הנחיות רשות לניירות ערך בנושא סיכוני סייבר ואבטחת מידע

חנן טויזר, CISA
שותף, מנהל מחלקת מערכות מידע
פאהן קנה ניהול בקרה

Fahn Kanne
Grant Thornton

Fahn Kanne
Grant Thornton

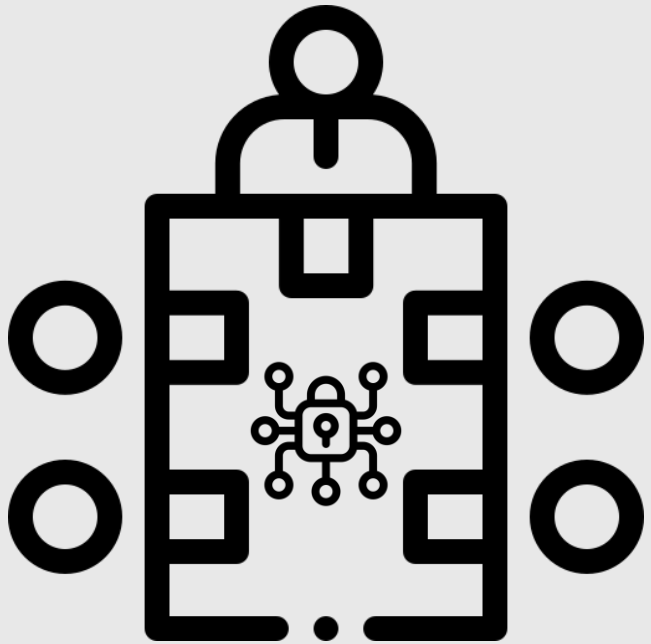
נושאים מרכזיים

ניהול סיכוני אבטחת
מידע וסייבר

גילוי בנוגע לסיכוני סייבר
ומתקפת סייבר

היערכות מוקדמת להתמודדות
עם תקיפות סייבר

מעורבות הדירקטוריון בפיקוח על ניהול סיכוני סייבר



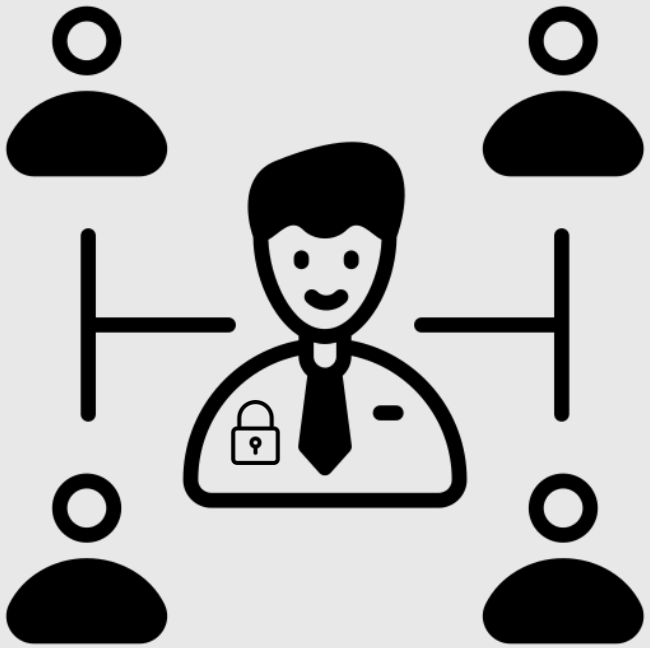
קיימת חשיבות גדולה בקבלת עדכונים שוטפים מבעלי התפקידים הרלוונטיים בתאגיד ולמעורבות של הדירקטוריון ונושאי המשרה בתאגיד באיתור, ניהול ופיקוח של סיכוני סייבר ואבטחת מידע.

מעורבות זו, תסייע בבניית מערך יעיל לניהול סיכונים ולתיאום בין היעדים העסקיים לבין המערך הטכנולוגי.

מעורבות הדירקטוריון וההנהלה בפיקוח על ניהול סיכוני הסייבר :

- קיום דיונים תדירים בנושאי סייבר.
- אשרור מדיניות סייבר, תוכניות עבודה ובקרה עליהם.
- אחריות על הערכת סיכוניי סייבר.
- אחריות על אשרור התקשרויות עם גורמי צד ג' בתחום הסייבר.
- מומחיות חברי הדירקטוריון לנושאי סייבר\קבלת יעוץ חיצוני בנושא.

