רשומות

הצעות חוק

הממשלה

ט"ז בטבת התשפ"ו | **1921** | 5 בינואר 2026

עמוד

הצעת חוק התמודדות עם תקיפות סייבר חמורות במגזר השירותים הדיגיטליים ושירותי האחסון (הוראת שעה) (תיקון מס' 4), התשפ"ו–2026 484

מתפרסמת בזה הצעת חוק מטעם הממשלה:

הצעת חוק התמודדות עם תקיפות סייבר חמורות במגזר השירותים הדיגיטליים ושירותי האחסון (הוראת שעה) (תיקון מס' 4), התשפ"ו–2026

תיקון סעיף 8

1. בחוק התמודדות עם תקיפות סייבר חמורות במגזר השירותים הדיגיטליים ושירותי האחסון (הוראת שעה), התשפ"ד–2023[1] (להלן – החוק העיקרי), בסעיף 8(א), בפסקה (4), במקום "פגיעה בקיום האספקה והשירותים החיוניים" יבוא "פגיעה, באופן חמור, ברציפות אספקתם של שירותים חיוניים לציבור".

דברי הסבר

כללי מתחילת הלחימה במסגרת מבצע "חרבות ברזל" (להלן – חרבות ברזל), ביום כ"ב בתשרי התשפ"ד (7 באוקטובר 2023), ניכרת עלייה בהיקף ובעוצמה של תקיפות הסייבר נגד גופים אזרחיים במשק הישראלי. מטרת תקיפות סייבר אלה היא לפגוע, כחלק מהמתקפה המשולבת המכוונת כלפי חוסנה של מדינת ישראל, במרחב הסייבר הישראלי, בכלכלה ובתפקודו התקין של המשק הישראלי, והן אף עלולות להוביל לפגיעה בחיי אדם. תקיפות הסייבר, לפי עמדת גורמי המקצוע במערך הסייבר הלאומי, בשירות הביטחון הכללי (להלן – שב"כ) ובממונה על הביטחון במערכת הביטחון (להלן – מלמ"ב) הולכות והופכות מתוחכמות ומורכבות יותר.

ספקים רבים של שירותי אחסון ושל שירותים דיגיטליים מהווים יעד מועדף לתקיפות סייבר, בין השאר, מאחר שהם מתאפיינים בחיבוריות גבוהה לגופים רבים במשק הישראלי, לרבות למשרדי ממשלה וגופים ציבוריים, ובהם גם גופים ביטחוניים, תשתיות מדינה קריטיות, ארגונים חיוניים לתפקודו של המשק ועוד. בשל חיבוריות זו, הנזק שעשוי להיגרם מתקיפה כנגד ספקים אלה עלול להתפשט ולהשפיע על חברות רבות במשק. בשים לב לאמור, תקיפות סייבר חמורות כנגד ספקים אלה עלולות להביא לפגיעה בביטחון המדינה, בביטחון הציבור או לפגיעה חמורה ברציפות אספקתם של שירותים חיוניים לציבור.

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 הראשונות), ובסמוך לאחר מכן, ביום י"ד בטבת התשפ"ד (26 בדצמבר 2023) פורסם ברשומות חוק התמודדות עם תקיפות סייבר חמורות במגזר השירותים הדיגיטליים ושירותי האחסון (הוראת שעה – חרבות ברזל), התשפ"ד–2023 (להלן – החוק), אשר החליף את תקנות שעת החירום הראשונות. יצוין כי החוק הוארך שלוש פעמים בחוק התמודדות עם תקיפות סייבר חמורות במגזר השירותים הדיגיטליים ושירותי האחסון (הוראת שעה – חרבות ברזל) (תיקון), התשפ"ד–2024, מיום י"ז בתמוז התשפ"ד (23 ביולי 2024), בחוק התמודדות עם תקיפות סייבר חמורות במגזר השירותים הדיגיטליים ושירותי האחסון (הוראת שעה – חרבות ברזל) (תיקון מס' 2), התשפ"ה–2025, מיום ב' בניסן התשפ"ה (31 במרץ 2025), וכן בחוק התמודדות עם תקיפות סייבר חמורות במגזר השירותים הדיגיטליים ושירותי האחסון (הוראת שעה – חרבות ברזל) (תיקון מס' 3), התשפ"ה–2025, מיום כ' באב התשפ"ה (14 באוגוסט 2025), במסגרתו גם תוקן החוק, כך שהוא עומד בתוקף עד יום י"ג בשבט התשפ"ו (31 בינואר 2026).

החוק מסמיך מנהל מוסמך במערך הסייבר הלאומי, בשב"כ או במלמ"ב (להלן – הגופים), וכן את ראש חטיבת ההגנה בסייבר בצבא הגנה לישראל לקבוע כי תקיפת סייבר היא תקיפת סייבר חמורה, אם יש חשש ממשי שיש בה כדי לפגוע בביטחון המדינה או בביטחון הציבור, או לפגוע באופן חמור ברציפות אספקתם של שירותים חיוניים לציבור; ובהמשך לכך – נתונה לעובד מוסמך באחד הגופים הסמכות להודיע לספק, כהגדרתו בחוק, על קיומו של חשש לתקיפת סייבר חמורה כנגדו או באמצעותו. אם הספק הנתקף לא הגיש תצהיר לפי החוק, וכן לא פעל באופן הולם ובתוך פרק זמן סביר שניתן לו לטיפול בתקיפת הסייבר החמורה, מסמיך החוק את העובד המוסמך לתת לספק הנתקף הוראות לצורך איתור התקיפה, מניעתה או בלימתה, תוך שהחוק קובע תנאים למתן ההוראות כאמור.

