الأمن السيبراني "أمن الفضاء الإلكتروني "

لماذا الأمن السيبراني مهم؟

الأمن السيبراني أمر بالغ الأهمية للأعمال التجارية لعدد لا يحصى من الأسباب. وسيركز هذا القسم على اثنين من الخروقات أمن البيانات والتخريب. يمكن أن يكون لكليهما آثار وخيمة على الشركة و/ أو عملائها.

يمكن أن تعرض خروقات أمان البيانات المعلومات الآمنة للخطر مثل:

- الأسماء وأرقام الضمان الاجتماعي
- بطاقة الائتمان والتفاصيل المصرفية
- أسرار تجارية
- الملكية الفكرية

يعمل تعطيل الكمبيوتر على تعليق أجهزة الكمبيوتر أو الشبكة الخاصة بالشركة لعرقلة قدرة الشركة على إجراء الأعمال.

التصيّد الاحتيالي

يهدف مجرمو الإنترنت الذين يستخدمون عمليات التصيد الاحتيالي إلى الحصول على معلومات شخصية من خلال الظهور بمظهر المصدر الشرعي. في كثير من الأحيان، يتنكرون كشركة كبرى، مثل البنك، مناشدين رغبتك في الحفاظ على معلوماتك آمنة.

على سبيل المثال، قد يرسلون بريدا إلكترونيايقول: "نشك في وجود معاملة غير مصرح بها على حسابك. للتأكد من عدم اختراق حسابك، يرجى النقر على الرابط أدناه وتأكيد هويتك.

يمكن أن يؤدي النقر على الرابط أو الرد على البريد الإلكتروني إلى الوصول إلى موقع ويب يبدو أصليا، ولكنه في الواقع موقع محاكاة ساخرة يعمل على سرقة معلوماتك واستخدامها لأغراض ضارة، مثل ارتكاب جرائم باستخدام اسمك أو استخدام معلوماتك المصرفية لتحقيق مكاسب شخصية.

التشفير

يعرف التشفير أساسا كطريقة سرية للكتابة. ويتم ذلك بحيث لا يمكن تفسير الرسالة إلا للأطراف المخولة.

ويستخدم في مختلف الصناعات، مثل الخدمات المصرفية والصحة لحماية خصوصية وأمن الشركات ومعلومات العملاء/ المرضى.

تتضمن أمثلة أساليب التشفير ما يلي:

- طريقة تشفير البيانات الدولية (IDEA)
- معيار التشفير المتقدم (AES)
- معيار تشفير البيانات (DES)