

# Cyber-Security, Data Protection and Privacy

## 10 צעדים לצמצום החשיפה המשפטית ממתקפות סייבר



בעת האחרונה אנו עדים לגידול משמעותי בהיקף מתקפות הסייבר כנגד חברות וארגונים בישראל. כפי שעולה מהאירועים האחרונים, המתקפות עלולות להשבית כליל את מערכות המחשוב של הארגון, לשבש משמעותית את פעילותו התפעולית ולהביא לדליפה של מידע סודי ורגיש, ובכלל זה מאגרים הכוללים מידע אישי.

מעבר להשלכות בפן התפעולי, המסחרי והתדמיתי, אירועי סייבר עלולים לגרור השלכות משפטיות משמעותיות על הארגון, לרבות הגשת תביעות ונקיטת הליכים מנהליים כנגד הארגון ונושאי המשרה בו.

הנחת העבודה של כל ארגון בישראל צריכה להיות שהוא עלול להיות יעד לתקיפה. מניסיוננו בליווי חברות שנפלו קורבן למתקפות סייבר עולה, כי מהר מאוד לאחר שמתגלה האירוע, עולות שאלות בדבר הצעדים שהארגון נקט, או לא נקט, מראש כדי לצמצם את הנזק מהתקיפה.

על רקע זה, ריכזנו עבורכם 10 צעדים שכל ארגון יכול לנקוט מראש במטרה לצמצם משמעותית את החשיפה המשפטית הנובעת ממתקפות סייבר:

- 1. מפו את המידע הארגוני:** קיימת חשיבות רבה לכך שהארגון ידע מהם נכסי המידע שלו, בדגש על מידע סודי או רגיש ומידע אישי, והיכן הם מאוחסנים (ובכלל זה, אצל אילו ספקי שירות של הארגון מצוי המידע). מיפוי זה קריטי לצורך הגדרה והפעלה של מנגנונים לאבטחת המידע.
- 2. היפטרו ממידע מיותר:** במקרים רבים, דווקא מידע רגיש שהארגון לא עושה בו שימוש (למשל, טבלת אקסל ישנה הכוללת מידע על לקוחות החברה) הוא זה שדולף במתקפות סייבר. מידע מיותר עלול לגרור חשיפה משפטית מיותרת. על כן, מומלץ לערוך בדיקה עיתית של המידע הקיים בארגון ולמחוק מידע שאיננו נדרש עוד (בכפוף למדיניות שמירת המידע הארגונית).
- 3. אמצו נהלי אבטחת מידע ומנו מנהל הגנת סייבר ארגוני:** תקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017 מחייבות את רוב החברות בישראל לאמץ נהלי אבטחת מידע. מעבר להיותם מחויבים על-פי דין, אימוץ נהלי אבטחת מידע חשוב לשם התאמת אמצעי ההגנה של הארגון לאיומי הסייבר הנשקפים לו וכדי לאפשר לו לגבש ולהבנות את תפיסת ההגנה שלו. במסגרת הנהלים, ראוי להסדיר גם את אופן ההתמודדות של הארגון במקרה של מתקפת סייבר. לצד זאת, חשוב שהארגון ימנה מנהל הגנת סייבר שאחראי, בין היתר, על כתיבת הנהלים, הטמעתם ועדכוןם.
- 4. הטמיעו כלים טכניים להגנה על המידע:** בנוסף להטמעת נהלים בתחום אבטחת המידע, קיימת חשיבות רבה גם לשימוש באמצעים טכניים מקובלים להגנה על מערכות הארגון ועל המידע המצוי בהן, כגון שימוש בתוכנת אנטי וירוס עדכנית, הצפנת מידע, שימוש באמצעי זיהוי ואימות של מורשי גישה למידע (כגון two-factor authentication) וכדומה. כמו כן, חשוב לוודא כי התוכנות המותקנות בארגון מעודכנות באופן שוטף בעדכוני אבטחה.
- 5. בדקו את הספקים שלכם:** בשנים האחרונות הרשות להגנת הפרטיות נקטה מספר הליכי אכיפה כנגד ארגונים בגין אירועים שבהם דלף מידע של הארגון שהוחזק אצל ספק חיצוני. טרם ההתקשרות עם ספק אשר מערבת גישה של הספק למידע של הארגון, ובמהלך ההתקשרות, על הארגון לוודא כי הספק נוקט אמצעי אבטחת מידע נאותים. על הסכם ההתקשרות עם הספק לכלול דרישות אבטחת מידע בהתאם.

