



הגנה דיגיטלית לעסק שלך : איך ביטוח סייבר יכול לשמור עליך בעולם המקוון

מהו ביטוח סייבר?

ביטוח סייבר (לעסקים) הפך לאחד מהביטוחים החשובים ביותר בעידן המודרני, במיוחד עבור עסקים הנשענים על תשתית מחשובית ודיגיטלית.



אם בעבר מתקפות סייבר נחשבו לאירועים נדירים המופנים כלפי תאגידי ענק בלבד, הרי שהיום – כל עסק, קטן כגדול, עלול להפוך ליעד. האקרים ומפגעים דיגיטליים רואים בעסקים קטנים טרף קל, מתוך ההנחה שאין להם את היכולת הכלכלית להגן על עצמם באמצעות מערכות אבטחה מתקדמות. כך, קל להם לחדור למאגרי מידע, לגנוב פרטים אישיים או עסקיים (החל מזהויות לקוחות ועד לפרטי כרטיסי אשראי) ולהשתמש בהם לרעה או לדרוש כופר תמורת שחרורם.

במקרה של מתקפת סייבר שכוללת חשיפה של מידע רגיש, בעיקר כזה ששייך לצד שלישי, הנזק הכלכלי והתדמיתי עלול להיות קשה אף יותר.





הקמה מחודשת של המערכות, טיפול משפטי ושיקום המוניטין מחדש – כל אלו הם הוצאות כבדות שעלולות להשפיע על המשך פעילות העסק ולעיתים אף להביא לקריסתו חלילה.

מדוע חשוב לבטח עסק או חברה מפני האפשרות של מתקפת סייבר בעידן הטכנולוגי?

בעידן הטכנולוגי הנוכחי, שבו החדשנות פורחת והקנייה ברשת הפכה לפשוטה ונגישה מתמיד – גם הסכנות התגברו. לצערנו, יחד עם ההזדמנויות שהעולם הדיגיטלי מציע, קמה גם תופעה מדאיגה: האקרים או בשמם העברי "פצחנים" (שיחד עימם הגיעו עוד קבוצות מחתרטיות ואנרכיסטיות) ששמו להן למטרה לבצע מתקפות סייבר מתוכננות ומתואמות. מדובר בעבריינים לכל דבר ועניין, עבריינים אשר מתכננים ומבצעים מתקפות סייבר על ארגונים מסוגים שונים – בנקים, חברות ביטוח, ממשלות, שרותי בריאות, חברות ציבוריות ואף עסקים פרטיים בכל הגדלים מהגדול ועד לקטן.

ביטוח סייבר בא להגן בדיוק על אותם תרחישים. הוא מספק כיסוי ביטוחי לעסקים המחזיקים מאגר מידע רגיש- "דאטה-בייס" (Database) עסקי ובו פרטים אישיים – בין אם מדובר בפרטי אשראי, פרטים אישיים של לקוחות, מידע עסקי חסוי או כל סוג אחר של דאטה שנמצא במערכת.

הביטוח רלוונטי לכל סוגי מתקפות הסייבר – החל מגניבת מידע, סחיטה, פגיעה תדמיתית ועד להשבתת מערכות וכו'...

סוגי מתקפות שביטוח הסייבר מכסה:

- **פישנינג (Phishing)** : מתקפה שבה האקר מתחזה לנציג של החברה דרך מייל או אתר שנראה זהה לנכס דיגיטלי קיים, במטרה להשיג מידע רגיש מהלקוחות.
- **הודעות ספאם (Spam)** : מיילים שנראים תמימים או שיווקיים, אך כוללים תוכנות זדוניות (רוגלה), שיכולות לחדור למערכת ולשאוב מידע, למחוק אותו או לשתק את כלל הפעילות.





- **התקפת סיסמאות (Passwords Attacks) :** מתקפה שנעשית דרך ניסיונות רבים לפרוץ לחשבונות באמצעות ניחוש סיסמאות, ולעיתים מצליחה להגיע למאגרי מידע רגישים של הארגון.
- **גניבת פרטים:** חדירה של האקר למערכת החברה וגניבת פרטי אשראי או פרטים אישיים של לקוחות, שנעשה בהם שימוש לא חוקי – בין אם לרכישות או גניבת זהויות.
- **סחיטה:** פריצה למערכת, גניבת מידע ושימוש בו כ"בן ערובה" לשם סחיטת כספים מהארגון. לרוב מדובר בדרישת כופר תמורת הבטחה שלא לעשות שימוש במידע או להחזירו.
- **השבתת או הפסקת פעילות:** מתקפה שמשתקת את מערכות המחשוב של החברה, ולעיתים גם את כלל הפעילות העסקית. במקרים כאלה נדרשת התערבות מיידית של מומחי סייבר לשם שיקום ושחזור מערכות.

