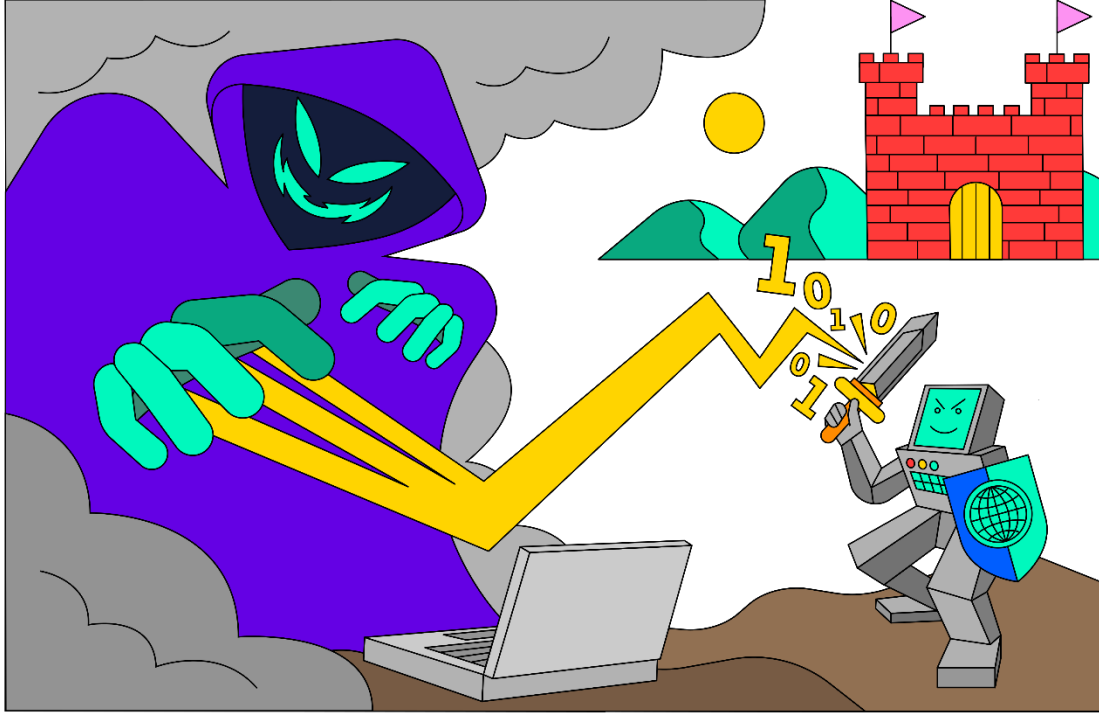


ما هو الأمن السيبراني؟

سوف نعرّف ما هو الأمن السيبراني بالضبط إمعاناً ازدیاد اتصالنا عبر الإنترنت من خلال الوصول عبر الكمبيوتر، هواتفنا، وحتى الأجهزة المنزلية، أصبحت مسألة الأمان موضوعاً ساخناً. يمكن أن تحدث الهجمات من أي زاوية. ماذا يحدث إذا تمكن شخص ما من السيطرة على جهاز الكمبيوتر أو الهاتف الخاص بك؟ أو شخص ما يسيطر فقط على حسابك في Google؟ على مستوى المؤسسات، يمكن للهجمات على أنظمة الكمبيوتر أن تخترق أيضاً ملايين القطع من البيانات الشخصية، بما في ذلك معلومات بطاقات الائتمان. كما أن الحكومات عرضة للهجمات التي تكشف البيانات الحساسة. الأمن السيبراني يشمل الجميع وكل كيان - منكم ومن جيرانكم، إلى المنظمات، إلى الشركات، إلى الحكومات.



الإنترنت قد أحدث ثورة كاملة في طريقة تواصلنا مع بعضنا البعض ومشاركة المعلومات. يقضي الكثير منا ساعات على وسائل التواصل الاجتماعي والردشات الجماعية عبر الإنترنت. تقريباً جميع المؤسسات لديها نوع من إدارة أنظمة الكمبيوتر لمتابعة الحسابات، وأصبح الشراء والبيع عبر الإنترنت هو القاعدة. واحدة تلو الأخرى، يتم توصيل حتى المعدات الطبية، أنظمة النقل، والمكانس بالويب.

