
إدارة المخاطر

المقدمة

الهدف العام لمقرر إدارة المخاطر هو تعليم الطلاب كيفية التعامل مع المخاطر بطريقة فعالة وتطبيق أساليب إدارة المخاطر في العمل اليومي. ويمكن تحقيق هذا الهدف من خلال توفير تعليم شامل ومتخصص للطلاب حول مختلف جوانب إدارة المخاطر، وإشراكهم في أنشطة عملية تساعدهم على توسيع مهاراتهم في هذا المجال.

الهدف العام من المقرر

- فهم مفهوم المخاطر السيبرانية وأنواعها وأهميتها في الأمن السيبراني.
- تنمية القدرة على تحليل المخاطر السيبرانية وتقييمها.
- ٣-تعلم كيفية تطبيق نظام إدارة المخاطر السيبرانية في المؤسسات والمشاريع.
- فهم أهمية إدارة المخاطر السيبرانية وتعلم كيفية التعامل مع التحديات الأمنية.
- تعلم كيفية تطبيق إدارة المخاطر السيبرانية.
- ٦-تنمية مهارات اختيار الأدوات الأمنية وتطبيقها في الحماية من التهديدات السيبرانية المختلفة.
- ٧ -فهم القوانين واللوائح والمعايير المتعلقة بالأمن السيبراني وكيفية تطبيقها.
- ٨- تعزيز القدرة على تحليل وتقييم المخاطر السيبرانية وإدارتها.

الأهداف التفصيلية للحقيبة : أن يكون المتدرب قادراً على ان

١ -مفهوم المخاطر السيبرانية.

٢ -تحليل وتقييم المخاطر السيبرانية.

٣ -تقنيات تحليل المخاطر السيبرانية.

٤ -إدارة المخاطر السيبرانية.

٥ -تطبيقات إدارة المخاطر السيبرانية.

٦ -القوانين واللوائح الخاصة بالأمن السيبراني.

٧ -تحليل الأداء الأمني.

٨- المراجعة.

الفهرس

الوحدة الأولى

- فهم مفهوم المخاطر السيبرانية.
- الفيروسات والبرامج الضارة.
- القرصنة الإلكترونية
- الاحتيال الإلكتروني.
- التجسس الإلكتروني.
- الهجمات الموزعة على الخدمة (DDoS)الاختراق الإلكتروني.

فهم مفهوم المخاطر السيبرانية.

في الوحدة الأولى، يتم التركيز على توضيح ماهية المخاطر السيبرانية وأهميتها في العصر الرقمي الحالي. المخاطر السيبرانية تشير إلى التهديدات التي تستهدف الأنظمة الإلكترونية، والشبكات، والبيانات التي يتم تخزينها ومعالجتها عبر الإنترنت. تتنوع هذه المخاطر لتشمل الهجمات الإلكترونية، مثل البرمجيات الخبيثة، والفيروسات، ومحاولات الاختراق، والتي قد تؤدي إلى فقدان البيانات، أو سرقتها، أو تعطيل الخدمات.

الهدف من هذه الوحدة هو تعريف المتعلمين بطبيعة المخاطر السيبرانية، والتهديدات المختلفة التي تواجه المؤسسات والأفراد، بالإضافة إلى تسليط الضوء على أهمية اتخاذ التدابير الوقائية لحماية الأصول الرقمية. يتم أيضًا استعراض بعض الأمثلة العملية والتحديات الشائعة في مجال الأمن السيبراني لتمكين المتعلمين من إدراك مدى تعقيد هذا المجال.

الفيروسات والبرامج الضارة.

الفيروسات والبرامج الضارة:

في هذا الجزء، يتم التطرق إلى أحد أخطر التهديدات السيبرانية وأكثرها شيوعًا: الفيروسات والبرامج الضارة. الفيروسات هي برامج خبيثة مصممة للتكاثر والانتشار عبر الأجهزة والشبكات، غالبًا بهدف إحداث أضرار، مثل تلف الملفات أو سرقة البيانات. يمكن أن تنتقل الفيروسات من جهاز لآخر عبر البريد الإلكتروني، التحميل من الإنترنت، أو حتى من خلال الأجهزة القابلة للإزالة مثل الأقراص الصلبة الخارجية.

أما البرامج الضارة(Malware) ، فهي فئة أوسع تشمل كل أنواع البرمجيات التي تم تطويرها بقصد إلحاق الضرر أو السيطرة على الأنظمة، بما في ذلك الفيروسات، وأحصنة طروادة(Trojans) ، والديدان(Worms) ، وبرامج الفدية(Ransomware) ، وبرامج التجسس.(Spyware)

الفيروسات: تعمل على إلحاق الضرر بالأجهزة والملفات، وتتطلب غالبًا تدخلًا بشريًا للانتقال من جهاز لآخر.

أحصنة طروادة: تبدو وكأنها برامج شرعية ولكنها تحتوي على شفرات خبيثة تتيح للمهاجمين الوصول غير المصرح به إلى النظام.

الديدان: تشبه الفيروسات ولكنها تختلف في أنها تستطيع الانتشار بشكل ذاتي دون الحاجة لتدخل المستخدم.

برامج الفدية: تقوم بتشفير ملفات المستخدمين وتجبرهم على دفع فدية مالية لاستعادة الوصول إلى بياناتهم.

برامج التجسس: تعمل بشكل خفي لجمع معلومات حساسة من الأجهزة دون علم المستخدم.

القرصنة الإلكترونية

القرصنة الإلكترونية هي أحد التهديدات السيبرانية الأكثر انتشارًا وتعقيدًا. يشير هذا المصطلح إلى الأنشطة التي يقوم بها المهاجمون (يطلق عليهم القراصنة أو الهاكرز) للوصول غير المصرح به إلى أنظمة الكمبيوتر، والشبكات، والبيانات الخاصة بالمستخدمين أو المؤسسات. القرصنة قد تتنوع بين اختراق الحسابات الشخصية على مواقع التواصل الاجتماعي، وصولًا إلى هجمات معقدة تستهدف البنية التحتية الرقمية للدول والشركات الكبرى.

يوجد عدة أنواع من القراصنة، ولكل نوع أهداف وأدوات مختلفة:

الهاكرز الأخلاقيون :(White Hat Hackers) يقومون باختبار أمان الأنظمة بشكل قانوني، ويعملون عادةً مع الشركات لتعزيز الحماية السيبرانية.

الهاكرز الخبيثون :(Black Hat Hackers) يقومون بأنشطة غير قانونية مثل سرقة البيانات، نشر البرمجيات الضارة، أو تعطيل الخدمات. هدفهم الرئيسي هو الربح المالي أو التخريب.

الهاكرز الرماديون :(Grey Hat Hackers) يقعون في منطقة وسط بين الهاكرز الأخلاقيين والخبيثين. قد يخترقون الأنظمة دون إذن لكن دون نية للتسبب بأضرار كبيرة، وأحيانًا يقومون بذلك لكشف الثغرات الأمنية دون الاستفادة الشخصية.

تقنيات القرصنة الإلكترونية تتنوع أيضًا:

الهجمات باستخدام الهندسة الاجتماعية: تعتمد على خداع المستخدمين للكشف عن معلومات حساسة، مثل كلمات المرور، من خلال أساليب مثل التصيد الاحتيالي.(Phishing)

الاختراق المباشر: يستغل القراصنة الثغرات البرمجية أو نقاط الضعف في الشبكات للوصول إلى الأنظمة والسيطرة عليها.

الهجمات الموزعة لحرمان الخدمة :(DDoS) يقوم القراصنة بإغراق الخوادم بكمية ضخمة من الطلبات في وقت قصير، مما يؤدي إلى تعطيلها.

سرقة الهوية: يقوم القراصنة بسرقة المعلومات الشخصية للمستخدمين واستخدامها بشكل غير قانوني، مثل استخدام بيانات البطاقة الائتمانية.

الاحتيال الإلكتروني.

الاحتيال الإلكتروني هو نوع من الجرائم السيبرانية التي يتم فيها استغلال الإنترنت لخداع الأفراد أو المؤسسات لتحقيق مكاسب مالية غير مشروعة. يتم هذا الاحتيال عبر مجموعة متنوعة من الأساليب والتقنيات التي تهدف إلى سرقة الأموال أو المعلومات الحساسة، وفي بعض الحالات الوصول إلى بيانات مهمة واستخدامها بطرق ضارة.

أبرز أساليب الاحتيال الإلكتروني تشمل:

التصيد الاحتيالي :(Phishing) يعتبر من أكثر أساليب الاحتيال شيوعًا. يقوم المحتالون بإرسال رسائل بريد إلكتروني أو رسائل نصية تبدو وكأنها من جهات موثوقة، مثل البنوك أو الشركات الكبيرة. تتضمن هذه الرسائل عادةً روابط تؤدي إلى مواقع مزيفة تطلب من المستخدمين إدخال معلوماتهم الشخصية أو المالية.

الاحتيال عبر البريد الإلكتروني للأعمال (Business Email Compromise - BEC): يحدث هذا

التجسس الإلكتروني.

التجسس الإلكتروني هو نشاط غير قانوني يهدف إلى الحصول على معلومات حساسة أو سرية من الأفراد أو المؤسسات أو حتى الدول، باستخدام تقنيات وأدوات رقمية. يعتبر هذا النوع من التجسس تهديدًا خطيرًا للأمن القومي، الأمن التجاري، والخصوصية الفردية، حيث يتم استهداف البيانات الهامة، مثل الأسرار التجارية، والمعلومات العسكرية، والبيانات الشخصية.

هناك عدة أساليب يتم من خلالها تنفيذ التجسس الإلكتروني

البرمجيات الخبيثة :(Malware) يستخدم المتجسسون برامج ضارة مثل برامج التجسس (Spyware)لاختراق الأنظمة وسرقة المعلومات دون علم المستخدم. هذه البرامج غالبًا ما تعمل بصمت في الخلفية، مما يجعل من الصعب اكتشافها.

التنصت على الاتصالات :(Eavesdropping) يقوم المتجسسون بمراقبة البيانات المتدفقة عبر الشبكات، مثل المكالمات الهاتفية، والبريد الإلكتروني، والمحادثات النصية. هذا النوع من التجسس يمكن أن يتم من خلال اختراق الشبكات اللاسلكية أو الوصول إلى قنوات الاتصال المشفرة.

الهجمات المستهدفة :(Targeted Attacks) مثل هجمات APT (Advanced Persistent Threats)، حيث يتم تخصيص هجمات معينة لاستهداف جهات محددة. يتم

تنفيذ هذه الهجمات على مدار فترة طويلة بهدف جمع أكبر قدر من المعلومات دون لفت الانتباه.

الهندسة الاجتماعية: يستخدم المتجسسون أساليب الهندسة الاجتماعية للحصول على معلومات من خلال خداع الأشخاص للتخلي عن بياناتهم الحساسة، مثل كلمات المرور أو تفاصيل الدخول إلى الأنظمة.

التهديدات الداخلية :(Insider Threats) في بعض الأحيان، يعتمد التجسس الإلكتروني على موظفين داخل المؤسسة يقومون بنقل المعلومات السرية إلى جهات خارجية. هؤلاء الأشخاص قد يكونون مدفوعين بأغراض مالية أو سياسية.

التجسس الإلكتروني لا يقتصر على سرقة المعلومات فقط؛ فقد يؤدي أيضًا إلى تعريض الضحايا للمخاطر الأخرى مثل الابتزاز أو تشويه السمعة. لمكافحة هذا النوع من التجسس، يتم استخدام عدة تدابير، مثل تشفير البيانات، وتعزيز أمن الشبكات، وتدريب الموظفين على التعرف على التهديدات المحتملة، بالإضافة إلى استخدام برامج الحماية المتقدمة التي ترصد أي نشاط مشبوه داخل الأنظمة.

الهجمات الموزعة على الخدمة (DDoS)الاختراق الإلكتروني.

الهجمات الموزعة على الخدمة، المعروفة اختصارًا بـ(DDoS)، هي نوع من الهجمات السيبرانية التي تهدف إلى تعطيل الخدمات الإلكترونية عن طريق إغراق الخوادم أو الشبكات بكمية هائلة من الطلبات في فترة زمنية قصيرة. تقوم هذه الهجمات بتحميل النظام فوق طاقته، مما يؤدي إلى إبطائه بشكل كبير أو حتى تعطيله تمامًا، مما يمنع المستخدمين الشرعيين من الوصول إلى الخدمات.

كيفية تنفيذ هجمات:DDoS

شبكات البوت نت :(Botnets) يعتمد المهاجمون على شبكات من الأجهزة المصابة ببرامج ضارة تُعرف بـ"بوتس(Bots) "، والتي يتم التحكم فيها عن بُعد. هذه الأجهزة المصابة قد تكون حواسيب شخصية، هواتف ذكية، أو حتى أجهزة إنترنت الأشياء .(IoT) عند شن الهجوم، يتم توجيه جميع هذه الأجهزة لإرسال عدد هائل من الطلبات إلى الخادم المستهدف في نفس الوقت.

الهجمات بحجب الخدمة الموزعة :(Distributed Attacks) على عكس الهجمات التقليدية لحجب الخدمة(DoS) ، تعتمد هجمات DDoS على استغلال عدد كبير من الأجهزة الموزعة جغرافيًا، مما يجعل من الصعب تتبع مصدر الهجوم أو إيقافه.

أنواع هجمات:DDoS

هجمات حجمية :(Volumetric Attacks) تهدف إلى استهلاك عرض النطاق الترددي (Bandwidth)بالكامل للخادم أو الشبكة، مما يؤدي إلى إبطاء أو توقف الخدمة.

الهجمات على بروتوكولات النقل :(Protocol Attacks) تستهدف نقاط الضعف في بروتوكولات الشبكة مثل TCP/IP لإرباك الخادم وتعطيله.

الهجمات على مستوى التطبيق :(Application Layer Attacks) تركز على طبقة التطبيق من النموذجOSI ، مثل الهجمات التي تستهدف طلباتHTTP ، وتعتبر هذه الهجمات أصعب في الكشف عنها لأنها تحاكي سلوك المستخدم العادي.

تأثيرات هجمات :DDoS تؤدي هجمات DDoS إلى خسائر مالية كبيرة للشركات، حيث يتم تعطيل مواقع الويب أو الخدمات الحيوية، مما يؤثر على سمعتها وثقة العملاء. قد تستمر الهجمات لعدة ساعات أو حتى أيام، مما يزيد من الأضرار الناتجة.

لمكافحة هجمات DDoS، تعتمد المؤسسات على حلول متقدمة مثل الجدران النارية الخاصة بتصفية حركة المرور (Firewalls)، وأنظمة كشف التطفل (Intrusion Detection Systems)، وشبكات توصيل المحتوى (Content Delivery Networks - CDN) التي تساعد في توزيع الحمل وتخفيف التأثير.

