# רשומות

# הצעות חוק

## ה מ מ ש ל ה



עמוד

הצעת חוק התמודדות עם תקיפות סייבר חמורות במגזר השירותים הדיגיטליים ושירותי האחסון (הוראת שעה – חרבות ברזל), התשפ"ד–2023 ..... 358

# הצעת חוק התמודדות עם תקיפות סייבר חמורות במגזר השירותים הדיגיטליים ושירותי האחסון (הוראת שעה – חרבות ברזל), התשפ"ד–2023

הגדרות

**1.** בחוק זה –

"חומר מחשב", "מחשב", "פלט" ו"תוכנה" – כהגדרתם בחוק המחשבים;

## דברי הסבר

**כללי** ביום כ"ב בתשרי התשפ"ד (7 באוקטובר 2023), פתחו ארגוני טרור במתקפה רצחנית נגד כוחות הביטחון ואזרחי מדינת ישראל. מתקפה זו גבתה את חייהם של מאות אזרחים ושיבשה את מערך החיים בחזית ובעורף במדינה. בעקבות מתקפה זו הכריז שר הביטחון, באותו היום, על מצב מיוחד בעורף, מכוח סמכותו לפי סעיף 9ג(ב)(1) לחוק ההתגוננות האזרחית, התשי"א–1951. בהתאם לסעיף 9ג(א)(5) לאותו חוק, החליטה ועדת החוץ והביטחון של הכנסת, ביום כ"ז בתשרי התשפ"ד (12 באוקטובר 2023), לאשר את ההכרזה בשטחה של כל מדינת ישראל, והכרזה זו מוארכת מזמן לזמן. כמו כן, הוכרז בצבא הגנה לישראל (להלן – צה"ל) על מבצע "חרבות ברזל", וועדת השרים לענייני ביטחון לאומי החליטה על נקיטת פעולות צבאיות משמעותיות, בהתאם לסעיף 40 לחוק־יסוד: הממשלה, והודיעה לגביהן לוועדת החוץ והביטחון של הכנסת ביום כ"ג בתשרי התשפ"ד (8 באוקטובר 2023) (להלן – הפעולות הצבאיות המשמעותיות).

במסגרת הפעולות הצבאיות המשמעותיות המתמשכות מאז המועד האמור, מתחוללת עלייה גם בהיקף ובעוצמה של תקיפות סייבר נגד גופים אזרחיים במשק הישראלי. מטרת תקיפות סייבר אלה היא לפגוע, כחלק מהמתקפה המשולבת המכוונת כלפי חוסנה של מדינת ישראל, גם בכלכלה ובתפקודו התקין של המשק הישראלי. תקיפות סייבר עלולות להביא לפגיעה במרחב הסייבר, לפגיעה בעולם הפיזי (למשל פגיעה במערכות רפואיות או בתשתיות אנרגיה), לפגיעה קשה בתפקוד המשק, ואף לפגיעה בחיי אדם. תקיפות הסייבר הולכות והופכות מתוחכמות יותר, ותוצאותיהן קשות יותר ומורכבות יותר לטיפול.

חברות המספקות שירותים דיגיטליים ושירותי אחסון, כהגדרתם בחוק המוצע, מתאפיינות בחיבוריות גבוהה לגופים רבים במשק הישראלי, לרבות משרדי ממשלה וגופים ציבוריים, ובהם גם גופים ביטחוניים, תשתיות מדינה קריטיות וארגונים חיוניים לתפקודו של המשק, ועוד. בשל חיבוריות זו, הנזק שנגרם מתקיפת חברות אלה עלול להתפשט ולהשפיע על חברות רבות במשק.

נוסף על כך, למרות רגישותן וחשיבותן המשקית של חברות אלה, אין כיום גורם ממשלתי האמון על הסדרת פעילותן בכל הנוגע להגנת הסייבר. לעניין חברות כאמור המחזיקות או מעבדות מידע אישי, קיימת הסדרה של פעילות זו על ידי הרשות להגנת הפרטיות.

בנסיבות אלה, ספקים של שירותי אחסון ושל שירותים דיגיטליים מהווים יעד מועדף לתקיפות סייבר. בייחוד בתקופת הלחימה הנוכחית, תקיפות סייבר חמורות נגד ספקים אלה עלולות להביא לפגיעה רחבה בביטחון המדינה, בביטחון הציבור או בקיום האספקה והשירותים החיוניים.

כדי להתמודד עם הצורך המתואר לעיל, התקינה הממשלה, ביום י"ד בכסלו התשפ"ד (27 בנובמבר 2023), את תקנות שעת חירום (חרבות ברזל) (התמודדות עם תקיפות סייבר חמורות במגזר השירותים הדיגיטליים ושירותי האחסון), התשפ"ד–2023 (להלן – תקנות שעת החירום), אשר מסמיכות עובד מוסמך במערך הסייבר הלאומי, בשירות הביטחון הכללי או במלמ"ב (להלן – הגופים), להודיע לספק על קיומו של חשש לתקיפת סייבר חמורה נגדו, ובהמשך לכך, במקרים מסוימים, לתת לספק הנתקף הוראות לצורך איתור התקיפה, מניעתה או בלימתה. החוק המוצע נועד להחליף את תקנות שעת החירום.

