אם אינך רואה מייל זה לחץ כאן

עדכון לקוחות תקופתי בנושא סייבר ואבטחת מידע

29 ביוני, 2025

כניסתן לתוקף של תקנות אבטחת הסייבר החדשות

ב-23 ביוני, 2025, נכנסו לתוקף **תקנות שעת חירום (חרבות ברזל) (סמכויות נוספות לשם התמודדות עם תקיפות סייבר חמורות במגזר השירותים הדיגיטליים ושירותי האחסון), התשפ"ה-2025** (להלן: "**התקנות**"). התקנות, שתוקפן לחודש ימים, נועדו לתת מענה מיידי לעלייה בהיקף ובתחכום של מתקפות הסייבר מאז פרוץ מלחמת "חרבות ברזל" ונוכח ההסלמה הביטחונית הנוכחית מול איראן. נקודת המוצא של התקנות היא שספקי שירותים דיגיטליים ואחסון מהווים יעד מועדף לתקיפות סייבר בשל החיבוריות הגבוהה שלהם לגופים רבים במשק. פגיעה בהם עלולה להתפשט במהירות, להשפיע על לקוחות קצה רבים, ובמקרים חמורים אף להעמיד בסיכון את ביטחון המדינה והרציפות התפקודית של שירותים חיוניים.

מי כפוף לתקנות?

התקנות חלות על "ספקים" של שירותים דיגיטליים ושירותי אחסון, המוגדרים כחוליה קריטית בשרשרת האספקה הדיגיטלית של המשק הישראלי. התקנות מכוונות לקשת רחבה מאוד של גופים, ומגדירים שירותי אחסון ושירותים דיגיטליים באופן הבא:

- התקנות מגדירות **שירותי אחסון** כאחסון של חומר מחשב עבור אחרים, או שירותי אספקת תשתית לאחסון או לעיבוד של חומר מחשב. הגדרה זו עשויה לכלול, בין היתר, ספקי שירותי ענן, חברות אחסון אתרים (hosting) וחוות שרתים (Data Centers).
- התקנות כוללות מספר סוגי ספקי **שירותים דיגיטליים**, ואלה כוללים:
  - חברות תוכנה העוסקות בפיתוח, תמיכה או בדיקת תוכנה.
  - ספקי שירותי IT וגופים המפעילים מערכות מחשוב עבור אחרים.
  - חברות המספקות שירותי הגנת סייבר, תפעול והתקנת תוכנות ורכיבים ממוחשבים או עיבוד נתונים.
  - גופים העוסקים בתחזוקה, ניהול או בקרה של כלל השירותים הנ"ל.

נציין כי היקף תחולתן של התקנות מותיר לדעתנו מספר שאלות פרשניות חשובות, ויש לבחון כיצד הרשויות השונות או בתי המשפט יתמודדו איתן.

מהן הדרישות המרכזיות החדשות?

התקנות קובעות שלוש חובות וסמכויות מרכזיות:

1. **סמכות לדרוש מידע**: כאשר קיים יסוד סביר להניח כי מתרחשת או עומדת להתרחש "תקיפת סייבר חמורה", "מנהל מוסמך" (במערך הסייבר, שב"כ או מלמ"ב) רשאי לדרוש מהספק כל ידיעה או מסמך, הנדרשים לו כדי להעריך את המצב.
2. **חובת דיווח מיידי על תקיפות**: ספק שנודע לו על תקיפת סייבר שמתרחשת נגדו, חייב לדווח על כך באופן מיידי למערך הסייבר (ספקים של מערכת הביטחון ידווחו ישירות למלמ"ב). חובת הדיווח חלה אם יש חשש שהתקיפה אינה מוגבלת לספק בלבד, או שהיא עלולה לפגוע באופן משמעותי בזמינות או במהימנות השירות. הדיווח יכלול פרטים על מועד התקיפה, מאפייניה, והשפעתה האפשרית על הספק ועל "ארגונים מקושרים" (גופים המחוברים למערכות הספק).
3. **חובת יידוע של "ארגון מקושר"**: לאחר שספק קיבל הודעה רשמית כי זוהתה תקיפת סייבר חמורה, עליו לעדכן **ללא דיחוי** כל ארגון מקושר אשר עלול להיפגע ממנה באופן ישיר וממשי. מטרת חובה זו היא למנוע "אפקט דומינו" והתפשטות הנזק במשק.

