גולדפרב זליגמן
עורכי דין | נוסד 1930

תל אביב
מגדל אמפא, רח' יגאל אלון 98
תל אביב 6789141, ישראל
טלפון (03) 608-9999
פקס (03) 608-9909
INFO@GOLDFARB.COM

ZURICH
14 Mittelstrasse
Zurich 8008, Switzerland
Tel +41 (44) 818 08 00
Fax +41 (44) 818 08 01
ZURICH@GOLDFARB.COM

WWW.GOLDFARB.COM

1.11.2021

מתקפות סייבר - סיכון ברור ומיידי

בצל התגברות מתקפות הסייבר – מהן הסכנות הטמונות לארגונים וכיצד להיערך נכון מבחינה ביטוחית.

התקפות סייבר דוגמת אירועי הנזק שאירעו לאחרונה בחברת הביטוח שירביט ובבית החולים הלל יפה, מבוצעות נגד תאגידים בעולם על בסיס יום יומי. חברות אשר מיישמות תכנית לניהול סיכון הסייבר כחלק מאסטרטגיית ניהול הסיכונים שלהן (תכנית הכוללת, בין היתר, נהלים ותוכניות בתחומי אבטחת מידע, הגנת הפרטיות, המשכיות עסקית, שרשרת אספקה, התקשרויות עם צדדים שלישיים, ביטוח סייבר, הדרכות לעובדים וכו') מגבירות את הסיכוי להתמודד בהצלחה עם אירוע מסוג זה.

הנזק הפיננסי והנזק למוניטין כתוצאה מאירוע סייבר, עלולים להיות משמעותיים ביותר ואף לסכן את המשך פעילותה של החברה. נזקים אלו כוללים, בין היתר, אבדן הכנסה, אבדן לקוחות, הוצאות כספיות מהותיות לצורך התמודדות וניהול המשבר, קנסות רגולטוריים, פיצויים חוזיים ללקוחות, דמי כופר, תביעות כספיות ופגיעה במוניטין.

<u>טרנדים עדכניים - עלייה מתמדת בסיכון בשל הגורמים הבאים</u>:

- **התקפות כופרה ממשיכות להוות סיכון משמעותי ביותר לתאגידים**: סך העלות הגלובלית של נזקי כופרה בשנת 2021 מוערך בסכום של כ- 20 מיליארד דולר; תשלום הכופר הממוצע בשנת 2020 גדל ב- 33% ביחס לשנת 2019 *
- **השפעות ה- COVID על אופן ניהול העסקים**: **התרחבות השימוש של חברות במודל תעסוקה הכולל חיבור מרחוק, הגידול בהיקף המסחר המקוון, והשימוש הגובר של תאגידים בטכנולוגיה** מנוצלים לרעה על-ידי גורמים חיצוניים לארגון ומגבירים את הסיכון.
- **גידול בחשיפה הנובעת משרשרת האספקה בארגון**: שימוש בספקי תכנה חיצוניים מגביר את הסיכון. מתקפות הסייבר במקרה של SolarWinds Orion platform ובמקרה של Microsoft Exchange, אשר השפיעו על תאגידים רבים בעולם הן דוגמאות למגמה זו.
- **התגברות הרגולציה בתחום הגנת הפרטיות ואכיפתה**: גידול במספר והיקף הקנסות מכוח רגולציית ה- GDPR, מגביר את הסיכון. לדוגמה חברת התעופה British Airways נקנסה בסך של כ- 20 מיליון פאונד בעקבות חשיפת מידע פרטי וכרטיסי אשראי של למעלה מ- 400,000 מלקוחותיה; חברת H&M בגרמניה נקנסה בסך של כ- 35 מיליון אירו בגין הפרת הפרטיות ביחס למידע של עובדיה.

ניהול סיכון הסייבר הינו באחריות נושאי המשרה והדירקטוריון של החברה, התרשלות בניהול סיכון זה עלולה לחשוף אותם לתביעות אישיות.

<u>ביטוח סייבר - אמצעי להקטנת הנזק הפיננסי וכלי עזר לניהול אירוע סייבר</u>:

ביטוח סייבר הינו פוליסת המכסה את אחריות החברה המבוטחת בגין נזק פיננסי הנגרם על-ידה לצד שלישי כתוצאה מכשל באבטחת המידע ו/או הגנת הפרטיות. בנוסף הפוליסה מכסה את הנזק הפיננסי לחברה עצמה כתוצאה מאירוע סייבר, הכולל פיצוי כספי בגין אבדן הכנסה, הוצאות ניהול אירוע הסייבר, הוצאות דמי כופר וקנסות רגולטורים הניתנים לשיפוי על-פי דין.

