

## 10 צעדים לצמצום החשיפה המשפטית בתחום הסייבר

איומי הסייבר כנגד חברות מסחריות גברו באופן משמעותי בשנים האחרונות. מעטות הן החברות שלא חוו כלל אירוע סייבר, בין אם מדובר בהשבתת מערכות הארגון לצד דרישת כופר (ransomware), בגניבת פרטי לקוחות, בגישה לא מורשית של עובדים למידע רגיש או בתקיפת אתרי אינטרנט. התגברות איומי הסייבר בצירוף הנזק החמור שהן עלולות לגרום לחברות (חשיפת מידע אישי של לקוחות, פגיעה בתהליכי ייצור, מחיקת רשומות, ריגול עסקי ועוד) עלולים ליצור חשיפות משפטיות משמעותיות לחברה. כפועל יוצא מכך, מנהלי החברה וחברי הדירקטוריון שלה עלולים אף הם להיות חשופים אם לא נקטו צעדים סבירים להכנת החברה להתמודדות עם אירועי סייבר.

דומה כי התפיסה הרווחת כיום היא כי לא ניתן לחסן את הארגון באופן מוחלט מפני התקפות סייבר, אולם ניתן לפעול לצמצום הסיכונים הנובעים מהתקפות כאלה באמצעות תכנון מראש ואימוץ מדיניות סדורה בנושא. על רקע זה, מובאים להלן 10 צעדים שעשויים לסייע לחברה לצמצם את הסיכונים המשפטיים הנשקפים לה, למנהליה ולחברי הדירקטוריון שלה כתוצאה מאירועי סייבר. למותר לציין, כי אין מדובר ברשימה ממצה וכי ההתמודדות עם הסיכונים המשפטיים בתחום זה מחייבת בחינה פרטנית של מאפייני הארגון, הסיכונים שלהם הוא חשוף, הרגולציה שחלה עליו וכיוצא בזה.

### 1. הערכת סיכונים:

הארגון יקיים הליך של הערכת סיכונים הסייבר שלו. בין היתר, במסגרת זו, הארגון יזהה את הנכסים שברשותו (ובפרט, נכסי מידע) וימפה את הסיכונים לנכסיו ואת האמצעים למזעורם. הערכת הסיכונים תעודכן בהתאם לצורך ולכל הפחות אחת לשנתיים.

### 2. אימוץ מדיניות סייבר ארגונית:

המדיניות תמפה את סיכונים הסייבר של הארגון לאור מאפייני פעילותו (לרבות לאור הרגולציה החלה על הארגון, סוגי המידע שהוא מחזיק וקשריו עם ספקים ולקוחות) ותגדיר יעדי הגנת הסייבר, תחומי אחריות, בעלי תפקידים וממשקי עבודה ביניהם. בין היתר, המדיניות תתייחס להתמודדות עם מצבי קיצון (הקמת צוות לניהול משברים, קביעת נהלי דיווח, חלוקת אחריות וסמכויות, תרגול מצבי קיצון וכו'). מדיניות הסייבר תאושר על-ידי דירקטוריון הארגון, תיבחן מחדש לפחות אחת לשנה ותעודכן בהתאם לצורך.

### 3. אימוץ תכנית עבודה:

התכנית תפרט, כנגזרת ממדיניות הסייבר, צעדים לצמצום סיכונים הסייבר, תיעדוף בין צעדים אלה ומנגנוני בקרה ומעקב למימוש התכנית. התכנית תאושר על-ידי הנהלת הארגון, אשר תקצה משאבים הולמים למימושה.

#### 4. אימוץ נהלי אבטחת סייבר:

הנהלים יגדירו, בהתאם למדיניות הסייבר, את הכללים שיחולו על עובדי הארגון במסגרת הפעילות השוטפת, לרבות בהיבטי אבטחת רשתות, עדכון סיסמאות, הרשאות גישה, מדיניות למכשירים המתחברים לרשת הארגונית, שימוש במחשב ענן, תהליכי הכנסת מידע לארגון והוצאתו, הצפנת מידע וביעור מידע שאין בו צורך. כמו כן, הנהלים יתייחסו להיבטים של אבטחה פיסית של הארגון מפני גישה של גורמים לא מורשים למתחם הארגון או למקומות רגישים במתחם.

#### 5. מינוי בעלי תפקידים:

א. הארגון ימנה מנהל הגנת סייבר (Chief Information Security Officer), שיפעל בכפיפות לדרג ניהולי בכיר בחברה ויהיה אמון על הובלת הגנת הסייבר הארגונית, לרבות באמצעות מעקב ובקרה אחר יישום תכנית העבודה.

ב. הארגון ימנה ועדת היגוי בראשות חבר בהנהלת הארגון ובהשתתפות מנהל הגנת הסייבר, יועץ משפטי, מנהלים מתחומי הכספים והתפעול ומשתתפים נוספים בהתאם לאופי הארגון. ועדת ההיגוי תהיה אמונה, בין היתר, על תיאום בין-אגפי בארגון לשם מימוש מדיניות הסייבר הארגונית.

#### 6. הדרכות לעובדים והטמעת צעדי הגנה בתהליך גיוס עובדים:

העברת הדרכות להגברת מודעות עובדי הארגון לסיכוני סייבר ולהטמעת נהלי אבטחת הסייבר – אחת לשנה לפחות (ביחס לעובדים בתפקידים רגישים מבחינת גישה למידע יש לשקול הדרכות תכופות יותר). כמו כן, בחינת הצורך בעריכת בדיקות אמינות למועמדים למשרות רגישות (למשל, משרות המאפשרות גישה למידע רגיש) ווידוא שהסכמי ההעסקה של הארגון כוללים התייחסות לאחריות העובד בנוגע לסיכוני סייבר.

#### 7. אכיפת נהלים:

ביצוע ביקורות ובקורות על מנת לוודא כי המדיניות, תכנית העבודה והנהלים אכן מקוימים הלכה למעשה.

#### 8. הסדרה הסכמית:

הטמעת דרישות מתחום הגנת הסייבר בהסכמים עם ספקים, לקוחות וגורמים אחרים שעשויים לבוא במגע עם מערכות הארגון או לקבל גישה למידע שברשותו.

#### 9. ביטוח סייבר:

בחינת רכישתה של פוליסה לביטוח סיכוני סייבר.

#### 10. יועץ סייבר:

התקשרות (במידת הצורך) עם יועץ סייבר, לבדיקת מערכות ההגנה הקיימות בארגון, ביצוע סקרים ומבחני חדירה ושיפור המוכנות לאירועי סייבר.

צוות הסייבר, הגנת הפרטיות ואבטחת המידע של גורניצקי מציע ללקוחות גישה מקיפה ורב תחומית להתמודדות עם האתגרים המשפטיים החדשים בתחום ניהול הגנת הסייבר והגנת הפרטיות.



אסף הראל (עו"ד)

assafh@gornitzky.com ✉

office: +972-3-7109191 ☎

fax: +972-3-5606555 📠



תימור בלן (שותף)

timorb@gornitzky.com ✉

office: +972-3-7109191 ☎

fax: +972-3-5606555 📠