – יסודות הגדרת "חשיפה קריטית" מבוססים על תובנות מקובלות בקהילה המקצועית לגבי מדידת החומרה של חולשות וחשיפות, בהתאם למדדים מקובלים, להקשרים הרלבנטיים לפעילות הגנת הסייבר. בהתאם לכך, חשיפה קריטית מתייחסת לשילוב בין חולשה לבין מאפייני סיכון נוספים, שביחד מגדילים את ההסתברות לניצול החולשה ואת עוצמת הנזק הפוטנציאלי לארגון.

בהתאם לתפיסות מקובלות בקהילה המקצועית, מאפיינים אלה מתחלקים לשלושה סוגים: מאפייניה הטכנולוגיים של החולשה; קיומן של שיטות ואמצעים לנצל את החולשה לתקיפת סייבר או למנוע ניצול של החולשה לתקיפת סייבר; ושכיחות החולשה.

במסגרת המאפיינים הטכנולוגיים של החולשה יש להביא בחשבון את התנאים הבאים: הנגישות של התוקף לביצוע התקיפה; המורכבות של התקיפה הנדרשת כדי לנצל את החולשה, לרבות תלות בפעולה מסוימת מצד משתמש וסוג הפעולה, רמת ההרשאה הנדרשת, הצורך בקבלת גישה למספר רב של מחשבים, הצורך באיסוף מידע מקדים כדי לבצע את התקיפה, חלון ההזדמנויות שבו ניתן לנצל את החולשה, הייחודיות של תצורת מערכת המחשבים והמיומנות הנדרשת לניצול החולשה; הצורך להתגבר על מנגנוני הזדהות, לרבות מספר המנגנונים ורמת ההגנה שלהם; מידת ההשפעה של ניצול החולשה על סודיות מידע; מידת ההשפעה של ניצול החולשה על מהימנות מידע; מידת ההשפעה של ניצול החולשה על נגישות מידע. במסגרת הבחינה של שיטות ואמצעים לניצול החולשה או למניעתה יש להביא בחשבון את התנאים הבאים: רמת הבשלות של הכלים והשיטות לניצול החולשה והאפשרות להשתמש בהם למנעד רחב של מצבים; ניצול החולשה בעבר – בארץ או בחוץ לארץ; מודיעין לגבי האפשרות של ניצול החולשה או לגבי זהות התוקף שניצל או מעוניין לנצל את החולשה; הימצאות של טלאי אבטחה לטיפול בחולשה, לרבות מידת האפקטיביות של הטלאי; ומהימנות המידע לגבי החולשה. במסגרת הבחינה של שכיחות החולשה יש לבחון את תפוצת החולשה במשק בכללותו ואת פוטנציאל הנזק הנשקף למשק בכללותו מניצול החולשה, בין היתר בשים לב לרמת הרגישות הלאומית בנקודת זמן ספציפית.

ההגדרה "מידע בעל ערך הגנתי" – בדומה להגדרה של "הגנת סייבר", גם ההגדרה של "מידע בעל ערך הגנתי" נועדה לאפיין את סוגי המידע המקצועי והטכנולוגי המשמש את אנשי הגנת הסייבר לצורך פעילות הגנת הסייבר, כגון איתור תקיפות סייבר, דרכי התמודדות איתן ופעולות לצמצום הנזק בגינן. כך למשל, מידע בעל ערך הגנתי כולל מאפיינים טכנולוגיים שיש בהם כדי להצביע על חשש לתקיפת סייבר, על השיטה, האמצעי לביצועה, המחשב שממנו התבצעה התקיפה או המחשב הנתקף, כתובות פרוטוקול תקשורת וכתובות דואר אלקטרוני שנוגעות לתקיפת סייבר, שמות מתחם (Domain Name) ומען משאבים אחיד (URL) שנוגע לתקיפת סייבר; מידע על חולשת סייבר; ונתונים בשפה ממוחשבת המעידים על מזהים של תבנית תקיפת סייבר.