מוצע כי אם גורם מוסמך קבע שתקיפת סייבר שמתרחשת או עומדת להתרחש נגד ספק שירותי אחסון או שירותים דיגיטליים, היא תקיפת סייבר חמורה, אזי יוכל עובד מוסמך כהגדרתו המוצעת להודיע לספק על התקיפה. על פי המוצע, הגורם שמוסמך לקבוע אם תקיפת סייבר נגד ספק כאמור היא תקיפת סייבר חמורה הוא מנהל מוסמך – גורם בכיר בתחום הסייבר במערך הסייבר הלאומי, בשירות הביטחון הכללי או במלמ"ב (להלן – הגופים), כמפורט בהגדרה המוצעת. המנהל המוסמך יקבע כי התקיפה היא תקיפת סייבר חמורה אם מצא כי יש חשש ממשי שיש בה כדי לפגוע בביטחון המדינה, ביטחון הציבור או בקיום האספקה והשירותים החיוניים, וזאת בשל מאפייניה, לרבות מיתאר התקיפה או זהות התוקף; בשל התרחשותה במהלך תקופת הפעולות הצבאיות המשמעותיות; ובשל קיומו של חשש ממשי שהיא בעלת השפעה משמעותית שאינה מוגבלת לספק הנתקף. אם קבע כאמור, יוכל עובד מוסמך מאותו גוף שעימו נמנה המנהל המוסמך, להודיע לספק, על קיומו של חשש כאמור.

בהמשך לכך, אם הודיע העובד המוסמך כאמור, וככל שהספק הנתקף לא יפעל באופן הולם ובתוך פרק זמן סביר לטיפול בתקיפת הסייבר החמורה או יגיש תצהיר בדבר יישום הנחיות אבטחה בתקן רלוונטי (כמפורט להלן בדברי ההסבר לסעיף 3 להצעת החוק), יהיה רשאי העובד המוסמך לתת לספק הנתקף הוראות לביצוע פעולה לצורך איתור התקיפה, מניעתה או בלימתה.

"חוק המחשבים" – חוק המחשבים, התשנ"ה–1995[1];

"חוק להסדרת הביטחון" – חוק להסדרת הביטחון בגופים ציבוריים, התשנ"ח–1998[2];

"מלמ"ב" – הממונה על הביטחון במערכת הביטחון כמשמעותו בסעיף 21 לחוק להסדרת הביטחון;

"מנהל מוסמך" – אחד מאלה או ממלא מקומו:

(1) ראש יחידת המודיעין וההכוונה בחטיבת איומי סייבר בשב"כ;

(2) ראש מרכז תגובה (IR) במערך הסייבר;

(3) ראש היחידה הטכנולוגית במלמ"ב;

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

"ספק" – אחד מאלה:

(1) מי שעיסוקו באספקת שירותי אחסון או שירותים דיגיטליים, ומתקיים חיבור פיזי או לוגי, קבוע או עיתי, או שמתבצעת העברת חומר מחשב קבועה או עיתית, ממחשבי הספק למחשבי מקבל שירותיו;

(2) מי שעיסוקו באספקת שירותי תחזוקה, ניהול או בקרה של שירותי אחסון או שירותים דיגיטליים;

"עובד מוסמך" – כל אחד מאלה:

(1) עובד השירות כהגדרתו בחוק שירות הביטחון הכללי, התשס"ב–2002[3], שהוסמך בכתב לעניין חוק זה בידי ראש חטיבת איומי סייבר בשב"כ או בידי ממלא מקומו;

(2) עובד מערך הסייבר שהוסמך בכתב לעניין חוק זה בידי ראש חטיבת ההגנה במערך הסייבר;

## דברי הסבר

נוסף על כך, כדי להבטיח כי יינתנו רק ההוראות החיוניות להתמודדות עם תקיפת הסייבר החמורה אשר פגיעתן בנסיבות העניין היא הפחותה ביותר, מוצע לקבוע את השיקולים שנדרש עובד מוסמך לשקול טרם מתן הוראות לספק. כמו כן, מוצע לקבוע הוראות לעניין סודיות המידע שיתקבל מספק, אפשרויות השימוש בו ומחיקתו.

הנחת העבודה של גורמי הממשלה הנוגעים בדבר היא שמרבית הספקים יטפלו באופן הולם בתקיפת הסייבר החמורה, בוודאי בעת מלחמה, ואם יבקשו אף יינתן להם סיוע והכוונה על ידי הגופים. ברם, החקיקה נועדה להקנות סמכות, בתקופת החירום הכרוכה בפעולות הצבאיות המשמעותיות, לתת הוראות לספקי שירותים דיגיטליים או שירותי אחסון אשר לא יפעלו כך.

בהתאם, מוצע להסדיר את סמכויות מערך הסייבר הלאומי, שירות הביטחון הכללי או הממונה על הביטחון במשרד הביטחון לתת הוראות כאמור, במסגרת הוראת שעה, שתפקע בתום שישה חודשים מיום תחילתו של החוק המוצע, אלא אם כן תוארך תקופה על ידי ראש הממשלה, בצו שייקבע בהתייעצות עם שר הביטחון ובאישור ועדת החוץ והביטחון של הכנסת, לתקופות נוספות שלא יעלו על שלושה חודשים כל אחת ולא יותר משישה חודשים במצטבר, אם מצא כי הדבר נדרש עקב התמשכותן של הפעולות הצבאיות המשמעותיות.

כאמור החוק המוצע בא להחליף את ההסדר שנקבע בתקנות שעת החירום ועל כן מוצע לבטלן.

**סעיף 1** בסעיף זה מוצע לקבוע הגדרות למונחים שנעשה בהם שימוש בחוק המוצע.

החוק המוצע נועד לחול על מי שעיסוקו באספקת שירותי אחסון או שירותים דיגיטליים, בעיקר בשל היותם חלק משרשרת האספקה של גופים רבים במשק הישראלי, כאשר החיבוריות הגבוהה של ספקים אלה עלולה להיות מנוצלת על ידי תוקפים לגרימת נזק רחב היקף.

בהתאם, מוצע להגדיר "ספק", שלגביו יחול החוק המוצע, כמי שעיסוקו באספקת שירותי אחסון או שירותים דיגיטליים בעבור אחרים וכן מתאפיין בחיבוריות גבוהה

[1] ס"ח התשנ"ה, עמ' 366.
[2] ס"ח התשנ"ח, עמ' 348.
[3] ס"ח התשס"ב, עמ' 179.

