GROSS GKH

גרוס ושות׳ עורכי דין

אחריות המבקר הפנימי לביקורת מערכות מידע בארגון בתחום הגנת הסייבר

עו״ד צביקה גלבוע

פברואר 2022

על מה נדבר?

- **מהו אירוע סייבר**
- **הנזקים הפוטנציאליים מאירוע סייבר**
- **סיכון סייבר וניהולו.**
- **רגולציה בתחום הגנת הסייבר.**
  - חוק החברות
  - חוק הגנת הפרטיות ותקנותיו
  - פקודת הבנקאות והנחיות המפקח על הבנקים
  - הנחיות מנהל רשות שוק ההון, ביטוח וחסכון
  - חובות גילוי לפי הנחיות רשות ני"ע
  - הנחיות מערך הסייבר הלאומי
- **תפקיד המבקר הפנימי כנגזרת מאחריות הדירקטוריון ונושאי המשרה.**

אירוע סייבר- פגיעה בסודיות, אמינות וזמינות המידע

- שיבוש פעולתו התקינה של מחשב או הפרעה לשימוש בו.
- מחיקת חומר מחשב, שינויו, שיבושו או הפרעה לשימוש בו.
- אחסון או הצגת מידע/ פלט כוזב או שיש בהם כדי להטעות בהתאם למטרות השימוש בהם
- חדירה שלא כדין לחומר מחשב כמשמעותה בחוק המחשבים.
- האזנת סתר לתקשורת בין מחשבים כמשמעותה בחוק האזנת סתר.
- גישה לא מורשית למידע השמור במחשב, לרבות פגיעה בתהליך הזדהות/ הדלפת מידע.
- הפרעה או מניעת נגישות של מחשב לרשת תקשורת.

נזקי אירוע סייבר

- פגיעה בזמינות ובמהלך העסקים הרגיל של הארגון – עצירת פעילות והכנסות.
- אובדן מידע או ידע בעל ערך מסחרי למתחרים או לגורמים פליליים אחרים.
- פגיעה במוניטין, חשיפה לתביעות משפטיות.
- הפעלת ביטוח סייבר ככל שישנו וככל שהוא מכסה את האירוע, עליית הפרמיה.
- השפעה שלילית על שווי תאגיד.
- השקעת משאבים בהמשכיות עסקית והחזרת המערכות לפעילות תקינה.
- ניהול עסקים כרגיל לאחר האירוע – צורך בנקיטת אמצעים להוכחת עמידותו של הארגון מפני תקיפות נוספות.

סיכון סייבר

- **סיכון** - תופעה העלולה לקרות שלא על פי התכנון, ואשר כתוצאה ממנה נגרם נזק, במובנים של עלות, זמן או ביצועים. הסיכון נמדד על פי: **סבירות** המימוש שלו, **ועוצמת הפגיעה** כתוצאה מהכשל, מחושבת ב**עלות**, ב**ביצועים** או ב**זמן**.
- כך גם במרחב הסייבר: סיכון = סבירות X עוצמת הפגיעה
- ניהול הסיכונים בארגון - ניהול שוטף שמטרתו לאתר סיכונים/מפגעים, הערכת עוצמת הפגיעה/הנזק, תעדוף הטיפול בהם על פי העוצמה, הגדרת השיפור הנדרש וההשקעה הנדרשת לשיפור ובקרה על ביצוע פעילויות השיפור.
- איך הארגון מתייחס לסיכון הסייבר במסגרת ניהול הסיכונים שהוא מבצע?

חוק החברות

- אחריות הדירקטוריון, הנהלת החברה ונושאי המשרה לפעול על מנת לצמצם את החשיפה לסיכוני סייבר באופן סביר ובהתאם למיומנות המצופה מהם לפי עמדתם ובאותן נסיבות. חובה זו צריכה להיות מותווית במדיניות החברה ובמסגרת פיקוח הדירקטוריון על ביצועי החברה.

- אחריות זו נגזרת מחובת הזהירות, חובת האמונים וחובת הפיקוח החלה עליהם מכוח החוק [סעיפים 253-254 וסעיף 92 לחוק החברות].

