



רשומות

ספר החוקים

26 בדצמבר 2023

3135

י"ד בטבת התשפ"ד

עמוד

חוק התמודדות עם תקיפות סייבר חמורות כתוצאה מתקיפת הדיגיטליים ושירותי האחסון
410
(הוראת שעה – חברות ברול) התשפ"ד-2023 2023-140

תיקונים עקיפים:

חוק בתי משפט לעניינים מינהליים, התש"ס-2000 – מס' 140
תקנות שעט חירום (חברות ברול) (התמודדות עם תקיפות סייבר חמורות כתוצאה מתקיפת הדיגיטליים ושירותי האחסון), התשפ"ד-2023 – ביטול

**חוק התמודדות עם תקיפות סייבר חמורות בגורם השירותים הדיגיטליים
ושירותי האחסון (הוראת שעה – חבות ברזל), התשפ"ד-2023***

הגדרות

1. בחוק זה –

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

"חוק המחשבים" – חוק המחשבים, התשנ"ה-1995¹;

"חוק להסדרת הביטחון" – חוק להסדרת הביטחון בגופים ציבוריים, התשנ"ח-1998²;

"מלמ"ב" – הממונה על הביטחון במערכת הביטחון;

"מנהל מוסמך" – אחד מלאה או ממלא מקומו:

(1) ראש ייחידה המודיעין וההכוונה בחטיבת אiomiy סייבר בשב"כ;

(2) ראש מרכז תגבה (IR) במרכז הסייבר;

(3) ראש היחידה הטכנולוגית במלמ"ב;

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

"ספר" – אחד מלאה:

(1) מי שעיסוקו באספקת שירותים אחסון או שירותים דיגיטליים, ומתקיים חיבור פיזי או לוגי, קבוע או עיתני, או שמתבצעת העברת חומר מחשב קבועה או עיתנית, ממוחשביו למוחשי מקבל שירותיו;

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

"עובד מוסמך" – כל אחד מלאה:

(1) עובד השירותים כהגדרתו בחוק שירות הביטחון הכללי, התשס"ב-2002³, שראש חטיבת אiomiy סייבר בשב"כ או ממלא מקומו הסמיר בכתב לעניין חוק זה;

(2) עובד מערך הסייבר שראש חטיבת ההגנה במרכז הסייבר הסמיר בכתב לעניין חוק זה;

(3) לעניין ספק של הגופים המנויים בפטרים 2 ו-3 לRTOSFT דוחאשונה לחוק להסדרת הביטחון – עובד המלמ"ב שראש היחידה הטכנולוגית במלמ"ב הסמיר בכתב לעניין חוק זה;

"פעולה להגנת סייבר בחויר מחשב" – מתן הוראות למחשב בשפה קרייאת מחשב לשם הגנת סייבר, ובכלל זה הוראה לסריקה, לעיבוד, להסורה של חומר מחשב הנוגע לתקיפת סייבר, להתקנת סוג תוכנה שפעולתה מוגבלת לרשות הספק בלבד, לחסימה או לניטוק 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: המושללה⁴, והוריעה לגביין לוועדת החוץ והביטחון של הכנסת ביום ג' בתשרי התשפ"ד

(8) באוקטובר 2023);

* התקבל בכנסת ביום י"ג בטבת התשפ"ד (25 בדצמבר 2023); הצעת החוק ודבריו הסבר פורסמו בהצעות חוק המושללה – 1688, מיום כ"ג בכסלו התשפ"ד (6 בדצמבר 2023), עמ' .358.

¹ ס"ח התשנ"ה, עמ' .366.

² ס"ח התשנ"ה, עמ' .348.

³ ס"ח התשס"ב, עמ' .179.

⁴ ס"ח התשס"א, עמ' .158.

"צה"ל" – צבא הגנה לישראל;
"شب"כ" – שירות הביטחון הכללי;

"שירותי אחסון" – שירותי אחסון של חומר מחשב הנחוצים בעבר אחד או שירותי אספקת תשתיות לאחסון או ליעבוד של חומר מחשב;

"שירותים דיגיטליים" – שירות שהוא אחד מכל, הניתן בעבר אחר;

(1) שירותי תוכנה, לרבות כתיבה, התאמת, שינוי, בדיקה, תמייה, מחקר ופיתוח של תוכנה;

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

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

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

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

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

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

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

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

(5) האזנת סתר לתקורתה בין מחשבים כמשמעותה בחוק האזנת סתר, התשל"ט-1979⁵;

(6) גישה של גורם שאינו מורשה למידע המשמר במחשב, ובכלל זה בדרך של פגיעה בתוכנן המדיניות, או הוצאתו שלא כדין של מידע לרבות בדרך של העתקה, על ידי גורם כאמור;