אחד היתרונות בפוליסת סייבר, הוא האפשרות להסתייע, לצורך ניהול המשבר בזמן אמת, בגורמים מומחים בעלי ניסיון בניהול אירוע הסייבר דוגמת יועצים משפטיים, מומחי פורנזיקה לזיהוי וטיפול בכשל האבטחה, מומחים בניהול מו"מ בתקיפת כופרה, ומשרד יחסי ציבור לניהול המשבר בתקשורת.

*Varonis cybersecurity statistics report 2021

<u>שינוי מגמה בשוק ביטוח הסייבר הגלובלי - צמצום הכיסוי ועליה בפרמיות:</u>

העלייה המשמעותית בנזקי הסייבר לאחרונה, אשר התגלגלה לפתחן של חברות הביטוח המבטחות סיכון זה, מתבטאת **בשינוי מגמה מהותי ביחס לעלויות, היקף ותנאי ביטוח הסייבר.**

מגמה זו מתבטאת **בצמצום היקף הכיסוי הביטוחי בפוליסות, עלייה מהותית בפרמיות הביטוח, עליה בסכומי ההשתתפות העצמית בפוליסות, ודרישה ממבוטחים ליתן גילוי מפורט ומקיף בטופס ההצעה לרכישת הביטוח ביחס לאופן בו הם מנהלים את סיכון הסייבר, לרבות עמידה בתנאי סף ביחס לרמת אבטחת המידע.**

דרישות המבטחים ביחס לרמת אבטחת המידע בחברה כתנאי לרכישת ביטוח הסייבר, מהוות גורם המאיץ את שיפור נהלי אבטחת המידע בחברות מחד, ומאידך מציבות אתגרים ועלויות נוספות לחברות. **חברות אשר אינן עומדות בדרישות רמת האבטחה, עלולות להתקשות למצוא כיסוי ביטוחי.**

דרישות הסף ביחס לאבטחת המידע כוללות בין היתר את הנושאים הבאים (הדרישות משתנות בין חברות הביטוח השונות):

- Multi Factor Authentication (MFA) for remote access and admin/privileged access
- Endpoint Detection and Response (EDR)
- Secured encrypted and detected backups
- Privilege access management
- Patch management /Vulnerability management
- Logging and monitoring network protections
- Email filtering and web security
- Cyber incident response planning and testing
- End of life system should be replaced or protected
- Remote Desktop Protocol (RDP) mitigation
- Vendors/Suppliers management
- Cyber security education and training to employees

ככל שנהלי אבטחת המידע והגנת הפרטיות בחברה מתקדמים יותר ומוטמעים בכל חלקי הארגון, כך יקל על החברה להשיג תנאים מיטביים בביטוח הסייבר.

על-פי נתוני הרבעון השלישי של 2021 מאת ברוקר הביטוח הגלובלי Marsh McLennan, מרבית המבוטחים בביטוח סייבר חוו עלייה בפרמיית הביטוח, ויותר ממחצית מהמבוטחים חוו עלייה בהשתתפות העצמית בפוליסה. מרבית אירועי הסייבר שדווחו למבטחים היו מתעשיית שירותי הבריאות, הטכנולוגיה, שירותים מקצועיים, מוסדות פיננסיים וקמעונאות**.

<u>המלצות בעת רכישה/חידוש פוליסת ביטוח סייבר:</u>

- מומלץ לבחון את דרישות המבטחים ביחס לרמת אבטחת המידע, ולוודא כי החברה הטמיעה או נמצאת בהליך בחינה של אמצעי אבטחת המידע הנדרשים.

**Cyber: State of the insurance market

- מומלץ לערב את הגורמים הרלוונטיים בחברה לצורך המענה על השאלונים מטעם המבטחים (מחלקת אבטחת מידע, מחלקת IT, המחלקה משפטית, מחלקת הכספים, ומחלקת רכש/ התקשרויות עם ספקים).
- **מומלץ להסתייע במומחים בתחום ביטוח הסייבר לצורך המענה על השאלונים מטעם המבטחים, לצורך משא ומתן עם המבטחים בעת רכישת הפוליסה, ולשם התאמת תנאי הכיסוי בפוליסה לצרכי החברה - על מנת להשיג תוצאות מיטביות לחברה בעת רכישת הפוליסה וחידושה.**

***

הסקירה לעיל הינה בבחינת תמצית. המידע הכלול בה נמסר למטרות אינפורמטיביות בלבד ואין במידע כדי להוות ייעוץ משפטי.

עו"ד דפנה לוטן מדוויר

שותפה, תחום ביטוח וניהול סיכונים

03-6089372 | dafna.lotan@goldfarb.com

**Cyber: State of the insurance market