מנגנון הפטור: תמריץ לאימוץ תקנים בינלאומיים

התקנות כוללות "מסלול ירוק" המעניק פטור משלוש החובות החדשות. ספקים יכולים להגיש תצהיר המעיד על עמידתם בדרישות אבטחה גבוהות, ויהיו פטורים מהחובה למסור מידע, מחובת הדיווח ומחובת היידוע.

כדי להיות זכאי לפטור, על הספק לעמוד באחת מהחלופות המפורטות בתקנות, המבוססות על שילוב של תקני ליבה מוכרים **(ISO/IEC 27001, SOC 2 Type 2, CMMC Level 3)** ותקנים משלימים **(ISO/IEC 27017/27018, PCI DSS)**. ההיגיון מאחורי האפשרות למתן פטור הוא שארגונים שכבר מיישמים מסגרות אבטחה וניהול סיכונים מתקדמות נהנים מחוסן ארגוני גבוה יותר, וכן יצירת תמריץ לגופים שטרם מיישמים מסגרות אבטחה ותקנים דומים לפעול כדי להתאים את עצמם לסטנדרטים המקובלים בתחום.

איזונים, פיקוח ומידתיות

לצד הסמכויות החדשות, התקנות כוללות מספר מנגנוני איזון ופיקוח שנועדו להבטיח מידתיות:

- **מחיקת מידע**: מידע שהתקבל מהספק מכוח התקנות יימחק עם סיום הטיפול באירוע, אלא אם מנהל מוסמך קבע שהמידע חיוני לזיהוי מאפייני התקיפה.
- **פיקוח הדוק**: חובת הדיווח של הגופים המוסמכים ליועצת המשפטית לממשלה ולוועדת החוץ והביטחון של הכנסת הורחבה ותתבצע אחת לשבועיים.
- **תוקף מוגבל**: תוקף התקנות הוגבל לחודש, ובמקביל יקודמו תקנות קבועות או הליך חקיקה ראשית.

בשורה התחתונה: המלצות לפעולה

התקנות מהוות עליית מדרגה משמעותית באסדרת התחום ומאותתות על הכיוון אליו צועדת החקיקה העתידית בישראל, שעשוי להיות דומה למודלים הנהוגים באיחוד האירופי. אנו ממליצים ללקוחותינו, ובפרט לספקי שירותים דיגיטליים ואחסון, לבצע את הפעולות הבאות באופן מיידי:

1. **בחינת תחולה**: ודאו האם פעילותכם נכנסת תחת הגדרת "ספק" והאם יש לכם "ארגונים מקושרים" התלויים בשירותכם.
2. **עדכון נהלים**: עדכנו את תוכניות הטיפול באירועי סייבר (Incident Response Plans) כך שיכללו את חובות הדיווח והיידוע החדשות, וודאו שהצוותים הרלוונטיים מכירים אותן. כמו כן, מומלץ לעדכן הסכמי שירות (SLA) כדי שישקפו את החובות החדשות.
3. **בחינת זכאות לפטור**: בחנו את רמת התאימות של הארגון לתקנים הבינלאומיים המפורטים בתקנות. השגת הסמכה ועמידה בתקנים אלו עשויה לא רק להעניק פטור מהחובות הרגולטוריות, אלא גם לחזק את חוסנו של הארגון ולהוות יתרון תחרותי.

ככלל, אנו ממליצים לכלל לקוחותינו לערוך באופן שגרתי הערכות סיכונים בנוגע לסיכוני אבטחת מידע וסייבר בארגוניהם, ולוודא כי אמצעי אבטחת המידע שלהם, ובכלל זאת הנהלים הפנימיים של הארגון הנוגעים לאבטחת מידע ולמתן מענה לאירועי אבטחת מידע וסייבר, מספקים מענה לסיכונים האמורים.