ביטוח סייבר – לא רק ל"חברות ענק". מרכיב חיוני בהגנה על הארגון מפני מתקפת האקרים.

המציאות מראה שמתקפות סייבר לא פוסחות על אף אחד: הן מופנות לעסקים קטנים, בינוניים, חברות גדולות ואף לגופים ממשלתיים. הנזק עלול להיות חמור – במיוחד לעסק קטן שקריסתו תלויה בנגישות למערכות המידע. ביטוח סייבר לא נועד להחליף פתרונות טכנולוגיים, אלא להשלים אותם. הוא מהווה שכבת הגנה נוספת, שמעניקה לעסק שקט נפשי במקרה של תקיפה. הוא עשוי לכסות על נזקים לתשתית המקומית, פגיעה בפרטיות הלקוחות, השבתת שירותים, תשלום דמי כופר, והוצאות משפטיות.

מה כוללת פוליסת ביטוח סייבר?

ביטוח סייבר איכותי מעניק הגנה מקיפה לבעל הפוליסה, הכוללת כיסוי מפני תביעות משפטיות שעלולות להגיע מצד לקוחות או ספקים שנפגעו כתוצאה ממתקפת סייבר. מעבר לכך, הפוליסה משלבת גם אמצעים טכנולוגיים שנועדו לסייע במניעה או בהפחתת נזקי תקיפה דיגיטלית למערכות החברה. בנוסף, הביטוח מעניק לעסק "מטריית הגנה" הכוללת את כלל המשאבים והכלים הנחוצים להתמודדות עם נזקים – הן ברמה הכלכלית והן ברמה התדמיתית.





פוליסת סייבר איכותית מעניקה לעסק הגנה רחבה שכוללת בין היתר:

- ✓ כיסוי בגין אובדן חלקי או מלא של מסדי נתונים.
- ✓ פיצוי על נזקים למערכות הדיגיטליות של הארגון.
- ✓ כיסוי בגין שירותי ניהול אירוע – למשל, במקרים שבהם נדרש ניהול משבר מול האקרים המחזיקים מידע כבן ערובה.
- ✓ הגנה משפטית במקרים של תביעות מצד לקוחות או ספקים בעקבות פגיעה במידע.
- ✓ פיצוי בגין נזקי מוניטין, גניבת מידע רגיש או סוד מסחרי.
- ✓ כיסוי בגין אובדן הכנסות – כתוצאה מחסימה של מאגרי מידע או השבתת פעילות בעקבות המתקפה.



לסיכום

ביטוח סייבר אינו מותרות – אלא צורך של ממש. בעידן שבו כל עסק מחזיק מידע רגיש ומנהל תהליכים באמצעות מחשב, החשיפה לאיומי סייבר היא ממשית ובלתי נמנעת. הביטוח מציע לא רק מענה כספי במקרה של תקיפה, אלא גם מעטפת תמיכה בזמן אמת – שכוללת ייעוץ, ליווי מקצועי, ושיקום מהיר של הנזק.





גם אם נראה שהעסק שלך "קטן מדי" או "לא מעניין אף אחד", הנתונים מוכיחים אחרת. לכן, כדאי לעצור לרגע, לבחון את הסיכונים, ולשקול ברצינות רכישת ביטוח סייבר – כי בעולם שבו הכל דיגיטלי, שמירה על המידע היא שמירה על העסק כולו.

רוצים לשמוע עוד? מוזמנים לפנות אליי

אין לראות באמור לעיל ייעוץ השקעות / ייעוץ פנסיוני ו/או שיווק פנסיוני המתחשב בנתונים ובצרכים המיוחדים של כל אדם. האינפורמציה המופיעה כאן אינה מהווה המלצה לביצוע או אי ביצוע מהלך כלשהו. מחובתך להתייעץ לפני כל פעולה. מסמך זה מנוסח בלשון זכר אך פונה לנשים ולגברים כאחד

