

התמודדות עם משברי סייבר וצמצום החשיפה המשפטית הנובעת מהם

מאז תחילת מלחמת 'חרבות ברזל' ניכרת עלייה של עשרות אחוזים במספר מתקפות הסייבר על יעדים בישראל, ולפי דיווחי הרשות להגנת הפרטיות מספר אירועי האבטחה החמורים שדווחו לרשות - הוכפלה.

בתוך כך, החשיפה המשפטית כתוצאה ממשברי סייבר, לחברות ולנושאי משרה בהן, גוברת אף היא. כך, פורסמו בחודשים האחרונים שינויי חקיקה והצעות חוק שמרחיבים את סמכויות הממשלה בתחום הסייבר ושואפים להגדיל את הסנקציות שניתן להטיל על חברות שאינן מיישמות אמצעי אבטחת מידע נאותים. לצד זאת, ניכרת התגברות בהגשת בקשות לאישור תובענות ייצוגיות כנגד חברות בגין אירועי דלף מידע.

אין כמעט ארגון שלא יתמודד עם משבר סייבר במהלך חייו, ועל הנהלת הארגון להיערך ברצינות ובמקצועיות לניהול המשבר. החמרת האיומים, והחשיפה המשפטית הנלווית להם, מחייבות חברות לנקוט גישה פרואקטיבית הן בשלב ההיערכות לאירועי סייבר, והן בשלב ניהול האירוע עצמו.

עקרונות מנחים בטיפול במשברי סייבר

השעות הראשונות הן "שעות הזהב".
בשעות אלה ניתן להציל את מה שיהיה קשה להציל לאחר מכן.

ניהול משבר לא דומה לניהול בשגרה.
בהתאם, קיימת חשיבות רבה לשילוב של צוות מקצועי המתמחה בניהול משברים.

ניהול המשבר לא מחליף את שיקול הדעת של המנהלים.
יחד עם זאת, הוא מאפשר לנהל ולצמצם את החשיפה לתביעות אישיות או לתביעות כנגד הארגון, ומאפשר "לכתוב את כתב ההגנה הארגוני" תוך כדי המשבר.

אם יש ספק, אין ספק – וחשוב להתייעץ.

ליווי משפטי 360 מעלות – בהיבטי ממשל תאגידי והגנה על נושאי משרה, הגנת הפרטיות, חובות דיווח לרשויות, דיני עבודה, חוזים מול לקוחות וספקים, חובות רגולטוריות של גופים מפוקחים (בנקים, מבטחים, חברות ציבוריות וכו'), בניית מוכנות להליכי ליטיגציה ועוד.

ליווי וייצוג מול הרשויות בהיבטים הנוגעים להשפעות המשבר, וצמצום הסיכון בהטלת הגבלות וקנסות. משרדנו מנוסה בעבודה עם הרשות להגנת הפרטיות, מערך הסייבר הלאומי, משרת ישראל ומגוון גופים ממשלתיים נוספים.

ביטוח סייבר – ליווי הארגון אל מול המבטחים כדי להבטיח מיצוי זכויות על-פי פוליסת ביטוח הסייבר.

חברות רב-לאומיות – ליווי חברות רב-לאומיות המתמודדות עם משברים המתנהלים במקביל במספר מדינות.

תגובה מהירה והקמה מיידית של חמ"ל מומחים ייעודי למשבר – קיימת חשיבות מכרעת לתגובה מהירה כדי לבלום את מתקפת הסייבר, לצמצם השפעתה על הארגון ולאפשר המשך עבודה באופן מיטבי.

ניהול המשבר וצוותי העבודה המטפלים בו – משרדנו עובד עם יועצים מובילים בתחום הטכנולוגיה, היח"צ, הדוברות והמו"מ למתן מענה לכל היבטי המשבר.

התמודדות עם מתקפות כופרה – הפעלת צוות מו"מ בעל ניסיון מול תוקפים וליווי בהיבטים המשפטיים והרגולטוריים הנוגעים לתשלומי כופרה.

הפעלת מומחים פורנזיים וטכנולוגיים לאיתור ומיגור התקיפה ושיקום המערכות.

ייעוץ בהיבטי המשכיות עסקית מול עובדים, ספקים ולקוחות ושחזור מערכות.

איתור והשבת כספים ונכסים שנגנבו בהונאות סייבר.



בניית מוכנות למשברי סייבר ודלף מידע

נקיטת צעדי היערכות מראש מצמצמת משמעותית את הסיכונים והחשיפה ממשברי סייבר ואת משך הטיפול בהם. בהקשר זה, אנו מציעים שלושה "מסלולים":

- מסלול בסיסי:** מסלול זה כולל הכנת תשתית בסיסית להתמודדות עם משבר סייבר, בדגש על בניית "תיק אתר" (מיפוי תשתיות ומערכות המידע של הארגון) והכוונה בסיסית בהיערכות למשברי סייבר בהיבטי ממשל תאגידי, חובות נושאי משרה, הגנת הפרטיות, דיני עבודה ומשאבי אנוש.
- מסלול ביניים:** מסלול זה כולל הכנה מקיפה יותר למשבר הסייבר ובנוסף למסלול הבסיס, כולל גם הכנת gap analysis מקיף ביחס למוכנות הארגון, מתן המלצות לטיפול בפערים, ובניית נוהל (playbook) להתמודדות עם משברי סייבר.
- מסלול מקיף:** מסלול זה כולל, בנוסף למסלול הביניים, בניית תהליך ניהול סיכונים סייבר, הטמעת דרישות רגולציה בתחום הסייבר בארגון (תקנות הגנת הפרטיות, דרישות שחלות על גופים מפוקחים וכו'), התאמת חוזים עם ספקים ולקוחות, ייעוץ מקיף בהיבטי ממשל תאגידי, חובות נושאי משרה, הגנת הפרטיות, דיני עבודה ומשאבי אנוש, ותרגילי הנהלה וסימולציות.



אסף הראל, שותף
asaf.h@gornitzky.com

השירותים ניתנים על-ידי משרדנו בשיתוף עם מומחים מנוסים ממגוון תחומים. צוות ניהול משברי הסייבר בהובלתו של עו"ד אסף הראל מזמין אתכם ליצור עמנו קשר לקבלת ייעוץ. הן בנוגע לאופן שבו נכון להיערך מראש לסוגים שונים של משברי סייבר ולמזער את החשיפה מהם, וכמובן מיד כאשר עולה חשד לפרוץ משבר סייבר, שבו אלמנט הזמן מהותי, ויש לקבל תמיכה מקצועית מהירה.