(3) לעניין ספק של הגופים המנויים בפרטים 2 ו־3 לתוספת הראשונה לחוק להסדרת הביטחון – עובד המלמ"ב שהוסמך בכתב לעניין חוק זה בידי ראש היחידה הטכנולוגית במלמ"ב;

"פעולה להגנת סייבר בחומר מחשב" – מתן הוראות למחשב בשפה קריאת מחשב לצורך הגנת סייבר, ובכלל זה הוראה לסריקה, עיבוד, הסרה של חומר מחשב הנוגע לתקיפת סייבר, התקנת סוג תוכנה שפעולתה מוגבלת לרשת הספק בלבד, חסימה או ניתוק של מחשב, או יצירת עותק של חומר המחשב;

"הפעולות הצבאיות המשמעותיות" – הפעולות הצבאיות המשמעותיות שעליהן החליטה ועדת השרים לענייני ביטחון לאומי לפי סעיף 40 לחוק־יסוד: הממשלה[4], והודיעה לגביהן לוועדת החוץ והביטחון של הכנסת ביום כ"ג בתשרי התשפ"ד (8 באוקטובר 2023);

"צה"ל" – צבא הגנה לישראל;

"שב"כ" – שירות הביטחון הכללי;

"שירותי אחסון" – שירותי אחסון של חומר מחשב הניתנים בעבור אחר, או שירותי אספקת תשתית לאחסון או לעיבוד של חומר מחשב;

"שירותים דיגיטליים" – שירות שהוא אחד מאלה, הניתן בעבור אחר:

(1) שירותי תוכנה לרבות כתיבה, התאמה, שינוי, בדיקה, תמיכה, מחקר ופיתוח;

(2) שירותי ניהול או הפעלה של מערכות מחשבים המשלבות חומרה, תוכנה וטכנולוגיות תקשורת;

(3) שירותי עיבוד נתונים, הזנתם או שחזורם, התקנה והגדרת תצורה של מחשבים, התקנת תוכנה או שירותי הגנת סייבר;

## דברי הסבר

כאמור (למקבלי השירותים), אשר אינה מזדמנת אלא קבועה או עיתית; וכן כמי שעיסוקו באספקת שירותי תחזוקה, ניהול או בקרה של שירותי אחסון או שירותים דיגיטליים.

מוצע להגדיר "שירותי אחסון" כשירותי אחסון של חומר מחשב הניתנים בעבור אחר או שירותי אספקת תשתית לאחסון או לעיבוד של חומר מחשב.

כמו כן מוצע למנות שורה של שירותים שייחשבו ל"שירותים דיגיטליים" לעניין החוק המוצע.

מוצע להגדיר "עובד מוסמך" כעובד מערך הסייבר הלאומי, עובד שירות הביטחון הכללי, ולעניין ספק של הגופים המנויים בפרטים 2 ו־3 בתוספת הראשונה לחוק הסדרת הביטחון – אף עובד המלמ"ב, ובלבד שכל עובד כאמור הוסמך בכתב על ידי גורם בכיר בגוף שעימו הוא נמנה, לעניין החוק המוצע.

עוד מוצע להגדיר את המונח "פעולה להגנת סייבר בחומר מחשב", אשר בהתקיים התנאים לכך העובד המוסמך יהיה רשאי להורות לספק לבצעה. על פי המוצע פעולה כאמור כוללת מתן הוראות למחשב בשפה קריאת מחשב לצורך הגנת סייבר, ובכלל זה הוראות המנויות בהגדרה המוצעת. לעניין התקנת סוג תוכנה שפעולתה מוגבלת לרשת הספק בלבד, אשר נכללת בהגדרה המוצעת, יובהר שבהתאם להנחיית היועצת המשפטית לממשלה מספר 1.2500 מיום י"א בתשרי התש"ף (10 באוקטובר 2019) בדבר "כללים מנחים לגיבוש הסדרים דיגיטליים", שלפיה "הסדר דיגיטלי לא יעדיף ככל הניתן אמצעי טכנולוגי אחד על פני אמצעי טכנולוגי אחר, אם שניהם מגשימים את השימושים והמטרות של אותו ההסדר", מוצע לקבוע שהעובד המוסמך יהיה רשאי להורות על התקנת סוג תוכנה ולא על התקנת תוכנה מסוימת, מקום שבו יש יותר מתוכנה אחת המגשימה את אותם השימושים והמטרות.

על פי המוצע, "תקיפת סייבר" היא פעולה או חשש ממשי לפעולה, שנועדה לפגוע שלא כדין בשימוש במחשב או בחומר מחשב, לרבות הפעולות המנויות בהגדרה המוצעת.

כאמור, מוצע לקבוע שבכל אחד מהגופים יוגדר מנהל מוסמך שיוקנו לו הסמכויות שלהלן:

א. סמכות לקבוע כי תקיפת סייבר שמתרחשת או עומדת להתרחש היא תקיפת סייבר חמורה בהתאם לתנאים המפורטים בסעיף 2 לחוק המוצע;

[4] ס"ח התשס"א, עמ' 158.

(4) אספקה או התקנה של מחשבים או של ציוד בקרה, המהווים חלק ממכונות וציוד תעשייתי;

"תקיפת סייבר" – פעולה או חשש ממשי לפעולה, שנועדה לפגוע שלא כדין בשימוש במחשב או בחומר מחשב השמור בו, לרבות –

(1) שיבוש פעולתו התקינה של מחשב או הפרעה לשימוש בו;

(2) מחיקת חומר מחשב, שינויו, שיבושו או הפרעה לשימוש בו;

(3) אחסון או הצגה של מידע או פלט כוזב, או שיש בהם כדי להטעות, בהתאם למטרות השימוש בהם;

(4) חדירה לחומר מחשב כהגדרתה בסעיף 4 לחוק המחשבים;

(5) האזנת סתר לתקשורת בין מחשבים כמשמעותה בחוק האזנת סתר, התשל"ט–1979[5];

(6) גישה של גורם שאינו מורשה למידע השמור במחשב, ובכלל זה בדרך של פגיעה בתהליך הזדהות, או הוצאתו שלא כדין של מידע לרבות בדרך של העתקתו, על ידי גורם כאמור;

(7) הפרעה או מניעה של חיבור של מחשב לרשת תקשורת.

