

G-Capital

עדכון עמדת סגל משפטית: גילוי בנושא סייבר

— יניזק יניזק יניזק —

ביום 25 בינואר 2023 פרסם סגל רשות ניירות ערך עדכון לעמדה משפטית מס' 105-33 שעניינה גילוי בנושא סייבר*. העמדה המקורית פורסמה ברקע עליית ההתמודדות מול איומי הסייבר לסדר היום הציבורי והתאגידי, וסקרה את היבטי הגילוי בתשקיף ובדוח התקופתי במסגרת גילוי על גורמי סיכון, ובמסגרת דוח מידי בנסיבות של תקיפות סייבר מהותיות. העדכון לעמדה בוצע לאור כך שלעמדת רשות ניירות ערך איומי סייבר הפכו לסיכון משמעותי ומוגבר וכן לאחר שבוצעה ברשות ביקורת רוחב בנושא סיכונים סייבר בתאגידים מדווחים (אשר פורסמה במקביל לפרסום עדכון זה של עמדת הסגל) אשר נגעה, בין היתר, במתודולוגיה בה השתמשו תאגידים לבחינת מהותיות סיכון הסייבר, וכן באופי הגילוי שניתן ביחס למדיניות ומנגנוני ההגנה לצורך הפחתת סיכון תקיפות סייבר שחוו תאגידים מדווחים.

בעקבות הביקורת, מונה סגל הרשות מספר תובנות:

- קיימת חשיבות במעורבות של הדירקטוריון ונושאי המשרה באיתור, ניהול ופיקוח של סיכונים סייבר ואבטחת מידע. מעורבות זו תסייע בבניית מערך יעיל לניהול סיכונים ולתיאום בין היעדים העסקיים לבין המערך הטכנולוגי.
- קיימת חשיבות לבסס את ניהול סיכונים הסייבר בהתאם לכלים מקובלים כגון, הערכת סיכונים תוך שימוש במתודולוגיות מקובלות דוגמת סקר סיכונים, קביעת תכנית עבודה שנתית/רב שנתית בתחום הסייבר וביצוע בקרות על ביצועה בפועל, הפעלת מערך אבטחת מידע תוך הסתייעות במומחים וביצוע בקרה באמצעות ביקורת פנים.
- יישום תהליך הערכת סיכונים סדור המבוסס על מתודולוגיה מקובלת דוגמת סקר סיכונים, מסייע לתאגיד להבטיח מתן גילוי נאות על סיכונים סייבר ואבטחת מידע ומאפשר בסיס לדיון בדירקטוריון בנוגע לגורמי הסיכון של התאגיד, דירוגם וגילויים בדוחות התקופתיים. ביחס לדירוג השפעת הסיכון הודגש כי הדירוג מחייב התייחסות לסיכון השיווי לו חשוף התאגיד הלכה למעשה, בהתחשב בבקרות הקיימות ובמאפיינים הייחודיים של התאגיד ולא לסיכון השורשי (שהינו הסיכון המובנה מעצם הפעילות שמקיימת החברה, בהתעלם מהבקרות המופעלות להפחתת סיכון).
- היערכות מוקדמת של התאגיד להתמודדות עם תקיפת סייבר (כולל הסדרת נהלים, תהליכי עבודה לטיפול ותגובה לתקיפת סייבר, ועיגון התהליכים הנדרשים לעניין גילוי ודיווח על אירוע סייבר), יאפשרו לתאגידים לנהל ולהתמודד בצורה אפקטיבית יותר עם תקיפת סייבר ולתת גילוי מתאים למשקיעים.

הלכה למעשה לפי ממצאי דוח הביקורת:

- **מעורבות דירקטוריון.** כגון - דיונים עתיים בדירקטוריון, אישור נוהל אבטחת מידע בדירקטוריון, דיווחים לדירקטוריון הנוגעים לסטטוס הגנת הסייבר ואבטחת המידע בחברה; קיום דיונים בכל הנוגע להשפעת סיכוני הסייבר על פעילותה העסקית של החברה, באופן עתי וסדיר; דיון אודות התקשרות לקבלת יעוץ ממומחים חיצוניים.
- **בחינת הצורך בבעלי ידע ומומחיות בין חברי הדירקטוריון** בדרך של מינוי דירקטור מומחה בתחום, או היוועצות עם מומחה חיצוני.
- **הקמת מערך אבטחת מידע אפקטיבי,** עצמאי או במיקור חוץ או בשילוב של שניהם, תוך יישום התקנים המקובלים בתחום אבטחת המידע או הסייבר.
- **תכנית עבודה שנתית/רב שנתית בתחום הסייבר,** תוך בקרה של הביצוע והיישום של תכנית העבודה הלכה למעשה על ידי דרגים בכירים בחברה.
- **עריכת סקר סיכונים** בנושא סייבר לשם הערכת סיכונים, וכנגזרת לכך קביעה ויישום תכנית לצמצום חשיפות שאותרו.
- **ביצוע בקרה על בחינת אופן הניהול של סיכוני סייבר באמצעות ביקורת פנים.**
- **עיגון נהלים ותהליכים נדרשים לעניין גילוי** בקרות תקיפת סייבר מהותית, הכולל צורך בקיומו של דיון בדירקטוריון החברה לצורך קביעת מהותיות האירוע ובחינת הצורך במתן גילוי בעניינו.
- בחינת נחיצות **הקמת צוות תגובה מיומן,** המיועד לתת מענה ראשוני בעת קרות אירוע סייבר.