الاختراق الإلكتروني:

الاختراق الإلكتروني هو عملية غير مصرح بها للوصول إلى أنظمة الكمبيوتر أو الشبكات بهدف سرقة أو تعديل أو تدمير البيانات. يمكن أن يتم الاختراق من قبل أفراد (الهاكرز) أو مجموعات أو حتى دول، وغالبًا ما يكون الدافع وراءه ماليًا، سياسيًا، أو بهدف الابتزاز.

أنواع الاختراق الإلكتروني:

اختراق الأنظمة :(System Hacking) يستهدف أنظمة التشغيل والخوادم لاستغلال الثغرات الأمنية والحصول على حقوق دخول غير مصرح بها.

اختراق الشبكات :(Network Hacking) يركز على الهجوم على الشبكات، مثل استهداف الموجهات (Routers) أو المودمات، للتجسس على حركة المرور أو تعطيل الشبكة.

اختراق قواعد البيانات :(Database Hacking) يهدف إلى الوصول إلى قواعد البيانات وسرقة المعلومات الحساسة مثل بيانات العملاء، السجلات المالية، أو حتى البيانات الطبية.

اختراق البرمجيات :(Software Hacking) يستغل الثغرات في البرامج أو التطبيقات للحصول على وصول غير مصرح به، مثل استغلال ثغرات في متصفحات الويب.

أدوات وتقنيات الاختراق

الهجمات بالقوة الغاشمة :(Brute Force Attacks) محاولة تخمين كلمات المرور عبر تجربة جميع التركيبات الممكنة حتى يتم الوصول إلى الكلمة الصحيحة.

الهندسة الاجتماعية :(Social Engineering) خداع الأفراد للكشف عن معلومات حساسة من خلال البريد الإلكتروني أو الاتصالات الهاتفية.

ثغرات اليوم صفر :(Zero-Day Exploits) استغلال ثغرات في البرامج التي لم يتم اكتشافها بعد من قبل المطورين.

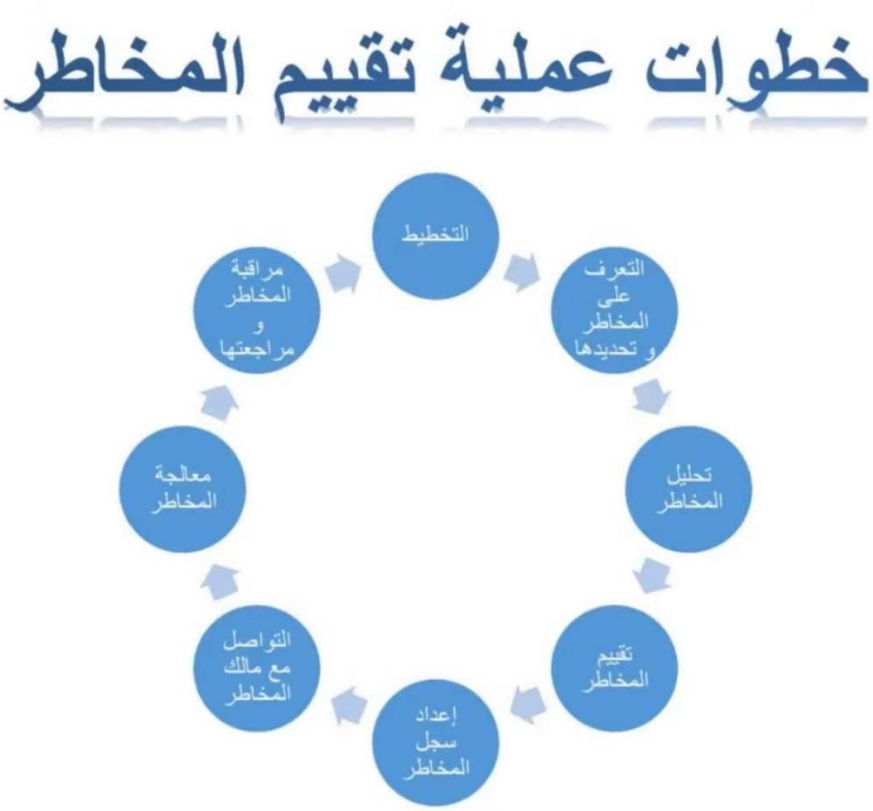
تأثيرات الاختراق الإلكتروني: يؤدي الاختراق إلى خسائر مادية مباشرة للشركات والأفراد، بما في ذلك سرقة البيانات المالية أو المعلومات الحساسة. كما قد يؤدي إلى أضرار معنوية، مثل فقدان الثقة بين العملاء والشركات.

لمكافحة الاختراق الإلكتروني، يجب اعتماد نهج شامل للأمن السيبراني يشمل تحديث الأنظمة بانتظام، استخدام كلمات مرور قوية، تفعيل التحقق الثنائي، وتوعية المستخدمين حول مخاطر الاختراق وأساليب الحماية منها.

الوحدة الثانية

- **تحليل وتقييم المخاطر السيبرانية.**
- **تحديد الأصول السيبرانية.**
- **٢-تحليل التهديدات السيبرانية.**
- **تقييم الثغرات الأمنية.**
- **تحديد المخاطر السيبرانية.**
- **تحديد الإجراءات الوقائية والتصحيحية تطبيق نظام إدارة المخاطر السيبرانية.**

تحليل وتقييم المخاطر السيبرانية:



في الوحدة الثانية، يتم التركيز على كيفية تحليل وتقييم المخاطر السيبرانية التي تواجه الأنظمة والشبكات في المؤسسات. هذه العملية ضرورية لتحديد مدى خطورة التهديدات المحتملة واتخاذ القرارات المناسبة لحماية الأصول الرقمية. تتضمن هذه الوحدة عدة خطوات ومنهجيات تساعد في تحديد المخاطر، تقييم تأثيرها، وتحديد الإجراءات اللازمة لتقليلها.

1 .تحديد الأصول والتهديدات: الخطوة الأولى في تحليل المخاطر السيبرانية هي تحديد الأصول الحساسة التي تحتاج إلى حماية، مثل البيانات المالية، المعلومات الشخصية، أو الأنظمة التشغيلية. بعد تحديد الأصول، يتم تحديد التهديدات المحتملة التي قد تستهدف هذه الأصول، مثل الهجمات الإلكترونية، الفيروسات، أو السرقة الداخلية.

2 .تحليل نقاط الضعف: يتم في هذه المرحلة تحليل نقاط الضعف الموجودة في الأنظمة والبنية التحتية التي يمكن أن يستغلها المهاجمون. يتضمن ذلك تقييم الثغرات الأمنية في البرامج، ضعف سياسات الأمان، أو نقص التدريب بين الموظفين. معرفة نقاط الضعف تساعد في تحديد المخاطر بشكل أكثر دقة.

3 .تقدير التأثير والاحتمالية: بعد تحديد التهديدات ونقاط الضعف، يتم تقييم مدى تأثير كل تهديد في حالة حدوثه. يتضمن ذلك النظر في التأثير المالي، القانوني، والتشغيلي. كما يتم تقدير احتمالية حدوث كل تهديد بناءً على العوامل البيئية والتقنية.

4 .حساب مستوى المخاطر: يتم جمع المعلومات من الخطوات السابقة لحساب مستوى المخاطر لكل تهديد. يمكن استخدام عدة منهجيات، مثل مصفوفات المخاطر التي تجمع بين احتمالية وقوع التهديد وتأثيره، لتحديد الأولويات في التعامل مع المخاطر.

5 .تطوير استراتيجيات التخفيف: بناءً على تقييم المخاطر، يتم وضع استراتيجيات لتخفيف المخاطر أو تقليلها. هذه الاستراتيجيات قد تشمل تحسين إجراءات الأمان، تحديث الأنظمة، تعزيز التوعية بين الموظفين، أو تنفيذ تقنيات الحماية مثل التشفير والجدران النارية.

6. مراقبة وتحديث التقييم: تحليل وتقييم المخاطر هو عملية مستمرة، حيث يجب مراقبة الأوضاع بشكل دوري وتحديث التقييمات بناءً على التغييرات في البيئة التقنية أو ظهور تهديدات جديدة. هذه المرحلة تضمن أن تظل التدابير الأمنية فعالة وملائمة.

أنواع المخاطر السيبرانية

تتعرض المؤسسات لأشكال متعددة من المخاطر السيبرانية، ومن أشهر هذه الأنواع ما يلي:

1 -التنصت

تتعرض الأنظمة الإلكترونية للمؤسسات للتنصت عند سرقة المعلومات الهامة اعتمادًا على حركة المرور التي تُخترق، وذلك نتيجة الوصول إلى المعلومات المرسلة والمتبادلة بين المواقع المضيفة والمستخدم.

2 -سرقة كلمة المرور

يعتمد المخترقون بشكل شائع على سرقة كلمة المرور في سرقة البيانات الهامة للمستخدم، فقد يحدث ذلك عبر التنصت أو من خلال التخمين، وكلما كانت كلمة المرور سهلة كلما سهل اختراقها.

3 -البرامج الضارة

لا تخلو المخاطر السيبرانية من البرامج الضارة التي تنشأ جراء وجود جزء ما داخل البرنامج المثبتة ويكون غير مألوف مما يلحق أضرار بالأجهزة، يستهدف المجرمون الإلكترونيون إطلاق البرامج الضارة بغرض سرقة البيانات الهامة للمستخدمين والي قد تكون بيانات شخصية أو مصرفية.

4 -عمليات الاحتيال

يعتمد المجرمون الإلكترونيون على وسائل أخرى للاحتيال وسرقة بيانات المستخدم من خلال إرسال رسالة عبر البريد الإلكتروني تتطلب من المستخدم تعبئة بياناته، وكثيرًا ما يقع المستخدمون في هذا الفخ مما يجعلها من أكثر الوسائل الناجحة في المخاطر السيبرانية.

5 -الهجوم عبر المواقع

في بعض الأحيان عند الرغبة في سرقة بيانات المستخدمين أو إلحاق الأضرار بخدمات الموقع فإن المجرمين الإلكترونين يستهدفون المواقع غير المشفرة عبر أكواد محددة تعطل الموقع، ويرسلون هذه الأكواد إلى الموقع بمجرد الوصول إليه من أجل التعطيل أو سرقة المعلومات المطلوبة.

6 -الهندسة الاجتماعية

يعتمد المحتالون على الهندسة الاجتماعية باستخدام مواقع التواصل الاجتماعي وهي جزء من عمليات الاحتيال التي يُستهدف فيها الحصول على كلمة المرور، البيانات المصرفية، جهاز المستخدم.

تحديد الأصول السيبرانية:

في هذه الخطوة الأساسية من عملية تحليل المخاطر السيبرانية، يتم تحديد الأصول السيبرانية التي تحتاج إلى حماية داخل المؤسسة. الأصول السيبرانية تشمل جميع العناصر الرقمية التي تمتلكها أو تديرها المؤسسة والتي تعتبر ذات قيمة كبيرة لعملياتها، سواء كانت مادية أو غير مادية. فهم وتحديد هذه الأصول بدقة يُعَدّ خطوة حاسمة لتقييم المخاطر السيبرانية بشكل صحيح وتطوير استراتيجيات حماية فعالة.

أنواع الأصول السيبرانية:

- البيانات:

البيانات الحساسة: مثل المعلومات الشخصية، البيانات المالية، والسجلات الطبية. هذه البيانات تعتبر هدفًا رئيسيًا للهجمات السيبرانية.

البيانات التشغيلية: مثل قواعد البيانات التي تحتوي على المعلومات الخاصة بإجراءات العمل أو بيانات العملاء.

- البنية التحتية التقنية:

الأجهزة: تشمل الخوادم، الحواسيب الشخصية، أجهزة الشبكات مثل الموجهات (Routers) والمحولات(Switches) ، وأجهزة التخزين.

الشبكات: تشمل جميع شبكات الاتصال المحلية (LAN) والواسعة (WAN) التي تُستخدم لنقل البيانات داخل وخارج المؤسسة.

أنظمة التشغيل: البرمجيات التي تُشغّل الأجهزة وتُدير العمليات، مثل أنظمة تشغيل الخوادم وأجهزة المستخدم النهائي.

- البرمجيات والتطبيقات:

البرامج الأساسية: مثل أنظمة إدارة قواعد البيانات(DBMS) ، وبرامج إدارة الموارد المؤسسية(ERP) ، وتطبيقات تخطيط المشاريع.

التطبيقات المخصصة: البرمجيات التي تم تطويرها داخليًا أو المخصصة لاحتياجات معينة داخل المؤسسة.

- الأشخاص:

الموظفون: الأفراد الذين لديهم وصول إلى الأنظمة والبيانات الحساسة، بما في ذلك المسؤولون عن إدارة الأنظمة والأمن السيبراني.

المستخدمون الخارجيون: مثل العملاء أو الشركاء الذين قد يكون لديهم وصول إلى بعض الأصول الرقمية.

- العمليات والسياسات:

إجراءات العمل: الوثائق والتوجيهات المتعلقة بتنفيذ العمليات اليومية وحماية الأصول الرقمية.

السياسات الأمنية: القواعد والإجراءات التي تحكم كيفية استخدام الأصول السيبرانية وحمايتها.

أهمية تحديد الأصول السيبرانية: تحديد الأصول السيبرانية بدقة يساعد في:

تحديد الأولويات الأمنية: فهم الأصول الأكثر أهمية للمؤسسة يمكن من تخصيص الموارد لحمايتها بشكل مناسب.

تقييم المخاطر: معرفة الأصول الحساسة تُمكّن من تحديد التهديدات المحتملة والتحديات الأمنية المرتبطة بها.

تطوير استراتيجيات الحماية: بناء خطط الحماية والتخفيف من المخاطر على أساس الأصول المحددة واحتياجاتها الأمنية.

الامتثال للمعايير: ضمان أن جميع الأصول المهمة تُدار وفقًا للمعايير والقوانين ذات الصلة بالأمن السيبراني.

تحديد الأصول السيبرانية هو جزء حيوي من إدارة المخاطر، حيث يُمكّن المؤسسات من التعرف على ما يجب حمايته، مما يتيح وضع استراتيجيات أكثر دقة وشمولية للأمن السيبراني.

تحليل التهديدات السيبرانية

تحليل التهديدات السيبرانية هو خطوة حاسمة في عملية إدارة المخاطر السيبرانية، حيث يتم فيها تحديد ودراسة التهديدات المحتملة التي قد تستهدف الأصول الرقمية للمؤسسة. الهدف من هذا التحليل هو فهم طبيعة هذه التهديدات، مصادرها، والطرق التي يمكن أن تستخدمها لإلحاق الضرر، مما يساعد على تصميم استراتيجيات فعالة لتقليل المخاطر أو تجنبها.

خطوات تحليل التهديدات السيبرانية:

تحديد التهديدات المحتملة:

التهديدات الداخلية: تشمل الأخطاء البشرية أو التصرفات الخبيثة من داخل المؤسسة مثل تسريب المعلومات، أو سرقة البيانات بواسطة موظفين غير راضين.

التهديدات الخارجية: تشمل الهجمات التي تأتي من خارج المؤسسة، مثل الهجمات الإلكترونية من قِبل مجرمي الإنترنت، القراصنة، أو مجموعات القرصنة المدعومة من دول.