תקיפת סייבר חמורה

**2.** (א) מנהל מוסמך רשאי לקבוע כי תקיפת סייבר שמתרחשת או עומדת להתרחש היא תקיפת סייבר חמורה, אם מצא כי יש חשש ממשי שיש בה כדי לפגוע בביטחון המדינה, בביטחון הציבור או בקיום האספקה והשירותים החיוניים, ובשל כל אלה (בחוק זה – תקיפת סייבר חמורה):

(1) התרחשותה במהלך תקופת הפעולות הצבאיות המשמעותיות;

(2) קיומו של חשש ממשי שהיא בעלת השפעה משמעותית שאינה מוגבלת לספק הנתקף;

(3) מאפייניה, לרבות מיתאר התקיפה או זהות התוקף.

## דברי הסבר

ב. סמכות לקבוע כי מידע שיתקבל לפי חוק זה לא יימחק בסמוך לאחר סיום הטיפול בתקיפת הסייבר החמורה, בשל היותו מידע על התוקף, התקיפה, מאפייני התקיפה, או אמצעי הטיפול בה או מידע אחר שקבע מנהל מוסמך שהוא חיוני לזיהוי מאפייני תקיפת הסייבר, הכול כמפורט בסעיף 6 לחוק המוצע.

על פי המוצע, המנהל המוסמך במערך הסייבר הלאומי יהיה ראש מרכז תגובה (IR) במערך, המנהל המוסמך במלמ"ב יהיה ראש היחידה הטכנולוגית במלמ"ב, והמנהל המוסמך בשירות הביטחון הכללי (להלן – שב"כ) יהיה ראש יחידת המודיעין וההכוונה בחטיבה לאיומי סייבר בשב"כ.

**סעיף 2** כאמור לעיל, הצעת חוק זו מוצעת על רקע צורך מבצעי שהתעורר בתקופת הפעולות הצבאיות המשמעותיות וכדי למנוע פגיעה בביטחון המדינה, בביטחון הציבור או בקיום האספקה והשירותים החיוניים. על כן, מוצע לקבוע שכדי שעובד מוסמך יהיה רשאי לתת הוראות לפי חוק זה, לא די בכך שמתרחשת תקיפת סייבר, אלא נדרש כי מנהל מוסמך יקבע כי קיים חשש ממשי שאותה תקיפה היא תקיפת סייבר חמורה.

מנהל מוסמך יוכל לקבוע כי תקיפת סייבר שמתרחשת או עומדת להתרחש היא תקיפת סייבר חמורה, אם מצא כי יש חשש ממשי, על בסיס אינדיקציה מודיעינית או מידע אחר, שיש בה כדי לפגוע בביטחון המדינה, ביטחון הציבור או בקיום האספקה והשירותים החיוניים, וזאת בשל כל אלה:

א. העובדה שהיא מתרחשת במהלך תקופת הפעולות הצבאיות המשמעותיות;

ב. קיומו של חשש ממשי שהיא בעלת השפעה משמעותית שאינה מוגבלת לספק הנתקף, כלומר תקיפה

[5] ס"ח התשל"ט, עמ' 118.

(ב) הסמכות הנתונה למנהל מוסמך לפי סעיף קטן (א) תהיה נתונה לראש חטיבת הגנה בסייבר בצה"ל, לעניין תקיפת סייבר שהוא מצא כי יש בה כדי לפגוע ברציפות התפקוד המבצעי של צה"ל, בשל האמור בפסקאות (1) עד (3) של אותו סעיף קטן.

התמודדות עם תקיפת סייבר חמורה

**3.** נקבע לפי הוראות סעיף 2 כי תקיפת סייבר שמתרחשת או עומדת להתרחש, נגד ספק, היא תקיפת סייבר חמורה, והודיע על כך עובד מוסמך לספק, לאחר שהזדהה לפניו, יחולו הוראות אלה:

(1) העובד המוסמך יפרט לפני הספק את התשתית העובדתית והמקצועית לקביעה כאמור, ככל שאין בכך כדי לחשוף מקורות מידע, שיטות או אמצעים;

(2) העובד המוסמך ייתן לספק הזדמנות לפעול באופן הולם לצורך איתור התקיפה, מניעתה או בלימתה, בתוך פרק זמן סביר שיימסר לספק, והכול בהתחשב במאפייני תקיפת הסייבר;

(3) הספק יעדכן את העובד המוסמך בדבר הפעולות שביצע לצורך איתור התקיפה, מניעתה או בלימתה או ימסור לעובד המוסמך תצהיר בנוסח שבתוספת בדבר אספקת שירותי האחסון או השירותים הדיגיטליים ללקוחותיו, או בדבר אספקת השירותים כאמור שהם מושאי התקיפה בלבד, תוך יישום הנחיות אבטחה בהתאם לתקן NIST 800–53 Security and Privacy Controls for Information Systems and Organizations, לעניין כלל השירותים שהוא מספק, או לעניין השירותים כאמור שנגדם בוצעה התקיפה, והכול בתוך פרק זמן סביר כאמור בפסקה (2);

## דברי הסבר

שעלולות להיות לה השלכות על גורמים נוספים. תקיפה תוגדר כבעלת השפעה משמעותית כאמור, בין השאר, אם היא עלולה להתפשט במהירות למחשבים רבים או בשל השפעתה האפשרית על עובדיו של ספק, ספקיו או לקוחות הספק (ובכלל זה, על פעילות גופים חיוניים או תשתיות מדינה קריטיות).

