الأمن السيبراني وتاثيره على التطبيقات التعليمية:

أصبح الأمن السيبراني ضرورة في عصرنا الحالي الذي أحكمت فيه التكنولوجيا قبضتها على العالم. وفي هذا المقال سوف نستعرض تعريف الأمن السيبراني عامة. بعدها سنوضح أهمية الأمن السيبراني، وسنذكر كيف يعمل الأمن السيبراني ومسؤوليات متخصص الأمن السيبراني، ثم سنتناول بالتفصيل مجالاته وأنواع التهديدات المحتملة، وأخيرًا سنلقي نظرة على مكونات استراتيجية الأمن السيبراني قبل أن نختم المقال بتقنيات الأمن السيبراني الحديثة .

قائمة المحتويات

ما الأمن السيبرانيCybersecurity ؟

تعريف مفهوم الأمن السيبراني Cyber Securityيتضح من تحليل المصطلح ذاته، فالمصطلح يتألف من كلمتين :

- الأمن Security وتعني الحماية والتأمين
- والسيبراني Cyber تعني إلكتروني أو عبر الإنترنت .

وعلى هذا فالمقصود بالأمن السيبراني هو تأمين الأجهزة الإلكترونية وتوفير الأمان لشبكات الإنترنت والأنظمة البرمجية وحماية البيانات الرقمية المهمة من أي تهديدات أو أخطار إلكترونية تؤدي إلى اختراقها وزعزعة استقرارها .

فالأمن السيبراني معنيّ من حيث الأصل بصد الهجمات الإلكترونية وتأمين الأنظمة والأجهزة الإلكترونية، ويحدث ذلك التأمين عن طريق توفير طبقات متعددة من الحماية تتوزع على الأنظمة والشبكات بمنهجيات معينة لكي يتعذر اختراقها، ومن ثم تُحفَظ البيانات الحساسة، ويتم تأمين سير عمليات التفاعل التجارية وغيرها عبر الفضاء الإلكتروني لضمان جريانها بسلاسة وأمان.

كيف يعمل الأمن السيبراني؟

يعمل الأمن السيبراني من خلال عملية منظمة تتألف بالأساس من 3 جوانب، هي الوقاية والرصد والصد، يستهدف من خلالها حماية الأنظمة والشبكات والبيانات الرقمية من الوصول غير المصرح به أو السرقة أو التلف.

1.الوقاية

جانب الوقاية يتضمن التنفيذ الاستراتيجي للتدابير الأمنية التي تهدف إلى تجنب الوصول غير المصرح به بشكل استباقي وإحباط الاختراقات المحتملة. يعد هذا الموقف الاستباقي أمرًا بالغ الأهمية لإنشاء بيئة رقمية محصنة تعمل كرادع ضد الجهات الخبيثة التي تسعى إلى استغلال نقاط الضعف.

2.الرصد

يؤدي جانب الرصد دورًا محوريًا في الأمن السيبراني، إذ يحدد التهديدات المحتملة ومواطن الضعف داخل النظام. يتضمن ذلك استخدام أدوات مراقبة متقدمة وأنظمة كشف التسلل وغيرها من التقنيات المتطورة لفحص حركة الزيارات على الشبكة وسلوك النظام. إن الرصد الدقيق في الوقت المناسب أمرًا أساسيًا لكي تبقى متقدمًا بخطوة على الاختراقات الأمنية المحتملة، مما يسمح بتنفيذ تدابير سريعة وفعالة.

3.الصد

جانب الصد هو الجانب الثالث في الأمن السيبراني، والذي يستلزم اتخاذ الإجراءات اللازمة لاحتواء حادثة خرق أمني. والسرعة في اتخاذ تلك الإجراءات عند حدوث خرق تكون عنصرًا حاسمًا وبالغ الأهمية. يتضمن ذلك عزل الأنظمة المتأثرة بالخرق الأمني بسرعة، وإبطال مفعول التهديدات، واستعادة البيانات المخترقة، وتنفيذ الإجراءات التصحيحية لتحصين النظام لعدم تكرار تلك الاختراقات مرة أخرى.