التهديدات الطبيعية: الكوارث الطبيعية مثل الفيضانات، الزلازل، أو انقطاع الكهرباء، والتي يمكن أن تؤثر على البنية التحتية الرقمية.

التهديدات التقنية: مثل الثغرات الأمنية في البرمجيات، أو فشل الأجهزة التي يمكن استغلالها من قبل المهاجمين.

دراسة سلوك المهاجمين:

أهداف المهاجمين: تحليل الدوافع التي قد تقود المهاجمين إلى استهداف المؤسسة، مثل السرقة المالية، الحصول على معلومات سرية، أو إحداث فوضى.

الطرق المستخدمة: فهم الأساليب والأدوات التي يستخدمها المهاجمون، مثل هجمات البرمجيات الخبيثة(Malware) ، هجمات التصيد(Phishing) ، أو هجمات حجب الخدمة الموزعة.(DDoS)

مستويات التعقيد: تحديد مدى تعقيد الهجمات المحتملة، سواء كانت هجمات بسيطة يمكن لأي مهاجم القيام بها أو هجمات متقدمة تتطلب خبرات متطورة.

تحليل التأثير:

تأثير مالي: دراسة الآثار المالية المحتملة في حالة نجاح التهديدات، مثل تكاليف استعادة الأنظمة، الغرامات، أو فقدان الإيرادات.

تأثير تشغيلي: تقييم كيفية تأثير التهديدات على العمليات اليومية للمؤسسة، مثل توقف الإنتاج، تعطيل الخدمات، أو فقدان بيانات هامة.

تأثير على السمعة: دراسة مدى تأثير الهجمات على سمعة المؤسسة وثقة العملاء والشركاء فيها.

تقييم احتمالية الحدوث:

التكرار السابق: تحليل التاريخ السابق للهجمات لتقدير احتمالية تكرارها.

بيئة التهديد: دراسة البيئة الرقمية المحيطة بالمؤسسة لتحديد احتمالية تعرضها لتهديدات معينة بناءً على التوجهات الراهنة في مجال الأمن السيبراني.

تحديد نقاط الضعف القابلة للاستغلال

الثغرات الأمنية: تحديد الثغرات البرمجية أو الإعدادات غير الصحيحة التي قد تُستغل من قبل المهاجمين.

نقص الحماية: تقييم مدى كفاية الإجراءات الأمنية الحالية، مثل الجدران النارية، برامج مكافحة الفيروسات، أو سياسات التحكم في الوصول.

أهمية تحليل التهديدات السيبرانية:

تحسين الاستجابة: فهم التهديدات المحتملة يُمكّن المؤسسات من تطوير خطط استجابة أكثر فعالية، وتقليل الوقت المستغرق للتعافي من الهجمات.

تخصيص الموارد: يساعد التحليل في تحديد الأولويات وتخصيص الموارد اللازمة لحماية الأصول الأكثر عرضة للتهديدات.

تقييم الثغرات الأمنية

تقييم الثغرات الأمنية هو عملية تحليل الأنظمة والبنية التحتية لتحديد النقاط الضعيفة التي قد تستغلها التهديدات السيبرانية. يهدف هذا التقييم إلى الكشف عن الثغرات التي قد تسمح بالوصول غير المصرح به، أو التسبب في أضرار، أو التأثير على سلامة الأنظمة والبيانات. يتم تنفيذ هذه العملية بطرق متعددة لضمان تغطية جميع جوانب الأمن.

خطوات تقييم الثغرات الأمنية

- جمع المعلومات

مسح الأنظمة: جمع معلومات حول الأنظمة، الشبكات، والبرمجيات المستخدمة. يتضمن ذلك تحديد التطبيقات المثبتة، إصدارات البرمجيات، ونقاط الدخول المحتملة.

التحقق من التكوينات: فحص إعدادات النظام والبنية التحتية للتأكد من أنها تتبع معايير الأمان الموصى بها.

- استخدام أدوات المسح

أدوات المسح التلقائي: استخدام أدوات متخصصة مثلNessus ، وOpenVAS، و Qualysلمسح الشبكات والأنظمة بحثًا عن ثغرات معروفة. هذه الأدوات تقوم بتحليل الأنظمة للكشف عن نقاط الضعف المتوقعة بناءً على قواعد بيانات محدثة.

اختبارات الأمان اليدوية: إجراء اختبارات يدوية لتكملة أدوات المسح التلقائي، مثل التحقق من الثغرات التي قد لا تكون مغطاة بواسطة الأدوات.

- تحليل النتائج

تصنيف الثغرات: تصنيف الثغرات المكتشفة بناءً على درجة خطورتها، مثل الثغرات الحرجة، العالية، المتوسطة، والمنخفضة. يتم ذلك بناءً على تأثيرها المحتمل واحتمالية استغلالها.

تحديد الأسباب الجذرية: تحديد الأسباب الأساسية للثغرات، مثل أخطاء في البرمجة، إعدادات غير آمنة، أو نقص في الحماية.

- تقييم التأثير والاحتمالية

تأثير الثغرات: تقييم كيفية تأثير كل ثغرة على النظام، مثل القدرة على الوصول إلى البيانات الحساسة، السيطرة على الأنظمة، أو التسبب في تعطيل الخدمة.

احتمالية الاستغلال: تقدير مدى احتمال استغلال الثغرات من قبل المهاجمين، بناءً على سهولة الاستغلال، وتوفر الأدوات، ومستوى الخبرة المطلوب.

- تطوير استراتيجيات التخفيف

تحديث البرمجيات: تنفيذ التحديثات والتصحيحات اللازمة لسد الثغرات المكتشفة.

تحسين التكوينات: ضبط إعدادات الأمان بشكل صحيح لتقليل نقاط الضعف.

تنفيذ حلول الأمان: مثل جدران الحماية، ونظم كشف التسلل، وبرامج مكافحة الفيروسات لتعزيز الحماية.

- التحقق من الإصلاحات

إعادة المسح: بعد تطبيق التصحيحات والإجراءات التصحيحية، يتم إعادة فحص الأنظمة للتحقق من أن الثغرات قد سُدّت وأن الإصلاحات كانت فعّالة.

اختبارات التحقق: إجراء اختبارات أمنية إضافية لضمان عدم وجود ثغرات جديدة أو غير مكتشفة.

تحديد المخاطر السيبرانية

تحديد المخاطر السيبرانية هو عملية تحديد وتوثيق المخاطر المحتملة التي قد تؤثر على الأصول السيبرانية للمؤسسة، وتحديد كيف يمكن أن تؤثر هذه المخاطر على الأمان الرقمي والعمليات التشغيلية. يتضمن هذا التحديد تحديد التهديدات ونقاط الضعف التي يمكن أن تؤدي إلى وقوع الحوادث الأمنية.

خطوات تحديد المخاطر السيبرانية

1. تحديد الأصول السيبرانية

فهم الأصول: جمع المعلومات حول الأصول الرقمية للمؤسسة، مثل الأنظمة، الشبكات، البيانات، البرمجيات، والأجهزة.

2. تحديد القيمة: تقييم أهمية كل أصل بناءً على قيمته للأعمال، وتأثير فقدانه أو تأثره بالتهديدات.
3. تحديد التهديدات:

مصادر التهديدات: تحديد مصادر التهديدات المحتملة مثل القراصنة، البرمجيات الخبيثة، الهجمات الداخلية، الكوارث الطبيعية، أو الأخطاء البشرية.

أساليب التهديدات: فهم طرق الهجوم التي قد تستخدمها التهديدات، مثل هجمات التصيد الاحتيالي، هجماتDDoS ، أو البرمجيات الخبيثة.

4. تحديد نقاط الضعف:

التحليل الفني: مراجعة الأنظمة والشبكات والبرمجيات لتحديد نقاط الضعف التقنية مثل الثغرات البرمجية أو إعدادات الأمان غير الصحيحة.

التحليل التنظيمي: تقييم العمليات والسياسات الإدارية والموارد البشرية لمعرفة نقاط الضعف في إدارة الأمان.

5. تقييم المخاطر:

الاحتمالية والتأثير: تحديد مدى احتمال حدوث كل تهديد وتأثيره على الأصول. يمكن تصنيف المخاطر بناءً على احتمالية وقوعها وتأثيرها المحتمل، مثل عالٍ، متوسط، أو منخفض.

تحديد الأولويات: ترتيب المخاطر بناءً على تقييم المخاطر لتحديد أيها يتطلب اهتمامًا فوريًا وأيها يمكن التعامل معه في وقت لاحق.

6. توثيق المخاطر:

إعداد سجل المخاطر: توثيق كل مخاطر محددة مع تفاصيل حول التهديدات، نقاط الضعف، تأثيراتها المحتملة، واحتمالية وقوعها.

تحديث السجلات: التأكد من تحديث سجل المخاطر بانتظام بناءً على التغيرات في الأنظمة، التهديدات، أو البيئة التنظيمية.

7. مراجعة وتحديث التحليل:

مراجعة دورية: إجراء مراجعات دورية للتحليل لضمان أنه يعكس التهديدات ونقاط الضعف الحالية. التهديدات السيبرانية تتطور باستمرار، لذا فإن تحديث التحليل بانتظام ضروري.

التحقق من التغيرات: تحليل تأثير التغيرات في البيئة التكنولوجية أو التنظيمية على المخاطر المحددة.

تحديد الإجراءات الوقائية والتصحيحية وتطبيق نظام إدارة المخاطر السيبرانية

1 .تحديد الإجراءات الوقائية:

الإجراءات الوقائية هي التدابير التي يتم اتخاذها لتجنب وقوع الحوادث الأمنية وتقليل احتمال حدوث المخاطر. تشمل هذه الإجراءات:

تحديث البرمجيات والنظام: ضمان تحديث جميع البرمجيات ونظم التشغيل بانتظام لسد الثغرات الأمنية المعروفة.

تطبيق تصحيحات الأمان: تثبيت تصحيحات الأمان الصادرة من الشركات المصنعة للتعامل مع الثغرات المكتشفة.

استخدام حلول الحماية: مثل الجدران النارية(Firewalls) ، وبرامج مكافحة الفيروسات، وأنظمة كشف التسلل (IDS) لحماية الأنظمة من الهجمات.

تشفير البيانات: حماية البيانات الحساسة بتشفيرها أثناء النقل والتخزين.

تدريب الموظفين: توعية وتدريب الموظفين على مخاطر الأمان السيبراني وأفضل الممارسات لتجنب الأخطاء البشرية.

إجراءات التحكم في الوصول: تنفيذ سياسات تحكم الوصول لضمان أن فقط الأشخاص المصرح لهم يمكنهم الوصول إلى الأنظمة والبيانات الحساسة.

2 .تحديد الإجراءات التصحيحية:

الإجراءات التصحيحية هي التدابير التي يتم اتخاذها بعد وقوع حادث أمني لتصحيح الأضرار ومنع تكرارها. تشمل هذه الإجراءات:

تحليل الحوادث: التحقيق في الحوادث الأمنية لتحديد أسبابها وتأثيراتها.

إصلاح الثغرات: معالجة نقاط الضعف التي استغلها الهجوم واتخاذ خطوات لضمان عدم تكرارها.

استعادة البيانات: استعادة البيانات والأنظمة من النسخ الاحتياطية لضمان عدم فقدان المعلومات.

مراجعة السياسات والإجراءات: تحديث السياسات والإجراءات الأمنية بناءً على الدروس المستفادة من الحادث.

تطبيق تحسينات: تنفيذ تحسينات على الأنظمة والبنية التحتية بناءً على نتائج التحقيق لتقليل المخاطر المستقبلية.

3 .تطبيق نظام إدارة المخاطر السيبرانية:

نظام إدارة المخاطر السيبرانية هو مجموعة من الإجراءات والسياسات التي تهدف إلى إدارة وتخفيف المخاطر السيبرانية بشكل منهجي. يشمل تطبيق نظام إدارة المخاطر السيبرانية الخطوات التالية:

تطوير سياسة إدارة المخاطر: وضع سياسة واضحة لإدارة المخاطر تحدد الأهداف والإجراءات والمسؤوليات.

إجراء تقييمات دورية: تقييم المخاطر السيبرانية بانتظام لضمان الكشف عن التهديدات الجديدة والتغيرات في البيئة.

تطبيق إطار عمل للأمن السيبراني: استخدام أطر عمل معترف بها مثل NIST Cybersecurity Framework، أو ISO/IEC 27001 لتوجيه سياسات وإجراءات الأمان.

إدارة الأزمات: تطوير خطط لإدارة الأزمات والتعامل مع الحوادث الأمنية لضمان استجابة فعالة.

التدقيق والمراجعة: إجراء تدقيقات ومراجعات دورية للتحقق من فعالية نظام إدارة المخاطر وتطبيق التحسينات اللازمة.

التواصل والتدريب: تعزيز التواصل الداخلي حول المخاطر السيبرانية وتوفير التدريب المستمر للموظفين.

الوحدة الثالثة

- تقنيات تحليل المخاطر السيبرانية.
- تقنية تحليل المخاطر الكمومية.
- تقنية تحليل المخاطر الإحصائية.
- تقنية تحليل المخاطر العكسية.
- تقنية تحليل المخاطر المعرفية.

تقنيات تحليل المخاطر السيبرانية

تقنيات تحليل المخاطر السيبرانية تشمل مجموعة من الأدوات والمنهجيات المستخدمة لتحديد، تقييم، وتحليل المخاطر السيبرانية التي تواجه الأنظمة والشبكات. هذه التقنيات تساعد في فهم المخاطر بعمق وتوجيه الإجراءات الوقائية والتصحيحية بشكل أكثر فعالية.

1 .التحليل النوعي:(Qualitative Analysis)

الوصف والمقارنة: يعتمد على الوصف وتقدير المخاطر باستخدام مصفوفات ومقاييس غير كمية. يشمل التقييم بناءً على الخبرة والتجربة.

مصفوفات المخاطر: استخدام مصفوفات لتحديد أولويات المخاطر بناءً على احتمالية حدوثها وتأثيرها المحتمل. يتم تصنيف المخاطر إلى مستويات مثل عالي، متوسط، ومنخفض.

2 .التحليل الكمي:(Quantitative Analysis)

تقدير الاحتمالية والتأثير: استخدام بيانات رقمية لتحديد احتمالية حدوث المخاطر وتأثيرها المالي المحتمل. يتضمن ذلك استخدام أساليب إحصائية لتقييم المخاطر.

نماذج تحليل المخاطر: مثل نموذج مونت كارلو، الذي يستخدم لمحاكاة نتائج متعددة وتحليل تأثير المخاطر عبر السيناريوهات المختلفة.

3 .تحليل السيناريوهات:(Scenario Analysis)

تقييم سيناريوهات الهجوم: دراسة سيناريوهات محتملة للهجمات السيبرانية لتحديد كيفية تأثيرها على الأنظمة. يشمل ذلك تحليل الهجمات المحتملة، مثل اختراق البيانات أو هجمات DDoS.

