29 נובמבר, 2023

תקנות סייבר חדשות בקשר עם מלחמת "חרבות ברזל"

עדכוני לקוחות

ביום 27.11.23 פרסמה הממשלה תקנות שעת חירום חדשות שנועדו להסמיך את גופי הביטחון לתת לחברות המספקות שירותים דיגיטליים או שירותי אחסון הוראות לביצוע פעולות לצורך איתור תקיפת סייבר, מניעתה או בלימתה.

תקנות שעת חירום (חרבות ברזל) (התמודדות עם תקיפות סייבר חמורות במגזר השירותים הדיגיטליים ושירותי האחסון), התשפ"ד-2023 ("**התקנות**") פורסמו במקביל לתזכיר חוק בעל תוכן דומה ("**תזכיר החוק**"), אשר נועד להחליף את התקנות עם אישורו בכנסת. לפי תזכיר החוק, ברקע פרסומו ופרסום התקנות עומדת עליה בהיקף ובעוצמת מתקפות הסייבר כנגד גופים אזרחיים, שמטרתן לפגוע בכלכלה ובתפקודו התקין של המשק. כמו כן, ברקע הדברים עומדים גם ניסיונות הממשלה לקדם, בשנים האחרונות, את תזכיר חוק הסייבר, שנועד להקנות סמכויות רחבות למערך הסייבר, כמו גם מתקפות סייבר שאירעו לאחרונה כנגד כמה ספקים של שירותי אחסון.

1. **על מי חלות התקנות?**

התקנות ותזכיר החוק חלים על מי שמספקים אחד או יותר מהשירותים הבאים ("**ספקים**"):

א) שירותי אחסון של מידע שנמסר לשם העלאתו לרשת האינטרנט, שירותי עיבוד ואחסון נתונים, ושירותים לאספקת מידע, תשתית לאחסון או עיבוד נתונים;

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

ג) שירותי ניהול או הפעלה של מערכות מחשבים המשלבות תוכנה וטכנולוגיות תקשורת;

ד) שירותי עיבוד, הזנת או שחזור נתונים, התקנה והגדרת תצורה של מחשבים, התקנת תוכנה או שירותי הגנת סייבר;

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

ו) שירותי תחזוקה, ניהול או בקרה ביחס לאחד או יותר מהשירותים המנויים לעיל.

לפי תזכיר החוק, חברות המספקות שירותים כאמור מתאפיינות בחיבוריות גבוהה לגופים רבים במשק הישראלי, לרבות משרדי ממשלה וגופים ציבוריים, בהם גם גופים ביטחוניים, תשתיות מדינה קריטיות וארגונים חיוניים לתפקודו של המשק. בשל חיבוריות זו, הנזק שנגרם מתקיפה כנגד חברות אלו עלול להתפשט ולהשפיע על חברות רבות במשק. בהתאם, ביחס לשירותים המנויים בסעיפים א'-ה' לעיל, תנאי לתחולה הוא שמתקיים חיבור פיזי או לוגי, קבוע או עתי, או העברת מידע תדירה ממחשבי הספק למחשבי מקבל השירות.

2. **מה המשמעות העיקרית של התקנות?**

התקנות מאפשרות לעובד מוסמך של מערך הסייבר, שב"כ או מלמ"ב לעדכן ספק על קיומו של חשש ממשי ל-"תקיפת סייבר חמורה" כנגד הספק ולדרוש מהספק דיווח על פעולות שביצע לאיתור התקיפה, מניעתה או בלימתה. לחילופין, הספק רשאי למסור תצהיר על עמידתו בתקן NIST 800-53 שהינו תקן של מכון התקנים האמריקאי שנועד לתת מענה לתקיפות סייבר. על פי התקנות ותזכיר החוק, מידע זה ישמש רק לצורך איתור תקיפת הסייבר החמורה, מניעתה או בלימתה.

ככל שהעובד המוסמך מצא שהספק לא פעל בהתאם לדרישתו ולא סיפק תצהיר כאמור, רשאי העובד המוסמך לתת לספק הוראות, ובכלל זה הוראות הנוגעות לחומר מחשב והוראות למסירת ידיעה או מסמך לידי העובד המוסמך. זאת, לאחר שנתן לספק הזדמנות להשמיע את טענותיו.

3. **האם ניתן לערער על הוראות שניתנו לפי התקנות?**

על החלטות לפי התקנות ניתן לעתור לבית המשפט לעניינים מינהליים, וכך מוצע גם בתזכיר החוק.

4. **מה תוקפן של התקנות?**

התקנות נכנסו לתוקף ויעמדו בתוקף עד ליום 26.12.23. ככל שיאושר, תזכיר החוק יחליף את התקנות ויעמוד בתוקף עד לחלוף חודש לאחר מועד פקיעתה של ההכרזה של שר הביטחון מיום 7.10.23 על מצב מיוחד בעורף.

נשמח לעמוד לרשותכם בכל שאלה בנושא.

אנשי קשר

אסף הראל
שותף

לינור ורטניק
עורכת דין