מערך אבטחת מידע



מרכיב חשוב בניהול סיכוני סייבר בארגון הוא קיום מערך אבטחת מידע אפקטיבי. מערך זה יכול להיות מופעל באופן עצמאי על ידי פונקציות פנימיות בארגון או באמצעות מיקור חוץ.

מערך אבטחת המידע:

- גורם אשר אחראי על נושא אבטחת המידע.
- תוכנית עבודה מסודרת בנושא אבטחת מידע.
- וועדת היגוי בנושא אבטחת מידע.
- יישום תקן אבטחת מידע.

הערכת סיכוני סייבר וניהולם

ישנה חשיבות לביסוס מרכיבי ניהול סיכוני הסייבר בהתאם לכלים מקובלים, כגון: הערכת סיכונים באמצעות מתודולוגיה מקובלת דוגמת סקר סיכונים, קביעת תכנית עבודה שנתית/רב שנתית בתחום הסייבר וביצוע בקרות על ביצועה בפועל.

הערכת סיכוני סייבר וניהולם:

- ביצוע הערכת סיכוני סייבר תקופתית.
- תקשור הערכת הסיכויים להנהלה ולדירקטוריון.
- גיבוש תוכנית עבודה לצמצום הסיכונים.
- ביצוע מעקב של דרגי ההנהלה אחר יישום תוכנית העבודה.
- בחינת מערך אבטחת המידע ע"י מבקרי הפנים של החברה.
- בחינת הערכת הסיכונים ע"י מבקרי הפנים של החברה.

גילוי בנוגע לסיכוני סייבר ומתקפת סייבר

יישום תהליך הערכת סיכונים סדור המבוסס על מתודולוגיה מקובלת דוגמת סקר סיכונים, מסייע לתאגיד להבטיח מתן גילוי נאות על סיכוני סייבר ואבטחת מידע. תהליך זה כאמור מאפשר בסיס לדיון בדירקטוריון בנוגע לגורמי הסיכון של התאגיד, דירוגם וגילוים בדוחות התקופתיים.

גילוי סיכוני סייבר ומתקפות סייבר:

ככל שקיים סיכון סייבר מהותי, האם החברה מיישמת את חובת הגילוי בעינינו?

- האם קיים תיאור של הסיכון
- האם קיימת התייחסות לקיומה של מדיניות הגנה
- האם מבוצע פיקוח על יישומה של תוכנית ההגנה
- האם מבוצעת בדיקת האפקטיביות של תוכנית ההגנה באופן תקופתי
- האם קיים דירוג השפעתו של הסיכון על החברה
- האם הסיכון המוצג הוא סיכון שיורי
- האם החברה עושה שימוש במתודולוגיה סדורה להערכת הסיכונים (כגון סקר סיכונים)
- האם החברה מפרסת את גורמי הסיכון ודירוגם בדוחות התקופתיים

היערכות מוקדמת להתמודדות עם תקיפות סייבר

נוהל גילוי על התרחשות מתקפת סייבר מהותית

היערכות מוקדמת של התאגיד וגילוי על מתקפות סייבר בעת התרחשותן, הכוללת הסדרה מראש של נהלים ותהליכי עבודה שיטתיים לטיפול ותגובה בנוגע לאירוע סייבר, וכן עיגון התהליכים הנדרשים לעניין גילוי ודיווח לציבור המשקיעים על התרחשות אירוע סייבר מהותי, יאפשרו לתאגידים לנהל ולהתמודד בצורה אפקטיבית יותר עם תקיפת סייבר בפועל ומתן הגילוי הנאות לציבור המשקיעים.

נוהל גילוי על התרחשות מתקפת סייבר מהותית:

- קיום נוהל להתמודדות עם אירוע סייבר.
- קיום דיון בדירקטוריון החברה לצורך קביעת מהותיות האירוע ובחינת הצורך במתן גילוי דעת בעינינו.
- ביצוע תרגיל סייבר תקופתי.
- עיגון בנוהל התייחסות לבחינת הצורך בדיווח לציבור בהתאם למהות האירוע.
- האם קיים נוהל עבודה לתהליך הגילוי לאירוע מהותי.
- האם נבחן הצורך והנחיצות של מינוי צוות תגובה.
- האם הוסדר אופיו, הרכבו, סמכויותיו והכשרתו של צוות התגובה.

תודה על ההקשבה!

Fahn Kanne
Grant Thornton

חנן טויזר
שותף, מנהל מחלקת מערכות מידע
050-8230209
Hanan.Twizer@il.gt.com