ما مسئوليات متخصص الأمن السيبراني؟

مسئوليات متخصص الأمن السيبراني تتمحور حول توفير الأمان الشامل للنظام الإلكتروني، إذ تظهر تهديدات أمنية مستحدثة طوال الوقت، ويجب على متخصصي الأمن السيبراني متابعة كل ما يستجد في الأساليب التي يستخدمها المتسللون في هذا المجال، لا سيما وأن الإحصائيات تشير إن الاقتصاد العالمي سوف يتكبد حوالي10.5تريليون دولار بحلول عام 2025. وسنذكر فيما يلي ماذا يفعل موظف الأمن السيبراني وأهم المسؤوليات الملقاة على عاتقه:

- وضع ضوابط وصول المستخدم إلى النظام أو الشبكة وفق معايير الأمان اللازمة.
- مراقبة أداء الشبكة والأنظمة لرصد الثغرات الأمنية وأي نشاط مشبوه .
- إجراء عمليات تدقيق منتظمة للتأكد من سير المنظومة الأمنية على ما يرام.
- التحديث المستمر لسياسات الأمان وتدابير الحماية الخاصة بالمؤسسة.
- تطبيق إجراءات ضد الاختراقات عند اكتشاف هجوم سيبراني .
- تتبُع التطورات والمستجدات البقاء على إطلاع بآخر الحيل المستخدمة لاستباق أي هجوم محتمل.
- توعية موظفي المؤسسة حول مخاطر الأمن السيبراني وكيفية التصدي لها وتزويدهم بالأساسيات اللازمة.

أهمية الأمن السيبراني للمؤسسات

أهمية الأمن السيبراني للمؤسسات والشركات تتجلى في حماية البيانات المهمة، واستدامة سير العمليات التجارية، والامتثال للوائح التنظيمية، وتعزيز ثقة العملاء، والبقاء في صدارة المنافسة. وسنتناول كل نقطة من تلك النقاط على حِدَةٍ فيما يلي :

1.حماية البيانات المهمة

حماية البيانات المهمة هي أحد الأسباب الرئيسية التي تدفع المؤسسات والشركات إلى الاستثمار في الأمن السيبراني. ويتضمن ذلك حماية معلومات العملاء والسجلات المالية والملكية الفكرية. من شأن الهجوم الإلكتروني الذي يؤدي إلى اختراق البيانات أن يكون له عواقب وخيمة، منها الخسائر المالية والإضرار بسمعة المؤسسة.

2.استدامة سير العمليات

استدامة سير العمليات تعني التصدي إلى أي هجوم إلكتروني يمكن أن يؤدي إلى تعطيل سير عمليات المؤسسة، مما يتسبب في شلل في العمل ونزيف في الإنتاجية. إن الحرص على تسليح مؤسستك باستراتيجية قوية للأمن السيبراني يؤدي إلى الحفاظ على استمرارية عملياتك وتقليل احتمالية التعطل الذي تكون تكلفته باهظة.

3 .تعزيز ثقة العملاء

تعزيز ثقة العملاء من الآثار الإيجابية التي تعود عليك من تعزيز الأمن السيبراني في مؤسستك، فقد أصبح العملاء يدركون أكثر فأكثر أهمية حماية بياناتهم، ومن خلال إظهار التزام قوي بالأمن السيبراني يتسنى للمؤسسة تعزيز ثقة عملائها فيها، مما يفضي إلى زيادة الولاء والعلاقات طويلة الأمد.

4 .البقاء في صدارة المنافسة

البقاء في صدارة المنافسة أثر إيجابي آخر يعود على مؤسستك من تعزيز الأمن السيبراني، فالمؤسسات التي تعطي الأولوية للأمن السيبراني تكون في وضع أفضل للبقاء في صدارة المنافسة مع منافسيها في السوق. وكذلك، فمن خلال تنفيذ تدابير أمنية قوية يتسنى للمؤسسات تقليل مخاطر التهديدات السيبرانية والتركيز على كفاءاتها الأساسية، مما يزودها بميزة تنافسية.

ما مجالات الأمن السيبراني؟

مجالات الأمن السيبراني تتنوع بحسب عوامل عديدة، إذ لا يوجد حل واحد يمكن تطبيقه على مختلف الأجهزة والشبكات والأنظمة لضمان أمنها. وفيما يلي نستعرض أنواع الأمن السيبراني، فنتناول أمن البنية التحتية، وأمن الشبكة، وأمن نقاط النهاية، وأمن التطبيق، والأمن السحابي، وأمن المعلومات، وأمن الهاتف .

