ביטוח סייבר (Cyber Liability Insurance)

הביטוח נועד להגן על עסקים וארגונים מפני הנזקים הכספיים, התפעוליים והמשפטיים הנובעים מאירועי סייבר, פריצות למערכות המחשוב, דליפת מידע רגיש, מתקפות כופרה (Ransomware) והשבתת מערכות מידע.

למי מיועד הביטוח?

הכיסוי מיועד לכל עסק או ארגון המחזיק במידע דיגיטלי, מנהל מערכות ממוחשבות או מסתמך על תשתית טכנולוגית:

- **חברות טכנולוגיה, הייטק ו-SaaS:** חברות המאחסנות מידע של לקוחות, מספקות שירותי ענן או מפתחות תוכנה.
- **חברות פיננסים, ביטוח ומשרדי עורכי דין/רואי חשבון:** ארגונים המחזיקים במידע פיננסי, משפטי ואישי רגיש מאוד.
- **רשתות קמעונאות ואתרי מסחר (E-commerce):** עסקים הסולקים אשראי ומנהלים מאגרי מידע של מועדוני לקוחות.
- **ארגוני בריאות, רפואה וחינוך:** גופים המנהלים תיקים רפואיים, מידע אישי מזהה (PII) ונתונים חסויים.

למה חשוב לרכוש אותו?

- **סיכון תפעולי וקיומי:** מתקפת כופרה או השבתת מערכות עלולה לשתק את העסק לימים ארוכים ולהוביל להפסדי עתק.
- **חשיפה רגולטורית וקנסות:** חוקי הגנת הפרטיות (כגון תקנות הגנת הפרטיות בישראל או ה-GDPR באירופה) מטילים אחריות כבדה וקנסות עתק על דליפת מידע.
- **עלויות תגובה ראשונית יקרות:** טיפול באירוע סייבר דורש מומחי פורנזיקה, חוקרי סייבר, יועצי ניהול משברים ועורכי דין מומחים.
- **פגיעה בתדמית ובאמון הלקוחות:** דליפת מידע פוגעת קשות במוניטין העסקי ודורשת מהלכי יחסי ציבור ושיקום אמון נרחבים.

מה כולל הכיסוי הביטוחי?

רכיב הכיסוי	פירוט
נזקי צד ראשון (נזק ישיר לעסק)	הוצאות חקירה פורנזית, שחזור נתונים ומערכות, ואובדן רווחים עקב השבתת עסק (Business Interruption).
אירועי כופרה (Ransomware)	כיסוי הוצאות ניהול המשא ומתן, ייעוץ מומחי כופר ותשלום הכופר (בכפוף למגבלות החוק).

רכיב הכיסוי	פירוט
נזקי צד שלישי (תביעות לקוחות)	כיסוי תביעות של לקוחות או שותפים שמידע שלהם דלף, כולל הוצאות הגנה משפטית ופיצויים.
ניהול משברים ויחסי ציבור	מימון שירותי יחסי ציבור, הודעות לנפגעים, ושירותי ניטור קרדיט/זהות לנפגעי הדליפה.
קנסות והליכים רגולטוריים	כיסוי הוצאות ייצוג מול רשויות הפרטיות וקנסות מינהליים (ככל שהחוק המקומי מתיר לבטח).

מה לא כולל הכיסוי? (חריגים עיקריים)

- **כשל בתשתיות כלליות:** נפילת רשת החשמל הארצית, ספקי תקשורת מרכזיים או אינטרנט כללי שלא בשליטת המבוטח.
- **הנדסה חברתית / עוקץ פיננסי (Social Engineering):** העברות כספים במרמה עקב התחזות (מכוסה בדרך כלל תחת הרחבה ייעודית או ביטוח נזקי מרמה/סייבר פיננסי).
- **בלאי, רשלנות מתמשכת או אי-עדכון גרסאות:** נזק שנגרם עקב הימנעות ממושכת מתחזוקת מערכות או אי-יישום דרישות אבטחה בסיסיות שהותנו בפוליסה.
- **סכסוכי קניין רוחני וגניבת מסחרי:** תביעות על גניבת סוד מסחרי, זכויות יוצרים או פטנטים באמצעות הסייבר.
- **מלחמה, טרור ואירועי סייבר מדינתיים:** מתקפות סייבר המוגדרות כפעולת איבה, מלחמה או מבוצעות על ידי מדינה זרה (מדינות אויב).

הוכן על ידי: שלמה מוסלי

אוג' 2026