חובות דיווח לרגולטורים
כתוצאה מפריצת סייבר

עו"ד אביעד לחמנוביץ'
בנקאות ופיננסים

Azrieli Center The Square Tower
132 Begin Rd. Tel Aviv 6701101 Israel
Office: +972-3-684-6000
Fax: +972-3-684-6001
Prof. Yuval Levy & Co. (1973)
Tadmor & Co. (2005)

על מה נשוחח?

01 חובות דיווח פרטניות במקרה של אירוע סייבר

- רשות הגנת הפרטיות
- רשות ניירות ערך
- רשות שוק ההון ביטוח וחיסכון
- בנק ישראל
- מערך הסייבר הלאומי
- משטרת ישראל

02 סקירה כללית על הצעת חוק הסייבר העדכנית ביותר

תקנות הגנת הפרטיות (אבטחת מידע), תשע"ז-2017

תיעוד של אירועי אבטחה ס' 11ד' | אירע אירוע

1. יודיע על כך בעל ,המאגר לרשם באופן מיידי, וכן ידווח לרשם על הצעדים שנקט בעקבות האירוע;
2. רשאי הרשם להורות לבעל מאגר המידע, למעט לבעל מאגר מידע מן המנויים בסעיף 13(ה) לחוק, לאחר שנועץ בראש הרשות הלאומית להגנת הסייבר, להודיע על אירוע האבטחה לנושא מידע שעלול להיפגע מן האירוע.

ס' 1- **"אירוע אבטחה חמור"** – כל אחד מאלה:

1. במאגר מידע שחלה עליו רמת אבטחה גבוהה – אירוע שנעשה בו שימוש במידע מן המאגר, בלא הרשאה או בחריגה מהרשאה או שנעשתה פגיעה בשלמות המידע;
2. במאגר מידע שחלה עליו רמת אבטחה בינונית – אירוע שנעשה בו שימוש בחלק מהותי מן המאגר, בלא הרשאה או בחריגה מהרשאה או שנעשתה פגיעה בשלמות המידע לגבי חלק מהותי מן המאגר.

"באופן מידי" עמדת הרשות, כפי שמוצאת ביטוי במסמך מדיניות שהרשות פרסמה לאחרונה היא כי על הדיווח להתבצע ככלל בתוך 24 שעות ממועד גילוי האירוע ובכל מקרה לא יאוחר מ-72 שעות מאותו מועד.

הדיווח מתבצע דרך טופס מקוון באתר הרשות.

הרשות לניירות ערך | עמדה משפטית מספר 105-33 :גילוי בנושא סייבר

על פי העמדה שפורסמה, הרשות לניירות ערך מבחינה בין חובות הגילוי בדיווח מידי, גילוי בתשקיף (ובדו"ח התקופתי) וגילוי בדו"ח הדירקטוריון, כמפורט להלן:

גילוי בדיווחים מידיים

בהתאם לתקנה 36 לתקנות הדוחות, תאגיד מדווח נדרש לדווח מידית על כל אירוע או עניין החורגים מעסקי התאגיד הרגילים, אשר יש להם או עשויה להיות להם השפעה מהותית על התאגיד. בנוסף, הדיווח יכלול כל פרט חשוב להערכת השלכות האירוע על עסקי התאגיד, ובכלל זה תיאור האירוע, תיאור הנזק, הערכת הנזק ודיווחים משלימים על האירוע.

גילוי בתשקיף ובדו"ח תקופתי

(ב) גילוי מכוח תקנה 36 לתוספת הראשונה לתקנות פרטי תשקיף, המטילה חובות גילוי במקרה של אירוע או עניין החורגים מעסקי התאגיד הרגילים. יש לכלול תיאור תמציתי של עיקרי האירוע, זהות או סוג התוקפים, נסיבות התקיפה, משך זמן התקיפה, הערכה האם התקיפה הסתיימה, היקף וסוג הנזק וכדומה.

TADMOR LEVY

המפקח על הבנקים | הוראת נב"ת 361 ניהול הגנת הסייבר

פרק ה'- יעדי בקרה ובקרות הגנת סייבר ס' 81-82

התאגיד הבנקאי יקיים מערך דיווח פנימי נאות כחלק מניהול סיכונים ואירועי סייבר. במסגרת זו תוגדר מדיניות דיווח מפורטת, שתקבע בין היתר את הגורמים הפנימיים והחיצוניים אליהם יתבצעו הדיווחים, את מתכונתם ואת תדירותם.

התאגיד הבנקאי ידווח לפיקוח על הבנקים על ***<u>אירוע סייבר</u>*** או על אירוע החשוד כאירוע סייבר, בהתאם להוראת ניהול בנקאי תקין מס' 366 בנושא "דיווח על אירועי כשל טכנולוגי ואירועי סייבר".

