بحث حول الامن السيبراني

للطالب: اسامة سعيد بن مخاشن
تخصص : علوم حاسوب مستوى اول

الاسم :اسامة سعيد بن مخاشن تخصص : علوم حاسوب مستوى اول

مفهوم الأمن السيبراني

يُعرف الأمن السيبراني (بالإنجليزية: Cyber Security) بأنّه توظيف التقنيات، والعمليات، والتدابير اللازمة لضمان أمن الأنظمة، والشبكات، والبرامج، والأجهزة، والبيانات وحمايتها من الهجمات الإلكترونية، ويتمثّل الغرض الرئيسي منه في تقليل المخاطر الإلكترونية التي قد تتعرّض لها الأنظمة والشبكات وحمايتها من الاستغلال غير المصرّح به.

فيما يأتي توضيح لمراحل نشأة الأمن السيبراني:

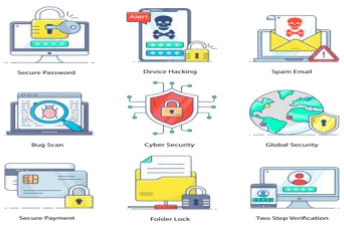
سبعينيات القرن العشرين

يعود تاريخ نشأة الأمن السيبراني إلى سبعينيات القرن العشرين، الوقت الذي لم تكُن فيه بعض المصطلحات شائعة كبرامج التجسس، والفيروسات، والديدان الإلكترونية.

ثمانينيات القرن العشرين

في ثمانينيات القرن العشرين، ابتكر روبرت تي موريس أول برنامج فيروس إلكتروني، والذي حاز على تغطية إعلامية هائلة نظرًا لانتشاره بين الأجهزة وتسبّبه بأعطال في الأنظمة، فحُكِم على موريس بالسجن والغرامة، وكان لذلك الحكم دور في تطوير القوانين المتعلقة بالأمن السيبراني.

أنواع الأمن السيبراني



أمن الشبكات (Network Security)

وفيه يجري حماية أجهزة الحاسوب من الهجمات التي قد يتعرّض لها داخل الشبكة وخارجها، ومن أبرز التقنيات المُستخدمة لتطبيق أمن الشبكات جدار الحماية الذي يعمل واقيًا بين الجهاز الشخصي والأجهزة الأخرى في الشبكة، بالإضافة إلى أمن البريد الإلكتروني.

أمن التطبيقات (Application)

وفيه يجري حماية المعلومات المتعلقة بتطبيق على جهاز الحاسوب، كإجراءات وضع كلمات المرور وعمليات المصادقة، وأسئلة الأمان التي تضمن هوية مستخدم التطبيق.

الأمن السحابى (Security)

تُعرف البرامج السحابية بأنّها برامج تخزين البيانات وحفظها عبر الإنترنت، ويلجأ الكثير إلى حفظ بياناتهم عبر البرامج الإلكترونية عوضًا عن برامج التخزين المحلية ممّا أدى إلى ظهور الحاجة إلى حماية تلك البيانات، فتعنى البرامج السحابية بتوفير الحماية اللازمة لمستخدميها.

الأمن التشغيلى (Operational Security)

وهو إدارة مخاطر عمليات الأمن السيبراني الداخلي، وفيه يوَظّف خبراء إدارة المخاطر لإيجاد خطة بديلة في حال تعرض بيانات المستخدمين لهجوم إلكتروني، ويشمل كذلك توعية الموظفين وتدريبهم على أفضل الممارسات لتجنب المخاطر.

اهمية الامن السيبراني

للأمن السيبراني أهمية كبيرة؛ لأنّه يحمي بيانات المستخدمين من الهجمات الإلكترونية الرامية إلى سرقة المعلومات واستخدامها لإحداث ضرر، فقد تكون هذه بيانات حساسة، أو معلومات حكومية وصناعية، أو معلومات شخصية.

وظائف الامن السيبرانى:

1. مسؤول أمن التطبيقات: ضمان سلامة البرامج والتطبيقات
2. خبير أمن الذكاء الاصطناعي: استخدام الذكاء الاصطناعي لمكافحة جريمة المعلومات
3. مهندس سلامة السيارات: حماية السيارات من التطفل الإلكتروني
4. مطورو / مهندسو Block chain: تطوير الترميز لمستقبل المعاملات الآمنة
5. أعضاء الفريق الأزرق: الدفاع عن مؤشرات / أنظمة تشغيل دفاعية أكثر صرامة
6. Bug Bounty Hunter كشف نقاط الضعف والأخطاء في الأنظمة الإلكترونية بسبب الأخطاء
7. Network Security Scrum Master: مراقبة وحماية جميع البيانات
8. رئيس ضابط أمن المعلومات: رئيس قسم أمن المعلومات

فوائد الأمن السيبرانى

يعد الأمن السيبراني أمرًا بالغ الأهمية. ويتضمن حماية أنظمة تكنولوجيا المعلومات والبيانات من التهديدات السيبرانية مثل الاحتيال أو التجسس أو التخريب. يمكن الاستفادة من فوائد الأمن السيبراني للحد من هذه الآثار، و تقليل الأضرار الناتجة عن التهديدات المُحتملة.

أهم فوائد الأمن السيبرانى:

- تحسين وحفظ بيانات اعتماد المؤسسات أو الشركات المحسّنة مع وجود ضوابط الأمان الصحيحة المعمول بها عالمياً
- تحسين ثقة أصحاب العمل في ترتيبات أمن المعلومات الخاصة بالمؤسسات أو الشركات
- تقليل أوقات استرداد البيانات والمعلومات في حالة حدوث خروقات للشبكات أو الأنظمة
- حماية الشبكات والبيانات من الوصول غير المصرح به
- إدارة استمرارية الأعمال
- تحسين أمن المعلومات