מעו"דכן טכנולוגיות מידע **ספטמבר 2016**

לקוחות נכבדים,

ביום 31 באוגוסט 2016, פרסמה הממונה על שוק ההון, ביטוח וחסכון במשרד האוצר חוזר בנושא ניהול סיכוני סייבר בגופים מוסדיים (להלן: "**חוזר ניהול סיכוני הסייבר**"). חוזר ניהול סיכוני הסייבר מבטל חוזר קודם משנת 2006 ומוסיף עליו בהיבטים העיקריים הבאים: (א) ממשל תאגידי ואחריות בעלי תפקידים שונים בארגון לאבטחת מידע; (ב) בחינת אימוץ תקינה חדשה; (ג) דרישות מפורטות לניהול סיכונים והגנה על מערכות מידע ו-(ד) אימוץ מדיניות אבטחת מידע בארגון. חוזר ניהול סיכוני סייבר ייכנס לתוקף ביום 2 באפריל 2017.

ממשל תאגידי ואחריות בעלי תפקידים לאבטחת מידע

חוזר ניהול סיכוני הסייבר קובע כללים מפורטים בעניין הממשל התאגידי ואחריות בעלי תפקידים לאבטחת מידע בגופים מוסדיים. כך למשל, על הדירקטוריון **לאשר מדיניות ניהול סיכוני סייבר** ולדון בתכניות ניהול והערכת סיכונים אחת לשנה, ואף למנות **ועדת היגוי** לניהול סיכוני סייבר. נקבע כי מנכ"ל החברה יהיה האחראי הראשי להבטחת הניהול התקין של תחום סיכוני הסייבר, בין היתר על ידי תקצוב הולם, אישור תכנית עבודה שנתית וקביעת מבנה ארגוני מתאים. המנכ"ל יעמוד בראש ועדת ההיגוי, שחבריה הנוספים יהיו מנהל מערכות המידע, מנהל הסיכונים ומנהל הגנת הסייבר. על הוועדה להתכנס אחת לרבעון, לדון בכל היבטי סיכוני הסייבר בארגון ולדווח על כך לדירקטוריון.

בחינת אימוץ תקינה חדשה

חוזר ניהול סיכוני הסייבר מתייחס לתקן מעודכן בתחום אבטחת המידע (ISO 27001)[1] במספר מישורים. ראשית, החוזר קובע שעל המנכ"ל לשקול לאמץ את התקן באופן גורף. שנית, על החברה לבחון באופן ספציפי את עמידתם של גופים חיצוניים בהוראות התקן. כך, הן כאשר החברה שוקלת להתקשר בהסכם לקבלת שירותים במיקור חוץ והן במקרים בהם

*

חוזר ניהול סיכוני סייבר בגופים מוסדיים

*

בקרו באתר שלנו
http://www.fbclawyers.com

[1] ת"י ISO 27001 הוא הגרסה הישראלית לתקן המעודכן משנת 2013 של ארגון התקינה העולמי העוסק במערכות לניהול אבטחת מידע. התקן קובע הוראות וכללים להקמת מערכת ניהול אבטחת מידע, לרבות סקרי הערכות סיכונים וניהול סיכונים, פיתוח המערכת, הטמעתה בארגון ועדכון ובדיקה שוטפים שלה. התקן אינו מחייב נכון למועד זה, אך הטמעתו בארגון מאפשרת קבלת תעודה המוכיחה שהארגון נוקט באמצעים המתאימים לאבטחת המידע בו.

מוענקת גישה לבעלי רישיון (דוגמת סוכני ביטוח ויועצים פנסיוניים) לרשתות החברה, עליה לשקול לדרוש מגופים חיצוניים אלו לעמוד בהוראות התקן.

דרישות קפדניות לניהול סיכונים, הרשאות והגנה על מערכות מידע

החוזר קובע דרישות קפדניות במגוון היבטים של ניהול סיכוני הסייבר בארגון. כך למשל, מעבר להערכת סיכונים ראשונית, על הארגון לבצע **הערכת סיכונים חדשה** עם כל שינוי משמעותי שחל בו **ולכל הפחות אחת לשלוש שנים**, וכן לעדכן את רשימת הנכסים שלו וסיווגם לפחות אחת לשנתיים. בנוסף, על הארגון לבצע **איסוף מודיעין אקטיבי** על סיכוני סייבר חדשים ולהיערך להם מבעוד מועד, וכן לשקול שיתוף פעולה עם המרכז הלאומי להתמודדות עם איומי סייבר.