التحليل الاستباقي: تطوير سيناريوهات محتملة لمستقبل المخاطر وتقييم كيفية الاستجابة لها.

4 .التحليل البارامتري:(Parametric Analysis)

تحديد معلمات المخاطر: استخدام معلمات محددة لتقييم المخاطر، مثل الثغرات الأمنية والتقنيات المستخدمة في الهجمات. يعتمد على فهم دقيق للبيئة التقنية.

تطبيق النماذج الرياضية: استخدام نماذج رياضية لتحليل العلاقة بين المتغيرات المختلفة والتأثيرات المحتملة.

5 .تحليل:SWOT (SWOT Analysis)

تحليل القوة والضعف والفرص والتهديدات: تحديد نقاط القوة والضعف في البنية التحتية الأمنية، والفرص لتحسين الأمان، والتهديدات المحتملة التي قد تؤثر على الأنظمة.

تطوير استراتيجيات التحسين: استخدام نتائج التحليل لتطوير استراتيجيات تعزز الأمان وتقليل المخاطر.

6 .اختبار الاختراق:(Penetration Testing)

محاكاة الهجمات: إجراء اختبارات لاكتشاف الثغرات الأمنية من خلال محاكاة هجمات فعلية على الأنظمة. يشمل ذلك استخدام أدوات وتقنيات لمحاولة اختراق الأنظمة والتطبيقات.

تقرير النتائج: تقديم تقرير مفصل حول الثغرات المكتشفة وكيفية إصلاحها، مما يوفر رؤى لتحسين الأمان.

7 .تقييم التهديدات ونقاط الضعف:(Threat and Vulnerability Assessment)

تحديد التهديدات ونقاط الضعف: تقييم المخاطر المرتبطة بالتهديدات ونقاط الضعف المحددة في الأنظمة. يتضمن ذلك استخدام أدوات وتقنيات لتحديد التهديدات ونقاط الضعف المحتملة.

توصيات التخفيف: تقديم توصيات للتعامل مع نقاط الضعف وتقليل التأثيرات المحتملة للتهديدات.

تقنية تحليل المخاطر الكمومية

تحليل المخاطر الكمومية هو مفهوم ناشئ يستخدم تقنيات التحليل الكمومي لتقدير وتقييم المخاطر السيبرانية. هذا النوع من التحليل يستفيد من مبادئ الحوسبة الكمومية لتقديم رؤى جديدة حول تقييم المخاطر. على الرغم من أن التقنية لا تزال في مراحلها الأولى من التطوير والتطبيق، إلا أنها تعد بنقل فهم المخاطر السيبرانية إلى مستوى أكثر تقدمًا.

مبادئ تقنية تحليل المخاطر الكمومية

1. الحوسبة الكمومية

التحليل المتقدم: تستخدم الحوسبة الكمومية القدرة على معالجة كميات هائلة من البيانات بشكل أسرع من الحوسبة التقليدية، مما يمكن من تحليل سيناريوهات المخاطر بشكل أكثر تعقيدًا وفعالية.

الاحتمالات غير المحددة: تعالج الحوسبة الكمومية احتمالات متعددة في وقت واحد بفضل مبدأ التراكب الكمومي، مما يوفر تقديرات أدق للمخاطر المحتملة.

2. نمذجة المخاطر الكمومية:

التحليل المتزامن: تتيح تقنيات الكمومية تحليل مجموعة متنوعة من سيناريوهات المخاطر في وقت واحد، مما يساعد في تحديد الأنماط والعلاقات بين المخاطر بشكل أسرع.

التحليل الاحتمالي: توفر تقنية الكمومية نماذج أكثر تعقيدًا لتحليل احتمالية وقوع الأحداث، مما يمكن من تحديد المخاطر التي قد تكون غير مرئية باستخدام التقنيات التقليدية.

3. تقدير التأثير والتفاعل

محاكاة الأحداث: تستخدم تقنيات الكمومية لمحاكاة تأثيرات مختلفة من المخاطر على الأنظمة بطريقة أكثر دقة، مما يعزز فهم كيفية تفاعل المخاطر مع الأصول السيبرانية.

تحليل التفاعل: تتيح التقنية تقييم كيفية تأثير المخاطر المتعددة عند التفاعل معًا، مما يساعد في فهم التأثيرات المعقدة على النظام ككل.

4. التحليل الاستباقي

توقع المخاطر المستقبلية: يمكن لتقنيات الكمومية أن تساعد في تطوير نماذج تنبؤية للمخاطر السيبرانية بناءً على بيانات تاريخية وسيناريوهات محتملة، مما يتيح الاستجابة السريعة للتغيرات في البيئة الأمنية.

تحليل السيناريوهات المحتملة: تحسين قدرة التحليل على التعامل مع سيناريوهات معقدة ومتعددة الأبعاد، مما يوفر رؤى أعمق حول المخاطر المستقبلية.

5. تحديات تقنية تحليل المخاطر الكمومية

التكنولوجيا الناشئة: بما أن الحوسبة الكمومية لا تزال في مراحلها المبكرة، فإن التطبيقات العملية لتحليل المخاطر الكمومية محدودة.

التعقيد التقني: تتطلب التقنية خبرة متقدمة في الحوسبة الكمومية، مما قد يكون عائقًا للتطبيقات الواسعة.

تكاليف التطوير: يمكن أن تكون تكاليف تطوير وتنفيذ الحلول الكمومية مرتفعة، مما قد يؤثر على إمكانية استخدامها في المؤسسات الصغيرة والمتوسطة.

6. أهمية تحليل المخاطر الكمومية

تحسين دقة التحليل: تقدم تقنية الكمومية إمكانية تحليل المخاطر بشكل أكثر دقة وسرعة.

توقع أفضل: توفر القدرة على التنبؤ بالمخاطر المستقبلية بشكل أكثر فعالية بفضل النمذجة المتقدمة.

تقنية تحليل المخاطر الإحصائية

تحليل المخاطر الإحصائية هو استخدام الأساليب الإحصائية لتقدير وتقييم المخاطر السيبرانية. تعتمد هذه التقنية على البيانات التاريخية والنماذج الرياضية لتحليل الاحتمالات والتأثيرات المرتبطة بالمخاطر المحتملة، مما يساعد في فهم وتوقع المخاطر بشكل منهجي.

أساسيات تقنية تحليل المخاطر الإحصائية

1. جمع البيانات

البيانات التاريخية: استخدام بيانات تاريخية عن الحوادث الأمنية، الثغرات، والتهديدات لتقييم المخاطر.

البيانات الوصفية: جمع معلومات حول الأنظمة، البنية التحتية، والعمليات لتوفير سياق أفضل لتحليل المخاطر.

2. تحليل البيانات

التوزيع الاحتمالي: تحديد توزيعات الاحتمالات التي تصف كيفية توزيع المخاطر. تشمل التوزيعات الشائعة مثل التوزيع الطبيعي، والتوزيع اللوجستي، والتوزيع الواسع النطاق.

التحليل التكراري: تحليل تكرار وقوع الأحداث لتحليل احتمالية حدوث المخاطر.

3. نمذجة المخاطر

نماذج التحليل الإحصائي: استخدام نماذج إحصائية مثل نماذج الانحدار لتحليل العلاقة بين المتغيرات المختلفة وتقدير تأثير المخاطر.

نماذج محاكاة مونت كارلو: إجراء محاكاة لتقييم تأثيرات المخاطر عبر سيناريوهات متعددة لتوفير رؤية شاملة حول التوزيع المحتمل للمخاطر.

4. تقدير التأثير

تحليل التأثير المالي: تقدير التأثير المالي المحتمل للمخاطر، بما في ذلك الأضرار المحتملة، التكاليف المرتبطة بالإصلاحات، والتأثيرات على العمليات.

تحليل التأثير على الأداء: تقييم كيفية تأثير المخاطر على أداء الأنظمة والعمليات، مثل التأثير على سرعة الاستجابة أو جودة الخدمة.

5. تقييم المخاطر

تقدير الاحتمالية: استخدام الأساليب الإحصائية لتقدير احتمالية حدوث المخاطر. يشمل ذلك استخدام نماذج إحصائية لتحديد مدى تكرار وقوع الحوادث.

تحديد الأولويات: تصنيف المخاطر بناءً على احتمالية حدوثها وتأثيرها لتحديد أولويات التخفيف.

6. تحليل الحساسية

اختبار السيناريوهات: تحليل كيف تتغير المخاطر بناءً على تغييرات في الافتراضات أو المتغيرات. يساعد في فهم تأثير التغيرات المحتملة على النتائج.

تحليل ما-إذا: تقييم تأثير تغييرات معينة في المتغيرات لتقدير تأثيرات المخاطر المختلفة.

تقنية تحليل المخاطر العكسية

تحليل المخاطر العكسية هو تقنية تستخدم لتقييم المخاطر من خلال التركيز على النواتج أو العواقب العكسية المحتملة لسيناريوهات معينة، بدلاً من التركيز فقط على الأسباب الأولية أو المسببات. تهدف هذه التقنية إلى فهم كيف يمكن أن تؤدي الأحداث غير المتوقعة أو غير المرغوب فيها إلى ظهور المخاطر.

أساسيات تقنية تحليل المخاطر العكسية

1. تحديد السيناريوهات العكسية

التفكير في العواقب: بدلاً من البدء بالتهديدات أو نقاط الضعف، يتم التركيز على النتائج السلبية المحتملة لنظام معين. يتم تحديد كيفية حدوث هذه النتائج وتأثيرها على النظام.

التفكير في أسوأ الحالات: تقييم كيف يمكن أن تحدث أسوأ السيناريوهات وكيف يمكن أن تؤثر على الأصول والعمليات.

2. تقييم العواقب غير المتوقعة:

تحليل الاحتمالات العكسية: دراسة كيف يمكن أن تؤدي الأحداث غير المتوقعة إلى ظهور المخاطر، بما في ذلك التغيرات في البيئة التكنولوجية أو التنظيمية التي يمكن أن تؤدي إلى نتائج سلبية.

محاكاة العواقب: استخدام نماذج ومحاكاة لتقدير العواقب المحتملة لسيناريوهات غير متوقعة.

3. تحليل التأثيرات غير المباشرة

تقييم التأثيرات غير المباشرة: فحص كيفية تأثير العواقب غير المباشرة على الأنظمة والعمليات. يشمل ذلك تحليل كيفية تأثير العواقب الثانوية على الأمان والسيطرة على المخاطر.

تحديد التأثيرات على الأنظمة الأخرى: دراسة كيف يمكن أن تؤثر نتائج المخاطر على الأنظمة أو العمليات الأخرى في المؤسسة.

4. تطوير استراتيجيات التخفيف

استراتيجيات مواجهة العواقب: تطوير استراتيجيات وإجراءات للتعامل مع العواقب العكسية المحتملة والتخفيف من تأثيرها.

تحديد الإجراءات الاحترازية: تحديد وتطبيق إجراءات وقائية لضمان التخفيف من المخاطر العكسية المحتملة.

5. مراجعة وتحسين:

تقييم النتائج: بعد تنفيذ الإجراءات والسيناريوهات، يتم مراجعة النتائج وتقييم فعالية استراتيجيات التخفيف.

تحسين الاستراتيجيات: تعديل وتحسين استراتيجيات التخفيف بناءً على تحليل النتائج وتقييم الأداء.

أهمية تحليل المخاطر العكسية

توفير رؤية شاملة: يقدم فهماً أعمق لكيفية تأثير العواقب غير المتوقعة على الأمان والعمليات، مما يساعد في تعزيز استراتيجيات التخفيف.

تحسين الاستجابة: يساعد في تطوير استراتيجيات استجابة فعالة للتعامل مع المخاطر غير المتوقعة.

زيادة المرونة: يعزز قدرة النظام على التكيف مع السيناريوهات غير المتوقعة والحد من التأثيرات السلبية.

تقنية تحليل المخاطر المعرفية

تحليل المخاطر المعرفية هو منهجية تركز على كيفية إدراك وفهم المخاطر من خلال العمليات المعرفية والذهنية للأفراد أو الفرق. يتمثل الهدف في فهم كيف تؤثر المعرفة، والتصورات، والآراء على تحديد وتقييم المخاطر، وكيف يمكن لهذه العمليات العقلية أن تؤثر على قرارات إدارة المخاطر.

أساسيات تقنية تحليل المخاطر المعرفية

1. فهم الإدراك البشري

التصورات الشخصية: دراسة كيفية إدراك الأفراد أو الفرق للمخاطر بناءً على خلفياتهم ومعرفتهم وتجاربهم.

التحيزات المعرفية: تحديد التحيزات المعرفية التي قد تؤثر على كيفية تقييم المخاطر، مثل التحيز للتفاؤل، أو تحيز التأكيد، أو التقدير المفرط للمخاطر.

2. تحليل المعرفة والخبرة

تحليل الخبرة: دراسة كيف تؤثر الخبرة السابقة والمعرفة على إدراك المخاطر وتقييمها.

تقييم المعرفة: فهم كيف يمكن أن يؤثر مستوى المعرفة الفنية أو التجريبية على قدرة الأفراد أو الفرق على تحديد المخاطر بدقة.

3. تأثير التفكير الجماعي

التحليل الجماعي: فحص كيفية تأثير التفكير الجماعي واتخاذ القرارات الجماعية على إدارة المخاطر.

المهارات الجماعية: تقييم كيفية استخدام مهارات التفكير الجماعي، مثل العصف الذهني، لتحديد وتقييم المخاطر بشكل شامل.

4. نمذجة العمليات المعرفية

نمذجة الإدراك: استخدام نماذج معرفية لفهم كيف يقوم الأفراد بمعالجة المعلومات وتقييم المخاطر.

تحليل القرارات: دراسة كيفية اتخاذ القرارات المتعلقة بالمخاطر بناءً على المعرفة والإدراك.

5. تطوير استراتيجيات التخفيف

تحسين التدريب: تقديم تدريب مستهدف لتحسين كيفية إدراك الأفراد للمخاطر وتقييمها بشكل أكثر دقة.

تطوير الأدوات المعرفية: استخدام أدوات وتقنيات تساعد في تقليل التحيزات المعرفية وتعزيز دقة تقييم المخاطر.

6. مراجعة وتحسين:

تقييم فعالية الإدراك: مراجعة كيف يؤثر الإدراك والمعرفة على تحديد وتقييم المخاطر، وتحسين العمليات بناءً على النتائج.

التغذية الراجعة: جمع التغذية الراجعة حول كيفية تحسين عمليات إدراك المخاطر والمعرفة.

أهمية تحليل المخاطر المعرفية

تحسين دقة التقييم: يساعد في فهم كيفية تأثير المعرفة والإدراك على تقييم المخاطر وتقديم رؤى لتحسينه.

تقليل التحيزات: يساعد في تقليل التحيزات المعرفية التي قد تؤثر على اتخاذ القرارات المتعلقة بالمخاطر.

