الأمن السيبراني

م.د.سارة علي سعيد

م.د.سهى جمال مولود

قسم إدارة الاعمال

ما المقصود بالأمن السيبراني؟

الأمن السيبراني هو ممارسة حماية أجهزة الكمبيوتر والشبكات وتطبيقات البرامج والأنظمة الهامة والبيانات من التهديدات الرقمية المحتملة. تتحمل المؤسسات مسؤولية تأمين البيانات للحفاظ على ثقة العملاء والامتثال للمتطلبات التنظيمية. فهي تعتمد تدابير وأدوات الأمن السيبراني من أجل حماية البيانات الحساسة من الوصول غير المصرّح به، وكذلك منع أي انقطاع للعمليات التجارية بسبب نشاط الشبكة غير المرغوب فيه. تطبّق المؤسسات الأمن السيبراني من خلال تبسيط الدفاع الرقمي بين الأفراد والعمليات والتقنيات.

ما أهمية الأمن السيبراني؟

تستخدم الشركات في مختلف القطاعات، مثل الطاقة والنقل وتجارة التجزئة والتصنيع، الأنظمة الرقمية والاتصال عالي السرعة لتوفير خدمة عملاء فعّالة وإجراء عمليات تجارية ميسورة التكلفة. مثلما تؤمّن هذه المؤسسات أصولها المادية، عليها أيضًا تأمين أصولها الرقمية وحماية أنظمتها من أي وصول غير مقصود. إنّ حدث الاختراق والحصول على وصول غير مصرّح به إلى نظام كمبيوتر أو شبكة أو منشآت متصلة يُسمّى "هجومًا سيبرانيًا" إن كان متعمّدًا. يؤدي الهجوم السيبراني الناجح إلى الكشف عن البيانات السرية أو سرقتها أو حذفها أو تغييرها. تدافع تدابير الأمن السيبراني ضد الهجمات السيبرانية وتوفّر الفوائد التالية:

منع الانتهاكات أو تقليل تكلفة عواقبها

تقلّل المؤسسات التي تطبق استراتيجيات الأمن السيبراني من العواقب غير المرغوب فيها للهجمات السيبرانية التي قد تؤثر في سمعة الشركات، ووضعها المالي، والعمليات التجارية، وثقة

العملاء. على سبيل المثال، تفعّل الشركات خطط التعافي من الكوارث لاحتواء التدخلات المحتملة وتقليل مدة تعطيل العمليات التجارية.

ضمان الامتثال للوائح التنظيمية

على الشركات في مجالات ومناطق محددة الامتثال للمتطلبات التنظيمية من أجل حماية البيانات الحساسة من المخاطر السيبرانية المحتملة. على سبيل المثال، على الشركات التي تعمل في أوروبا الامتثال للائحة العامة لحماية البيانات (GDPR)، التي تتوقع من المؤسسات اتخاذ تدابير الأمن السيبراني المناسبة لضمان خصوصية البيانات.

الحدّ من التهديدات السيبرانية المتطوّرة

مع تغيّر التقنيات، تنشأ أشكال جديدة من الهجمات السيبرانية. يستخدم المجرمون أدوات جديدة ويبتكرون استراتيجيات جديدة للوصول إلى النظام بدون إذن. تتبنّى المؤسسات تدابير الأمن السيبراني وتحدّثها لمواكبة تقنيات وأدوات الهجوم الرقمي الجديدة والمتطورة.

ما هي أنواع الهجمات التي يحاول الأمن السيبراني الدفاع عنها؟

يسعى محترفو الأمن السيبراني إلى احتواء التهديدات الحالية والجديدة التي تتسلل إلى أنظمة الكمبيوتر بطرق مختلفة، والحدّ منها. نقدم أدناه بعض الأمثلة على التهديدات السيبرانية الشائعة.

البرمجيات الخبيثة

البرمجيات الخبيثة تعني البرامج الضارة. وهي تتضمّن مجموعة من البرامج التي تم إنشاؤها من أجل منح أطراف ثالثة إمكانية الوصول غير المصرّح به إلى المعلومات الحساسة أو السماح لها بتعطيل سير العمل العادي للبنية الأساسية بالغة الأهمية. تشمل الأمثلة الشائعة للبرمجيات الخبيثة أحصنة طروادة وبرامج التجسس والفيروسات.

برامج الفدية

تشير برامج الفدية إلى نموذج عمل ومجموعة واسعة من التقنيات ذات الصلة التي تستخدمها الجهات المسيئة لابتزاز الأموال من الكيانات. سواء كنت قد بدأت للتو باستخدام AWS أو سبق

أن بدأت بالتطوير، فلدينا موارد مخصصة لمساعدتك على حماية أنظمتك الهامة وبياناتك الحساسة من برامج الفدية.