בנוסף, מונה סגל הרשות **היבטי גילוי** (נוספים על אלו המנויים בעמדה המקורית) הנדרשים לפי העדכון לעמדה:

גילויים נוספים הנדרשים במסגרת התשקיף ובדוח התקופתי:

• **גילוי על מדיניות ניהול סיכוני סייבר ואבטחת מידע**

אם קיים בתאגיד סיכון מהותי הרלוונטי לפעילותו, על התאגיד לפרט את אסטרטגיית ניהול הסיכונים בנושא, הכוללת את מדיניות ניהול הסיכון, מתודולוגיות, נהלים, תהליכי עבודה, פעולות ובקרות לשם ניהול והתמודדות עם סיכון הסייבר בתאגיד ואת הערכתו בדבר אפקטיביות מדיניות ניהול הסיכונים בהתמודדות והפחתת סיכון הסייבר.

בנוסף, על התאגיד לציין אילו משאבים מוקצים על ידו לניהול סיכוני סייבר, ולפרט את זהות הגורמים הרלוונטיים (זהות הגורם המאשר את מדיניות ניהול הסיכון הסייבר בתאגיד, בעל התפקיד בתאגיד אשר אחראי ליישום המדיניות, ככל שקיימת) באופן שכלל שמדובר בשירותי מיקור חוץ יש לציין זאת ולפרט את מהות השירותים שמתקבלים.

• **גילוי על מומחיות נושאי משרה וחברי דירקטוריון בתחום הסייבר**

במסגרת המידע הניתן על השכלתם ועיסוקם של הדירקטורים ונושאי המשרה ב-5 השנים האחרונות, אם לנושא המשרה בתאגיד יש ניסיון, מומחיות או מיומנות בנושא אבטחת מידע או סייבר, על התאגיד לציין עובדה זו ולפרטה. לצד זאת, מצוין בעמדה כי על אף היתרונות בידע ובמיומנות של חברי הדירקטוריון ונושאי המשרה בתחום הסייבר, בפני התאגיד פתוחות אפשרויות נוספות לקבלת סיוע מקצועי נדרש בנושא הסייבר ובכלל זה האפשרות להיוועץ עם מומחים חיצוניים במידת הצורך - אם בחר התאגיד להשתמש בשירותי מיקור חוץ ובמומחים חיצוניים, עליו לפרט שימוש בסיוע כאמור כחלק ממדיניות ניהול הסיכון.

• גילוי על אירועים החורגים מעסקי התאגידים הרגילים

בהמשך לדרישת הגילוי כעולה מהעמדה המקורית (לפיה במקרה של תקיפות סייבר מהותיות בתקופת הדוח, על התאגיד לבחון תיאור תמציתי של עיקרי האירועים שהתרחשו בתקופת הדוח או הכללה על דרך הפניה לדוחות מיידיים שפרסם התאגיד שבמסגרתם נכלל תיאור אודות האירועים כאמור), מבהיר סגל הרשות כי אם פורסם דוח מידי על אירוע סייבר, על התאגיד לבחון האם התגלה מידע מהותי נוסף בנוגע לאירוע ולפרטו במסגרת הדוח התקופתי. מידע נוסף כאמור יכול שיכלול השפעות על המצב הפיננסי של התאגיד, שינוי במדיניות החברה בעקבות האירוע וכיוצא בזה.

גילוי בדיווחים מיידים:

בהתייחס לגילוי הנדרש בדיווח מידי מכוח תקנה 36(א) לתקנות ניירות ערך (דוחות תקופתיים ומיידיים), תש"ל-1970 ("תקנות הדוחות"), במקרה של אירוע או ענין החורגים מעסקי התאגיד הרגילים, מבהיר סגל הרשות כי בקרות תקיפת סייבר והבחינה של מהותיות האירוע ובהתאם אם אירוע זה מחייב פרסום דוח מידי, **תאגיד נדרש, בין היתר, לשקלל את מכלול הנזק ופוטנציאל הנזק שנגרם/עלול להיגרם כתוצאה מהתקיפה, הן במישרין והן בעקיפין.** לאור כך שמהותיות של אירוע צריכה להיבחן הן בהתאם לפרמטרים כמותיים והן בהתאם לפרמטרים איכותיים, יתכן שאירוע ייחשב כמהותי ובהתאם מחייב דיווח מידי גם במקרים בהם מחד לא צפוי נזק כספי ממשי לתוצאות התפעוליות של התאגיד, אך מאידך קיימת השפעה מהותית על התאגיד במישור האיכותי.

בהקשר זה אף מבהיר סגל הרשות, למען הסר ספק, כי מקום שקמה לתאגיד חובת דיווח מידי כאמור בקשר עם איומי או תקיפות סייבר, הרי שקיימת לו גם הזכות לעכב דיווח בהתאם לקבוע בתקנה 36(ב) לתקנות הדוחות ובפרט כאשר פרסום הדיווח עלול למנוע השלמת פעולה של תאגיד כקבוע בהוראות תקנה 36(ב)1(2) לתקנות הדוחות. כרגיל, זכות העיכוב פוקעת אם המידע בדבר האירוע פורסם ברבים.

לקישור לעדכון עמדת הסגל בנושא סיכוני סייבר מינואר 2023 לחץ [כאן](#).

לקישור לדוח ריכוז ממצאי ביקורת רוחב בנושא סיכוני סייבר בתאגיד מדווח מינואר 2023 לחץ [כאן](#).

נשמח לעמוד לרשותכם בכל שאלה בנושא,



עו"ד אסף הראל
שותף

assafh@gornitzky.com



יאיר שילוני
שותף

shiloni@gornitzky.com



שרון ורקר-שגיא
שותפה

sagy@gornitzky.com

גורניצקי