ביום י"ז בסיוון התשפ"ה (13 ביוני 2025) החלה המערכה מול איראן, במסגרת מבצע "עם כלביא", וזאת בעקבות החלטתה מאותו היום של ועדת השרים לענייני ביטחון לאומי על נקיטת פעולות צבאיות משמעותיות לפי סעיף 40 לחוק־יסוד: הממשלה. לנוכח המערכה נגד איראן והערכת הגופים באשר לחומרת איומי הסייבר והסיכונים הנשקפים מהם, ועל רקע הצורך המבצעי הדחוף בהקניית סמכויות וכלים חיוניים נוספים לשם התמודדות עם אותם איומים, הותקנו ביום כ"ז בסיוון התשפ"ה (23 ביוני 2025) תקנות שעת חירום (חרבות ברזל) (סמכויות נוספות לשם התמודדות עם תקיפות סייבר חמורות במגזר השירותים הדיגיטליים ושירותי האחסון), התשפ"ה–2025 (להלן – תקנות שעת החירום השניות).

[1] ס"ח התשפ"ד, עמ' 410; התשפ"ה, עמ' 798.

2. בסעיף 12 לחוק העיקרי, במקום "עד יום י"ג בשבט התשפ"ו (31 בינואר 2026)" יבוא "עד יום כ"ג בשבט התשפ"ז (31 בינואר 2027)". תיקון סעיף 12

דברי הסבר

ביום כ' באב התשפ"ה (14 באוגוסט 2025) פורסם ברשומות חוק התמודדות עם תקיפות סייבר חמורות במגזר השירותים הדיגיטליים ושירותי האחסון (הוראת שעה – חרבות ברזל) (תיקון מס' 3), התשפ"ה–2025 (להלן – תיקון מס' 3) שתיקן את החוק, האריך את תוקפו עד יום י"ג בשבט התשפ"ו (31 בינואר 2026) וביטל את תקנות שעת החירום השניות. במסגרת התיקון עוגנו בחוק הכלים הנוספים אשר הותקנו בתקנות שעת החירום השניות, ועיקרם סמכות מנהל מוסמך לדרוש מספק להציג לו כל ידיעה או מסמך הנדרשים לשם בחינת התקיימותם של התנאים לקביעה כי תקיפת סייבר היא תקיפת סייבר חמורה; חובת דיווח של ספק למנהל מוסמך על תקיפת סייבר משמעותית נגדו; וחובת ספק הנתקף בתקיפת סייבר חמורה ליידע ארגון מקושר אשר עלול להיפגע מן התקיפה באופן ישיר וממשי. נוסף על כך, התיקון ניתק את הזיקה של החוק לפעולות הצבאיות המשמעותיות, שעל נקיטתן החליטה ועדת השרים לענייני ביטחון לאומי לפי סעיף 40 לחוק־יסוד: הממשלה, בסמוך לאחר אירועי השבעה באוקטובר, כך שהפעלת הכלים והסמכויות מכוח החוק לא תלויה במצב הלחימה במסגרת חרבות ברזל.

סעיף 1 במסגרת תיקון מס' 3, תוקן סעיף 2 לחוק כך שנקבע בו כי 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 או בביטחון הציבור, או לפגוע באופן חמור ברציפות אספקתם של שירותים חיוניים לציבור". בהמשך לתיקון האמור, נדרש תיקון טכני מקביל בנוסח סעיף 8 לחוק לעניין דיווח ליועץ המשפטי לממשלה ולוועדת החוץ והביטחון של הכנסת על קביעות מנהל מוסמך לפי סעיף 2, כך שסעיף הדיווח יתאים לתיקון שנעשה בסעיף 2 לחוק.

סעיף 2 לנוכח מאפייניו הייחודיים של מרחב הסייבר ולנוכח ההערכות המקצועיות של הגופים באשר לחומרת איומי הסייבר במגזר השירותים הדיגיטליים והסיכונים הנשקפים מהם, עמדת הגופים היא כי יש צורך לשמר את הסמכויות והכלים הנדרשים לצורך ההתמודדות עם תקיפות במרחב הסייבר שנקבעו בחוק. הסמכויות והכלים החיוניים, אשר נקבעו בחוק לצורך התמודדות עם תקיפות סייבר חמורות במגזר השירותים הדיגיטליים ושירותי האחסון, נדרשים לשם שמירה על ביטחון המדינה, ביטחון הציבור ומניעת פגיעה חמורה ברציפות אספקתם של שירותים חיוניים לציבור. על כן, ובמקביל להשלמת עבודת מטה לקידום הסדר קבע במסגרת חוק הגנת הסייבר הלאומית, מוצע להאריך את תוקפו של החוק לתקופה נוספת של שנה, עד יום כ"ג בשבט התשפ"ז (31 בינואר 2027).