1.أمن البنية التحتية الحيويةCritical infrastructure security

يحمي أمن البنية التحتية الحيوية Critical infrastructure security الأنظمة الحاسوبية والتطبيقات والشبكات والبيانات والأصول من المنتجات الرقمية التي يعتمد عليها المجتمع لضمان الأمن القومي والمصلحة العامة، مثل مجالات النقل والاتصالات والطاقة، إذ تعتمد المؤسسات في تلك المجالات على أُطر معينة في الأمن السيبراني، لأن تعطل تلك الخدمات أو تلف البيانات من شأنه زعزعة استقرار المجتمع.

2.أمن الشبكةNetwork security

أمن الشبكة Network security يمنع الوصول غير المصرح به إلى موارد الشبكة، إذ يرصد الهجمات الإلكترونية والاختراقات ويعترضها، وذلك للحيلولة دون تغيير المعلومات الخاصة بالمستخدمين أو سرقتها أو إتلافها. وفي الوقت ذاته يتيح للمستخدمين المصرح لهم بالدخول الآمن إلى موارد الشبكة، وذلك بالتحكم في عمليات تسجيل الدخول والتدقيق في كلمات المرور وغيرها من أذونات الدخول.

3.أمن نقاط النهايةEndpoint security

أمن نقاط النهاية Endpoint security معنيّ بحماية الأجهزة ومستخدميها من الهجمات، كما يحمي الشبكة أيضًا من القراصنة الذين يستفيدون من نقاط النهاية تلك لشن الهجمات. والمقصود بنقاط النهاية هي الخوادم وأجهزة الحاسوب المكتبية والمحمولة والهواتف، أي الأجهزة التي تقع في أيدي المستخدمين.

4.أمن التطبيقاتApplication security

أمن التطبيقات Application security يحمي التطبيقات في أطوار تصميمها وبعد إطلاقها، ويمنع الوصول غير المصرح به إلى التطبيقات والبيانات ذات الصلة واستخدامها، ويسد الثغرات التي يمكن أن يستغلها المتسللون .

5.الأمن السحابيCloud security

يعمل الأمن السحابيّ Cloud security على تأمين الخدمات السحابية الخاصة بالمؤسسة. وبشكل عام، يعمل الأمن السحابي وفقًا لنموذج المسؤولية المشتركة: حيث يكون مقدم الخدمة السحابية مسؤولًا عن تأمين الخدمات التي يقدمها والبنية التحتية السحابية، بينما يكون العميل مسؤولًا عن حماية بياناته .

6.امن المعلوماتInformation security

يتعلق أمن المعلومات Information security بحماية جميع المعلومات المهمة الخاصة بالمؤسسة – الملفات والبيانات الرقمية، والمستندات، والوسائط – ضد الوصول غير المصرح به أو انكشاف السرية أو الاستخدام غير المصرح به أو التغيير والتبديل .

7.أمن الهاتفMobile security

يشمل أمن الهاتف Mobile security مجموعة من المعايير والتقنيات الخاصة بالهواتف الذكية والأجهزة المحمولة، وفي الآونة الأخيرة يدخل أمن الأجهزة المحمولة تحت مظلة حلول إدارة نقاط النهاية الموحدة.(UEM)

ما أنواع تهديدات الأمن السيبراني؟

أنواع تهديدات الأمن السيبراني المختلفة تُشكل خطرًا محدقًا بالمؤسسات والشركات، وفهم أنواع تلك التهديدات أمرًا ضروريًا لحماية مؤسستك. وسوف نتناول أشهر أنواع تلك التهديدات، ومنها البرمجيات الخبيثة، وبرامج الفدية، والتصيد المعلوماتي، والتهديد الداخلي.

1.البرمجيات الخبيثة

البرمجيات الخبيثة هي أي تعليمات برمجية يُقصد بها إلحاق ضرر بالنظام الحاسوبي، وتتضمن الغالبية العظمى من الهجمات الإلكترونية الحديثة نوعًا من البرمجيات الخبيثة، حيث يقوم القراصنة بالتسلل عن طريق إنشاء برمجيات خبيثة ويستخدمونها للوصول غير المصرح به إلى أنظمة الحاسوب والبيانات الحساسة أو تعطيلها أو إتلافها .

2.برامج الفدية

برامج الفدية هي نوع من البرمجيات الخبيثة التي تقوم بتشفير بيانات الضحية أو جهازه وتهدد بإبقائها مشفرة – أو إتلافها ومحوها – ما لم يدفع الضحية فدية للمبتز. ووفقًا للإحصائيات فقد شكلت هجمات برامج الفدية17%من جميع الهجمات الإلكترونية التي تم شنها في عام 2022.