חוק החברות (2)

GROSS GKH
– גרוס ושות' עורכי דין –

המבקר הפנימי

- המבקר הפנימי הוא אחד משומרי הסף של החברה – תפקידו לוודא כי החברה פועלת כחוק.
- עליו לוודא כי הדירקטורים ונושאי המשרה פועלים לצמצום החשיפה לסיכוני סייבר באופן סביר ובהתאם למיומנות המצופה מהם לפי עמדתם ובאותן נסיבות.
- הכלים העומדים לרשות המבקר הפנימי:
  - יגיש לאישור הדירקטוריון הצעה לתכנית עבודה שנתית או תקופתית.
  - יבדוק את **תקינותן של פעולות החברה** מבחינת השמירה על החוק ונוהל עסקים תקין.
  - יגיש דין וחשבון על ממצאיו ליו"ר הדירקטוריון, למנכ"ל וליו"ר ועדת הביקורת.

(סעיפים 149, 151-152 לחוק החברות, התשנ"ט-1999)

- יערוך את הביקורת על פי תקנים מקצועיים מקובלים (ס' 4(ב) לחוק הביקורת הפנימית)

חוק הגנת הפרטיות ותקנות אבטחת מידע

- **בעל מאגר מידע** בארגון נושא בחובת רישום המאגר, הגבלת השימוש בו למטרותיו, אבטחתו ושמירת סודיותו, פיקוח ובקרה על מחזיק מטעמו ומינוי ממונה אבטחת מידע.
- יש לוודא **קיום מסמך הגדרות המאגר** – הכולל את פעולות האיסוף והשימוש במאגר, מטרותיו, הסיכונים העיקריים לפגיעה באבטחת המידע ואת דרכי ההתמודדות עמם.
- יש לוודא כי מונה **ממונה** על אבטחת המידע במקרים הנדרשים בתקנות.
- יש לוודא כי קיים **נוהל אבטחת מידע** בהתאם לתקנות הכולל התייחסות למספר פרמטרים ובהם - אבטחה פיזית וסביבתית, הרשאות גישה בקרה ותיעוד, תיאור אמצעי הגנה ואופן הפעלתם, הוראות למורשי גישה, תיאור הסיכונים לחשיפת המידע והטיפול בהם כגון הצפנה, קביעת אופן התמודדות עם אירועי אבטחת מידע, אמצעי בקרה וזיהוי, גיבוי נתונים, אבטחה בניהול כוח אדם (מיון, שיבוץ, הדרכה), תיאור מבנה מערכות מאגר המידע.

חוק הגנת הפרטיות ותקנות אבטחת מידע (2)

- בהתאם לתקנות, עבור מאגר מידע הדורש רמת אבטחה **גבוהה**, חלה חובה לערוך סקר סיכונים לאיתור סיכוני אבטחת מידע אחת ל-18 חודשים לפחות.

- בעל מאגר המידע ידון בתוצאות הסקר ויפעל לתיקון הליקויים אם התגלו, ולערוך מבדקי חדירות למערכות המאגר אחת ל-18 חודשים לפחות על מנת לבחון עמידותן בפני סיכונים פנימיים וחיצוניים.

- החובות האמורות בחוק ובתקנות הן חובות כלליות אשר נקבעות לפי סוג מאגר המידע ולמעשה חלות על כל המשק הישראלי (כל מאגר לפי רמת האבטחה שלו).

פקודת הבנקאות והוראות המפקח על הבנקים

- **אחריות הדירקטוריון**: התווית אסטרטגיית הגנת סייבר ואישורה; אישור מסגרת ניהול סיכוני סייבר ומדיניות; קביעת אופן מעקב ופיקוח על ההנהלה הבכירה לגבי ניהול סיכוני סייבר; קבלת דיווח על אירועי סייבר משמעותיים **(סעיף 15 לנב"ת 361)**.

- **אחריות ההנהלה**: יצירת מסגרת כוללת לניהול סיכוני הסייבר ופיקוח נאות עליה; גיבוש מדיניות הגנת הסייבר התאגידית; יישום עקבי ותחזוקה של מסגרת העבודה לניהול סיכוני סייבר לרבות הקצאת משאבים נאותים; מעקב אחר אפקטיביות מערך הגנת הסייבר ותיאום פעילותו מול גורמי ניהול סיכון פנימיים וחיצוניים; קבלת דיווח על תמונת מצב עדכנית של איומי הסייבר ודרכי ההתמודדות מולם, בהתאם לתוצאות הערכת הסיכונים; קבלת דיווח תקופתי על אירועי סייבר רלבנטיים וניתוח המשמעויות הנגזרות מהם; דיון בהשלכות האופרטיביות, של סיכוני סייבר והנחיה ובקרה על ביצוע שינויים או התאמות במערך ההגנה ו/או בפעילות העסקית, לפי הצורך. **(סעיף 16 לנב"ת 361)**.