هجوم الوسيط

في هجوم الوسيط، يحاول طرف خارجي الوصول بشكل غير مصرّح به إلى الاتصالات في شبكة أثناء تبادل البيانات. تزيد مثل هذه الهجمات من المخاطر الأمنية للمعلومات الحساسة، مثل البيانات المالية.

التصيد الاحتيالي

التصيد الاحتيالي هو تهديد سيبراني يستخدم تقنيات الهندسة الاجتماعية من أجل خداع المستخدمين للكشف عن معلومات التعريف الشخصية. على سبيل المثال، يرسل المهاجمون السيبرانيون رسائل إلكترونية تستدرج المستخدمين للنقر عليها وإدخال بيانات بطاقة الائتمان في صفحة ويب وهمية لإتمام الدفع. يمكن أن تؤدي هجمات التصيد الاحتيالي أيضًا إلى تنزيل مرفقات ضارة تثبّت برامج ضارة على أجهزة الشركة.

الهجوم الموزَّع لتعطيل الخدمة (DDoS)

الهجوم الموزَّع لتعطيل الخدمة (DDoS) عبارة عن جهد منسّق لإرباك الخادم عن طريق إرسال عدد كبير من الطلبات المزيفة. تمنع مثل هذه الأحداث المستخدمين العاديين من الاتصال بالخادم المستهدف أو الوصول إليه.

تهديد داخلي

التهديد الداخلي هو خطر أمني يسبّبه الأفراد ذوي النوايا السيئة داخل مؤسسة. يمتلك الموظفون وصولاً عالي المستوى إلى أنظمة الكمبيوتر ويمكن أن يزعزعوا استقرار أمن البنية الأساسية من الداخل.

كيف يعمل الأمن السيبراني؟

تنفّذ المؤسسات استراتيجيات الأمن السيبراني من خلال العمل مع متخصّصين في الأمن السيبراني. يقيّم هؤلاء المتخصصون المخاطر الأمنية لأنظمة الحوسبة الحالية، والشبكات، ومخازن البيانات، والتطبيقات، والأجهزة المتصلة الأخرى. بعد ذلك، ينشئ متخصصو الأمن السيبراني إطار عمل شامل للأمن السيبراني وينفّذون تدابير وقائية في المؤسسة.

لضمان نجاح برنامج الأمن السيبراني، يجب إعلام الموظفين في سياقه بأفضل الممارسات الأمنية واستخدام تقنيات الدفاع السيبراني الآلية في البنية الأساسية الحالية لتكنولوجيا المعلومات. تعمل هذه العناصر معًا لإنشاء طبقات متعددة من الحماية ضد التهديدات المحتملة على جميع نقاط الوصول إلى البيانات. فهي تحدّد المخاطر، وتحمي الهويات والبنية الأساسية والبيانات، وترصد أوجه الخلل والأحداث، وتستجيب وتحلل السبب الجذري، وتتعافى بعد وقوع الحدث.

ما هي أنواع الأمن السيبراني؟

تنفّذ المؤسسات استراتيجيات الأمن السيبراني من خلال العمل مع متخصّصين في الأمن السيبراني. يقيّم هؤلاء المتخصصون المخاطر الأمنية لأنظمة الحوسبة الحالية، والشبكات، ومخازن البيانات، والتطبيقات، والأجهزة المتصلة الأخرى. بعد ذلك، ينشئ متخصصو الأمن السيبراني إطار عمل شامل للأمن السيبراني وينفّذون تدابير وقائية في المؤسسة.

لضمان نجاح برنامج الأمن السيبراني، يجب إعلام الموظفين في سياقه بأفضل الممارسات الأمنية واستخدام تقنيات الدفاع السيبراني الآلية في البنية الأساسية الحالية لتكنولوجيا المعلومات. تعمل هذه العناصر معًا لإنشاء طبقات متعددة من الحماية ضد التهديدات المحتملة على جميع نقاط الوصول إلى البيانات. فهي تحدّد المخاطر، وتحمي الهويات والبنية الأساسية والبيانات، وترصد أوجه الخلل والأحداث، وتستجيب وتحلل السبب الجذري، وتتعافى بعد وقوع الحدث.

ما هي أنواع الأمن السيبراني؟

يعالج نهج فعّال للأمن السيبراني المخاوف التالية داخل المؤسسة.

الأمن السيبراني للبنية الأساسية بالغة الأهمية

تشير البنية الأساسية بالغة الأهمية إلى الأنظمة الرقمية التي يجدها المجتمع مهمة، مثل الطاقة والاتصالات والنقل. تتطلب المؤسسات العاملة في هذه المجالات نهجًا منهجيًا للأمن السيبراني، لأن انقطاع الخدمة أو فقدان البيانات يمكن أن يزعزع استقرار المجتمع.