ההגדרה "פעולות הגנת סייבר" – הביטוי פעולות הגנת סייבר נועד לתאר את הפעולות במחשב או בחומר מחשב שמבצע מגן הסייבר כדי לאתר ולהתמודד עם תקיפת סייבר. פעולות אלה נגזרות מהבנה של דפוסי פעילות התוקף. כך, כדי להוציא לפועל תקיפת סייבר משתמש התוקף בתקשורת הממוחשבת הנכנסת ויוצאת מהארגון הנתקף כדי לנצל חולשה במערכות הארגון ולחדור פנימה. בהמשך לכך התוקף מתקין ברשת הארגון את התוכנות הזדוניות המאפשרות לו שליטה והפעלה מרחוק כדי להשיג את מטרותיו.[12]

על רקע זה, בעת קיומה של תקיפת סייבר או חשש לתקיפה נדרש מגן הסייבר להבין אם אכן התבצעה תקיפה, ואם כן, מה חומרתה וכן הוא נדרש לצמצם את השפעתה. במסגרת זו, המגן נדרש לאתר את המחשבים שנתקפו ברשת הארגונית ואת האופן שבו התבצעה החדירה לרשת, להבין אילו פעולות התוקף מסוגל לבצע בעקבות התקיפה, למנוע מהתוקף את היכולת לבצע פעולות ברשת או להכיל את הנזק, להסיר את כלי התקיפה ולמנוע את הישנותה.

על כן מוצע כי ההגדרה של "פעולה בחומר מחשב" תכלול את כל מגוון הפעולות לצורך איתור תקיפת סייבר וטיפול בה, ובכלל זה מתן הוראות למחשב בשפה קריאת מחשב, כדי לאתר או להתמודד עם תקיפות (כולל הסרת תוכנות זדוניות) סריקה, הקלטה, העתקה ובחינה של חומר מחשב ותקשורת נתונים, וביצוע פעולות לגילוי מתקדם. לעניין זה יודגש כי פעולות אלה יכולות להתבצע גם באמצעות התקנת מחשב או תוכנה ברשת הארגונית הרלוונטית. פעולות אלה אמורות להתבצע בידי הארגון בהתאם להנחיות מקצועיות שיקבל לפי סעיף 4 או 5, או בידי מערך הסייבר הלאומי בהתאם לצו לפי סעיף 6.

ההגדרה "תבנית תקיפת סייבר" – המונח "תבנית תקיפת סייבר" מתייחס לשלבים השונים במעגל החיים של תקיפת סייבר, ובכלל זה הכנה לקראת התקיפה. החלוקה לשלבים האמורים מתבססת על תפיסות מקובלות בקרב קהילת אנשי הסייבר, בין היתר על ההמשגה של ארגון MITRE המכונה MITRE ATT&CK[13], והיא נועדה בין היתר ליצור שפה משותפת בין העוסקים בתחום הגנת הסייבר, לאפיין את ההתנהגות של תוקפים שונים, לסייע בשיפור מערכות הגנת הסייבר ולסייע באיתור מהיר של תקיפות סייבר.

להלן השלבים המרכזיים בתקיפת סייבר בהתאם למסמכים אלה: "איסוף מקדים" על מערכות היעד לקראת תקיפת סייבר; הכנת כלי תקיפת סייבר המתאים למערכות; הגעה אל היעד; השגת גישה ראשונית לרשת הנתקפת; ניצול חולשה ברשת הנתקפת; הוצאה לפועל של תקיפת סייבר; שהייה ברשת; העלאת הרשאות; התחמקות מכלי הגנה; נגישות להרשאות; חשיפת מבנה רשת והכרת המערכות ברשת; תנועה רוחבית ברשת; איסוף מידע; שליטה ובקרה; הזלגת מידע; והשפעה.

---

[12] ראו את החיבור: Lockheed Martin, Intelligence Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intursion Kill chains, https://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf

[13] ראו: MITRE Att&ck, https://attack.mitre.org/

ההגדרה "תקיפת סייבר" – לנוכח ריבוי הטכניקות הקיימות כיום לביצוע תקיפות סייבר מוצע כי הגדרה זו תכלול את מגוון הפעולות שמטרתן היא פגיעה בפעילות של מחשב או השפעה עליה. פעילות זו אסורה בהתאם לדינים אחרים האזנת סתר לתקשורת נתונים, פגיעה בתקשורת נתונים או השפעה עליה; פגיעה בסודיות מידע, מהימנותו ונגישותו; הפרעה לחיבור של מחשב לרשת תקשורת או מניעת חיבור כאמור; וחדירה אסורה לחומר מחשב שלא כדין כמשמעותה בסעיף 4 לחוק המחשבים, התשנ"ה-1995.

