

ביטוח סייבר – Cyber:

סיכוני סייבר אינם עוד נחלת סרטי מדע בדיוני בלבד, מידי יום מתפרסמות ידיעות על מתקפות מתוככמות שמבוצעות כנגד מדינות, ארגונים פרטיים וציבוריים, רשתות ציבוריות ופרטיות, תשתיות לאומיות ועוד. תוצאות מתקפות אלה עלולות להיות הרסניות עד כדי הפסקת פעילות של המותקף, אובדן הכנסות, פגיעה במוניטין, הוצאות משפטיות ואף פגיעה בחיי אדם.

האיום של מתקפות ההאקרים - בין אם המניע שלהם הוא כלכלי, פוליטי, אנרכיסטי או פוליטי – הולך ומחמיר עד לדרגה כזו שבה המומחים בתחום מודים כי כיום כבר בלתי אפשרי למנוע את החדירה באופן מוחלט.

לצד חברות אשראי, בנקים, מגה אתרי אינטרנט כגון פייסבוק וטוויטר או אתרי קניות באינטרנט, ההאקרים אינם פוסחים על חברות קטנות ובינוניות ואולי אף מתעניינים בהן יותר, באשר הן מניבות תגמול גבוה ביחס ל"השקעה" הכרוכה בפריצתן.

על-פי מחקר של ארגון מנהלי הסיכונים האירופי, סכנות הסייבר הן אחת מהדאגות העיקריות של מנהלי סיכונים בארגונים, לצד פגיעה במוניטין, שרשרת אספקה והמשכיות עסקית. מדובר בנזק ממוצע של עד 400,000 שקל לארגון קטן, ו-75% מהפריצות בארה"ב היו לעסקים עם פחות מ-100 עובדים.

דמיינו לרגע מה עלול לקרות לעסק, אם פעילות המחשוב בו פוסקת לשעה, ליום, לשבוע? מה הנזק העלול להיגרם לעסק שלך, ללקוחות, לעובדים?

במסגרת הפוליסות הקיימות בשוק, נכללים הכיסויים הבאים:

הוצאות:

1. הוצאות אם העסק גורם נזק לצד ג', כגון:

- ✓ עלות ההודעה ללקוחות (או לרשות המפקחת) שנתונייהם הושפעו מפריצת אבטחה.
- ✓ הוצאות סבירות לצורך הדרכה בנוגע לגניבת זהות וניטור פעילות האשראי של הפרטים שהושפעו.
- ✓ הוצאות הגנה ופיצויים אם העסק (או הפירמה המטפלת בענייניו במיקור חוץ) גרם לפריצה לנתונים אישיים או לנתוני התאגיד.
- ✓ הוצאות הגנה ופיצויים אם העסק נפגע מגניבת קוד גישה לנתונים באמצעים לא אלקטרוניים.
- ✓ הוצאות הגנה ופיצויים אם העסק נפגע מגניבת חומרה המכילה נתונים אישיים.
- ✓ הוצאות הגנה ופיצויים אם עובד בעסק גרם לחשיפת נתונים.

2. הוצאות אבטחת מידע והגנת הפרטיות, כגון:

- ✓ עלויות הייעוץ המשפטי והייצוג בקשר עם חקירת אבטחת מידע.
- ✓ קנסות והיטלים ברי ביטוח שתטיל רשות רגולטורית.

שירותי ייעוץ:

1. יועצים מומחי IT שפעלו למען העסק במהלך ואחרי פריצת סייבר, שבעיקר כולל הוצאות לאנשי מקצוע לשם קביעת היכולת להשבת נתונים אלקטרוניים, איסופם או יצירתם מחדש.
2. יועצים וממומחים להגנה על המוניטין של החברה ולשיקומו לאחר פריצת סייבר, כגון:
 - ✓ הוצאות ייעוץ מקצועי למניעת השלכות אפשריות או לצמצומן לאחר אירוע סייבר מתקשר
 - ✓ הוצאות ייעוץ מקצועי לצמצום הנזק האפשרי למוניטין של כל אדם פרטי בחברה (למשל קצין המידע הראשי).

כיסויים אופציונאליים:

1. הפרעה ברשת - אבדן רווחים (נטו) כתוצאה מהפרעה מהותית לרשת המבוטח שנגרמה כתוצאה מפריצת אבטחה.
2. סחיטת סייבר - תשלומי כפר (נזקי סחיטה) לצדדים שלישיים שישולמו על מנת לפתור איום אבטחה.
3. אחריות מולטימדיה - הוצאות הגנה ופיצויים שישולמו בקשר עם פריצה לקניין הרוחני של צד ג' או רשלנות בקשר עם תוכן אלקטרוני.