3.التصيد المعلوماتي

هجمات التصيد المعلوماتي هي رسائل بريد إلكتروني أو رسائل نصية أو صوتية تحاول التحايل على المستخدمين لتنزيل برامج ضارة أو مشاركة معلومات حساسة أو تحويل أموال إلى المحتالين. ومن أكثرها شيوعًا عمليات التصيد المعلوماتي الجماعية – وهي رسائل احتيالية يتم إرسالها عبر البريد بشكل جماعي وتتستر تحت شعارات علامات تجارية كبيرة وموثوقة، ثم تطلب من الناس إعادة تعيين كلمات المرور الخاصة بهم أو إعادة إدخال معلومات بطاقات الائتمان .

4.التهديدات من الداخل

التهديد من الداخل يسببه أفراد سيئون من داخل المؤسسة ذاتها، أو من خلال استيلاء القراصنة على حساباتهم. قد يكون اكتشاف التهديدات الداخلية أكثر صعوبة من اكتشاف التهديدات الخارجية لأن نشاطها مصرح به، ولأنها غير مرئية لبرامج مكافحة الفيروسات وجدران الحماية والحلول الأمنية الأخرى التي تهدف إلى منع الهجمات الخارجية.

5.الهجوم المتعدد لتعطيل الخدمة(DDoS)

الهجوم المتعدد لتعطيل الخدمة (DDoS) يهدف إلى تعطيل خادم أو موقع أو شبكة عن طريق زيادة التحميل عليه بزيارات كثيرة جدًا في وقت واحد، وهو ما يؤدي إلى تعطل الخدمة وسد الطريق أمام المستخدمين للوصول إلى الموقع أو الشبكة. وقد شهدت معدلات هذا النوع من الهجمات ارتفاعًا كبيرًا خلال جائحة كوفيد-19، وعادة ما تكون مقترنة بهجمات برامج الفدية .

ما مكونات استراتيجية الأمن السيبراني؟

توجد مكونات رئيسية لاستراتيجية الأمن السيبراني، ولا بد لكل شركة ومؤسسة من مراعاة تلك العناصر لحماية أصولها الرقمية والحفاظ على ثقة العملاء والامتثال للوائح. ومن أهم تلك المكونات تقييم المخاطر، ووضع السياسات والإجراءات الأمنية، وتنفيذ إجراءات أمنية قوية للشبكات ونقاط النهاية، وإنشاء ضوابط وصول صارمة، وتشفير البيانات الحساسة، وإعداد خطة استجابة للطوارئ.

1.تقييم المخاطر

إن تقييم المخاطر التي تواجه مؤسستك يزودك بفهم يكون هو الأساس لوضع استراتيجية قوية للأمن السيبراني. عليك بإجراء تقييم شامل للمخاطر من أجل تحديد التهديدات المحتملة ونقاط الضعف والتأثيرات المحتملة على مؤسستك، ومن شأن هذا أن يساعدك على تحديد أولويات جهودك وتخصيص الموارد بشكل فعال.

2.وضع السياسات والإجراءات الأمنية

من المهم وضع سياسات وإجراءات أمنية واضحة وشاملة تحدد أدوار الموظفين ومسؤولياتهم، وتحدد الاستخدام المقبول للتكنولوجيا، والخطوات التي يجب اتخاذها في حالة وقوع خرق أمني. عليك بمراجعة هذه السياسات وتحديثها بانتظام لمواكبة التغييرات في المشهد التكنولوجي والتهديدات المستجدة على الساحة.

3.تنفيذ إجراءات أمنية قوية للشبكات ونقاط النهاية

من الضروري تنفيذ إجراءات أمنية قوية للشبكات ونقاط النهاية، بما في ذلك تهيئة جدران الحماية، وأنظمة كشف التسلل والوقاية منه، وبرامج مكافحة البرمجيات الخبيثة، والوصول الآمن إلى الشبكات. عليك بتحديث البرامج وتصحيحها بانتظام لمعالجة نقاط الضعف المرصودة.

4.وضع ضوابط وصول

يجب وضع ضوابط وصول صارمة لإحكام السيطرة على وصول المستخدمين إلى البيانات والأنظمة الحساسة. عليك بوضع ضوابط الوصول مُحكمة لكل فئة من المستخدمين في النظام، وتطبيق عملية مُصادقة قوية، وتطبيق عمليات تدقيق باستمرار فيما يخص الامتيازات الممنوحة للمستخدمين من أجل تحجيم مخاطر الوصول غير المصرح به.