ההגדרה של "תקיפת סייבר חמורה" – תקיפת סייבר חמורה היא תקיפת סייבר שתוחלת הנזק שלה היא גבוהה באופן יחסי לתקיפות סייבר אחרות או שהאינטרס הציבורי הכרוך בטיפולה הוא גבוה במיוחד. ההגדרה כוללת ארבע חלופות: 1) תקיפת סייבר שתוחלת הנזק שלה לאינטרס חיוני היא משמעותית. במסגרת הבחינה של חלופה זו יש לבחון את מכלול המאפיינים של התקיפה, ובכלל זה רמת התחכום של התקיפה, העדרם של אמצעים טכנולוגיים זמינים לטיפול בתקיפה ולצמצום הנזקים ממנה, משך הזמן שנדרש להיערכות להגנה מפני התקיפה או משך הזמן שנדרש לטיפול בתקיפה; 2) תקיפת סייבר אשר עלולה להתפשט למחשבים רבים אחרים; 3) תקיפת סייבר שמכוונת כלפי ארגון חיוני; 4) תקיפה שיש בה כדי לסכן את הביטחון הלאומי בשל כך שהיא מבוצעת בידי אויב מדינתי, ארגון טרור או ארגון משמעותי אחר.

סעיף 2

מוצע לאפשר לראש מערך הסייבר הלאומי למנות עובד בכיר מבין עובדי המערך שיהיה אחראי על קבלת החלטות וביצוע פעולות לצורך הגנת הסייבר כמפורט בחוק. הביטוי "עובד בכיר" מכוון לכך שנדרש למנות לתפקיד זה מי שמוגדר כבכיר בכללי שירות המדינה, כביטוי לאחריות הרבה שמייחס המערך לפעולות הגנת סייבר שמבצע המערך לפי החוק המוצע.

סעיף 3

מוצע לאפשר לראש מערך הסייבר הלאומי למנות עובד בעל הכשרה מתאימה לתפקיד של "עובד מוסמך" כדי לבצע פעולות בחומר מחשב בהתאם לצו של בית המשפט. בשונה מגורם אחראי, עובד מוסמך הוא בעל יכולת ביצוע פעולות בחומר מחשב בעצמו. כמו כן מוצע לקבוע דרישות סף לתפקיד, וכן לקבוע כללים להתנהלות של עובד מוסמך מול ארגונים ונושאי משרה בעת מילוי תפקידו.

סעיף 4

סעיף זה מסמיך את הגורם האחראי להנחות ארגון שפעילותו חיונית לבצע פעולות הנדרשות לטובת הגנת הסייבר בארגון אם קיימת בארגון חולשה שעולה כדי חשיפה קריטית אשר עלולה לסכן אינטרס ציבורי, והארגון אינו נוקט בפעולות הנדרשות לטיפול בחשיפה.

במסגרת הפעלת שיקול הדעת המינהלי לפי סעיף זה, על המערך להביא בחשבון, בנוסף לשיקולים הרלוונטיים להגדרה של "חשיפה קריטית", גם את המאפיינים הבאים: פוטנציאל הנזק הנשקף לארגון בשל החולשה, ובכלל זה נזק פיזי למערכת, או פגיעה ברציפות התפקודית של הארגון; השפעת החולשה על משאבי המיחשוב בארגון; ומידת ההשפעה של ניצול חולשה בארגון על סודיות, מהימנות ונגישות מידע.

ההנחיות המקצועיות שיינתנו לפי סעיף זה כוללות את מגוון הפעולות אשר נדרש לבצע לטובת הגנת סייבר, ובכלל זה ביצוע עדכוני אבטחה למחשבים בארגון, הגבלת גישה למחשבים קריטיים בארגון, הוראות לסגירת חולשה, החלפת סיסמאות, סריקה של תקשורת נתונים לצורך ניטור חשש לניצול החולשה או פעולות הנובעות מניצולה, הגדרת אימות רב-שלבי, פעולות להגנת התקשורת הארגונית, הטמעת אמצעי הגנה רלבנטיים, עדכון מערכת האנטי וירוס, חסימת מזהים או שינויים נדרשים בתהליכים. על הנחיות אלה להיות קשורות במישרין להתמודדות עם איתור החשיפה הקריטית או התמודדות עמה.