"אירוע סייבר הינו אירוע אשר במהלכו מתבצעת תקיפת מערכות מחשוב ו/או מערכות ותשתיות משובצות מחשב על ידי, או מטעם, יריבים (חיצוניים או פנימיים לתאגיד הבנקאי) אשר עלולה לגרום להתממשות סיכון סייבר. יצוין, כי בהגדרה זו נכללים גם ניסיון לביצוע תקיפה כאמור גם אם לא נגרם נזק בפועל".

רשות שוק ההון | חוזר גופים מוסדיים 14-9-2016

ניהול סיכוני סייבר בגופים מוסדיים | ס' 5- הגנת סייבר של גוף מוסדי

ס' 5א3יא'

"גוף מוסדי ידווח בהקדם האפשרי לדירקטוריון הגוף המוסדי ולממונה על שוק ההון, ביטוח וחיסכון על כל **<u>אירוע סייבר</u>** **<u>משמעותי</u>** שכתוצאה ממנו, באופן ישיר או עקיף:

1) נפגעו או הושבתו מערכות ייצור המכילות מידע רגיש למשך של יותר מ-3 שעות.
2) יש אינדיקציות לכך ש**<u>מידע רגיש</u>** של לקוחות הגוף המוסדי או עובדיו נחשף או דלף".

ס' 2, ס' ההגדרות:

"אירוע סייבר" כל מקרה של תקיפת מערכות או אמצעי טכנולוגי אחר ששייכים לגוף מוסדי, העלולה לפגוע בסודיות, שלמות או זמינות מערכות או המידע של גוף מוסדי.

"מידע רגיש" כהגדרתו בחוק הגנת הפרטיות, תשמ"א-1981 ,וכל מידע אשר סווג על ידי הגוף כרגיש.

משטרת ישראל

- גוף אופציונלי שניתן ואף רצוי לדווח לו בעת אירוע פריצת סייבר.

- במשטרה היחידה הרלוונטית היא יחידת הסייבר הארצית בלהב 433- היחידה אמונה על חשיפת פשעי סייבר, איסוף מודיעין ברשת, נטרול גורמי פשיעה במרחב המקוון המאיימים על תשתיות קריטיות, טיפול בתופעות כגון סחיטה במרחב הקיברנטי, גניבת מידע, הפצת רוגלות וחקירת עבירות סייבר מתוחכמות. היחידה עובדת בשיתוף פעולה עם גורמים אזרחיים, ארגוני אכיפה בארץ ובעולם, מוסדות אקדמיים וארגונים בינלאומיים.

- בשנים האחרונות, היחידה הגבירה את פעילותה, וניתן למצוא דוגמאות לאירועי סייבר שנפתרו בעזרתה כדוגמת, "פרשיית ההאקר מאשקלון".

מערך הסייבר הלאומי

- גוף אופציונלי נוסף שניתן לפנות אליו בעת הצורך.

- המערך הוא הגוף הממלכתי המופקד על הגנת מרחב הסייבר הלאומי של מדינת ישראל מפני איומי סייבר, ועל קידום וביסוס עוצמתה בתחום.

- למערך הסייבר אין סמכויות אכיפה משלו והוא מספק שירותי ייעוץ, הנחיה והכוונה בלבד. כמו כן המערך אינו יכול לקבוע מדיניות או לפקח על יישומה. בסופו של דבר מדובר בגוף מייעץ בעיקר, שלו גם יכולות פיתוח טכנולוגיות.

- בנוסף המערך אחראי על המרכז הארצי לניהול אירועי סייבר (CERT - ה) שמטפל באירועי סייבר במרחב האזרחי במדינה.

הצעת חוק סמכויות לשם חיזוק הגנת הסייבר (הוראת שעה), התשפ"א-2021

ההצעה הונחה על שולחן הממשלה ב- 26.02.2021, ועל כן רלוונטית ומרמזת על כיוון המדיניות העתידית.

כיום, למערך אין סמכות אכיפה (למעט ביחס לגופים המנויים בתוספת החמישית לחוק הסדרת הביטחון בגופים ציבוריים) והוא בבחינת גוף מייעץ ומנחה.

במידה ותאושר הצעת החוק יוכל המערך להורות לארגון שמקיים פעילות חיונית לבצע הנחיות מקצועיות שלו תחת תנאים מסוימים. ההנחיות יחייבו גם חברות פרטיות. סוג ההוראות אינו מפורט בהצעת החוק.

המערך יוכל לשלוח מטעמו עובד באישור בית משפט לבצע פעולות הכנת סייבר בארגון, כולל כניסה למקום הארגון והחרמת חפצים, ובמקרים מסוימים גם איסוף מידע מוגן פרטיות, במקרה שהארגון מסרב לציית להוראות המערך.

גורם במערך יוכל לפנות לשב"כ או לספק אינטרנט בכדי לקבל מידע לגבי זהות לקוח, אם בידיו מידע שלפיו מחשבי הלקוח נמצאים בסיכון או שהם נמצאים תחת מתקפת סייבר.

מבקרי הצעת החוק טוענים כנגד הקניית כוח רב מדי למערך, ויצירת רגולטור נוסף שיהווה נטל מיותר על הגופים העסקיים בישראל.

תודה רבה

TADMOR LEVY