

1. הגדרות

בחוק זה -

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

"חוק המחשבים" - חוק המחשבים, התשנ"ה-1995;

"חוק להסדרת הביטחון" - חוק להסדרת הביטחון בגופים ציבוריים, התשנ"ח-1998;

"מלמ"ב" - הממונה על הביטחון במערכת 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, ממחשביו 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, שראש חטיבת איומי סייבר

בשב"כ או ממלא מקומו הסמיך בכתב לעניין חוק זה;

(2) עובד מערך הסייבר שראש חטיבת ההגנה במערך הסייבר הסמיך בכתב לעניין חוק זה;

(3) לעניין ספק של הגופים המנויים בפרטים 2 ו-3 לתוספת הראשונה לחוק להסדרת הביטחון - עובד

המלמ"ב שראש היחידה הטכנולוגית במלמ"ב הסמיך בכתב לעניין חוק זה;

"פעולה להגנת סייבר בחומר מחשב" - מתן הוראות למחשב בשפה קריאת מחשב לשם הגנת סייבר, ובכלל זה

הוראה לסריקה, לעיבוד, להסרה של חומר מחשב הנוגע לתקיפת סייבר, להתקנת סוג תוכנה שפעולתה מוגבלת

לרשת הספק בלבד, לחסימה או לניתוק של מחשב, או ליצירת עותק של חומר המחשב;

"הפעולות הצבאיות המשמעותיות" - הפעולות הצבאיות המשמעותיות שעליהן החליטה ועדת השרים לענייני

ביטחון לאומי לפי סעיף 40 לחוק-יסוד: הממשלה, 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 של תוכנה;

(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;
(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, שינוי, 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;
- (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.

2. תקיפת סייבר חמורה

(א) מנהל מוסמך רשאי לקבוע כי תקיפת סייבר שמתרחשת או שיש חשש ממשי כי 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.

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

3. התמודדות עם תקיפת סייבר חמורה

קבע מנהל מוסמך או ראש חטיבת הגנה בסייבר בצה"ל 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 לאיתור התקיפה, מניעתה או בלימתה, בתוך פרק זמן סביר שיימסר לספק, והכול בהתחשב במאפייני תקיפת הסייבר;
- (3) הספק יעדכן את העובד המוסמך בדבר הפעולות שביצע לאיתור התקיפה, מניעתה או בלימתה או ימסור לעובד המוסמך תצהיר בנוסח שפרסם ראש מערך הסייבר באתר האינטרנט של מערך הסייבר בדבר אספקת שירותי האחסון או השירותים הדיגיטליים ללקוחותיו או בדבר אספקת שירותי תחזוקה, ניהול או בקרה של שירותים כאמור, תוך יישום הנחיות אבטחה בהתאם לתקן המנוי בתוספת או לפיה, לעניין כלל השירותים שהוא מספק, או לעניין השירותים כאמור שנגדם בוצעה התקיפה, והכול בתוך פרק זמן סביר כאמור בפסקה (2);

(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 לאיתור 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, שיבצע 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 לאיתור 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 5 עד המועד האמור.

4. תיעוד

עובד מוסמך יתעד בכתב את ההוראות שנתן לספק לפי סעיף 3 וימסור לו נוסח כתוב של ההוראות שאינו מכיל מידע מסווג, בהקדם האפשרי לאחר מתן ההוראה; בסעיף זה, "מידע מסווג" - מידע שסיווגו הביטחוני נקבע בידי מערך הסייבר, שב"כ, צה"ל או מלמ"ב, לפי העניין, כסיווג ברמת 'שמור' ומעלה.

5. אופן הפעלת סמכויות

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.

6. סודיות, הגבלת שימוש ומחיקה

(א) אדם שהגיע לידי מידע שהתקבל מספק לפי חוק זה ישמור אותו בסוד, לא יגלה אותו לאחר ולא יעשה בו כל שימוש, אלא לאיתור 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) פרסום פומבי ברבים של זהות הספק, שהתקבלה לפי חוק זה, יהיה באישור מנהל מוסמך לאחר שנתן לספק הזדמנות להשמיע את טענותיו.

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

7. עונשין

אדם שגילה מידע שהתקבל מספק לפי חוק זה או עשה שימוש במידע שהתקבל מספק לפי חוק זה, תוך כדי מילוי תפקידו או במהלך מילוי תפקידו, בניגוד להוראות סעיף 6(א), דינו - מאסר שלוש שנים.

8. דיווח

(א) מערך הסייבר, שב"כ ומלמ"ב ידווחו ליועץ המשפטי לממשלה ולוועדת החוץ והביטחון של הכנסת, אחת לחודש, על כל

- (1) המקרים שבהם ניתנו הוראות לספק לפי סעיף 3(4), הנימוק למתן ההוראות וסוגן, ומספר המקרים שבהם ספק לא מילא אחר הוראות כאמור;
- (2) מספר המקרים שבהם העובד המוסמך סייע לספק במילוי ההוראות שניתנו לו לפי סעיף 3;
- (3) סוגי הספקים שמנהל מוסמך קבע כי תקיפתם היא תקיפת סייבר חמורה לפי סעיף 2(א);
- (4) מספר המקרים שבהם מנהל מוסמך קבע כי תקיפת סייבר היא תקיפת סייבר חמורה לפי סעיף 2(א), בפילוח בשל פגיעה בביטחון המדינה, פגיעה בביטחון הציבור או פגיעה בקיום האספקה והשירותים החיוניים.
- (ב) דיווח לפי חוק זה יהיה חסוי ופרסומו אסור.

9. שמירת דינים

- (א) הוראות חוק זה באות להוסיף על הוראות כל דין אחר ולא לגרוע מהן.
- (ב) בלי לגרוע מהוראות סעיף קטן (א), הוראות חוק זה באות להוסיף על כל הוראה בעניין הנוגע להגנת סייבר, לפי החלטת הממשלה או הסכם, אולם במקרה של סתירה, יגברו הוראות חוק זה.

10. תיקון חוק בתי משפט לעניינים מינהליים - הוראת שעה - מס' 140

- בתקופת תוקפו של חוק זה, כאמור בסעיף 12, יקראו את חוק בתי משפט לעניינים מינהליים, התש"ס-2000, 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".

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

- תקנות שעת חירום (חרבות ברזל) (התמודדות עם תקיפות סייבר חמורות במגזר השירותים הדיגיטליים ושירותי האחסון), התשפ"ד-2023 - בטלות.

12. תוקף

- סעיפים 1 עד 10 לחוק זה יעמדו בתוקפם עד תום שבעה חודשים מיום פרסומו.

13. הוראת מעבר

- 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.

תוספת

(סעיף 3(3))

1. תקן nist 800-53 security and privacy controls for information systems and organizations ;

2. תקן שראש מערך הסייבר, בהסכמת ראש השב"כ ומלמ"ב, פרסם ברשומות ובאתר האינטרנט של מערך הסייבר, אם פרסם תקן כאמור, ובלבד שיש בו כדי להבטיח ברמת סבירות גבוהה את הגבלת השפעתה של תקיפת סייבר חמורה מעבר לספק הנתקף וטיפול הולם בתקיפות סייבר חמורות.

בנימין נתניהו ראש
הממשלה

יצחק הרצוג נשיא
המדינה

אמיר אוחנה יושב
ראש הכנסת

[1] [ס"ח 3135](#), התשפ"ד (26.12.2023), עמ' 410. הצ"ח - ממשלה 1688, התשפ"ד, עמ' 358.

//