סעיף 5

סעיף זה מסמיך את הגורם האחראי להנחות ארגון לבצע פעולות הנדרשות לטובת הגנת הסייבר בעת התרחשות של תקיפת סייבר חמורה או לקראת התרחשותה. הפעולות שתצאנה אל הפועל מכוח ההנחיות המקצועיות של הגורם האחראי תבוצענה בידי נציג הארגון הנתקף או גורם אחר מטעמו, היינו ללא פעולה ישירה בחומר מחשב בידי עובד מערך הסייבר הלאומי. סבר הגורם האחראי כי נדרש לבצע פעולה על ידי עובד מוסמך של המערך, נדרש לבקש צו לפי סעיף 6 או לקבל את הסכמת הארגון לביצוע הפעולה על ידי המערך.

סעיף 6

סעיף זה מסמיך את הגורם האחראי לפנות לבית המשפט בבקשה למתן צו שיפוטי שיאפשר לעובד מוסמך מטעם מערך הסייבר הלאומי לבצע בעצמו פעולות בחומר מחשב במערכות הממוחשבות של הארגון או ליתן הוראות אחרות נדרשות. בקשה כאמור תוגש לבית המשפט רק בהתקיים אחד התנאים המנויים בסעיף, ובית המשפט יקבל את הבקשה רק אם הוכח כי הפעולות בחומר מחשב המבוקשות על ידי הגורם האחראי נדרשות לצורך מניעת פגיעה באינטרס ציבורי חיוני. על בית המשפט להביא בחשבון, בין היתר, את השיקולים המנויים בסעיף 8 לחוק. מנגנון זה יאפשר למערך הסייבר הלאומי למלא את ייעודו ולטפל בתקיפות סייבר חמורות או לטפל במקרים של חשיפה קריטית גם אם ארגון מסרב לכך, או לבצע פעולות להגנת סייבר כאמור במקרים שבהם לא ניתן להשיג את התכלית באמצעות הנחיות מקצועיות בלבד.

כמו כן, מוצע לקבוע כי בסמכות בית המשפט לאפשר לעובד מוסמך לבצע פעולות עזר הנגזרות מהצו, כגון כניסה למקום ותפיסת חפץ לצורך ביצוע פעולות בחומר מחשב המנויות בצו, ובתנאי שהדבר התבקש במפורש ואושר בידי בית המשפט.

בקשות מטעם מערך הסייבר הלאומי למתן צו לפי סעיף זה תוגשנה לבית המשפט לענינים

מינהליים, וכך גם מוצע להחיל על בקשות אלה את סדרי הדין שחלים בבית המשפט לענינים מינהליים, לרבות דיון על יסוד תצהירים ואפשרות לעריכת דיון בדלתיים סגורות או במעמד צד אחד, שבמסגרתו רשאי בית המשפט לקבל מידע והסברים מנציג היועץ המשפטי לממשלה או מגורם אחראי, אף בהיעדר יתר בעלי הדין. בהתאם לכך, מוצע לבצע תיקון לתוספת הראשונה לחוק בתי משפט לענינים מינהליים.
כמו כן, מוצע להסמיך את שר המשפטים לקבוע בתקנות סדרי דין לעניין הליכים לפי סעיף זה, ככל שהדבר יידרש.