פקודת הבנקאות והוראות המפקח על הבנקים

- המבקר הפנימי צריך לבדוק את תקינות פעולות הגוף הבנקאי לרבות קיום הוראות המפקח על הבנקים ובהן הוראותיו בנושא הגנת הסייבר **(סעיף 14ה פקודת הבנקאות, 1941).**
- ניהול הגנת הסייבר ואופן יישומה יבוקרו באופן תקופתי ע"י הביקורת הפנימית **(סעיף 20 לנב"ת 361).**
- מנהל הגנת הסייבר יקיים ממשקי עבודה מול מנהל הסיכונים הראשי והביקורת הפנימית תוך התאמה להוראות הרלבנטיות **(סעיף 23 לנב"ת 361).**
- מנגנוני הערכת בקרות הגנת הסייבר יתואמו וישולבו במנגנוני הערכה קיימים בתאגיד ובהם **תהליכי ביקורת פנימית** על פי הוראת ניהול בנקאי תקין מס' 307.

הוראות רשות שוק ההון – ניהול סיכוני סייבר בגופים מוסדיים

- הגדרת **תכנית עבודה שנתית** לניהול סיכוני סייבר ודיון בה בדירקטוריון.
- מינוי **ועדת היגוי** בר' המנכ"ל עם מנהל מע' המידע, מנהל הסיכונים ומנהל הגנת הסייבר.
- הגדרת **מדיניות** ניהול סיכוני סייבר, תכנית עבודה, הערכת סיכוני סייבר, דיווח וניטור סיכונים, יישום **בקרות** שוטפות, נוהל **מוכנות למקרה אסון והמשכיות עסקית**.
- ביצוע **סקרי סיכונים** ומבדקי חדירה, הצגתם בוועדת ההיגוי ועדכון הבקרות ותכנית העבודה בהתאם לממצאים.
- **נהלי אבטחת מידע** – אבטחת רשת וגישה מרחוק, קישוריות לרשת האינטרנט, הוצאת נתונים ומחשוב ענן, הצפנה, מניעת קוד עוין, אבטחה בהליכי רכש ובמיקור חוץ, הפרדת סביבות, ניהול הרשאות משתמשים ובקרות גישה, אבטחה פיזית וסביבתית, הגנת סייבר בתחום משאבי האנוש, אבטחת קשר עם גורמי חוץ (לקוחות, ספקים).

תקנות ניירות ערך ועמדת רשות ני"ע 33-105 (1)

GROSS GKH
– גרוס ושות' עורכי דין –

חובת גילוי בתשקיף ובדוח התקופתי

חובות הגילוי החלה על תאגיד כלפי משקיעים ביחס לגורמי הסיכון שלו (סעיף 39 לתוספת הראשונה לתקנות פרטי תשקיף מבנה וצורה) :

- התרחשות תקיפות סייבר קודמות, לרבות חומרתן ותדירותן.
- ההסתברות להתרחשות תקיפות סייבר.
- אפקטיביות יכולות התאגיד למנוע או להקטין את החשיפה לסיכוני הסייבר.
- היבטים עסקיים של התאגיד ופעילותו, היוצרים סיכונים מהותיים בתחום הסייבר, והעלויות וההשלכות הפוטנציאליות של סיכונים אלה, לרבות סיכונים ספציפיים לתחום פעילותו וסיכונים של ספקי שירות וצדדים שלישיים אחרים עימם התאגיד בא במגע.
- המשאבים הכרוכים בשמירה על הגנות סייבר לרבות כיסוי ביטוחי.
- הפוטנציאל לפגיעה בנכסים ובכללם קנין רוחני ומוניטין, וכן עוצמת הפגיעה האפשרית ביתרונות תחרותיים שיש לתאגיד.
- חוקים ותקנות קיימים או תלויים ועומדים, אשר עשויים להשפיע על העלויות.

תקנות ניירות ערך ועמדת רשות ני"ע 33-105 (2)

GROSS GKH
– גרוס ושות' עורכי דין –

חובת גילוי בתשקיף ובדוח התקופתי

- חובות הגילוי במקרה של אירוע או ענין החורגים מעסקי התאגיד הרגילים (סעיף 36 לתוספת הראשונה לתקנות פרטי תשקיף):

תיאור אודות זהות או סוג התוקפים, נסיבות התקיפה, כמות התקיפות ומשך זמן התקיפה, האם להערכת התאגיד היא הסתיימה, היקף וסוג הנזק שאירע לרבות השלכות עקיפות, הערכת התאגיד האם אותר מלוא הנזק הישיר, התמודדות התאגיד עם התקיפה, הפקת לקחים והאמצעים שננקטו כדי למנוע תקיפה חוזרת ועוד.

