الأمن السيبراني

المقدمة

كانت البداية الحقيقية للأمن السيبراني في السبعينات. بدأ كل هذا بمشروع شبكة وكالة مشاريع البحوث المتقدمة أربانت وكانت هذه شبكة الاتصال التي وجدت قبل الإنترنت. اكتشف رجل اسمه بوب توماس أن برنامج الكمبيوتر يمكن أن ينتقل عبر الشبكة وأنه أثناء انتقاله فسيترك البرنامج أثرًا وراءه. فقام بتصميم برنامج قادرٍ على التنقل بين 10 شبكات خارجية عبر أربانت يسمى بكريبر.

قام راي توملينسون وهو مبتكر البريد الإلكتروني بإنشاء برنامج ريبر وهو برنامج تتبع يتعقب ويتخلص من برنامج الكريبر، وبهذا أصبح برنامج الريبر أول دودة حاسوبية وأول برنامج لمكافحة الفيروسات وأول برنامج ذاتي النسخ.

التعريف

إن الأمن السيبراني هو استخدام التكنولوجيا والعمليات والضوابط للدفاع ضد الهجمات الإلكترونية على الأنظمة والشبكات والبرامج والأجهزة والبيانات.

متى يستخدم

يعد الخيار الأفضل للأفراد والشركات الذين يرغبون في حماية وإدارة مخاطرهم أثناء استخدامهم للإنترنت.

الشرح

إن الأمن السيبراني هو إجراء يحمي الشبكات والأجهزة ضد الهجمات الخارجية. توظف الشركات بشكل عام خبراء متميزين في مجال الأمن السيبراني لحماية المعلومات الحساسة والحفاظ على إنتاجية الموظفين وتعزيز ثقة العملاء في المنتجات والخدمات. إنها مجموعة من الاستراتيجيات المستخدمة لحماية سلامة الشبكات والبرامج والبيانات ضد الهجمات والأضرار أو دخول المستخدمين المتطفلين.

أدركت الحكومات أن دخول المستخدمين غير المصرح بهم إلى هذه البنية التحتية الكبيرة قد يتسبب في حدوث عدد كبير من المشكلات. في النصف الثاني من العقد تم نشر عدد من المنشورات العلمية والتي بحثت في تقنيات لضمان الأمن كما وناقشت المخاطر المحتملة.

تشمل أنواع المخاطر السيبرانية ما يلي:

1. **البرامج الضارة -** تشير البرامج الضارة إلى البرمجيات الخبيثة وهي الطريقة الأكثر انتشارًا للهجوم الإلكتروني. يستخدمه المجرم الإلكتروني أو الهاكر لتعطيل نظام المستخدم الشرعي أو الإضرار به. إن برامج البوت نت والرات وفيروس الروتكيت والبوتكيت وبرامج التجسس وأحصنة طروادة والفيروسات والديدان أمثلة على البرامج الضارة
2. **التصيد الإحتيالي -** يعد التصيد الإحتيالي نوع من الجرائم الإلكترونية والتي يبدو فيها المرسل بأنه كيان شرعي كبايبال وايباي والمؤسسات المالية أو الأصدقاء وزملاء العمل. وعادةً ما يكون على شكل رابط ينقل المستخدمين إلى موقع مزيف حيث سيُطلب منهم إدخال معلومات حساسة كالمعلومات الشخصية والمعلومات المصرفية وبطاقة الائتمان وأرقام الضمان الاجتماعي وأسماء المستخدمين وكلمات المرور. بالضغط على الرابط سيتم تثبيت البرمجيات الخبيثة على الأجهزة المستهدفة مما يسمح للقراصنة بالتحكم بهم عن بعد
3. **حقن النصوص البرمجية للغة الاستعلامات المهيكلة -** تعد حقن إس كيو إل هجوم نموذجي حيث يقوم المحتالون بالتلاعب في قواعد البيانات باستخدام نصوص إس كيو إل ضارة للوصول إلى المعلومات الهامة. يمكن للمهاجم رؤية أو تعديل أو إزالة بيانات الشركة الحساسة أو قوائم المستخدم أو تفاصيل العملاء الخاصة المخزنة في قاعدة بيانات إس كيو إل بعد نجاح الهجوم.
4. **هجوم نظام أسماء المجال دي ان اس -** إن هجمات دي ان اس السامة تخرب الدي ان اس من أجل إعادة توجيه الحركة إلى مواقع الويب الضارة. يستخدم اللصوص الإلكترونيون نقاط الضعف في نظام أسماء المجال لإعادة توجيه المستخدمين إلى مواقع الويب الضارة وسرقة البيانات من الأجهزة المستهدفة.
5. **هجوم حجب الخدمة دي دوس -** وهو شكل من أشكال التهديدات السيبرانية أو الجهود الخبيثة التي يقوم بها المحتالون باستخدام الحركة على الإنترنت لتلبية الطلبات المشروعة للهدف أو البنية التحتية المحيطة به مما يتسبب في تعطيل الحركة العادية للأهداف.

أمثلة

أمن البنية التحتية الحيوية

نظرًا لأن أنظمة SCADA (التحكم الإشرافي والحصول على البيانات) تعتمد عمومًا على البرامج القديمة، فإن مؤسسات البنية التحتية الحيوية أكثر عرضة للهجوم من غيرها. تتطلب القوانين، بالإضافة لأمور أخرى، أن تتخذ الشركات خطوات فنية وتنظيمية مناسبة للسيطرة على مخاطرها الأمنية.

أمن الشبكات

تعتبر معالجة الثغرات الأمنية في أنظمة التشغيل وبنية الشبكة بما في ذلك الخوادم والمضيفين وجدران الحماية ونقاط الوصول اللاسلكية وبروتوكولات الشبكة جزءًا من أمن الشبكات.

الأمن السحابي

إن الأمن السحابي هو عبارة عن مجموعة من الإجراءات والتكنولوجيا التي تهدف إلى معالجة المخاوف الأمنية الخارجية والداخلية. تتطلب الشركات أمنًا سحابيًا أثناء تنفيذهم لاستراتيجية التحول الرقمي الخاصة بهم وإدراج الأدوات والخدمات المستندة إلى الحوسبة السحابية في بنيتهم التحتية.

أمن انترنت الأشياء

إن أمن الإنترنت هو عملية حماية أجهزة الإنترنت والشبكات التي تتصل بها من التهديدات والخروقات من خلال تحديد المخاطر ومراقبتها وحمايتهم منها، فضلاً عن المساعدة في إصلاح الثغرات الأمنية من مجموعة متنوعة من الأجهزة التي يمكن أن تشكل مخاطر أمنية لعملك.

أمن التطبيقات

إن أمن التطبيقات هو عملية إنشاء ودمج واختبار الإجراءات الأمنية في التطبيقات لحمايتها من المخاطر كالدخول والتعديل غير القانوني. إن معالجة نقاط الضعف الناشئة عن عمليات التطوير غير الآمنة في تصميم البرامج أو المواقع وترميزها ونشرها هو أساس أمن التطبيقات.

المراجع

https://www.ibm.com/ph-en/topics/cloud-security#:~:text=Cloud%20security%20is%20a%20collection,as%20part%20of%20their%20infrastructure.

https://cybermagazine.com/cyber-security/history-cybersecurity

https://www.simplilearn.com/introduction-to-cyber-security-article#cyber_security_education

https://www.itgovernance.co.uk/what-is-cybersecurity

https://www.fortinet.com/resources/cyberglossary/iot-security#:~:text=Security%20in%20IoT%20is%20the,security%20risks%20to%20your%20business.