סעיף 7
ככלל, מערך הסייבר הלאומי אינו אוסף מידע מוגן פרטיות לצורך ביצוע תפקידו, אלא מידע טכני שיש בו כדי לסייע להגנת סייבר, אשר הוגדר בחוק כ"מידע בעל ערך הגנתי". עם זאת, לעתים עלול להגיע לידי המערך מידע מוגן פרטיות כ"תופעת לוואי" של ביצוע פעולות הגנה. ודוק, פעולות הגנה רבות דורשות לבצע סריקה ממוחשבת, שבסופה מופק פלט הכולל מידע בעל ערך הגנתי, ובכלל זה מידע על אודות קיומה של תקיפה או סממנים לה.
בהתאם למוצע בהוראת שעה זו, ועל מנת להקטין כמה שיותר את החשש לפגיעה בפרטיות, מוצע שמידע מוגן פרטיות ייאסף על ידי המערך בנסיבות מצומצמות המנויות בסעיף, הנחלקות לשלושה סוגי מקרים: מקרים שבהם פוטנציאל הפגיעה בפרטיותו של אדם מזוהה הוא נמוך מאוד למול התועלת להגנת הסייבר, מקרים שבהם הפעילות מותרת לפי דין אחר המסדיר את ההגנה על הפרטיות, ומקרים שבהם לנוכח הרצון להקטין כמה שיותר את החשש לפגיעה בפרטיות, יידרש אישור שיפוטי בנסיבות שבהן אין דרך אחרת לבצע את פעילות הגנת הסייבר.
באשר למקרים מהסוג הראשון, מוצע לקבוע כי המערך רשאי לאסוף מידע מוגן פרטיות בנסיבות הבאות: איסוף של מידע בעל ערך הגנתי לגבי המאפיינים הטכנולוגיים של תקיפת סייבר, ובכלל זה המחשב שממנו התבצעה התקיפה או המחשב הנתקף, כתובות פרוטוקול תקשורת וכתובות דואר אלקטרוני שנוגעות לתקיפת סייבר, שמות מתחם (Domain Name) ומען משאבים אחיד (URL) שנוגעים לתקיפת סייבר; איסוף מידע שנוגע לשלבים השונים ב"מעגל החיים" של תקיפת סייבר; מקרים שבהם האיסוף מותר על פי דין אחר ואיסוף מידע באישור בית משפט, בכפוף לשיקולים המנויים בסעיף 8, ובפרט הצורך באיסוף של מידע מוגן כדי להגן על אינטרס ציבורי חיוני מול הפגיעה הנובעת מכך לפרטיותו של אדם.
עוד מוצע להבהיר כי המידע הפרטי שייאסף לפי החוק ישמש רק לצרכי הגנת הסייבר. כמו כן הסעיף קובע תנאים להעברת מידע שייאסף לפי החוק בהתאם לגוף המקבל את המידע ובהתאם לסוג המידע.

סעיף 8
מוצעות אמות מידה להבניית שיקול הדעת של גורם אחראי במערך בבואו להנחות ארגון, וכן להבניית שיקול הדעת של בית המשפט בבואו לדון בבקשה של גורם אחראי להוציא צו

לביצוע פעולות הגנת סייבר שעשוי לפגוע בזכויות של ארגון או של אדם כתוצאה מביצוע הפעולה המבוקשת בצו. בטרם קבלת החלטה על הגורם האחראי או השופט, לפי העניין, לשקול את מכלול השיקולים הרלבנטיים לעניין זה, ובין השאר את מאפייני הארגון, את מהות האינטרס החיוני המוגן ואת עוצמת הסיכון הנשקף לו כתוצאה מתקיפת סייבר, את ההתאמה בין פעולת ההגנה המבוקשת לבין הטיפול בתקיפה, ואת האפשרות של הארגון או מי מטעמו להשיג את תכלית הפעולה באמצעות אדם בעל ידע ומומחיות מטעם הארגון, ללא צורך בביצוע הפעולה על ידי עובד מוסמך מטעם המערך.

סעיף 9

סעיף זה מסמיך גורם אחראי לפנות לספק גישה לאינטרנט ולקבל מידע לגבי ארגון, שהוא לקוח של הספק, ופרטי קשר עמו. קבלת מידע לפי סעיף זה מוגבלת לנסיבות שבהן הגורם האחראי, על בסיס המידע שמצוי בידיו, מידע לגבי כתובות IP מסוימת, סבור כי מתרחשת תקיפת סייבר נגד הלקוח או כי קיימת חשיפה קריטית אצל הלקוח. המידע על אודות זהות הלקוח ופרטי הקשר עמו נועד לאפשר למערך לסייע לארגון בביצוע עדכוני התוכנה או לבצע פעילויות הגנה הנדרשות לצמצום החשיפה או לטיפול בתקיפה, לפי העניין.