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

2. (א) מנהל מוסמך רשאי לקבוע כי תקיפת סייבר שמתארת או שיש חשש ממשי כי עומדת להתרחש היא תקיפת סייבר חמורה, אם מצא כי יש חשש ממשי שיש בה כדי לפגוע בביטחון המדינה, בביטחון החיבור או בקיים האספקה והשירותים החיווניים, ובשל כל אלה (להלן – "תקיפת סייבר חמורה"):

(1) התרחשותה במהלך תקופת הפעולות העכאיות המשמעותיות;

(2) קיומו של חשש ממשי שהוא בעל השפעה משמעותית שאינה מוגבלת לספק הנתקף;

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

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

תקיפת סייבר
חמורה

⁵ ס"ח התשל"ט, עמ' 118.

קבע מנהל מוסמך או ראש חטיבת הגנה בסיביר לצה"ל לפי הוראות סעיף 2 כי תקיפת סייבר שמתורחשת או עומדת להתרחש, נגד ספק, היא תקיפת סייבר חמורה, והודיע על כך>User מוסמך לספק, לאחר שהזודהה לפניו, יחולו הוראות אלה:

(1) העובד המוסמך יפרט לפני הספק את התשתיות העובdotיות והמקצועית לקביעה כאמור, ככל שאין בכך כדי לחושף מקורות מידע, שיטות או אמצעים;

(2) העובד המוסמך ייתן לספק הזדמנות לפעול באופן הולם לאייתור התקיפה, מניעתה או בלימתה, תוך פרק זמן סביר שיימסר לספק, והיכול בהתחשב במאפייני תקיפת הסייבר;

(3) הספק יעדכן את העובד המוסמך בדבר הפעולות שביצע לאייתור התקיפה, מניעתה או בלימתה או ימסור לעובד המוסמך תצהיר בנוסח שפרסם ראש מערך הסייבר באתר האינטרנט של מערך הסייבר בדבר אספקת שירותים האחסון או השירותים הדיגיטליים ללקוחותיו או בדבר אספקת שירותים תחזקה, ניהול או בקרה של שירותים כאמור, תוך יישום הנחיות אבטחה בהתאם לתקין המניין בתוספת או לפחות, לעניין כל השירותים שהוא מספק, או לעניין השירותים כאמור שנגדם בוצעה התקיפה, והיכול בתוך פרק זמן סביר כאמור בפסקה (2);

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

(5) במתן הוראות לספק לפי פסקה (4) –

(א) ישקוּל העובד המוסמך את השפעתן האפשרית על הזכות לפרטיות, על פעילות הספק ועל צד שלישי, וכן את הועלות הכלכליות המעורכתי של יישום ההוראות והשפעתן האפשרית על הרציפות התפקודית של הספק, למיטב ידיעתו של העובד המוסמך, ואם הספק מסר הערכה לעניין זה – בהתחשב בהערכתה שmaser;

(ב) יורה העובד המוסמך לנוקוט אמצעי שפגיעתו פחותה לאייתור 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), וידוח על אופן ביצועה לעובד המוסמך עד המועד האמור.

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

הסמכויות לפי סעיף 3 לעניין תקיפת סייבר מסוימת נגד ספק, או לעניין כמה תקיפות כאמור המתורחשות באותו מועד, יופעלו לפני הספק בידי עובד מוסמך מקרוב גוף אחד בלבד.