أمان الشبكة

أمان الشبكة يشكّل حمايةً للأمن السيبراني على أجهزة الكمبيوتر والأجهزة المتصلة بشبكة. تستخدم فرق تكنولوجيا المعلومات تقنيات أمان الشبكة، مثل جدران الحماية والتحكم في الوصول إلى الشبكة، لتنظيم وصول المستخدمين وإدارة الأذونات لأصول رقمية معينة.

أمن السحابة

يصف أمان السحابة الإجراءات التي تتخذها المؤسسة لحماية البيانات والتطبيقات التي تعمل في السحابة. يُعتبر ذلك مهمًا لتعزيز ثقة العملاء، وضمان العمليات القادرة على تجاوز الأخطاء، والامتثال للوائح التنظيمية حول خصوصية البيانات في بيئة قابلة للتطوير. تتضمن استراتيجية أمان السحابة الفعّالةالمسؤولية المشتركة بين مورّد السحابة والمؤسسة.

أمان إنترنت الأشياء (IoT)

يشير المصطلح إنترنت الأشياء (IoT) إلى الأجهزة الإلكترونية التي تعمل عن بُعد على الإنترنت. على سبيل المثال، يُعتبر المنبّه الذكي الذي يرسل تحديثات منتظمة إلى هاتفك الذكي جهاز إنترنت الأشياء (IoT). تقدّم أجهزة إنترنت الأشياء (IoT) طبقة إضافية من المخاطر الأمنية بسبب الاتصال المستمر وأخطاء البرامج المخفية. وبالتالي، من الضروري اعتماد سياسات أمنية في البنية الأساسية للشبكة بهدف تقييم المخاطر المحتملة لأجهزة إنترنت الأشياء (IoT) المختلفة، والحدّ منها.

أمان البيانات

يعمل أمان البيانات على حماية البيانات أثناء النقل وفي حالة عدم النشاط من خلال نظام تخزين فعّال ونقل آمن للبيانات. يتبنّى المطورون تدابير وقائية، مثل التشفير والنسخ الاحتياطية المعزولة، لضمان المرونة التشغيلية عند التعامل مع انتهاكات البيانات المحتملة. في بعض الحالات، يستخدم المطورون نظام AWS Nitro System للحفاظ على سرية مساحات التخزين وتقييد وصول المشغّلين.

أمان التطبيقات

أمان التطبيقات هو جهد مُنسَّق يهدف إلى تحسين مستويات حماية التطبيقات من محاولات التضليل غير المصّرح بها في مراحل التصميم والتطوير والاختبار. يكتب مبرمجو البرامج تعليمات برمجية آمنة من أجل منع الأخطاء التي يمكن أن تزيد من مخاطر الأمان.

أمان نقاط النهاية

يعالج أمان نقاط النهاية مخاطر الأمان التي تنشأ عند وصول المستخدمين إلى شبكة المؤسسة عن بُعد. تعمل ميزة حماية أمان نقاط النهاية على فحص الملفات من الأجهزة الفردية وتقليل التهديدات عند اكتشافها.

التعافي من الكوارث وتخطيط استمرارية الأعمال

يصف هذا خطط الطوارئ التي تسمح للمؤسسات بالاستجابة سريعًا لحوادث الأمن السيبراني، ومواصلة العمل بدون أي انقطاع أو مع حدوث انقطاعات لمدة قصيرة. فهي تنفّذ سياسات لاستعادة البيانات من أجل استجابة إيجابيًا لحالات فقدان البيانات.

مشاركة المعلومات مع المستخدمين النهائين

يؤدي الأفراد العاملين داخل المؤسسة دورًا مهمًا في ضمان نجاح استراتيجيات الأمن السيبراني. وتُعتبر مشاركة المعلومات مفتاحًا لضمان تدريب الموظفين على أفضل ممارسات الأمان، مثل حذف الرسائل الإلكترونية المشبوهة والامتناع عن توصيل أجهزة USB غير معروفة.

ما هي مكونات استراتيجية الأمن السيبراني؟

تتطلب استراتيجية الأمن السيبراني القوية اتباع نهج مُنسّق يشمل أفراد المؤسسة وعملياتها وتقنياتها.

الأفراد

معظم الموظفين غير مدركين لأحدث التهديدات وأفضل ممارسات الأمان التي تساعد على حماية أجهزتهم وشبكاتهم وخادمهم. إن تدريب الموظفين وإعلامهم بمبادئ الأمن السيبراني يقلل من مخاطر الرقابة التي قد تؤدي إلى حوادث غير مرغوب فيها.

