

חשיבותו של ביטוח הסייבר

כך תשמרו על העסק בעידן הדיגיטלי

בעידן הטכנולוגיה המתקדמת שבו אנחנו חיים היום, המידע והמערכות הדיגיטליות הפכו למוצר חיוני לעסקים. בין אם מדובר במקום עבודה מסורתי או בעסק דיגיטלי בלבד, אבטחת המידע הפכה להיות חיונית יותר מתמיד.



במה מדובר?

מדובר במנגנון הגנה שיכול לשמור על העסק מפני איומים כופר דיגיטליים, ריגול תעשייתי, גניבת זהויות, פריצות אבטחה ועוד. ואף להפסדים כלכליים כתוצאה מכך. כך, ביטוח סייבר יכול לפצות על נזק כלכלי כתוצאה מפריצת אבטחה ואף במקרים מסוימים להציל את העסק, לא פחות!

מהי חשיבותו?

אחת החשיבויות המרכזיות של ביטוח סייבר היא הגנה על מידע הלקוחות. בעידן בו פרטיות המידע האישי שלנו נמצאת במרכז הדיונים הציבוריים, אנו צריכים לתת חשיבות מרבית לנתונים הסודיים של הלקוחות שלנו. ביטוח סייבר מספק כלים ומנגנונים שמטרתם למנוע פריצות אבטחה וגישה למידע רגיש של הלקוחות, כמו פרטים אישיים, פרטי כרטיסי אשראי ועוד. בכך העסק מסייע בשמירה על הפרטיות והאמון של הלקוחות ומוכר כארגון מקצועי ואמין בעיניהם.

למה ביטוח סייבר חשוב גם לעסק?

בנוסף להגנה על מידע הלקוחות, ביטוח סייבר מספק הגנה מול פריצות אבטחה והתקפות סייבר. עם התפשטות הטכנולוגיה והמרחב הדיגיטלי, האיומים הדיגיטליים הפכו לגדולים ומורכבים יותר. **פריצות אבטחה יכולות לגרום להפסדים כלכליים משמעותיים, כגון סנקציות משפטיות, הפסקת פעילות לזמן בלתי מוגבל, או אפילו פגיעה במוניטין ובתדמית העסק.**

באמצעות ביטוח סייבר העסק מקבל הגנה מול פיצויים כלכליים למקרה של נזק, תהליכי שיקום ותמיכה באבחון וטיפול בהתקפות סייבר.

לאחרונה, ניתן לראות עליה משמעותית בפריצות אבטחה ותקיפות סייבר בעסקים קטנים ובינוניים. הסיבות לכך מגוונות, כוללות חולשות במערכות אבטחה, חוסר מודעות לסיכונים או פשוט חוסר משאבים להקניית תשתיות וכלים אבטחתיים מתקדמים כמו ביטוח סייבר.



דוגמא לפריצת אבטחה לעסק שביטוח סייבר היה יכול למנוע:

דמיינו עסק קטן שבעיקר מספק שירותים מקוונים וצורך לאחסן נתונים רבים של לקוחות במערכת המחשב שלו.

בזמן מה, התקיים התקפת פשינג במערכת הדואר האלקטרוני של העסק. האקרים חדרו למערכות של העסק והשיגו גישה למידע אישי של לקוחותיו, כולל שמות, כתובות ומספרי תעודת זהות כ.א וכדומה. לאחר מכן, הם ביצעו הונאת זהות וניצלו את



המידע שנפל לידיהם לצורך פעילויות פקידותיות ותמיכה בזמן שיחות טלפון עם לקוחות של העסק.

אם העסק היה מבוטח עם ביטוח סייבר, התהליך היה נמנע בגלל מנגנון הגנה מתקדם. החברה הביטוחית הייתה מספקת לעסק כלי הגנה, כמו אימות דו-שלבי, זיהוי חשודים וסינון דואר זבל. בנוסף, העסק היה זכאי לתמיכה טכנית מיועץ בטחוני, שהיה מסייע בזיהוי התקפות פשינג ופעילות מזויפת, ובפעולות תקן כדי למנוע גישה למידע הרגיש שיש לבית עסק.

היכן ניתן לעשות ביטוח סייבר?

ביטוח סייבר זמין במגוון חברות ביטוח ברחבי העולם. ניתן למצוא מידע ולרכוש ביטוח סייבר דרך חברות ביטוח מובילות, בנקים, וסוכני ביטוח. כדי למצוא את התוכנית המתאימה ביותר לצרכים שלך, יש לבחון את התנאים, התמחורים והשירותים הניתנים ע"י כל חברות הביטוח. חשוב לשים לב למהלך האבחון של החברה המבצעת את הביטוח. יש לבדוק את רמת הביצועים הטכנולוגיים והניסיון של החברה בתחום, כולל יכולת לזהות, למנוע ולטפל באיומים סייברניים. כמו כן, כדאי לבדוק את התנאים של הביטוח, כולל התיאור המדויק של תהליכי הפיצוי, תהליך הדיווח והתמיכה במקרי אירוע.

מומלץ לפנות למומחה או ליועץ ביטוח עצמאי שיכול לספק לך מידע ויועץ מקצועי על בחירת הביטוח המתאים ביותר לצרכים שלך!

רכישת ביטוח סייבר

לסיכום רכישת ביטוח סייבר היא צעד חיוני בעידן הדיגיטלי שבו אנחנו חיים. כמו כן אתם חייבים הגנה על מידע הלקוחות: בעידן שבו פרטיות המידע והמידע הרגיש של לקוחות הוא יקר וסודי, ביטוח סייבר מספק הגנה מול פריצות אבטחה וגישה למידע רגיש של הלקוחות, מסייע בשמירה על פרטיותם ובהקניית האמון של הלקוחות שלך. בנוסף הביטוח מקנה הגנה מפריצות אבטחה ותקיפות סייבר. עם התפשטות הטכנולוגיה והמרחב הדיגיטלי, האיומים הסייברניים הפכו לגדלים מאי פעם ואבטחה ותקיפות סייבר יכולות לגרום להפסדים כלכליים משמעותיים, אז למה לא למנוע אותם מראש?

האמור אינו מהווה ייעוץ ו/או שיווק ביטוח סייבר ו/או תחליף לייעוץ/שיווק ביטוח סייבר המתחשב בנתונים ובצרכים של כל אדם.