ג. מאפיינים של תקיפת הסייבר, המקנים לה ממד מיוחד של חומרה, כגון מיתאר התקיפה או זהות התוקף.

עוד מוצע לקבוע כי הסמכות הנתונה למנהל מוסמך כאמור לקבוע כי תקיפת סייבר מסוימת היא בגדר תקיפת סייבר חמורה, תהיה נתונה גם לרח"ט הגנה בסייבר בצה"ל, וזאת לעניין תקיפת סייבר שהוא מצא שיש בה כדי לפגוע ברציפות התפקוד המבצעי של צה"ל בשל התנאים כמפורט לעיל.

**סעיף 3** מוצע שאם נקבע כי תקיפת סייבר שמתרחשת או עומדת להתרחש היא תקיפת סייבר חמורה, והודיע על כך עובד מוסמך לספק, לאחר שהזדהה לפניו, יחולו הוראות המסדירות את אופן פעולתו של העובד המוסמך למול הספק, וזאת באופן מדורג, בכמה שלבים כמפורט להלן:

תחילה, העובד המוסמך יפרט לפני הספק את התשתית העובדתית והמקצועית לקביעה שהתקיפה היא תקיפת סייבר חמורה כאמור, ככל שאין בכך כדי לחשוף מקורות מידע, שיטות או אמצעים (פסקה (1)).

לאחר מתן ההודעה לספק על תקיפת סייבר חמורה כאמור, תינתן לספק הזדמנות לפעול באופן הולם לצורך איתור התקיפה, מניעתה מבעוד מועד או מניעת הישנותה, או בלימתה לאחר שהחלה, והכול בתוך פרק זמן סביר שיודיע עליו העובד המוסמך לספק, ובהתחשב במאפייני תקיפת הסייבר החמורה (פסקה (2)).

בהמשך לכך, ובתוך פרק הזמן שהוגדר ונמסר לספק כאמור, הספק יידרש לעדכן את העובד המוסמך בדבר הפעולות שביצע לצורך איתור התקיפה, מניעתה או בלימתה, וזאת בלי שתחול עליו חובה לגלות במסגרת העדכון סוד מסחרי. לחלופין, הספק יוכל למסור תצהיר בנוסח שבתוספת לחוק המוצע, בדבר יישום הנחיות אבטחה, בהתאם לתקן הבין־לאומי NIST 800–53 Security and Privacy Controls for Information Systems and Organizations (פסקה (3)). מדובר בתקן בין־לאומי מקצועי הנותן מענה לתקיפות בעלות רמת מורכבות ועוצמה גבוהה אשר שחקני תקיפה מתקדמים ועתירי משאבים (APT), עשויים לעשות בהן שימוש. התקן כולל הוראות שיש בהן כדי להביא לצמצום משמעותי של התקיפה מהספק הנתקף למקבלי שירותיו, והוא כולל, בין השאר, בקרות ברזולוציה מפורטת, הוראות לעניין ניטור עצמי רציף של חברות, עמידה ברמת הגנה בסייבר והתמודדות עם תקיפות. מדובר בתקינה מוכרת ונגישה, וניתן למצוא מידע על אודותיה באתר מכון התקנים האמריקאי. כמו כן, כדי להנגיש את המידע ביתר קלות, תוצג באתר מערך הסייבר הלאומי הפניה לתקן זה באתר מכון התקנים האמריקאי.

על פי המוצע, התצהיר שהספק יוכל להגיש, אפשר שיתייחס לשירותים מושא התקיפה בלבד, ולא לכלל השירותים שהוא מספק. בכל מקרה, סביר להניח שיידרש שיתוף פעולה של נציגי הספק עם העובד המוסמך לצורך בירור השאלה אילו שירותים הם מושא תקיפת הסייבר

(4) לא מסר הספק תצהיר כאמור בפסקה (3), ומצא העובד המוסמך כי הספק לא פעל באופן הולם לאיתור התקיפה, מניעתה או בלימתה, כאמור בפסקה (2), רשאי העובד המוסמך, אם מצא שהדבר נדרש לצורך איתור התקיפה, מניעתה או בלימתה, ולאחר שהודיע לספק על כוונתו לתת לו הוראות לפי פסקה זו ונתן לו הזדמנות להשמיע את טענותיו, לתת לספק הוראות, בכתב או בעל פה, שיבוצעו בידי הספק, ובכלל זה הוראות לביצוע פעולות להגנת סייבר בחומר מחשב או הוראות למסירת ידיעה או מסמך לרבות העתק מחומר מחשב, לידי העובד המוסמך;

(5) במתן הוראות לספק לפי פסקה (4) –

(א) ישקול העובד המוסמך את השפעתן האפשרית על הזכות לפרטיות, על פעילות הספק ועל צד שלישי, וכן את העלות הכלכלית המוערכת של יישום ההוראות והשפעתן האפשרית על הרציפות התפקודית של הספק, למיטב ידיעתו של העובד המוסמך, ואם הספק מסר הערכה לעניין זה – בהתחשב בהערכה שמסר;

(ב) יורה העובד המוסמך לנקוט אמצעי שפגיעתו פחותה לצורך איתור התקיפה, מניעתה או בלימתה;

(ג) יפרט העובד המוסמך את המועד האחרון לביצוע ההוראה;

(6) נתן עובד מוסמך לספק הוראה לפי פסקה (4), יפעל הספק בהתאם לה עד המועד האחרון שנקבע לביצועה כאמור בפסקה (5)(ג), וידווח על אופן ביצועה לעובד המוסמך עד המועד האמור.

## דברי הסבר

החמורה. יודגש, כי לא יינתנו הוראות מכוח החוק המוצע לספק אשר טיפל באופן הולם באיתור התקיפה, מניעתה או בלימתה, וכן לא יינתנו הוראות לספק אשר מסר תצהיר כאמור. במקרה כזה הספק גם לא יהיה מחויב למסור עדכון לעובד המוסמך על אופן הטיפול בתקיפת הסייבר החמורה שלגביה התריעו לפניו.