לנוכח החשיבות של טיפול מהיר בתקיפה או בחולשה הקריטית בנסיבות מסוימות, מוצע לקבוע כי העברת המידע מספק הגישה לאינטרנט לידי המערך תתבצע ככלל בתוך 72 שעות, ואם מדובר בחשד לתקיפת סייבר חמורה – בתוך 24 שעות.

עוד מובהר כי אין להעביר למערך פרטי קשר או פרטים אחרים על אודות לקוח שהוא יחיד. בהתאם לדין הקיים, שירות הביטחון הכללי מקבל מידע זה מספקיות התקשורת, כחלק מביצוע תפקידיו בתחום הסייבר והגנת הסייבר. על כן לצורך יעילות הפעילות מול ספקיות התקשורת מוצע כי ברירת המחדל היא כי המערך יקבל מידע זה משירות הביטחון הכללי, המקבל מידע זה בהתאם לייעודו. עוד מוצע להבהיר כי ההסדר המנהלי שבין שירות הביטחון הכללי לבין מערך הסייבר הלאומי על קבלת מידע זה, אינו מקנה עילה לספק תקשורת לסרב לפנייה של מערך הסייבר הלאומי, ככל שהתקבלה כזו.

סעיף 10

שירות הביטחון הכללי מופקד במסגרת תפקידו ובכפוף לייעודו גם על פעולות בתחום הגנת הסייבר. בהתאם לכך מוצע לקבוע שעובד בכיר בשירות הביטחון הכללי שנקבע לכך, יוכל במקרים קונקרטיים ועל פי היתר מאת ראש השירות להפעיל סמכויות לפי סעיפים 5 ו-6 לחוק בתנאים הקבועים בחוק לשם מילוי תפקידי השירות לפי סעיף 7(ב)((1) לחוק שירות הביטחון הכללי, התשס"ב-2002.

סעיף 11

מטרת הסעיף להבהיר שאין בחוק הנוכחי כדי למנוע או להגביל פעילויות שמבצע המערך או אחד מהגופים המיוחדים לפי דין אחר.

המערך פועל כיום לפי החוק להסדרת הביטחון בגופים ציבוריים, התשנ"ח-1998 כלפי הגופים המנויים בתוספת החמישית לחוק זה, וכלפי שאר המשק לפי התפקידים שהטילה עליו הממשלה לפי חוק-יסוד: הממשלה ובכפוף למסגרת שנקבעה בהחלטות הממשלה בתחום הסייבר ולעקרונות ה-CERT הלאומי, אשר תואמו עם היועץ המשפטי לממשלה. מסגרת זו מבוססת על עבודה בהסכמה מדעת מול ארגוני המשק תוך יישום של עקרונות אחריותיות ובכלל זה התייחסות מיוחדת לאיסוף ולעיבוד של מידע מוגן ואופן השימוש בו.

הגופים המיוחדים פועלים כיום בהתאם לסמכויותיהם וייעודם הבטחוני גם בתחום הגנת הסייבר, ואין הכוונה בחוק זה לגרוע מסמכויותיהם או לשנות את אופן פעולתם.

מערך הסייבר הלאומי ממוקד בקידום ההגנה על גופי המשק, בשיתוף מידע בעל ערך הגנתי ובטיפול בתקיפות חמורות המסכנות פעילות חיונית. בינו לבין הגופים המיוחדים מופעלים הסדרי תיאום ומנגנוני תיאום שוטפים, העברות מידע רלבנטי להגנת הסייבר, והסדרה שמטרתה אחדות הפעולה. הסדרים אלה נדרשים ליכולת עדכון ושינוי מעת לעת, בהתאם למתאר האיומים המתפתח והמשתנה, וכמענה לדינאמיות הרבה בתחום זה.

סעיף 12

ארגון הרוכש שירותים שיש בהם חשיפה לסיכוני סייבר, נדרש להסדיר את מסגרת סיכוני הסייבר במסגרת הסכם הרכש. היבט זה של הגנת הסייבר ידוע כהגנה מפני סיכוני "שרשרת האספקה". הגנת זו מבטאת את הצורך להתמודד עם תקיפות שמנצלות חולשות אצל ספקים, כאמצעי כניסה לארגון.