בכל הנוגע להתמודדות עם אירועי סייבר ותכנית המשכיות עסקית, על הארגון לעדכן את תכנית ההתמודדות אחת לשנה, להקים צוות התמודדות עם אירועי סייבר שיערוך **תרגול כולל לפחות אחת לשנה** ולדווח לממונה על אגף שוק ההון, ביטוח וחסכון על אירועי סייבר משמעותיים.

סקרים ומבחני חדירה יתבצעו אחת לשנה וחצי למערכות שיש אליהן גישה מרשת ציבורית ואחת לשלוש שנים למערכות פנימיות ולמערכות במיקור חוץ, והכל על ידי גורם מקצועי ובלתי-תלוי. בנוסף, על הארגון לבצע סקירה של חשבונות המשתמשים והרשאותיהם לפחות אחת לשנה **ולהטמיע מערכי הצפנה** למידע המאוחסן בהתקנים ניידים והמוצא מחוץ לגבולות הארגון, וכן לנהל ולעדכן את תעודות ומפתחות ההצפנה כדי לוודא שהיא יעילה ומאובטחת. החוזר קובע גם הוראות לגבי אמצעי ההזדהות של לקוחות אל מול רשתות הארגון, וביניהן שימוש באמצעי זיהוי חזקים או חד פעמיים בגישת לקוחות מרחוק (למשל על ידי זיהוי ביומטרי או הנפקת קוד חד פעמי באמצעות טלפון נייד), וכן הוראות מיוחדות לשימוש בשירותי מחשוב בענן על ידי הארגון.

מדיניות אבטחת מידע בארגון

חוזר ניהול סיכוני הסייבר קובע הנחיות מפורטות באשר **לקביעת מדיניות אבטחת המידע בארגון**. המדיניות תיקבע בשלוש רמות שונות. *ראשית*, תיקבע מדיניות כללית לניהול סיכוני סייבר שתכלול עקרונות מנחים בתחומי אבטחת המידע השונים (רשתות, מחשוב בענן, משאבי אנוש, ציוד קצה וכדומה). *שנית*, ייקבעו נהלים מפורטים להטמעת המדיניות בכל אחד מתחומי אבטחת המידע בארגון. הנהלים יעודכנו לאחר כל שינוי משמעותי בארגון ולפחות אחת לשנתיים. *שלישית*, הארגון יקבע **תכנית עבודה מפורטת** להטמעת מערכי אבטחת המידע הנדרשים, אשר תכלול, לכל הפחות, תכנית לניהול סיכוני סייבר, תכנית להעלאת רמת המודעות אצל עובדים, תכנית לביצוע סקרים ומבחני חדירה ותכנית להיערכות וניהול אירועי סייבר.

סיכום

חוזר ניהול סיכוני הסייבר מעדכן ומוסיף הוראות מפורטות בדבר אבטחת מידע ואבטחת מערכות מידע בגופים מוסדיים, וקובע הוראות ודרישות קפדניות הן בנוגע לאימוץ מדיניות, נהלים ותכניות עבודה, הן בנוגע לממשל תאגידי ואחריות בעלי תפקידים בארגון, והן בנוגע להטמעתם של מנגנוני אבטחת מידע בפעולות שגרתיות של הגופים המוסדיים.

החוזר מצטרף למגמה כללית של **אסדרת תחום אבטחת המידע**, המוצאת את ביטויה, למשל, בדירקטיבה האירופית החדשה בעניין אבטחת מידע אשר כללים מפורטים מכוחה ייקבעו בחודש אוגוסט 2017 (להרחבה על הדירקטיבה האירופית ראו עדכוננו מחודש יולי 2016), וכן בהנחיות מטה

הסייבר הלאומי במשרד ראש הממשלה.

חוזר ניהול סיכוני הסייבר חל אמנם רק על הגופים המוסדיים הכפופים להוראות הממונה על אגף שוק ההון, ביטוח וחסכון במשרד האוצר, אך אנו סבורים שהטמעת הוראותיו או חלקים מהן תועיל גם לארגונים אחרים בהתמודדות מול סיכוני סייבר ובעמידה בסטנדרט התנהגות נאות כלפי לקוחות ובעלי מניות.

עדכון זה נכתב על ידי עו"ד עמרי רחום-טוויג

אנו עומדים לרשותכם בכל שאלה או הבהרה ונשמח לסייע ככל הנדרש.

למידע נוסף ניתן לפנות אל:

עמית דת **adat@fbclawyers.com** **03-6941320**

.....