עוד מוצע כי אם הספק לא הגיש תצהיר בדבר יישום הנחיות אבטחה בהתאם לתקן כאמור, ואם העובד המוסמך מצא כי הספק הנתקף לא פעל באופן הולם לאיתור התקיפה, מניעתה או בלימתה, יוכל העובד המוסמך להודיע לספק על כוונתו לתת לו הוראות, ולספק תינתן הזדמנות להשמיע את טענותיו לעניין הכוונה לתת לו הוראות מחייבות. החוק המוצע אינו שולל את האפשרות של הגופים לסייע לספק, בהסכמתו, להתמודד עם התקיפה בדרכים אחרות. ואולם אם לאחר שמיעת הספק מצא העובד המוסמך כי הדבר נדרש לצורך איתור התקיפה, מניעתה או בלימתה, הוא יהיה מוסמך לתת הוראות מחייבות לספק שאינו מתמודד באופן הולם עם תקיפת סייבר חמורה או שלא הגיש תצהיר כאמור (פסקה (4)).

בכלל זה, העובד המוסמך יהיה רשאי לתת לספק הוראות שיבוצעו על ידי הספק. יובהר, בעניין זה, כי גם בשלב מתקדם זה של מתן הוראות, החוק המוצע אינו מסמיך את העובד לבצע בעצמו פעולות במחשביו של הספק, וההוראות שייתן העובד צריך שיתבצעו על ידי הספק או עובדיו, ולא על ידי העובד המוסמך או מי מטעמו. בין השאר, יוכל העובד המוסמך לתת לספק הוראות לביצוע פעולות להגנת סייבר בחומר מחשב, או הוראות למסירת ידיעה או מסמך, לרבות העתק מחומר מחשב הנדרש לאיתור, מניעת או בלימת תקיפת סייבר חמורה, לידי העובד המוסמך, וזאת בתנאי שמדובר באמצעי שפגיעתו היא הפחותה ביותר בנסיבות העניין.

מוצע להתוות את שיקול הדעת של העובד המוסמך ולקבוע שבמתן הוראות ישקול העובד המוסמך את השפעתן האפשרית על הזכות לפרטיות של כל מי שמידע אודותיו מצוי בידי הספק, בכלל זה מידע על לקוחות ועובדים, וכן את השפעתן על פעילות הספק ועל צד שלישי כגון לקוחות שנותנים שירותים חיוניים לציבור, ואת העלות הכלכלית המוערכת של יישום ההוראה והשפעתה האפשרית על הרציפות התפקודית של הספק. זאת, למיטב ידיעתו של העובד המוסמך או בהתחשב בהערכה שמסר הספק לעניין זה, אם מסר.

כמו כן, מוצע להדגיש את חובתו של העובד המוסמך לפעול במידתיות. בהתאם לכך, מוצע לקבוע שהוא יורה לנקוט אמצעי שפגיעתו פחותה לצורך איתור התקיפה, מניעתה או בלימתה. במסגרת חובה זו, העובד המוסמך יימנע מפעולות לזיהוי האנשים שהם נושאי המידע שיקבל מהספק, אם הדבר אינו חיוני לצורך איתור התקיפה, מניעתה או בלימתה. יובהר בעניין זה שבמרבית המקרים המידע המתקבל הוא מידע טכנולוגי שאינו מכיל מידע אישי.

לבסוף, מוצע לקבוע שבעת מתן ההוראה לספק, העובד המוסמך יפרט את המועד האחרון לביצועה. עד למועד זה הספק יפעל בהתאם להוראה שקיבל וידווח לעובד המוסמך על אופן ביצועה (פסקאות (5) ו־(6)).

תיעוד

4. עובד מוסמך יתעד בכתב את ההוראות שנתן לספק לפי סעיף 3 וימסור לו נוסח כתוב של ההוראות שאינו מכיל מידע מסווג, בתוך פרק זמן סביר ממתן ההוראה; לעניין זה, "מידע מסווג" – מידע שסיווגו הביטחוני נקבע בידי מערך הסייבר, שב"כ, צה"ל או מלמ"ב, לפי העניין, כסיווג ברמת 'שמור' ומעלה.

אופן הפעלת סמכויות

5. הסמכויות לפי סעיף 3 לעניין תקיפת סייבר מסוימת נגד ספק, או לעניין כמה תקיפות כאמור המתרחשות באותו מועד, יופעלו כלפי הספק בידי עובד מוסמך מקרב גוף אחד, בלבד.

סודיות, הגבלת שימוש ומחיקה

6. (א) אדם שהגיע לידיו מידע שהתקבל מספק לפי חוק זה ישמור אותו בסוד, לא יגלה אותו לאחר ולא יעשה בו כל שימוש, אלא לצורך איתור תקיפת סייבר חמורה, מניעתה או בלימתה.

(ב) מידע שהתקבל מספק לפי חוק זה יימחק בסמוך לאחר סיום הטיפול בתקיפת הסייבר החמורה, אלא אם כן קבע מנהל מוסמך שהמידע כאמור חיוני לזיהוי מאפייני תקיפת הסייבר; מידע שנקבע לגביו כאמור יישמר בהיקף המזערי הנדרש.

(ג) בסעיף זה, "מידע" – למעט מידע על התוקף, התקיפה, מאפייני התקיפה או אמצעי הטיפול בה.

דיווח

7. (א) מערך הסייבר, השב"כ ומלמ"ב ידווחו אחת לשבועיים ליועצת המשפטית לממשלה ולוועדת החוץ והביטחון של הכנסת בדבר המקרים שבהם ניתנו הוראות לספק לפי סעיף 3(4), הנימוק למתן ההוראות וסוגן.

(ב) דיווח לפי חוק זה יהיה חסוי ופרסומו אסור.