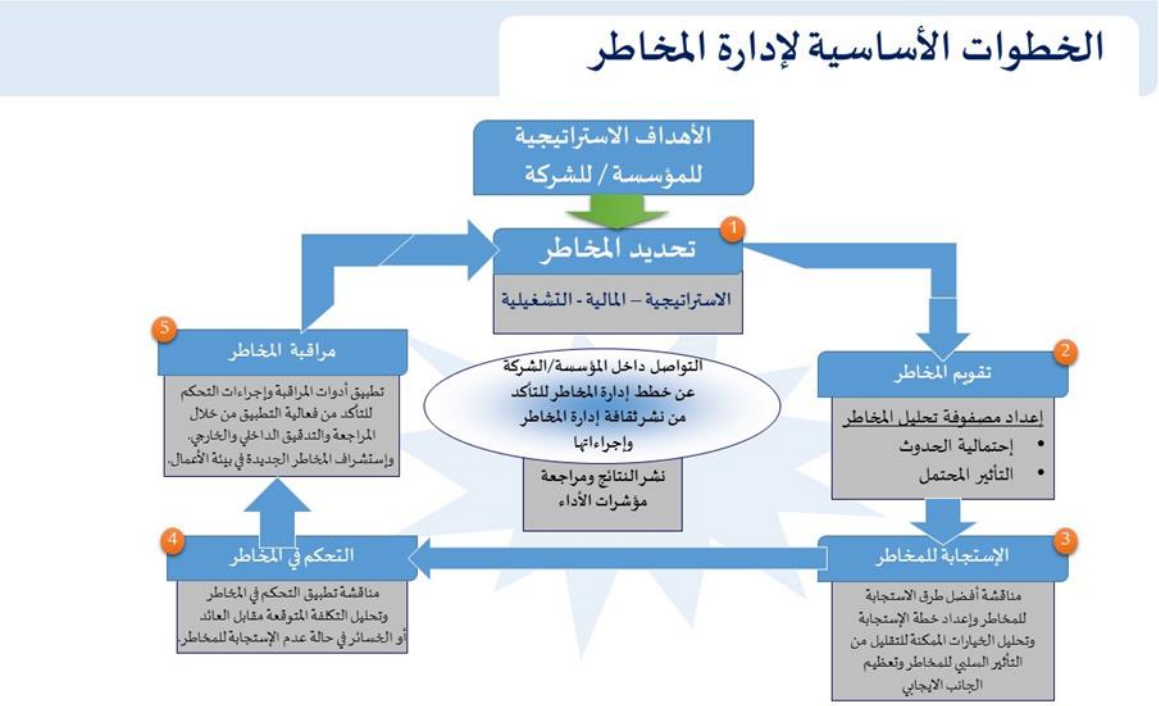
تعزيز الاستجابة: يعزز القدرة على اتخاذ قرارات إدارة المخاطر بناءً على فهم أعمق لعمليات الإدراك والمعرفة.

الوحدة الرابعة

- **إدارة المخاطر السيبرانية.**
- **تحديد الأصول السيبرانية.**
- **تحليل التهديدات السيبرانية.**
- **تقييم الثغرات الأمنية.**
- **تحديد المخاطر السيبرانية.**
- **تحديد الإجراءات الوقائية والتصحيحية.**
- **تطبيق نظام إدارة المخاطر السيبرانية.**

إدارة المخاطر السيبرانية

إدارة المخاطر السيبرانية هي عملية منهجية تهدف إلى تحديد وتقييم ومراقبة المخاطر المتعلقة بالأمن السيبراني، وتطوير استراتيجيات لتقليل أو إدارة هذه المخاطر. تشمل هذه العملية مجموعة من الأنشطة والسياسات التي تساعد المؤسسات على حماية أصولها الرقمية وضمان استمرارية الأعمال.



1. تحديد المخاطر

تحديد الأصول السيبرانية: تصنيف وتوثيق الأصول الرقمية التي تحتاج إلى الحماية، مثل البيانات، الأنظمة، والبنية التحتية.

تحديد التهديدات ونقاط الضعف: تحديد التهديدات المحتملة ونقاط الضعف في الأنظمة التي قد تستغلها هذه التهديدات.

2. تقييم المخاطر

تقييم الاحتمالية والتأثير: تقدير احتمالية وقوع المخاطر وتأثيرها المحتمل على الأصول السيبرانية. يستخدم التقييم الكمي والنوعي لتحديد مدى خطورة كل خطر.

تحليل الأثر: دراسة تأثير المخاطر على العمليات، البيانات، والسمعة، وكذلك التأثير المالي المحتمل.

3. استراتيجيات التخفيف

تنفيذ الإجراءات الوقائية: وضع تدابير وإجراءات لحماية الأنظمة والبيانات، مثل التشفير، الجدران النارية، وأنظمة الكشف عن التسلل.

تطوير سياسات الأمان: إنشاء سياسات وإجراءات أمان واضحة لضمان التعامل مع المخاطر بفعالية.

التدريب والتوعية: تدريب الموظفين على كيفية التعامل مع المخاطر والأمان السيبراني لتحسين الوعي وتقليل الأخطاء البشرية.

4. الاستجابة للحوادث

تطوير خطط الاستجابة: إعداد خطط واستراتيجيات للاستجابة السريعة للحوادث الأمنية والتقليل من تأثيرها.

إجراءات الطوارئ: وضع إجراءات للطوارئ لاستعادة الأنظمة والبيانات في حالة وقوع حادث أمني.

5. المراقبة والمراجعة

مراقبة الأنظمة: استخدام أدوات لرصد الأنظمة والشبكات لاكتشاف الأنشطة غير الطبيعية أو الخروقات الأمنية في وقت مبكر.

مراجعة دورية: إجراء مراجعات دورية للسياسات والإجراءات لضمان فعاليتها وتحديثها بناءً على التهديدات الجديدة والتغيرات في البيئة.

6. التحسين المستمر

تقييم الأداء: قياس فعالية استراتيجيات إدارة المخاطر وتحديد المجالات التي تحتاج إلى تحسين.

تحديث الاستراتيجيات: تحديث استراتيجيات إدارة المخاطر بناءً على نتائج التقييم والتغيرات في البيئة السيبرانية.

7 .الامتثال والتشريعات

الامتثال للمعايير: التأكد من التزام المؤسسة بالمعايير واللوائح الأمنية مثلGDPR ، HIPAA، أو.ISO/IEC 27001

التقارير والتوثيق: إعداد التقارير اللازمة وتوثيق جميع الأنشطة والإجراءات المرتبطة بإدارة المخاطر السيبرانية.

تحديد الأصول السيبرانية

تحديد الأصول السيبرانية هو عملية أساسية في إدارة المخاطر السيبرانية، تهدف إلى تحديد وتصنيف الأصول الرقمية التي تحتاج إلى حماية. يتضمن ذلك تحديد كل من الأصول المادية وغير المادية التي تشكل جزءًا من البيئة التكنولوجية للمؤسسة.

خطوات تحديد الأصول السيبرانية

1. إعداد قائمة بالأصول:

جمع المعلومات: بدءًا من جمع معلومات حول جميع الأصول التقنية التي تستخدمها المؤسسة، بما في ذلك الأجهزة، البرمجيات، البيانات، والشبكات.

التفاصيل الفنية: توثيق التفاصيل الفنية لكل أصل، مثل نوع الجهاز، نظام التشغيل، التطبيقات المستخدمة، ومواقع التخزين.

2. تصنيف الأصول:

الأصول المادية: تشمل الأجهزة مثل الخوادم، أجهزة الكمبيوتر، أجهزة التوجيه، والأنظمة الأخرى.

الأصول الرقمية: تتضمن البرمجيات، قواعد البيانات، الملفات، والمستندات.

الأصول الشبكية: تشمل الشبكات، بروتوكولات الاتصال، والبنية التحتية للشبكات.

الأصول البشرية: تشمل الأشخاص الذين لديهم وصول إلى الأصول والتقنيات المعرفية الخاصة بهم.

3. تقييم القيمة:

تحديد أهمية الأصول: تقييم قيمة كل أصل بناءً على دوره وأهميته في دعم عمليات الأعمال. يشمل ذلك الأثر الذي قد يحدث إذا فقدت أو تعرضت للضرر.

تقدير التأثير: تحديد تأثير فقدان أو تعرض الأصول للخطر على العمل والعمليات والسمعة.

4. تحديد مواقع الأصول:

تحديد المواقع الجغرافية: توثيق مواقع الأصول في الأماكن المادية أو الافتراضية. يشمل ذلك مواقع الخوادم، مراكز البيانات، وأماكن تخزين البيانات.

التوثيق الرقمي: توثيق مواقع الأصول الرقمية في البيئة السحابية أو على الشبكات المحلية.

5. تحديث وتعديل:

مراجعة دورية: إجراء مراجعات دورية لتحديث قائمة الأصول والتأكد من أنها تعكس التغيرات في البيئة التكنولوجية.

إضافة وإزالة الأصول: تحديث القائمة بإضافة أصول جديدة وإزالة الأصول التي لم تعد قيد الاستخدام.

أهمية تحديد الأصول السيبرانية

توفير الحماية الفعالة: يساعد في فهم ما يجب حمايته، مما يتيح تطبيق تدابير أمان ملائمة لحماية الأصول ذات القيمة.

تقدير المخاطر: يوفر قاعدة أساسية لتقييم المخاطر من خلال تحديد الأصول التي قد تكون مستهدفة أو معرضة للخطر.

تحسين الاستجابة: يعزز القدرة على الاستجابة للحوادث من خلال معرفة مواقع الأصول وأهميتها.

تحديد الأصول السيبرانية هو خطوة أولى حيوية في عملية إدارة المخاطر السيبرانية، حيث يوفر الأساس لفهم كيفية حماية الأصول الرقمية والفيزيائية للمؤسسة من التهديدات المحتملة.

تحليل التهديدات السيبرانية

تحليل التهديدات السيبرانية هو عملية تقييم وتحديد التهديدات المحتملة التي قد تؤثر على الأصول السيبرانية. يهدف هذا التحليل إلى فهم الأنواع المختلفة من التهديدات، كيفية عملها، وتأثيرها المحتمل على الأنظمة والشبكات والبيانات.

خطوات تحليل التهديدات السيبرانية

1. تحديد الأنواع الرئيسية للتهديدات

الهجمات الخارجية: مثل الهجمات من قراصنة الإنترنت، برمجيات الفدية، وهجمات الحجب (DDoS).

الهجمات الداخلية: تتضمن تهديدات من داخل المؤسسة مثل التصرفات غير المصرح بها من قبل الموظفين أو المتعهدين.

التجسس الصناعي: الحصول على معلومات حساسة من المنافسين بطريقة غير قانونية.

البرامج الضارة: تشمل الفيروسات، والديدان، والبرمجيات الخبيثة الأخرى.

2. تقييم مصدر التهديدات

مهاجمون محتملون: تحديد الأطراف التي قد تكون مسؤولة عن التهديدات، مثل القراصنة، الأعداء، أو الجهات الداخلية غير المصرح بها.

التقنيات والأساليب: دراسة الأساليب والتقنيات التي قد يستخدمها المهاجمون، مثل أدوات البرمجيات الخبيثة أو أساليب الهندسة الاجتماعية.

3. تحديد دوافع التهديدات

أهداف الهجوم: فهم الأهداف التي قد يسعى المهاجمون لتحقيقها، مثل سرقة البيانات، تعطيل الخدمات، أو تحقيق مكاسب مالية.

النية والقدرة: تقييم النية والقدرة لدى المهاجمين، بما في ذلك مدى خبرتهم والتقنيات التي يمكن أن يستخدموها.

4. تحليل تأثير التهديدات:

تقدير التأثير المحتمل: تقدير كيف يمكن أن تؤثر التهديدات على الأصول السيبرانية، بما في ذلك التأثير المالي، الأضرار التشغيلية، وتأثيرات السمعة.

تأثير على الأنظمة: دراسة كيفية تأثير التهديدات على النظام الكلي، بما في ذلك التأثير على الأداء والأمان.

5. تطوير استراتيجيات التصدي:

تحديد الإجراءات الوقائية: وضع تدابير أمان للتقليل من احتمالية تعرض الأنظمة للتهديدات، مثل تحديث البرمجيات، وتعزيز الرقابة.

إجراءات الاستجابة: تطوير استراتيجيات للتعامل مع التهديدات عندما تحدث، بما في ذلك الاستجابة للحوادث واستعادة البيانات.

6. مراجعة وتحسين:

مراجعة مستمرة: إجراء مراجعات دورية لتحليل التهديدات لتحديثه بناءً على التهديدات الجديدة والتغيرات في البيئة الأمنية.

تحسين الإجراءات: تعديل استراتيجيات التصدي بناءً على الدروس المستفادة من الحوادث والتحليلات السابقة.

أهمية تحليل التهديدات السيبرانية

تحديد المخاطر المحتملة: يساعد في فهم التهديدات التي قد تواجه الأصول السيبرانية، مما يمكن من تطوير استراتيجيات حماية فعالة.

تحسين الاستجابة: يوفر معلومات حول كيفية التعامل مع التهديدات، مما يعزز القدرة على الاستجابة السريعة.

توفير الحماية: يمكن من تنفيذ تدابير أمان وقائية للتقليل من احتمالية وقوع هجمات.

تقييم الثغرات الأمنية.

تقييم الثغرات الأمنية هو عملية منهجية تهدف إلى تحديد نقاط الضعف في الأنظمة والشبكات التي قد يستغلها المهاجمون. يتضمن هذا التقييم فحص الأنظمة والبنية التحتية لتحديد الثغرات التي قد تؤدي إلى اختراقات أمنية أو تهديدات.

خطوات تقييم الثغرات الأمنية:

1. جمع المعلومات:

تحديد الأصول: جمع معلومات حول الأصول التي سيتم تقييمها، بما في ذلك الخوادم، التطبيقات، الأجهزة، والشبكات.

فحص التكوينات: مراجعة إعدادات التكوين للأجهزة والبرمجيات للتحقق من صحتها وملاءمتها.

2. إجراء الفحص التقني:

استخدام أدوات فحص الثغرات: تطبيق أدوات مخصصة لفحص الثغرات الأمنية، مثل الماسحات الأمنية (Vulnerability Scanners) التي تبحث عن نقاط الضعف المعروفة.

التحليل اليدوي: إجراء اختبارات يدوية مثل اختبار الاختراق (Penetration Testing) لتحليل الثغرات بشكل أعمق وتحديد كيفية استغلالها.

3. تقييم الثغرات:

تصنيف الثغرات: تصنيف الثغرات بناءً على شدتها، ونوعها، وتأثيرها المحتمل. يمكن استخدام نظام تصنيف مثل CVSS (Common Vulnerability Scoring System)لتحديد مستوى الخطر.

تحليل الأثر: تقدير التأثير المحتمل لكل ثغرة على الأصول والأنظمة، بما في ذلك التأثير المالي، التشغيلي، والأمني.

4. تحديد الأولويات:

تحديد الأهمية: تحديد أي من الثغرات يتطلب معالجة فورية بناءً على حجم التأثير واحتمالية الاستغلال.