	<p>(א) אדם שהגיע לידי מידע שהתקבל מספק לפי חוק זה ישמור אותו בסוד, לאיגלה אותו לאחר ולא יעשה בו כל שימוש, אלא לאייתו תקיפת סייבר חמורה, מניעתה או בלימתה.</p> <p>(ב) מידע שהתקבל מספק לפי חוק זה יימחק בסמוך לאחר סיום הטיפול בתקיפת הסייבר חמורה, אלא אם כן קבע מנהל מוסמך שהמידע כאמור חוני לזרחי מאפייני תקיפת הסייבר; מידע שנקבע לגביו כאמור ישמר בהיקף המוער הנדרש.</p> <p>(ג) פרסום פומבי ברבים של זהות הספק, שהתקבלה לפי חוק זה, יהיה באישור מנהל מוסמך לאחר שנתן לספק הזדמנויות להשמע את טענותיו.</p> <p>(ד) בסעיף זה, "מידע" – למעט על התוקף, התקיפה, ניגוד להוראות סעיף 6(א), דינו – מסר שלוש שנים.</p>	סודיות, הגבלת שימוש ומחיקה
7.	<p>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, בגין הוראות סעיף 6(א), דינו – מסר שלוש שנים.</p>	עונשין
8.	<p>(א) מערכת הסייבר שב"כ ומיל"ב ידוווחו ליועץ המשפטי לממשלה ולוועדת החוץ והביטחון של הכנסת, אחת לחודש, על כל אלה:</p> <p>(1) המקרים שבהם ניתנו הוראות לספק לפי סעיף 3(4). הנימוק למתן ההוראות וסוגן, ומספר המקרים שבהם ספק לא מילא אחר ההוראות כאמור;</p> <p>(2) מספר המקרים שבהם העובד המוסמך סייע לספק במילוי ההוראות שניתנו לו לפי סעיף 3;</p> <p>(3) סוגים הסקיינים שמנהל מוסמך קבע כי תקיפתם היא תקיפת סייבר חמורה לפי סעיף 2(א);</p> <p>(4) מספר המקרים שבהם מנהל מוסמך קבע כי תקיפת סייבר היא תקיפת סייבר חמורה לפי סעיף 2(א), בפילוח בשל פגיעה בביטחון המדינה, פגעה בביטחון הציבור או פגעה בקיום האספה והירויות החינוכיים.</p> <p>(ב) דיווח לפי חוק זה יהיה חסוי ופרסומו אسوוה.</p>	ڌيوه
9.	<p>(א) הוראות חוק זה באות להוסיף על הוראות כל דין אחר ולא לגרוע מהן. (ב) בלי לגרוע מההוראות סעיף קטן (א), הוראות חוק זה באות להוסיף על כל הוראה בעניין הנוגע להגנת סייבר, לפי החלטת הממשלה או הסכם, אולם במקרים של סתירה, יגבשו הוראות חוק זה.</p>	שמירת דין
10.	<p>בתקופת תוקפו של חוק זה, כאמור בסעיף 12, יקרוואו את חוק בתי משפט לעניינים מינהליים, התש"ס-2000⁶, בך שבתopsisת הראשונה, בסופה יבווא:</p> <p>"65. החלטה של רשות לפי חוק התמודדות עם תקיפות סייבר חמורות ברגע השירותים הדיגיטליים ושירותי האחסון (הוראות שעיה – חרבות ברול), התשפ"ד-2023⁷.</p> <p>תקנות שעת חירום (חרבות ברול) (התמודדות עם תקיפות סייבר חמורות ברגע השירותים הדיגיטליים ושירותי האחסון), התשפ"ד-2023⁸ – בטלות.</p>	תיקון חוק בתי משפט לעניינים מינהליים – הוראת שעיה – מס' 140
11.	<p>ביטול תקנות שעיה חירום (חרבות ברול) (התמודדות עם תקיפות סייבר חמורות ברגע השירותים הדיגיטליים ושירותי האחסון) ברגע השירותים הדיגיטליים (תקנות שעיה חירום (חרבות ברול) (התמודדות עם תקיפות סייבר חמורות ברגע השירותים הדיגיטליים ושירותי האחסון))</p>	ביטול תקנות שעיה חירום (חרבות ברול) (התמודדות עם תקיפות סייבר חמורות ברגע השירותים הדיגיטליים (תקנות שעיה חירום (חרבות ברול) (התמודדות עם תקיפות סייבר חמורות ברגע השירותים הדיגיטליים ושירותי האחסון)))

⁶ ס"ח התש"ס, עמ' 190; התשפ"ה, עמ' 216.

⁷ ס"ח התשפ"ה, עמ' 410.

⁸ ק"ת התשפ"ה, עמ' 618.

12. **תוקף**
סעיפים 1 עד 10 לחוק זה יעדכו בתוקפם עד תום שבעה חודשים מיום פרסומו.
13. **הוראת מעבר**
הוראות שניתנו ופעולות שבוצעו לפי התקנות שעת חירום (חבות ברול) (התמודדות עם תקיפות סייבר חמורות במרחב השירותים הדיגיטליים ושירותי האחסון), התשפ"ד-2023, לפני יום תחילתו של חוק זה, יראו אותן כאילו נעשו לפי חוק זה והוראותיו יחולו עליהם.

תוספת

(סעיף 3(3))

1. **NIST 800-53 Security and Privacy Controls for Information Systems and Organizations**
2. תקן שראש מערכת הסיביה בהסכמה ראש השב"כ ומיל"ב, פרסם ברשותם ובאותו האינטרנט של מערכת אם פרסם תקן כאמור ובלבד שיש בו כדי להבטיח ברמת סבירות גבוהה את הגבלת השפעתה של תקיפה סייבר חמורה מעבר לספק הנטקף וטיפול הולם בתקיפות סייבר חמורות.

בנימין נתניהו ראש הממשלה

אמיר אוחנה
יושב ראש הכנסת

יצחק הרצוג
 נשיא המדינה