5.تشفير البيانات

يجب تشفير البيانات الحساسة أثناء تخزينها وأثناء نقلها، وذلك من أجل حمايتها من وصول المستخدمين غير المصرح لهم بالاطلاع عليها، ومن أجل تجنُب الانتهاكات الأمنية والاختراقات المحتملة. يضيف التشفير طبقة أخرى من الأمان، مما يزيد من صعوبة وصول المتطفلين والمهاجمين إلى المعلومات الحساسة.

6.إعداد خطة استجابة للطوارئ

يجب إعداد خطة استجابة للطوارئ، بحيث تكون تلك الخطة محددة التفاصيل لتحديد الخطوات والإجراءات والتدابير التي ستُتخذ في حالة حدوث خرق أمني. يجب أن تتضمن هذه الخطة بروتوكولات اتصال وتحديد أدوار ومسؤوليات واضحة وتوضيح إرشادات فعالة لمعالجة الوضع واحتوائه وتجاوزه والتعافي منه.

ما أهم تقنيات الأمن السيبراني الحديثة؟

من الضروري البقاء على دراية بأهم تقنيات الأمن السيبراني الحديثة، وذلك من أجل التصدي للتهديدات المستجدة بأساليب فعالة وتوفير حماية حقيقية للبيانات الحساسة. ولهذا سوف نستعرض فيما يلي 5 من أهم التقنيات الحديثة المستخدمة في مجال الأمن السيبراني، هي الذكاء الاصطناعي، وتحليلات السلوك، ونموذج انعدام الثقة، وتقنية سلسلة الكتل، والتشفير الحسابي .

1.الذكاء الاصطناعي (AI) والتعلم العميق

يُحدث الذكاء الاصطناعي (AI) والتعلم العميق ثورة في مجال الأمن السيبراني حاليًا، حيث تقوم هذه التقنيات بتحليل كميات هائلة من البيانات، والتعلم من الأنماط، والتنبؤ بالتهديدات المحتملة. ومن خلال استخدام هذه التقنيات يمكن لخبراء الأمن السيبراني تحديد التهديدات والاستجابة لها بشكل أسرع وأكثر دقة من أي وقت مضى.

2.تحليلات السلوك

تحليلات السلوك هي تقنية جديدة للأمن السيبراني تستخدم خوارزميات التعلم الآلي لتحليل سلوك المستخدم. يمكن لهذه التقنية اكتشاف الأنماط من الطريقة التي يتفاعل بها المستخدمون مع الأجهزة، مثل سرعة الكتابة وحركة الماوس وأسلوب التنقل. ومن خلال تحليل تلك الأنماط، يمكن تحديد التهديدات المحتملة، مثل المتسللين الذين تمكنوا من الوصول إلى حساب المستخدم.

3.نموذج انعدام الثقةZero-Trust Model

نموذج انعدام الثقة Zero-Trust Model هو نموذج أمني يتطلب التحقق الصارم من هوية كل شخص أو جهاز يحاول الوصول إلى شبكة المؤسسة أو نظامها ومواردها. يفترض هذا النموذج أنه لا يوجد أحد موثوق به دائمًا، حتى لو كانوا داخل محيط شبكة المؤسسة بالفعل. وقد اكتسب نموذج انعدام الثقة زخمًا خلال السنوات الأخيرة بسبب العدد المتزايد من الهجمات الإلكترونية التي تستهدف الشركات والمؤسسات.

4.تقنية سلسلة الكتلBlockchain

ترتبط تقنية سلسلة الكتل Blockchain ارتباطًا كبيرًا بالعملات المشفرة، ولكنها قادرة على التأثير بقوة في مجال الأمن السيبراني أيضًا. إذ من خلال إنشاء قاعدة بيانات لا مركزية، يمكن لهذه التقنية توفير تخزين آمن للمعلومات الحساسة وتهيئة شبكة شبه منيعة تصد المتسللين، وهي أفضل رهان لدينا في الوقت الحاضر لحماية البيانات من أي اختراق، وتتضاعف جدواها إذا ما اقترنت بتقنيات الذكاء الاصطناعي.

5.التشفير السحابي

يأتي التشفير السحابي تماشيًا مع كوّن الحوسبة السحابية أصبحت جزءًا أساسيًا من العديد من المؤسسات والشركات، وترتكز هذه التقنية على تشفير البيانات قبل أن تُخزَن في قواعد البيانات السحابية، مما يحول دون وصول المتسللين إلى المعلومات الحساسة .