إعداد قائمة بالثغرات: إنشاء قائمة منظمة بالثغرات التي تحتاج إلى تصحيح، مع ترتيبها حسب الأولوية.

5. تطوير استراتيجيات التصحيح:

توصيات التصحيح: وضع توصيات لإصلاح الثغرات، مثل تطبيق التحديثات الأمنية، تغيير إعدادات التكوين، أو تعديل البرمجيات.

تنفيذ الإصلاحات: تنفيذ إجراءات التصحيح وإعادة التحقق لضمان حل الثغرات بشكل فعال.

6. مراجعة وتحسين:

تحديث التقييمات: إجراء مراجعات دورية لتحديث تقييمات الثغرات بناءً على التغييرات في الأنظمة والتكنولوجيا.

تحسين العملية: تحسين عملية تقييم الثغرات بناءً على الدروس المستفادة من عمليات التقييم السابقة.

أهمية تقييم الثغرات الأمنية

حماية الأنظمة: يساعد في تحديد نقاط الضعف التي قد يستغلها المهاجمون، مما يتيح تعزيز الأمان وحماية الأنظمة.

تقليل المخاطر: يوفر معلومات تساعد في تقليل المخاطر الأمنية من خلال معالجة الثغرات المهمة.

تحسين الأمان: يعزز من استراتيجية الأمان من خلال تقديم رؤى حول كيفية تحسين الأمان وإغلاق الثغرات المحتملة.

تحديد المخاطر السيبرانية

تحديد المخاطر السيبرانية هو عملية تهدف إلى اكتشاف وتوثيق المخاطر المحتملة التي قد تؤثر على الأصول السيبرانية للمؤسسة. يتضمن هذا التحليل فحص التهديدات والثغرات لتقدير المخاطر التي قد تنشأ وكيفية تأثيرها على الأنظمة والبيانات.

خطوات تحديد المخاطر السيبرانية:

1. جمع المعلومات الأساسية:

تحديد الأصول: توثيق جميع الأصول السيبرانية المهمة، بما في ذلك البيانات، التطبيقات، الأنظمة، والأجهزة.

تحديد التهديدات: تحديد أنواع التهديدات المحتملة مثل الهجمات السيبرانية، البرمجيات الخبيثة، أو الأخطاء البشرية.

2. تحديد نقاط الضعف:

تحليل الثغرات: استخدام نتائج تقييم الثغرات الأمنية لتحديد النقاط الضعيفة في الأنظمة التي قد تؤدي إلى مخاطر.

مراجعة التكوينات: تقييم إعدادات الأمان والتكوينات للتأكد من أنها لا تحتوي على ثغرات قد تؤدي إلى المخاطر.

3. تقييم التهديدات:

فهم التهديدات المحتملة: تحديد كيفية عمل التهديدات وكيفية تأثيرها على الأصول. يشمل ذلك التهديدات الداخلية والخارجية.

تحليل الأساليب المستخدمة: دراسة الأساليب والتقنيات التي قد يستخدمها المهاجمون، مثل الهجمات المعروفة أو تقنيات جديدة.

4. تحديد المخاطر:

تقدير الاحتمالية والتأثير: تقدير احتمالية حدوث كل خطر وتأثيره المحتمل على الأصول. يشمل ذلك تقييم الأثر المالي، التشغيلي، والأمني.

تصنيف المخاطر: تصنيف المخاطر بناءً على شدتها وأولويتها لتحديد أي منها يتطلب اهتماماً فوريًا.

5. تطوير استراتيجيات التعامل مع المخاطر:

تحديد الإجراءات الوقائية: وضع تدابير وإجراءات للحد من المخاطر، مثل تطبيق سياسات أمان قوية وتدريب الموظفين.

تطوير خطط الاستجابة: إعداد خطط للتعامل مع المخاطر إذا حدثت، بما في ذلك إجراءات الاستجابة للطوارئ وإعادة بناء الأنظمة.

6. مراجعة وتحسين:

مراجعة دورية: إجراء مراجعات دورية لتحديث قائمة المخاطر بناءً على التغيرات في البيئة السيبرانية والتكنولوجيا.

تحسين الإجراءات: تحسين استراتيجيات تحديد وإدارة المخاطر بناءً على النتائج والتجارب السابقة.

تحديد الإجراءات الوقائية والتصحيحية

تحديد الإجراءات الوقائية والتصحيحية هو جزء أساسي من إدارة المخاطر السيبرانية، حيث يهدف إلى وضع استراتيجيات لحماية الأنظمة والبيانات من التهديدات المحتملة، وتقديم حلول لمعالجة المشكلات التي قد تظهر. تشمل الإجراءات الوقائية والتصحيحية تدابير استباقية لتجنب المخاطر، وإجراءات لمعالجة المشكلات بعد حدوثها.

الإجراءات الوقائية؟

1. تطبيق سياسات أمان قوية:

إنشاء السياسات: وضع سياسات وإجراءات أمان واضحة لتحديد كيفية حماية الأصول الرقمية.

التحديث الدوري: تحديث السياسات بشكل دوري للتكيف مع التهديدات والتغيرات في البيئة السيبرانية.

2. تدريب الموظفين:

تدريب الأمان: تقديم دورات تدريبية دورية للموظفين حول الأمان السيبراني، تشمل الوعي بالتهديدات وأفضل الممارسات.

محاكاة الهجمات: إجراء تدريبات ومحاكاة للهجمات لتعزيز القدرة على التعرف على التهديدات والتعامل معها.

3. تحديث البرمجيات:

تصحيح الثغرات: تطبيق التحديثات والتصحيحات الأمنية للبرمجيات والنظم بشكل منتظم لتصحيح الثغرات الأمنية.

إدارة التصحيحات: استخدام أدوات إدارة التصحيحات لضمان تطبيق التحديثات بشكل فعال.

4. تطبيق تدابير الأمان التقنية:

تشغيل الجدران النارية: استخدام جدران نارية لحماية الشبكات من الوصول غير المصرح به.

تشفير البيانات: تطبيق تقنيات التشفير لحماية البيانات أثناء النقل والتخزين.

5. إجراء تقييمات أمنية دورية:

فحص الثغرات: إجراء فحوصات دورية للثغرات لتحديد نقاط الضعف وإصلاحها.

اختبارات الاختراق: إجراء اختبارات اختراق دورية لتقييم فعالية الإجراءات الأمنية.

الإجراءات التصحيحية؟

1. استجابة للحوادث:

تطوير خطط الاستجابة: وضع خطط للتعامل مع الحوادث الأمنية تشمل الإجراءات اللازمة للتصدي ومعالجة الحوادث.

تكوين فريق الاستجابة: إنشاء فريق متخصص للاستجابة السريعة للحوادث وتحليل أسبابها.

2. تحليل الحوادث:

تحديد الأسباب الجذرية: تحليل الحوادث لتحديد الأسباب الجذرية لها وتقديم حلول للتعامل معها.

التوثيق والتقارير: توثيق جميع الحوادث الأمنية وإعداد تقارير تفصيلية حول كيفية التعامل معها.

3. إعادة بناء الأنظمة:

استعادة البيانات: استعادة البيانات والنظم من النسخ الاحتياطية في حالة تعرضها للفقد أو التلف.

إصلاح الأنظمة: تطبيق إصلاحات على الأنظمة المتأثرة لمعالجة الثغرات التي استغلت.

4. تحسين الإجراءات:

مراجعة وتحديث السياسات: تعديل السياسات والإجراءات الأمنية بناءً على تحليل الحوادث والدروس المستفادة.

تحسين الاستراتيجيات: تحديث استراتيجيات الأمان بناءً على التجارب والخبرات المكتسبة من الحوادث.

أهمية تحديد الإجراءات الوقائية والتصحيحية؟

تقليل المخاطر: يساعد في تقليل احتمالية حدوث المخاطر من خلال اتخاذ تدابير استباقية.

تحسين الاستجابة: يعزز القدرة على التعامل مع الحوادث بشكل فعّال ويقلل من تأثيرها.

حماية الأصول: يساهم في حماية الأصول الرقمية من التهديدات وتعزيز أمان النظام.

تطبيق نظام إدارة المخاطر السيبرانية

تطبيق نظام إدارة المخاطر السيبرانية هو عملية متكاملة تهدف إلى تحديد، تقييم، وإدارة المخاطر السيبرانية لضمان حماية الأصول الرقمية والتقليل من الأثر المحتمل لأي تهديدات. يشمل ذلك مجموعة من الأنشطة والسياسات التي تساهم في تعزيز الأمان السيبراني للمؤسسة.

خطوات تطبيق نظام إدارة المخاطر السيبرانية

1. تأسيس إطار عمل:

تطوير سياسات وإجراءات: وضع سياسات وإجراءات واضحة لإدارة المخاطر السيبرانية. يشمل ذلك تحديد الأدوار والمسؤوليات، وتطوير استراتيجيات إدارة المخاطر.

اختيار إطار عمل: استخدام إطار عمل معترف به مثل NIST Cybersecurity Framework، ISO/IEC 27001، أو COBIT لتوجيه عملية إدارة المخاطر.

2. تحديد وتقييم المخاطر:

تحديد الأصول السيبرانية: تصنيف الأصول السيبرانية وتحديد قيمتها وأهميتها.

تحليل التهديدات والثغرات: تحليل التهديدات المحتملة ونقاط الضعف لتحديد المخاطر.

تقييم المخاطر: تقدير احتمالية حدوث المخاطر وتأثيرها المحتمل على الأصول.

3. تطوير استراتيجيات التخفيف:

تحديد التدابير الوقائية: وضع إجراءات وتدابير لتقليل احتمالية وقوع المخاطر، مثل تعزيز الأمان، التدريب، والتحديثات الأمنية.

تطوير خطط الاستجابة: إعداد خطط لاستجابة فعالة للحوادث الأمنية، بما في ذلك كيفية التعامل مع الحوادث واستعادة الأنظمة.

4. تنفيذ النظام:

تنفيذ الإجراءات: تطبيق السياسات والإجراءات المعتمدة على الأنظمة والعمليات اليومية.

توفير الموارد: تخصيص الموارد اللازمة، بما في ذلك الأدوات والتقنيات والفريق البشري، لدعم عملية إدارة المخاطر.

5. مراقبة ومراجعة:

مراقبة الأداء: متابعة أداء نظام إدارة المخاطر وتقييم فعاليته من خلال استخدام أدوات المراقبة والتحليل.

مراجعة دورية: إجراء مراجعات دورية للسياسات والإجراءات لتحديثها بناءً على التغيرات في البيئة السيبرانية والمخاطر.

6. تحسين مستمر:

تقييم التحسينات: جمع التغذية الراجعة من عملية إدارة المخاطر وتحديد المجالات التي تحتاج إلى تحسين.

تحديث السياسات: تعديل السياسات والإجراءات بناءً على نتائج المراجعات والتقييمات.

أهمية تطبيق نظام إدارة المخاطر السيبرانية

حماية الأصول: يعزز حماية الأصول الرقمية من التهديدات المحتملة من خلال تحديد وتخفيف المخاطر.

تحسين الاستجابة: يوفر استراتيجيات فعالة للتعامل مع الحوادث الأمنية وتقديم استجابة سريعة.

تحقيق الامتثال: يساعد في ضمان الالتزام بالمعايير والتشريعات الأمنية ذات الصلة.

تعزيز الأمان: يساهم في تحسين مستوى الأمان السيبراني للمؤسسة من خلال إدارة المخاطر بشكل فعال.

الوحدة الخامسة

- تطبيقات إدارة المخاطر السيبرانية.
- أدوات تحليل المخاطر.
- أدوات تصميم الأمن السيبراني.
- أدوات إدارة المخاطر السيبرانية.
- أدوات تنفيذ الأمن السيبراني.
- أدوات تقييم المخاطر السيبرانية.

تطبيقات إدارة المخاطر السيبرانية

تطبيقات إدارة المخاطر السيبرانية هي الأدوات والحلول التي تُستخدم لتسهيل وتحسين إدارة المخاطر السيبرانية في المؤسسات. تشمل هذه التطبيقات مجموعة متنوعة من البرامج والخدمات التي تساعد في تحديد، تقييم، وإدارة المخاطر السيبرانية بشكل فعال.

أنواع التطبيقات وأمثلتها

1. أنظمة إدارة المعلومات الأمنية:(SIEM)

الوظيفة: جمع وتحليل البيانات من الأنظمة والشبكات لتحديد الأنشطة غير الطبيعية والتهديدات المحتملة.

المثال: Splunk, IBM QRadar.

2. أدوات فحص الثغرات:

الوظيفة: فحص الأنظمة والتطبيقات للكشف عن الثغرات الأمنية ونقاط الضعف.

المثال: Nessus, Qualys.

3. برامج إدارة الأمان:

الوظيفة: إدارة السياسات الأمنية، تكوين الأمان، والتعامل مع الحوادث الأمنية.

المثال: Cisco SecureX, Palo Alto Networks Cortex.

4. حلول تشفير البيانات:

الوظيفة: حماية البيانات الحساسة من الوصول غير المصرح به من خلال التشفير.

المثال: Vormetric, Symantec Encryption.

5. أدوات إدارة الهوية والوصول:(IAM)

الوظيفة: التحكم في الوصول إلى الأنظمة والبيانات بناءً على هوية المستخدمين.

المثال: Okta, Microsoft Azure Active Directory.

6. برامج الاستجابة للحوادث:

الوظيفة: إدارة والتحقيق في الحوادث الأمنية وتقديم استجابات سريعة وفعالة.

المثال: CrowdStrike, FireEye.

7. أنظمة إدارة التهديدات والضعف:(TVM)

الوظيفة: تقييم وإدارة التهديدات والثغرات لتحسين الأمان السيبراني.

المثال: Rapid7 InsightVM, Tenable.io :

8. أدوات تحليل البرمجيات الخبيثة:

الوظيفة: تحليل البرمجيات الخبيثة لتحديد خصائصها وأثرها على النظام.

المثال: Cuckoo Sandbox, VirusTotal :

9. برامج النسخ الاحتياطي واستعادة البيانات:

الوظيفة: إنشاء نسخ احتياطية من البيانات وإعادة استعادتها في حالة حدوث فقد أو تلف.

المثال: Acronis, Veeam :

10. حلول إدارة الامتثال:

الوظيفة: ضمان الالتزام بالمعايير والتشريعات الأمنية مثل GDPR و HIPAA.

المثال: OneTrust, Qualys Compliance :

أهمية تطبيقات إدارة المخاطر السيبرانية

تحسين الأمان: تساهم في تعزيز الأمان من خلال تقديم أدوات متقدمة لتحليل التهديدات وإدارة الحماية.

زيادة الكفاءة: توفر حلولاً فعالة لإدارة المخاطر، مما يسهل عملية الكشف والاستجابة للحوادث.

توفير الوقت والموارد: تقلل من الحاجة للإجراءات اليدوية وتساهم في تحسين عمليات الأمان بشكل عام.

تحقيق الامتثال: تساعد في ضمان الالتزام بالمعايير الأمنية والتشريعات ذات الصلة.