العملية

يطوّر فريق أمن تكنولوجيا المعلومات إطار عمل أمني قوي لضمان المراقبة المستمرة والإبلاغ عن نقاط الضعف المعروفة في البنية الأساسية الحاسوبية للمؤسسة. إطار العمل هو خطة تكتيكية تضمن استجابة المؤسسة وتعافيها فوريًا من الحوادث الأمنية المحتملة.

التقنية

تستخدم المؤسسات تقنيات الأمن السيبراني لحماية الأجهزة والخوادم والشبكات والبيانات المتصلة من التهديدات المحتملة. على سبيل المثال، تستخدم الشركات جدران الحماية وبرامج مكافحة الفيروسات وبرامج الكشف عن البرامج الضارة وفلترة نظام أسماء النطاقات (DNS) من أجل اكتشاف الوصول غير المصرّح به إلى النظام الداخلي تلقائيًا، ومنعه. تستخدم بعض المؤسسات التقنيات التي تعمل على أمان انعدام الثقة لتعزيز الأمن السيبراني بشكل أكبر.

ما هي تقنيات الأمن السيبراني الحديثة؟

هذه هي تقنيات الأمن السيبراني الحديثة التي تساعد المؤسسات على تأمين بياناتها.

انعدام الثقة

انعدام الثقة هي أحد مبادئ الأمن السيبراني الذي يَفترض عدم الوثوق بأي تطبيقات أو مستخدمين تلقائيًا، حتى في حالة استضافتهم داخل المؤسسة. بدلاً من ذلك، يفترض نموذج انعدام الثقة أنّ عنصر التحكم في الوصول هو الأقل امتيازًا، ما يتطلب مصادقة صارمة من السلطات المعنية ومراقبة مستمرة للتطبيقات. تستخدم AWS مبادئ انعدام الثقة لمصادقة كل طلب فردي لواجهة برمجة التطبيقات (API) والتحقق منه.

تحليلات السلوك

تراقب تحليلات السلوك عملية نقل البيانات من الأجهزة والشبكات لاكتشاف الأنشطة المشبوهة والأنماط غير المعتادة. على سبيل المثال، يتم تنبيه فريق أمن تكنولوجيا المعلومات بحدوث ارتفاع مفاجئ في نقل البيانات أو بتنزيل ملفات مشبوهة إلى أجهزة معينة.

نظام كشف التسلل

تستخدم المؤسسات أنظمة كشف التسلل لتحديد الهجوم السيبراني والاستجابة له بسرعة. تستخدم حلول الأمان الحديثة تقنية تعلّم الآلة وتحليلات البيانات بهدف الكشف عن التهديدات الخاملة في البنية الأساسية الحاسوبية للمؤسسة. تحدّد آلية الدفاع ضد التسلل أيضًا مسارًا للبيانات في حالة وقوع حادث، ما يساعد فريق الأمن على اكتشاف مصدر الحادث.

التشفير السحابي

يعمل التشفير السحابي على تشفير البيانات قبل تخزينها في قواعد البيانات السحابية. هذا يمنع الأطراف غير المصرّح لها من إساءة استخدام البيانات في انتهاكات محتملة. تستخدم المؤسسات خدمة إدارة مفاتيح التشفير من AWS (AWS KMS) للتحكم في تشفير البيانات في أعباء عمل AWS.

كيف تساعد AWS في تحسين مستوى الأمن السيبراني؟

كأحد عملاء AWS، ستستفيد من مراكز بيانات AWS ومن الشبكة المصممة لحماية معلوماتك وهويتك وتطبيقاتك وأجهزتك. باستخدام AWS، يمكنك تحسين قدرتك على تلبية متطلبات الأمان والامتثال الرئيسية، مثل محلية البيانات وحمايتها وسريتها، بفضل الخدمات والميزات الشاملة التي نقدّمها. تمكنّك AWS من تحويل مهام الأمان اليدوية إلى آلية حتى تتمكن من التركيز على الارتقاء بعملك التجاري وتحديثه.

توفر AWS خدمات الأمن السيبراني التي تساعدك على القيام بما يلي:

حماية البيانات والحسابات وأعباء العمل من الوصول غير المصرّح به.

إدارة الهويات والموارد والأذونات على نطاق واسع.

فرض سياسة أمان دقيقة في نقاط التحكم في الشبكة في مؤسستك بكاملها.

مراقبة نشاط الشبكة وسلوك الحساب باستمرار داخل بيئة السحابة الخاصة بك.

الحصول على عرض شامل لحالة الامتثال الخاصة بك باستخدام عمليات التحقق من الامتثال المؤتمة.

ابدأ باستخدام الأمن السيبراني على AWS من خلال إنشاء حساب AWS اليوم.