כך, ארגונים שעשויים להיות מוגנים מאוד במערכותיהם שלהם, עלולים להיחשף לסיכונים הנובעים מפעילות מיחשוב או קישוריות של ספקים שלהם. במשק כלכלי מתקדם שבו יש חשיבות למיקור חוץ לגופים כלכליים בעלי יתרון יחסי, נדרש אם כן לאפשר מיקור חוץ ולצד

זאת, לנהל את הסיכונים הנובעים מהיבט הסייבר.
מטרת הסעיף האמור להבהיר כי החוק לא מיועד להתערב בהוראות הסכמיות – חוזיות, שגופים כוללים בהסכמים שלהם, ובפרט לעניין ספקי הגופים המיוחדים וספקי מערכת הביטחון.
מערכת הביטחון מסדירה את הדרישות מספקים הקשורים להגנה על אינטרסים בטחוניים כחלק ממכלול הסכמי הרכש, ובכלל זה גם בהיבטי סייבר. הסעיף מבהיר כי החוק לא נועד לפגוע בהוראות חוזיות אלה, להתערב בהן או להשפיע עליהן. הוראות אלה מעוצבות באופן ספציפי בהתאם למאפיינים המקצועיים הכלכליים והמשפטיים של ההתקשרות, ולכן מבטאות מסגרת ספציפית לטיפול בסיכוני הסייבר.

סעיף 13

מוצע כי החוק יקודם כהוראת שעה והוא יעמוד בתוקפו לשנתיים מעת קבלתו.

סעיף 14

מוצע כי הסמכויות המוצעות בחוק למערך הסייבר הלאומי לא יחולו לעניין הגופים המיוחדים, שבהתאם להחלטות הממשלה בתחום הסייבר, אחראים על הגנת הסייבר של עצמם.
הגופים המנויים בפרט (2) ו-(3) לתוספת הראשונה לחוק להסדרת הביטחון בגופים ציבוריים הם גופים המונחים על ידי הממונה על הביטחון במערכת הביטחון מכוח סעיף 18 לחוק זה. לנוכח מאפייני הפעילות של גופים אלה ולנוכח החלטות הממשלה בתחום הסייבר, גופים אלה מצויים באחריותו המלאה של הממונה על הביטחון במערכת הביטחון, כולל בהיבטי סייבר, ומוצע כי החוק לא יחול עליהם.
לצד גופים אלה, יש ספקים של מערכת הביטחון המספקים רכיבים או שירותים בעלי רגישות בטחונית שפגיעה בהם עלולה לגרום לפגיעה בבטחון המדינה, אולם אינם מנויים בצו האמור, וזאת גם משום שמדובר בספקים המשתנים מעת לעת, וכי הם מבצעים גם פעילות שאינה רק עבור משרד הביטחון.
לאחר בחינה של אופן הטיפול בהגנת הסייבר בגופים מעורבים אלה, נקבע בין מערך הסייבר הלאומי לבין הממונה על הביטחון במערכת הביטחון עקרונות לטיפול בהיבטי הגנת הסייבר בגופים אלה. בהתאם לכך, החוק המוצע לא יחול על גופים אשר נקבע בהסדרה שבין מערך הסייבר הלאומי לבין הממונה על הביטחון במערכת הביטחון כי ניתן להסדיר את הסיכונים לבטחון המדינה בשל תקיפת סייבר נגדם בדרך שבה הם מטופלים כיום, קרי הוראות הסכמיות הכלולות במסגרת הוראות הרכש של משרד הביטחון. בהתאם לכך, הממונה על הביטחון במערכת הביטחון יהיה אחראי לבצע פעולות הגנה נדרשות, וזאת מכוח אותם חוזים. במקרים אלה החוק לא יחול, והסמכות תהא נתונה לממונה על הביטחון במערכת הביטחון בלבד.

סעיף 15

מוצע כי השר הממונה על ביצוע החוק יהיה ראש הממשלה.

סעיף 16

מוצע לתקן את התוספת הראשונה לחוק בתי המשפט לענינים מינהליים, לתקופת תוקפה של הוראת השעה, על מנת להבהיר שביקורת שיפוטית על החלטות המערך לפי חוק זה תתבצע באמצעות הגשת עתירה מינהלית בהתאם להוראות חוק ותקנות בתי המשפט לענינים מינהליים.