أدوات تحليل المخاطر:

أدوات تحليل المخاطر هي برامج وتقنيات تستخدم لتقييم المخاطر السيبرانية وتقديم رؤى حول كيفية التعامل معها. تساعد هذه الأدوات في تحديد وتقييم التهديدات والثغرات وتقديم استراتيجيات لتقليل المخاطر وتحسين الأمان.

أنواع أدوات تحليل المخاطر:

أدوات فحص الثغرات الأمنية:

الوظيفة: تبحث عن الثغرات في الأنظمة والتطبيقات وتقدم تقارير حول نقاط الضعف.

المثال.Nessus, Qualys, OpenVAS :

أدوات تقييم المخاطر السيبرانية:

الوظيفة: تقييم المخاطر بناءً على تحليلات التهديدات والثغرات وتأثيرها المحتمل.

المثال.(RiskWatch, FAIR (Factor Analysis of Information Risk :

أنظمة إدارة المعلومات الأمنية(SIEM)

الوظيفة: تجمع وتحلل بيانات الأمان من مختلف المصادر لاكتشاف الأنشطة غير العادية والتهديدات.

المثال.Splunk, IBM QRadar, LogRhythm :

أدوات تحليل البرمجيات الخبيثة:

الوظيفة: تحليل البرمجيات الخبيثة لتحديد خصائصها وأثرها على الأنظمة.

المثال.Cuckoo Sandbox, VirusTotal, Hybrid Analysis :

أدوات إدارة الثغرات:(Vulnerability Management)

الوظيفة: إدارة الثغرات الأمنية من خلال تتبع نقاط الضعف والتوصية بالإصلاحات.

المثال.Rapid7 InsightVM, Tenable.io :

أدوات تحليل التهديدات:

الوظيفة: تحليل التهديدات المحتملة وتقديم معلومات حول كيفية تنفيذ الهجمات وأساليب الحماية.

المثال.ThreatConnect, Anomali :

أدوات التقييم النفسي للسلوكيات الأمنية:

الوظيفة: تقييم سلوكيات المستخدمين للكشف عن الأنشطة المشبوهة أو غير المعتادة.

المثال.Cylance, Darktrace :

أدوات إدارة الامتثال:

الوظيفة: ضمان التزام المؤسسات بالمعايير والتشريعات الأمنية من خلال تحليل المخاطر وتحسين الأمان.

المثال.OneTrust, Qualys Compliance :

أدوات إدارة المخاطر المتعلقة بالشبكات:

الوظيفة: تقييم ومراقبة المخاطر المتعلقة بالشبكات وتقديم رؤى حول كيفية تحسين الأمان.

المثال.Nmap, SolarWinds Network Performance Monitor :

أدوات التحليل العكسي:

الوظيفة: تحليل الأكواد المصدرة والبرمجيات الخبيثة لتحديد كيفية عملها وأثرها.

المثال.IDA Pro, Ghidra :

أهمية استخدام أدوات تحليل المخاطر

تحسين الأمان: تساعد في اكتشاف وتحديد الثغرات والتهديدات، مما يعزز الأمان السيبراني.

توفير معلومات دقيقة: توفر رؤى دقيقة حول المخاطر، مما يسهل اتخاذ قرارات مبنية على البيانات.

إدارة المخاطر بفعالية: تساعد في تحديد المخاطر وإدارتها بشكل منهجي، مما يعزز حماية الأصول.

أدوات تصميم الأمن السيبراني

أدوات تصميم الأمن السيبراني هي برامج وتقنيات تستخدم لتطوير وتصميم أنظمة الأمان وحمايتها من التهديدات السيبرانية. تساعد هذه الأدوات في بناء بنية أمان قوية ومستدامة من خلال توفير حلول لتصميم وتنفيذ تدابير الحماية.

أنواع أدوات تصميم الأمن السيبراني:

أدوات تحليل التهديدات والضعف:

الوظيفة: تقييم التهديدات المحتملة ونقاط الضعف في الأنظمة لتصميم تدابير الأمان المناسبة.

المثال.ThreatModeler, Microsoft Threat Modeling Tool :

أدوات إدارة التكوين والأمان.

الوظيفة: إدارة وضبط إعدادات الأمان والتكوين لضمان توافق الأنظمة مع سياسات الأمان.

المثال: Chef InSpec, Puppet, Ansible.

أدوات تحليل وتصميم الشبكات:

الوظيفة: تصميم وتحليل بنية الشبكات لتحديد وإدماج تدابير الأمان المناسبة.

المثال: Cisco Packet Tracer, GNS3.

أدوات تشفير البيانات

الوظيفة: تصميم وتنفيذ حلول لتشفير البيانات لضمان حمايتها من الوصول غير المصرح به.

المثال: Vormetric, Thales e-Security.

أدوات إدارة الهوية والوصول(IAM)

الوظيفة: تصميم حلول لإدارة هوية المستخدمين والوصول إلى الأنظمة والبيانات.

المثال: Okta, Microsoft Azure Active Directory.

أدوات تصميم وإدارة الجدران النارية:

الوظيفة: تصميم وتنفيذ جدران نارية لحماية الشبكات من الهجمات والتهديدات.

المثال: Palo Alto Networks, Fortinet.

أدوات تصميم حلول الأمان المتكاملة

الوظيفة: توفير حلول متكاملة للأمان تشمل جميع جوانب النظام، مثل الحماية من البرمجيات الخبيثة، والتشفير، وإدارة الأمان.

المثال: IBM Security QRadar, McAfee Total Protection.

أدوات اختبار الأمان:

الوظيفة: اختبار الأنظمة والتطبيقات لاكتشاف الثغرات والتحقق من فعالية تدابير الأمان.

المثال: Burp Suite, OWASP ZAP.

أدوات تحليل البرمجيات:

الوظيفة: تحليل الكود المصدري والبرمجيات لاكتشاف الثغرات الأمنية وإصلاحها.

المثال.SonarQube, Veracode :

أدوات إدارة الامتثال للأمان:

الوظيفة: تصميم حلول لضمان الالتزام بالمعايير والتشريعات الأمنية من خلال مراقبة وتقييم الأمان.

المثال.Qualys Compliance, Rapid7

أدوات إدارة المخاطر السيبرانية:

أدوات إدارة المخاطر السيبرانية هي برامج وتطبيقات تستخدم لتخطيط وتنفيذ ومراقبة استراتيجيات إدارة المخاطر السيبرانية. تساعد هذه الأدوات المؤسسات في تحديد وتقييم وإدارة المخاطر السيبرانية بشكل فعال.

أنواع أدوات إدارة المخاطر السيبرانية:

أنظمة إدارة المخاطر:(Risk Management Systems)

الوظيفة: توفر إطار عمل متكامل لإدارة المخاطر، بما في ذلك تحديد وتقييم وتخفيف المخاطر.

المثال.RSA Archer, MetricStream :

أدوات تقييم المخاطر السيبرانية:

الوظيفة: تقييم المخاطر السيبرانية بناءً على تحليل التهديدات والثغرات.

المثال.(RiskWatch, FAIR (Factor Analysis of Information Risk :

أدوات تحليل تأثير الأعمال:(Business Impact Analysis)

الوظيفة: تحليل تأثير المخاطر على العمليات التجارية لتحديد الأولويات في إدارة المخاطر.

المثال.Fusion Risk Management, Continuity Logic :

أدوات إدارة الحوادث:(Incident Management Tools)

الوظيفة: إدارة الحوادث الأمنية، من الكشف إلى الاستجابة والتعافي.

المثال.ServiceNow Security Operations, PagerDuty :

أدوات إدارة الثغرات الأمنية:

الوظيفة: تتبع وإدارة الثغرات الأمنية في الأنظمة والتطبيقات.

المثال: Tenable.io, Qualys Vulnerability Management.

أدوات إدارة الامتثال:

الوظيفة: ضمان الالتزام بالمعايير والتشريعات الأمنية من خلال تتبع ومراقبة التوافق.

المثال: OneTrust, Qualys Compliance.

أدوات تحليل التهديدات:(Threat Intelligence Tools)

الوظيفة: جمع وتحليل معلومات التهديدات لمساعدة في فهم وتحليل المخاطر.

المثال: ThreatConnect, Anomali.

أدوات إدارة السياسات الأمنية:

الوظيفة: إدارة وتحديث السياسات الأمنية ومراقبة تنفيذها.

المثال: Tufin, Skybox Security.

أدوات إدارة أمان الشبكة:

الوظيفة: إدارة أمان الشبكة بما في ذلك جدران النيران وأنظمة الكشف عن التسلل.

المثال: Cisco Firepower, Palo Alto Networks.

أدوات تحليل الأمان وإدارة التكوين:

الوظيفة: تحليل الأمان وضبط التكوينات لضمان حماية فعالة.

المثال: Chef InSpec, Puppet Enterprise.

أدوات تنفيذ الأمن السيبراني

أدوات تنفيذ الأمن السيبراني هي البرامج والتقنيات التي تُستخدم لتطبيق ومراقبة سياسات وإجراءات الأمان في الأنظمة والشبكات. تركز هذه الأدوات على تنفيذ تدابير الحماية بشكل فعال وتوفير الحماية ضد التهديدات السيبرانية.

أنواع أدوات تنفيذ الأمن السيبراني:

جدران الحماية:(Firewalls)

الوظيفة: تحكم حركة البيانات بين الشبكات وتمنع الوصول غير المصرح به.

المثال: Palo Alto Networks, Cisco ASA.

أنظمة الكشف والوقاية من التسلل:(IDS/IPS)

الوظيفة: مراقبة الشبكة واكتشاف ومنع الأنشطة الضارة.

المثال: Snort, Suricata.

أدوات مكافحة البرمجيات الخبيثة:(Antivirus/Malware Protection)

الوظيفة: الكشف عن البرمجيات الخبيثة وإزالتها من الأنظمة.

المثال: Symantec, Malwarebytes.

أدوات تشفير البيانات:

الوظيفة: تشفير البيانات أثناء النقل والتخزين لحمايتها من الوصول غير المصرح به.

المثال: Vormetric, Thales e-Security.

أدوات إدارة الهوية والوصول:(IAM)

الوظيفة: إدارة هويات المستخدمين وتحديد مستويات الوصول إلى الأنظمة والبيانات.

المثال: Okta, Microsoft Azure Active Directory.

أنظمة إدارة التكوين:(Configuration Management)

الوظيفة: إدارة وضبط التكوينات الأمنية لأنظمة الحوسبة والتطبيقات.

المثال: Chef, Puppet, Ansible.

أدوات نسخ البيانات الاحتياطي والتعافي:

الوظيفة: إجراء نسخ احتياطي للبيانات وإعادة استعادتها في حالة فقدانها أو تلفها.

المثال: Veeam, Acronis.

أدوات إدارة الأمن السحابي:

الوظيفة: تأمين البيئات السحابية وتوفير حلول للحماية والتشفير في السحابة.

المثال: Cloudflare, AWS Security Hub.

أدوات تحليل الأمان وإدارة الحوادث:

الوظيفة: تحليل الحوادث الأمنية وتوفير أدوات لإدارة الاستجابة للحوادث.

المثال: ServiceNow Security Operations, Splunk.

أدوات إدارة السجلات:(Logging and Monitoring)

الوظيفة: جمع وتحليل سجلات النظام لمراقبة الأنشطة والكشف عن الأنشطة المشبوهة.

المثال: Splunk, ELK Stack (Elasticsearch, Logstash, Kibana).

أدوات تقييم المخاطر السيبرانية:

أدوات تقييم المخاطر السيبرانية هي برامج وتقنيات تستخدم لتحديد وتحليل وتقييم المخاطر المحتملة التي تهدد الأنظمة والبيانات في مؤسسة ما. تهدف هذه الأدوات إلى تقديم رؤى حول المخاطر وتقييم تأثيرها واحتمالية حدوثها.

أنواع أدوات تقييم المخاطر السيبرانية:

أدوات تقييم المخاطر الشاملة:

الوظيفة: تقدم إطار عمل متكامل لتقييم المخاطر بناءً على تحليل التهديدات والثغرات.

المثال: RiskWatch, FAIR (Factor Analysis of Information Risk).

أدوات تحليل الثغرات:

الوظيفة: فحص الأنظمة والتطبيقات للكشف عن الثغرات الأمنية وتقديم تقارير مفصلة عن نقاط الضعف.

المثال: Nessus, Qualys, OpenVAS.

أدوات تحليل التأثيرات:(Business Impact Analysis)

الوظيفة: تقييم تأثير المخاطر المحتملة على العمليات التجارية لتحديد الأولويات في إدارة المخاطر.

المثال: Fusion Risk Management, Continuity Logic.

أدوات إدارة التهديدات:

الوظيفة: تحليل وتقييم التهديدات السيبرانية وتقديم معلومات حول كيفية تنفيذ الهجمات وأساليب الحماية.

المثال: ThreatConnect, Anomali.

أدوات تحليل المخاطر الاستراتيجي:

الوظيفة: تقديم تحليل للمخاطر على مستوى استراتيجي يساعد في اتخاذ قرارات طويلة الأجل بشأن الأمان.

المثال: Palantir, RiskLens.

أدوات تقييم الأمن السحابي

الوظيفة: تقييم المخاطر الخاصة بالبيئات السحابية وتقديم حلول لتأمين البيانات والتطبيقات السحابية.

المثال: Cloud Security Alliance (CSA) STAR, AWS Security Hub.

أدوات تحليل المخاطر المتعلقة بالتطبيقات:

الوظيفة: تحليل المخاطر المرتبطة بتطوير واستخدام التطبيقات لتحديد الثغرات المحتملة.

المثال: Veracode, Checkmarx.

أدوات تقييم المخاطر الخاصة بالموردين:

الوظيفة: تقييم المخاطر المرتبطة بالشركاء والموردين وتقديم رؤى حول الأمان في سلاسل الإمداد.

المثال: BitSight, SecurityScorecard.

أدوات تقييم الأمان الرقمي:

الوظيفة: تحليل الأمان الرقمي وتقديم تقارير حول المخاطر والتهديدات في البيئة الرقمية.

المثال: Digital Guardian, Forcepoint.

أدوات مراجعة التكوينات الأمنية:

الوظيفة: تقييم تكوينات الأمان لأنظمة وتطبيقات لتحديد مدى توافقها مع السياسات الأمنية.

المثال: Tufin, Skybox Secu

الوحدة السادسة

- القوانين واللوائح الخاصة بالأمن السيبراني.
- تحديد القوانين واللوائح الخاصة بالأمن السيبراني المعمول بها في البلدان المختلفة والمؤسسات الحكومية والخاصة.
- تحليل المتطلبات الأمنية المفروضة من هذه القوانين واللوائح.
- تطبيق معايير الأمن السيبراني.
- تحديد الإجراءات الوقائية والتصحيحية.
- تطبيق نظام إدارة الأمن السيبراني.