שמירת דינים

8. (א) הוראות חוק זה באות להוסיף על הוראות כל דין אחר ולא לגרוע מהן.

## דברי הסבר

**סעיף 4** מוצע לקבוע שהעובד המוסמך יתעד בכתב את ההוראות שנתן לספק וימסור לספק נוסח כתוב של ההוראות שאינו מכיל מידע מסווג, בתוך פרק זמן סביר ממתן ההוראה. המסמך המפרט את ההוראות שניתנו יוכל לשמש את הספק לכל צורך שימצא לנכון בכפוף לכל דין.

**סעיף 5** מוצע לקבוע כי הסמכויות לעניין תקיפת סייבר מסוימת נגד ספק או לעניין כמה תקיפות כאמור המתרחשות באותו מועד, יופעלו כלפי הספק בידי עובד מוסמך מקרב גוף אחד בלבד. זאת במטרה למנוע מצב שבו ספק נדרש לעמוד בקשר, לתת דין וחשבון או למלא אחר הוראות מצד גורמים ממשלתיים שונים, ביחס לאותה תקיפה או במהלך אותו פרק זמן רלוונטי.

**סעיף 6** כדי להגן על הזכות לפרטיות ולקניין של הספקים ולקוחותיהם, מוצע לקבוע כי אדם שהגיע אליו מידע שהתקבל מספק לפי החוק המוצע, תחול עליו חובת סודיות לגבי אותו מידע, והוא לא יוכל לגלותו לאחר או לעשות בו שימוש, אלא לצורך איתור תקיפת סייבר חמורה, מניעתה או בלימתה.

כמו כן, מוצע לקבוע שמידע שיתקבל מספק לפי החוק המוצע באחד הגופים, יימחק בסמוך לאחר סיום הטיפול בתקיפת הסייבר החמורה. יובהר בעניין זה, כפי שצוין לעיל, שבמרבית המקרים המידע המתקבל הוא מידע טכנולוגי שאינו מכיל מידע אישי או סודות מסחריים.

עוד מוצע לקבוע שלמנהל מוסמך בכל אחד מהגופים תהיה סמכות לקבוע, לגבי מידע שהתקבל כאמור מספק, שיש לשמור אותו (על אף החובה העקרונית למוחקו, כאמור לעיל), אם מצא שהוא חיוני לזיהוי מאפייני תקיפת סייבר. אם קבע כאמור, יישמר המידע האמור בהיקף המזערי הנדרש.

לבסוף, מוצע להבהיר כי בכל הנוגע להסדר המוצע לעניין סודיות בסעיף 6 לחוק המוצע, המונח "מידע" אינו כולל מידע על התוקף, התקיפה (לרבות זהות הנתקף), מאפייני התקיפה או אמצעי טיפול בה, ועל כן החובות המפורטות בסעיף זה אינן חלות לגבי מידע כאמור.

**סעיף 7** לשם קיום פיקוח ובקרה שוטפים על פעולותיהם של מערך הסייבר הלאומי, שב"כ ומלמ"ב לפי חוק זה, מוצע להטיל על הגופים האמורים חובת דיווח, אחת לשבועיים, ליועצת המשפטית לממשלה ולוועדת החוץ והביטחון של הכנסת בדבר המקרים שבהם ניתנו הוראות לספק לפי סעיף 3(4) לחוק המוצע. בדיווח כאמור יפורטו הנימוק למתן ההוראות וסוגן. לנוכח מהות המידע ואופיו הרגיש, מוצע לקבוע שדיווחים כאמור יהיו חסויים ויהיה אסור לפרסמם.

**סעיף 8** מוצע, למען הסר ספק, לקבוע שהוראות החוק המוצע באות להוסיף על הוראות כל דין אחר ולא לגרוע מהן. עוד מוצע להבהיר שהוראות החוק המוצע באות להוסיף על כל הוראה בעניין הנוגע להגנת סייבר, לפי

(ב) בלי לגרוע מהאמור בסעיף קטן (א), הוראות חוק זה באות להוסיף על כל הוראה בעניין הנוגע להגנת סייבר, לפי החלטת הממשלה או הסכם, ואולם בכל מקרה של סתירה יגברו הוראות חוק זה.

תיקון חוק בתי משפט לעניינים מינהליים – הוראת שעה

**9.** בתקופת תוקפו של חוק זה, כאמור בסעיף 11, יקראו את חוק בתי משפט לעניינים מינהליים, התש"ס–2000[6], כך שבתוספת הראשונה, בסופה יבוא:

"65. החלטה של רשות לפי חוק התמודדות עם תקיפות סייבר חמורות במגזר השירותים הדיגיטליים ושירותי האחסון) (הוראת שעה – חרבות ברזל), התשפ"ד–2023."

ביטול תקנות שעת חירום (חרבות ברזל) (התמודדות עם תקיפות סייבר חמורות במגזר השירותים הדיגיטליים ושירותי האחסון)

**10.** תקנות שעת חירום (חרבות ברזל) (התמודדות עם תקיפות סייבר חמורות במגזר השירותים הדיגיטליים ושירותי האחסון), התשפ"ד–2023[7] – בטלות.

תוקף

**11.** (א) סעיפים 1 עד 9 לחוק זה יעמדו בתוקפם עד תום שישה חודשים מיום פרסומו.

(ב) ראש הממשלה, בהתייעצות עם שר הביטחון ובאישור ועדת החוץ והביטחון של הכנסת, רשאי להורות בצו על הארכת תקופת תוקפו של חוק זה לתקופות נוספות שלא יעלו על שלושה חודשים כל אחת, אם מצא כי הדבר נדרש עקב התמשכותן של הפעולות הצבאיות המשמעותיות, ובלבד שסך כל תקופות ההארכה לא יעלה על שישה חודשים.