תקנות ניירות ערך ועמדת רשות ני"ע 33-105 (3)

גילוי בדו"ח הדירקטוריון:

דוח **מצב התאגיד** (תקנה 10 לתקנות הדוחות) **והשפעת גורמים חיצוניים** (סעיף 6 לתוספת הראשונה לתקנות הדוחות) -

במסגרת ההסברים תינתן התייחסות להשפעת האירועים על סעיפים מהדוחות הכספיים שהושפעו מהותית בשל סיכוני סייבר או תקיפות סייבר, כגון:

- סעיפים מאזניים כדוגמת לקוחות, מלאי, רכוש בלתי מוחשי כקנין רוחני, מוניטין וכדומה.
- סעיפים תוצאתיים כדוגמת אובדן הכנסות, ירידות ערך, הפרשות, פגיעה ברווחיות.
- סך העלויות שנוצרו לתאגיד הנובעות מהיערכות בגין הגנת סייבר.
- השפעת אירועי סייבר שטרם קיבלו או לא יקבלו ביטוי במסגרת הדוחות הכספיים אך הם מהותיים לפעילות התאגיד, למשל – הגשת תביעות, פגיעה בפיתוח מוצר של התאגיד או פעילות אחרת שלו, פגיעה בתיק הלקוחות, פגיעה במוניטין או ביתרונות תחרותיים וכו'.

תקנות ניירות ערך ועמדת רשות ני"ע 33-105 (4)

גילוי בדו"חות מידיים:

- אירוע או ענין החורגים מעסקי התאגיד הרגילים (תקנה 36(א) לתקנות הדוחות)

- תיאור האירוע – על התאגיד לכלול מידע בקשר עם מועד תחילת האירוע ומועד סיומו, מה כלל האירוע, סוג הנתונים שנחשפו, הגורמים שהביאו לקרות האירוע וצעדים שננקטו בעניינו.

- תיאור הנזק והערכת הנזק – הפעילויות והנכסים שהושפעו מהאירוע והערכת הפגיעה בהם, השפעה אפשרית על תוצאות פעילות התאגיד ובכלל זה פגיעה אפשרית בהכנסות, פגיעה ביחסי לקוחות, ספקים, או פגיעה במוניטין של התאגיד.

- דיווחים משלימים עם התבררות היקף הנזק, חשיפות לתביעות משפטיות, עלויות מהותיות להקמת מערכות הגנה חדשות וכדומה.

הנחיות מערך הסייבר הלאומי

- מערך הסייבר הלאומי הוא גוף ממלכתי, ביטחוני וטכנולוגי האמון על הגנת מרחב הסייבר הלאומי ועל קידום וביסוס עוצמתה של ישראל בתחום. עם זאת, מעמדו טרם הוסדר בחקיקה על אף ניסיונות לעשות כן.
- מסמך תורת ההגנה בסייבר לארגון (גרסה 2) מהווה **מסמך המלצה** לכלל הארגונים במשק המגדיר את כללי הממשל התאגידי בתחום הגנת הסייבר המצופים מהדירקטוריון, הנהלת החברה והממונים על המידע ואבטחתו בארגון.

תקנים מקצועיים בינ"ל – לשכת המבקרים הפנימיים העולמית (IIA)

GROSS GKH
– גרוס ושות' עורכי דין –

תקן 1210 - המבקרים פנימיים חייבים להיות בעלי הידע, המיומנויות והיכולות האחרות, הדרושים לביצוע הפעילויות, שבאחריותם האישית. הביקורת הפנימית, כיחידה, חייבת להיות או לרכוש את הידע, המיומנויות והיכולות, הדרושים לביצוע הפעילויות שבאחריותה.