לעיון בנוסח המלא של התקנות, אנא לחץ כאן.

צעדים לחיזוק אבטחת המידע בממשל האמריקאי

ב-23 ביוני 2025 נכנס לתוקף איסור על השימוש באפליקציית WhatsApp במכשירים רשמיים של חברי הקונגרס ועובדיהם, בהתאם להנחיות חדשות של לשכת מנהל המידע של בית הנבחרים של ארצות הברית. האיסור הוטל בעקבות הערכה של מחלקת הסייבר, לפיה WhatsApp מהווה סיכון אבטחתי גבוה בשל היעדר שקיפות בנוגע להגנה על נתוני משתמשים, היעדר הצפנה של נתונים המאוחסנים בענן, וכן פגיעות אפשרית לריגול זר. גורמים בבית הנבחרים ציינו את הצורך להגן על מידע רגיש ותקשורת ממשלתית, והבהירו כי ההצפנה מקצה לקצה של WhatsApp אינה נותנת מענה מלא לסיכונים הקשורים ל-Metadata ולגיבויים בענן. ההנחיה חלה על כלל גרסאות האפליקציה (מובייל, מחשבים ודפדפנים) ונמסר כי מכשירים ממשלתיים שיימצא עליהם WhatsApp יחויבו בהסרתה.

צעד זה ממשיך את המגמה שהחלה לפני מספר שנים עם הטלת האיסור על התקנת אפליקציית 'טיקטוק' במכשיריהם של חברי קונגרס, והמשיכה לאחרונה עם החלטת קצין המינהל הראשי של בית הנבחרים האמריקאי בעניין איסור השימוש בכלי הבינה המלאכותית הסיני DeepSeek AI במכשירים רשמיים של בית הנבחרים, וכן איסור על אנשי הצוות להתקינו על טלפונים, מחשבים וטאבלטים ממשלתיים. נציין כי איסור דומה על השימוש בכלי הבינה המלאכותית DeepSeek AI במכשירים רשמיים חל גם במדינות כמו ניו יורק טקסס ומדינות אחרות בארצות הברית.

לדיווח אודות איסור התקנת אפליקציית WhatsApp ראו כאן. לדיווח אודות איסור השימוש בתוכנת DeepSeek AI לחצו כאן.

בישראל, בינתיים, על אף רמת האיום הגבוהה בתחום הסייבר, לא ידוע לנו על הגבלות כלשהן מטעמי אבטחת מידע הנוגעות להתקנה או שימוש באפליקציות או תוכנות מסוימות – ובייחוד כאלו חינמיות – על ידי גורמי ממשל; למעשה, ההחלטה בנוגע לתקנות המוזכרות מעלה התקבלה בהחלטת ממשלה בקבוצת WhatsApp – מהלך שגרר תגובות ביקורתיות מצד מומחי אבטחת מידע, על השימוש של ממשלת ישראל באפליקציה לא מאובטחת דיה לצורך פעילות הממשלה ככלל וקבלת החלטות רגישות בפרט.

צוות הציות הבינלאומי, אכיפה, יצוא ביטחוני וסייבר במיתר ישמח לעמוד לשירותכם בנוגע לכל שאלה או התייעצות.

פרטי קשר

יובל ששון, שותף
ציות בינלאומי
03-6103190
ysasson@meitar.com

ד"ר שמרית איתי-חורב, שותפה
ציות בינלאומי
03-6103190
shimriti@meitar.com

נועם חורהאוס, עו"ד
ציות בינלאומי
03-6144041
noamg@meitar.com

אנו עומדים לרשותכם בכל שאלה ו/או הבהרה ונשמח לסייע בכל עניין.

למידע נוסף אודות מחלקת ציות בינלאומי במשרדנו, לחץ כאן.
למידע נוסף אודות מחלקת סייבר במשרדנו, לחץ כאן.