6. **בצעו מבדקי חדירה וסקרי סיכונים:** כלי חשוב למניעת אירועי סייבר הוא זיהוי מוקדם של פרצות אבטחה וסיכונים לדלף מידע, בין השאר באמצעות מבדקי חקירה וסקרי סיכונים תקופתיים, שנערכים באמצעות גורם חיצוני לארגון, ונקיטת פעולות לתיקון הליקויים שעלו מהם.

7. **הדריכו את העובדים:** במקרים רבים, תוקפים מצליחים לחדור לארגונים בזכות חוסר תשומת לב של עובד שלחץ על קישור דדוני שנשלח לו בדוא"ל או מסר לאחר את סיסמת ההתחברות שלו. על רקע זה, חשוב לערוך הדרכות עיתיות לעובדים שמטרתן להעלות את מודעותם לסיכוני הסייבר ולאמצעים שכל עובד יכול לנקוט כדי למזער סיכונים אלו.

8. **גבו את המידע:** היכולת של ארגון להתאושש ממתקפת סייבר מושפעת, במידה רבה, מטיב הגיבויים של הארגון ומהמהירות שבה ביכולתו לשחזר מידע מהם. על רקע זה, חשוב לוודא שהמידע הארגוני מגובה באופן שוטף ושהגיבויים נשמרים באופן שיבטיח את שלמות המידע ואפשרות השחזור שלו במקרה הצורך. חשוב גם לבדוק, באופן עיתי, את הגיבויים והיכולת לשחזר מידע מהם.

9. **מעורבות פעילה של הדירקטוריון:** לאור הסיכונים המשמעותיים שעלולים להיות למתקפת סייבר על פעילותה של חברה, על הדירקטוריון להיות מעורב, לקיים דיונים עיתיים בשילוב גורמי מקצוע רלוונטיים ולדרוש מידע בנוגע להיערכות החברה להתמודדות עם איומי סייבר. חשוב שהדירקטוריון יוודא שהחברה נוקטת צעדי היערכות למתקפת סייבר וישאל **מראש** את כל השאלות שממילא תישאלנה בדיעבד אם חלילה תותקף החברה.

10. **ביטוח סייבר:** פוליסת ביטוח סייבר מאפשרת לארגון לצמצם את הנזקים הכספיים שנובעים ממתקפת סייבר (כגון הפסדים הנובעים מהשבתה, הוצאות על מומחי פורנזיקה, תביעות צד ג' וכו'), לרבות במקרים שבהם הארגון נדרש לשלם כופר לתוקפים (בכפוף לכיסוי מתאים). לכן, מומלץ לוודא כי קיימת לארגון פוליסת ביטוח סייבר עם כיסוי הולם ולדרוש מספקים אשר מעבדים מידע של הארגון לרכוש פוליסת ביטוח מתאימה המכסה פעילות זו.

נקיטת צעדי היערכות לא תמנע בהכרח מתקפת סייבר על הארגון, אך צעדים אלה עשויים להקטין את הסיכוי לתקיפת סייבר כנגד הארגון ולצמצם משמעותית את ההשלכות מתקיפה, ככל שתתרחש, ואת החשיפה המשפטית הנובעת ממנה.

צוות הסייבר והגנת המידע בגורניצקי מסייע לארגונים לצמצם את החשיפה הנשקפת להם ממתקפות סייבר. בתוך כך, הצוות שלנו מלווה ארגונים במיפוי מאגרי מידע, גיבוש נהלי אבטחת מידע, הטמעת דרישות הדין בקשר עם הגנת סייבר ואבטחת מידע, ניסוח הסכמי הגנת מידע עם ספקים, ליווי משפטי לארגונים שהותקפו והתמודדות עם הליכי אכיפה מנהליים בקשר עם אירועי דלף מידע.

## לפרטים נוספים:



עו"ד רבקה גני

[rebeccage@gornitzky.com](mailto:rebeccage@gornitzky.com)



עו"ד אסף הראל, שותף

[assafh@gornitzky.com](mailto:assafh@gornitzky.com)

גורניצקי