הוראת מעבר

**12.** הוראות שניתנו ופעולות שבוצעו לפי תקנות שעת חירום (חרבות ברזל) (התמודדות עם תקיפות סייבר חמורות במגזר השירותים הדיגיטליים ושירותי האחסון), התשפ"ד–2023, לפני יום תחילתו של חוק זה, יראו אותן כאילו נעשו לפי חוק זה והוראותיו יחולו עליהן.

## דברי הסבר

החלטת ממשלה או הסכם, ואולם, בכל מקרה של סתירה יגברו הוראות חוק זה. כך לדוגמה, אין בחוק המוצע, ובכלל זה בהוראות שיינתנו מכוחו, כדי לגרוע מחובות הדיווח של ספק לפי כל דין או הסכם.

**סעיף 9** כדי לאפשר ביקורת שיפוטית וגישה לערכאות בנוגע להוראות שייתן גורם מוסמך לספק לפי החוק המוצע, מוצע לתקן בתיקון עקיף את התוספת הראשונה לחוק בתי משפט לעניינים מינהליים, התש"ס–2000, כך שבית המשפט לעניינים מינהליים יהיה מוסמך לדון בעתירות בעניין החלטות לפי חוק זה.

**סעיפים 10 עד 12** כאמור, חוק זה נועד לאפשר התמודדות עם העלייה בהיקף ועוצמת מתקפות הסייבר אגב הלחימה המתמשכת במסגרת הפעולות הצבאיות המשמעותיות ובמהלכה. בשים לב לאמור, ומכיוון שלא ניתן לדעת כיום עד מתי תימשך הלחימה, מוצע לקבוע, בסעיף 11 לחוק המוצע, שהחוק יעמוד בתוקפו למשך שישה חודשים מיום פרסומו ברשומות.

כאמור, לפי סעיף 2 לחוק המוצע, אחד התנאים המצטברים להפעלת סמכותו של מנהל מוסמך לקבוע כי תקיפת סייבר מסוימת היא תקיפת סייבר חמורה, הוא התרחשותה במהלך תקופת הפעולות הצבאיות המשמעותיות, כך שגם אם תסתיים הלחימה לפני תום שישה חודשים מיום תחילתו של החוק המוצע, ממילא לא יהיה ניתן להפעיל את הסמכות. מאחר שייתכן שהפעולות הצבאיות המשמעותיות יימשכו מעבר לשישה חודשים כאמור, מוצע להסמיך את ראש הממשלה, בהתייעצות עם שר הביטחון ובאישור ועדת החוץ והביטחון של הכנסת, להורות בצו על הארכת תקופת תוקפו של החוק המוצע בתקופות נוספות שלא יעלו על שלושה חודשים כל אחת, ובלבד שסך כל תקופת ההארכה לא יעלה על שישה חודשים.

הוראות החוק המוצע נועדו להחליף את הוראות תקנות שעת חירום (חרבות ברזל) (התמודדות עם תקיפות סייבר חמורות במגזר השירותים הדיגיטליים ושירותי האחסון), התשפ"ד–2023. לפיכך, מוצע לקבוע כי עם תחילתו של החוק המוצע, הן יבוטלו. לצד ביטול תקנות שעת החירום, וכדי להבטיח את רציפות הדין בין תקנות שעת החירום לבין החוק המוצע, מוצע לקבוע הוראת מעבר שלפיה הוראות שניתנו ופעולות שבוצעו מכוח תקנות שעת החירום האמורות כאילו נעשו לפי חוק זה, והוראותיו יחולו עליהן.

[6] ס"ח התש"ס, עמ' 190.

[7] ק"ת התשפ"ד, עמ' 618.

## תוספת

(סעיף 3(3))

**תצהיר ספק על אספקת שירותי אחסון או שירותים דיגיטליים תוך יישום הנחיות אבטחה בהתאם לתקן NIST 800–53 Security and Privacy Controls for Information Systems and Organizations לפי חוק התמודדות עם תקיפות סייבר חמורות במגזר השירותים הדיגיטליים ושירותי האחסון (הוראת שעה – חרבות ברזל), התשפ"ד–2023**

אני .....‏, נושא/ת ת"ז מס' .....‏, נציג/ת חברת .....‏ (להלן – הספק) משמש/ת בתפקיד .....‏, כתובת .....‏, דוא"ל .....‏, מספר טלפון .....‏, מספר טלפון נוסף .....‏, בהמשך לפניית העובד המוסמך אל הספק מיום ..... בנוגע לתקיפת סייבר חמורה בהתאם לחוק התמודדות עם תקיפות סייבר חמורות במגזר השירותים הדיגיטליים ושירותי האחסון (הוראת שעה – חרבות ברזל), התשפ"ד–2023 (להלן – החוק), לאחר שהוזהרתי כי עליי לומר את האמת וכי אהיה צפוי/ה לעונשים הקבועים בחוק אם לא אעשה כן, במסגרת תפקידי מצהיר/ה בזה בכתב כלהלן:

1. הספק מספק ללקוחותיו שירותי אחסון או שירותים דיגיטליים, כהגדרתם בחוק, או את השירותים כאמור שהם מושאי התקיפה תוך יישום הנחיות אבטחה בהתאם לתקן NIST 800–53 Security and Privacy Controls for Information Systems and Organizations בגרסתו העדכנית ותוך ניהול הסיכונים הרלוונטיים.
2. אם יחול שינוי בנוגע לאמור בתצהיר זה, במהלך התקופה שעד לסיום הטיפול בתקיפת הסייבר החמורה שבגינה נעשתה פנייה לספק, הספק יעדכן את העובד המוסמך בכך בלא שיהוי ובתוך זמן סביר.

אני מצהיר/ה כי השם שלעיל הוא שמי, והחתימה שלמטה היא חתימתי, וכי תוכן תצהירי זה אמת.

..... .....

חתימה תאריך

המחיר 4.86 שקלים חדשים ISSN 0334-3030 סודר במח׳ רשומות, משרד המשפטים, והודפס במדפיס הממשלתי