ما هو الأمن السيبراني بالضبط؟

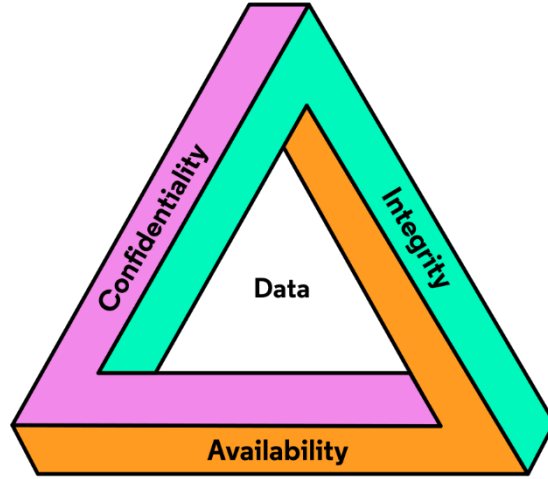
لا يوجد رجوع إلى الوراء، حتى مع أن المزيد من الاتصالات بالإنترنت تؤدي إلى مخاوف أكبر بشأن الخصوصية ومخاطر الأمان. لا نريد أن يصل الغرباء إلى حساباتنا أو أرقام بطاقات الائتمان الخاصة بنا. إلى جانب ممارسة الأمن الشخصي، تحتاج المنظمات والشركات أيضاً إلى القيام بدورها في تنفيذ الحماية المناسبة. الأمن السيبراني هو مجال الدراسة والممارسة الذي يستجيب لهذه التحديات مع تطور التكنولوجيا. في تعريف رسمي من CISCO:

"الأمن السيبراني هو ممارسة حماية الأنظمة والشبكات والبرامج من الهجمات الرقمية."

يمكن أن تغطي الهجمات الرقمية مجموعة كاملة من الرسائل الاحتمالية إلى إغلاق مستهدف لحركة المرور على موقع ويب. لذلك، يجب تعلم وتنفيذ الدفاعات ضد هذه الهجمات على جميع المستويات.

نموذج CIA

نموذج أساسي وشامل للأمن السيبراني، خاصة فيما يتعلق بالمعلومات، هو نموذج CIA. يرمز CIA إلى Confidentiality (السرية)، Integrity (السلامة)، و Availability (التوافر) (وليس وكالة المخابرات المركزية الأمريكية). تعود جميع سياسات أمن المعلومات تقريباً إلى هذا النموذج. دعونا نستعرض كل مكون من مكونات هذا النموذج الثلاثي.



السرية

يشير هذا الركن من النموذج إلى حماية المعلومات الخاصة من العيون التي لا يجب أن تصل إليها. السرية هي الحاجة إلى فرض الوصول - من يمكنه رؤية هذا، ومن لا ينبغي له؟ على سبيل المثال، لا نريد إعطاء رقم الضمان الاجتماعي الخاص بنا لأي شخص، ولكن نثق في أن المؤسسات التي نعطيها لهم - مثل خدمات الضرائب - تنفذ التدابير الأمنية المناسبة للحفاظ على سريتها. فما هي الأدوات المستخدمة لضمان الوصول الصحيح؟ بعض الطرق التي تتم بها إدارة السرية هي:

- الحفاظ على مستويات الوصول وتحديد الأذونات
- تشفير البيانات والملفات
- طلب المصادقة متعددة العوامل

السلامة

تشير السلامة هنا إلى سلامة البيانات. نحتاج إلى ضوابط أمنية تحمي البيانات من التغيير أو الحذف. يجب علينا أيضاً ضمان إمكانية عكس الضرر إذا تم تغيير البيانات عن طريق الخطأ أو من قبل الشخص الخطأ. بعض التقنيات المتعلقة بالسلامة هي:

- الحفاظ على نسخ احتياطية للبيانات في حالتها الصحيحة، وتسجيل الإصدارات
- استخدام التشفير للتحقق من التغييرات
- متابعة التوقعات الرقمية لإثبات سلامة البيانات

التوافر

يشير هذا الركن الأخير إلى أن البيانات تكون متاحة باستمرار وبشكل موثوق للمصرح لهم. على سبيل المثال، عندما تسجل الدخول إلى حساب وسائل التواصل الاجتماعي وتريد ضبط إعدادات الخصوصية الخاصة بك، تتوقع ظهور جميع الإعدادات الصحيحة التي قمت بضبطها مسبقاً فوراً. تضمن شركة وسائل التواصل الاجتماعي أنه حتى مع حركة المرور العالية، تصل المعلومات إلى شاشتك. كيف يتم تحقيق ذلك؟

- مراقبة الخوادم والشبكات باستمرار
- صيانة الأجهزة والبرامج
- وجود خطة للتعافي من الكوارث

ومع ذلك إيفر نموذج CIA أساساً لأمن المعلومات بشكل خاص. سنغطي العديد من المبادئ والأطر الأمنية الأخرى، ونستكشف التقنيات بشكل أعمق في هذه الدورة، ستحصل على فهم أساسي لمجال الأمن السيبراني. سوف تتعلم:

- كيف تطور الأمن السيبراني، بما في ذلك كيفية تشكيله للمعايير واللوائح الحديثة
- كيف تعمل الهجمات الرقمية، وأهدافها ودوافعها المختلفة
- معرفة أساسية بالتشفير وتقنيات المصادقة والتفويض
- كيفية جعل أجهزتك الشخصية وشبكائك أكثر أماناً
- تشريح الشبكات
- كيف يبدو الأمن السيبراني في عصر تكنولوجيا السحابة

لنبدأ!