1210 .A3 - מבקרים פנימיים חייבים להיות בעלי ידע מספק אודות עיקרי הסיכונים בתחום טכנולוגיות המידע, הבקרות וטכניקות ביקורת מבוססות- טכנולוגיה, הזמינות לביצוע עבודתם. עם זאת, אין לצפות מכל המבקרים הפנימיים, שתהיה להם המומחיות של מבקר פנימי שאחריותו העיקרית היא ביקורת טכנולוגיות מידע

1220.A3 - מבקרים פנימיים חייבים להיות ערים לסיכונים משמעותיים, העלולים להשפיע על השגת יעדים, על פעולות או על משאבים. עם זאת, נוהלי הביקורת כשלעצמם, אפילו אם הם מבוצעים בזהירות מקצועית ראויה, אינם מבטיחים שכל הסיכונים המשמעותיים יזוהו.

תקן 2120 - ניהול סיכונים - הביקורת הפנימית חייבת להעריך את האפקטיביות, ולתרום לשיפור תהליכי ניהול סיכונים.

תפקיד המבקר הפנימי בתחום ניהול סיכוני הסייבר – הלכה למעשה

- המבקר הפנימי יערוך תכנית ביקורות תקופתיות בתחום הגנת הסייבר.
- המבקר הפנימי יבדוק איזו רגולציה חלה אל הארגון בתחום הגנת הסייבר וכיצד הארגון פועל ליישומה בתוך הארגון.
- המבקר הפנימי יבדוק האם יש תקינה שהארגון עומד/נדרש לעמוד בה (ISO, NIST, HIPAA)
- המבקר הפנימי יאסוף מידע באמצעות גורמי מפתח שונים בארגון, לרבות מנהל מערכות מידע, מנהל אבטחת המידע וקצין הציות.

תפקיד המבקר הפנימי בתחום ניהול סיכוני הסייבר – הלכה למעשה (2)

- **ממשל תאגידי** – המבקר הפנימי יבדוק האם קיימים **תהליכי עבודה ונהלים ברמת ההנהלה הבכירה והדירקטוריון בתחום הסייבר**; והאם הוגדרו תפקידים וחלוקת אחריות ברורה בין בעלי התפקידים בכדי להבטיח תכנית עבודה יעילה ואפקטיבית.
- האם מונה ממונה הגנת סייבר בארגון והאם הוקצו משאבים לפעילותו על פי תכנית העבודה שתאושר בדירקטוריון.
- האם הוצגה ואושרה מדיניות אבטחת המידע והגנת הסייבר הארגונית אחת לשנה לפחות?
- האם קיימים נהלים לניהול משברי סייבר – החל מדיווח וכלה בהתאוששות מאסון והמשכיות עסקית (תיעוד ולוגים, תהליכי גיבוי ופעולה ידניים ומנותקים, הפרדת סביבות)?
- האם מתקיים דיון תקופתי בדירקטוריון (בו נוכח המבקר) בנושאים הקשורים לסיכוני סייבר, במסגרתו ניתנים דיווחים על אירועי סייבר ומקרים של כשלים באבטחת מידע.

תפקיד המבקר הפנימי בתחום ניהול סיכוני הסייבר- הלכה למעשה

ביצוע סקר סיכונים/השתלבות בסקר סיכונים המתבצע על ידי מומחה סייבר :

1. **סקר סיכוני סייבר -** זיהוי סיכוני הסייבר המשפיעים על הארגון (BIA)

2. **הערכת ותיעדוף סיכוני סייבר -** הערכת עוצמת סיכוני הסייבר והסבירות להתממשותם ותיעדוף הטיפול בסיכונים בראיית ההנהלה.

3. **תכנית עבודה להקטנת החשיפה לסיכוני סייבר ולוחות זמנים -** יצירת תכנית יעילה למענה לסיכוני הסייבר והמלצות לשימוש בכלים אפקטיביים לנטרולם בלוחות זמנים תואמים. במקביל לכך - הטמעה של תוכנית העבודה בדרגים הרלוונטיים על מנת לוודא את יישומה.

4. **ניטור ומעקב שוטפים -** קבלת דיווחים אמינים על הנתונים המנוטרים באמצעות כלי הבקרה של הארגון, תוך קיום תקשורת עם ההנהלה ושימוש במומחים בתחום.

5. **אכיפה יעילה** – טיפול הארגון בכשלים והפרות של נהלי הארגון בתחום הגנת הסייבר לצורך צמצום החשיפה לסיכונים.

6. **דיווח תקופתי והפקת לקחים** – באופן שוטף.

GROSS GKH

גרוס ושות׳ עורכי דין

תודה רבה!

צביקה גלבוע, עו״ד

גרוס ושות׳

טל׳: 6044810- 03 דוא״ל: ZVIG@GKH-LAW.COM