القوانين واللوائح الخاصة بالأمن السيبراني

تتضمن القوانين واللوائح الخاصة بالأمن السيبراني مجموعة من القواعد والتشريعات التي تهدف إلى حماية الأنظمة المعلوماتية والبيانات من التهديدات السيبرانية وضمان الأمان الرقمي. تشمل هذه القوانين تنظيمات دولية ومحلية تتناول جوانب مختلفة من الأمان السيبراني.

أنواع القوانين واللوائح الخاصة بالأمن السيبراني:

قوانين حماية البيانات الشخصية:

الوظيفة: حماية المعلومات الشخصية للأفراد وضمان استخدامها بشكل آمن وفقًا للمعايير المحددة.

المثال: اللائحة العامة لحماية البيانات (GDPR) في الاتحاد الأوروبي، قانون حماية خصوصية المستهلك في كاليفورنيا.(CCPA)

قوانين الأمان الوطني:

الوظيفة: حماية البنية التحتية الوطنية والمعلومات الحساسة من التهديدات السيبرانية.

المثال: قانون أمان البنية التحتية الوطنية في الولايات المتحدة ,(NIST) قانون الأمان السيبراني الصيني.

قوانين مكافحة الجرائم السيبرانية:

الوظيفة: مكافحة الأنشطة غير القانونية على الإنترنت، مثل القرصنة والاحتيال الإلكتروني.

المثال: قانون مكافحة الجرائم الإلكترونية في المملكة المتحدة (Computer Misuse Act), قانون مكافحة الجرائم الإلكترونية في الولايات المتحدة.(CFAA)

لوائح الأمان في القطاع المالي:

الوظيفة: تنظيم الأمان السيبراني في المؤسسات المالية لضمان حماية البيانات المالية والتجارية.

المثال: قانون حماية بيانات المريض (HIPAA) في الولايات المتحدة، تنظيم الأمان المالي من هيئة السلوك المالي (FCA) في المملكة المتحدة.

لوائح الأمان في القطاع الصحي:

الوظيفة: حماية بيانات المرضى وسجلاتهم الطبية من التهديدات السيبرانية.

المثال: قانون حماية البيانات الشخصية للمرضى (HIPAA) في الولايات المتحدة.

لوائح الأمان السحابي:

الوظيفة: تنظيم الأمان وحماية البيانات في بيئات الحوسبة السحابية.

المثال: الالتزام بمعايير الأمان السحابي من خلال جمعية الأمان السحابي.(CSA)

قوانين تنظيم الأمان في الإنترنت:

الوظيفة: تنظيم سلوك الأمان على الإنترنت وتحديد مسؤوليات مقدمي الخدمات.

المثال: قانون حماية الأمان الرقمي للأطفال (COPPA) في الولايات المتحدة.

لوائح الأمان في قطاع التعليم:

الوظيفة: حماية بيانات الطلاب والمعلومات الأكاديمية من التهديدات السيبرانية.

المثال: قانون الخصوصية في التعليم (FERPA) في الولايات المتحدة.

قوانين الأمان السيبراني الدولية:

الوظيفة: توحيد معايير الأمان السيبراني عبر الدول وتعزيز التعاون الدولي في مواجهة التهديدات.

المثال: اتفاقية بودابست لمكافحة الجريمة الإلكترونية.

قوانين تنظيم الأمان في التكنولوجيا:

الوظيفة: تنظيم الأمان في تطوير واستخدام التكنولوجيا لحماية البيانات والمعلومات.

المثال: قانون الأمان السيبراني لقطاع التكنولوجيا في الصين، التوجيهات الأمنية للاتحاد الأوروبي.

تحديد القوانين واللوائح الخاصة بالأمن السيبراني في البلدان المختلفة والمؤسسات الحكومية والخاصة

تتفاوت القوانين واللوائح الخاصة بالأمن السيبراني من بلد إلى آخر وتعتمد على السياسات الوطنية ومتطلبات القطاع. هنا نظرة عامة على بعض القوانين واللوائح المعروفة في بلدان مختلفة:

قوانين ولوائح الأمن السيبراني الدولية:

اتفاقية بودابست لمكافحة الجريمة الإلكترونية:

الوظيفة: توحيد الجهود الدولية لمكافحة الجرائم الإلكترونية وتعزيز التعاون بين الدول.

البلدان المعنية: الدول الأعضاء في مجلس أوروبا والدول الموقعة من خارج المجلس.

اللائحة العامة لحماية البيانات(GDPR)

الوظيفة: تنظيم حماية البيانات الشخصية للأفراد داخل الاتحاد الأوروبي.

البلدان المعنية: دول الاتحاد الأوروبي، وبعض الشركات العالمية التي تتعامل مع بيانات مواطني الاتحاد.

قوانين الأمن السيبراني في بعض الدول:

الولايات المتحدة الأمريكية:

قانون حماية البيانات الشخصية للأفراد :(HIPAA) ينظم حماية البيانات الصحية الشخصية.

قانون حماية الخصوصية للأطفال عبر الإنترنت :(COPPA) يحدد متطلبات حماية بيانات الأطفال دون سن 13 عامًا.

قانون مكافحة الجرائم الإلكترونية :(CFAA) يتناول الجرائم المرتكبة عبر الحواسيب والأنظمة الإلكترونية.

المملكة المتحدة:

قانون حماية البيانات 2018: يعزز الأمان للبيانات الشخصية بما يتماشى مع.GDPR

قانون الأمن السيبراني 2018: ينظم متطلبات الأمان السيبراني للشركات الهامة والبنية التحتية الأساسية.

قوانين ولوائح الأمن السيبراني في المؤسسات الحكومية والخاصة:

الولايات المتحدة:

قانون فدرالي لإدارة المعلومات الأمنية :(FISMA) يتطلب من الوكالات الفيدرالية تطبيق معايير الأمان السيبراني.

معايير :NIST تقدم إطارًا للمعايير والتوجيهات في إدارة الأمان السيبراني.

الاتحاد الأوروبي:

التوجيه الأوروبي للأمن السيبراني :(NIS Directive) يفرض متطلبات للأمان السيبراني على الشركات والهيئات العامة ذات الأهمية الحيوية.

البنك الدولي:

معايير الأمان السيبراني: يضع معايير خاصة بالأمان السيبراني للمؤسسات المالية العالمية.

تحليل المتطلبات الأمنية المفروضة من القوانين واللوائح الخاصة بالأمن السيبراني:

تختلف المتطلبات الأمنية التي تفرضها القوانين واللوائح حسب الأهداف المحددة لكل قانون، ولكنها عادةً ما تشمل مجموعة من العناصر الأساسية المتعلقة بحماية البيانات والأمان السيبراني. فيما يلي تحليل للمتطلبات الأمنية التي تفرضها بعض القوانين واللوائح البارزة:

1 .اللائحة العامة لحماية البيانات(GDPR)

حماية البيانات الشخصية: يتطلب GDPR حماية المعلومات الشخصية للأفراد، بما في ذلك البيانات التي يمكن استخدامها لتحديد هوية الشخص.

الموافقة: يجب الحصول على موافقة صريحة من الأفراد لجمع واستخدام بياناتهم.

الحق في الوصول والتصحيح: يحق للأفراد الوصول إلى بياناتهم الشخصية وتصحيح أي معلومات غير دقيقة.

الإخطار بالخرق: يجب إخطار السلطات والأفراد المتأثرين في حالة حدوث خرق للبيانات خلال 72 ساعة.

تقييم الأثر: يتطلب إجراء تقييم لتأثير الأمان السيبراني للبيانات الشخصية.

2 .قانون حماية البيانات الشخصية - (PIPL) الصين

جمع واستخدام البيانات: يجب الحصول على موافقة واضحة من الأفراد قبل جمع بياناتهم.

حماية البيانات: يتعين على المؤسسات اتخاذ تدابير لحماية البيانات من الوصول غير المصرح به والتسريب.

الحق في الوصول والحذف: يحق للأفراد الوصول إلى بياناتهم وطلب حذفها.

إخطار السلطات: يتطلب إخطار السلطات بشأن أي خرق للبيانات.

3 .قانون الأمان السيبراني الصيني

حماية البنية التحتية الأساسية: يشمل متطلبات لحماية المعلومات والبنية التحتية الحيوية للأمن الوطني.

إدارة المخاطر: يتطلب من الشركات تنفيذ استراتيجيات إدارة المخاطر الأمنية.

تدابير الأمان: يتعين على المؤسسات اتخاذ تدابير أمان لحماية البيانات والمعلومات الحساسة.

4 .قانون حماية البيانات الشخصية - (HIPAA) الولايات المتحدة

حماية البيانات الصحية: يتطلب حماية المعلومات الصحية الشخصية للأفراد من الوصول غير المصرح به.

أمن البيانات: يشمل تنفيذ تدابير أمان مادية وإدارية وتقنية لحماية البيانات الصحية.

إخطار الأفراد: يجب إخطار الأفراد بشأن أي خرق للمعلومات الصحية الشخصية.

5 .قانون الأمن السيبراني 2018 - المملكة المتحدة

حماية البيانات: يشمل متطلبات لحماية البيانات الشخصية وأمن المعلومات.

تقييم المخاطر: يتطلب من المؤسسات إجراء تقييمات دورية للمخاطر الأمنية.

الإبلاغ عن الحوادث: يتطلب الإبلاغ عن الحوادث الأمنية والتعامل معها بطريقة مناسبة.

6 .قانون تكنولوجيا المعلومات - 2000 (IT Act) الهند

حماية البيانات: يشمل متطلبات لحماية المعلومات الشخصية والبيانات من التهديدات السيبرانية.

إدارة الأمن: يتطلب تنفيذ إجراءات أمان لحماية البيانات والمعلومات الإلكترونية.

التعامل مع الجرائم الإلكترونية: يتناول التعامل مع الأنشطة غير القانونية عبر الإنترنت.

7 .قوانين الأمان السيبراني في المؤسسات الحكومية

التوافق مع معايير الأمان: يجب على المؤسسات الحكومية الالتزام بمعايير الأمان السيبراني التي تحددها الهيئات التنظيمية.

التقييم والاختبار: يتطلب إجراء تقييمات واختبارات دورية لأنظمة الأمان.

الإبلاغ عن الحوادث: يشمل الإبلاغ عن الحوادث الأمنية والتعامل معها وفقًا للمتطلبات المحددة.

تطبيق معايير الأمن السيبراني:

تطبيق معايير الأمن السيبراني يشمل تنفيذ وتطبيق إطار عمل ومعايير محددة لحماية الأنظمة والمعلومات من التهديدات السيبرانية. تساعد هذه المعايير المؤسسات على تحسين أمان المعلومات وضمان التزامها بأفضل الممارسات. إليك كيفية تطبيق معايير الأمن السيبراني:

1 .تحديد الإطار والمعايير المناسبة

اختيار الإطار المناسب: بناءً على متطلبات المؤسسة، اختر إطارًا معترفًا به مثل NIST Cybersecurity Framework أو ISO/IEC 27001.

تحديد المعايير: اختر المعايير التي تتماشى مع أهداف الأمان الخاصة بالمؤسسة ومتطلبات الصناعة.

2 .تنفيذ السياسات والإجراءات

إنشاء السياسات: طور سياسات أمنية تتناول جوانب مختلفة مثل حماية البيانات، إدارة الوصول، والاستجابة للحوادث.

إجراءات التشغيل: وضع إجراءات مفصلة لتنفيذ السياسات وضمان تحقيق الأهداف الأمنية.

3 .تقييم الأصول وتحديد المخاطر

تحديد الأصول: تحديد جميع الأصول المعلوماتية مثل الأنظمة والشبكات والبيانات.

تقييم المخاطر: إجراء تحليل للمخاطر لتحديد التهديدات والثغرات المرتبطة بكل أصل.

4 .تنفيذ تدابير الأمان

التدابير الوقائية: تنفيذ أدوات الأمان مثل جدران الحماية، أنظمة الكشف والوقاية من التسلل، ومكافحة البرمجيات الخبيثة.

تشفير البيانات: تأمين البيانات من خلال التشفير أثناء النقل والتخزين.

5 .تدريب وتوعية الموظفين

التدريب الأمني: تقديم تدريب منتظم للموظفين حول السياسات الأمنية والممارسات الجيدة.

التوعية: تعزيز الوعي حول التهديدات السيبرانية وأساليب الحماية.

6 .اختبار ومراجعة الأمان

الاختبارات الأمنية: إجراء اختبارات دورية مثل اختبارات الاختراق والتحقق من الأمان للتأكد من فعالية التدابير.

المراجعة والتقييم: مراجعة سياسات الأمان والإجراءات بانتظام وتحديثها بناءً على التغيرات في البيئة والتهديدات.

7 .الاستجابة للحوادث والتعافي

إجراءات الاستجابة: تطوير خطة للاستجابة للحوادث تتضمن خطوات للإبلاغ والتعامل مع الحوادث الأمنية.

التعافي: وضع خطط للتعافي من الكوارث لضمان استعادة الأنظمة والبيانات بشكل فعال.

8 .الامتثال والتوثيق

التوثيق: الحفاظ على توثيق دقيق لجميع السياسات، الإجراءات، والتقارير الأمنية.

الامتثال: ضمان التزام المؤسسة بالمعايير القانونية والتنظيمية ذات الصلة.

9 .تحسين مستمر

مراجعة الأداء: تقييم فعالية التدابير الأمنية بانتظام وتحليل نتائج الحوادث.

التطوير: تحديث الاستراتيجيات والأدوات بناءً على التقييمات والمراجعات لضمان تحسين مستمر.

تحديد الإجراءات الوقائية والتصحيحية في الأمن السيبراني:

الإجراءات الوقائية: الإجراءات الوقائية هي التدابير التي تُتخذ لتجنب وقوع الحوادث الأمنية وحماية الأنظمة والمعلومات من التهديدات المحتملة. تشمل:

تحديث الأنظمة والتطبيقات:

الوظيفة: تصحيح الثغرات الأمنية من خلال تطبيق التحديثات الأمنية والتصحيحات.

التطبيق: تحديث برامج التشغيل والبرامج بانتظام.

تنفيذ التحكم في الوصول:

الوظيفة: ضمان أن الوصول إلى الأنظمة والبيانات محصور على الأفراد المصرح لهم فقط.

التطبيق: استخدام كلمات مرور قوية، نظام المصادقة متعددة العوامل، وأذونات وصول محددة.

تشفير البيانات:

الوظيفة: حماية البيانات من الوصول غير المصرح به أثناء النقل والتخزين.

التطبيق: تشفير المعلومات الحساسة بطرق قوية.

إجراءات الأمان الأساسية:

الوظيفة: تأمين الأنظمة والشبكات من التهديدات المحتملة.

التطبيق: تركيب جدران الحماية، وأنظمة كشف التسلل، وبرامج مكافحة الفيروسات.

التدريب والتوعية:

الوظيفة: تعزيز الوعي حول الممارسات الأمنية الجيدة بين الموظفين.

التطبيق: تنظيم دورات تدريبية منتظمة حول الأمان السيبراني وأفضل الممارسات.

إعداد الخطط الأمنية:

الوظيفة: تحديد سياسات وإجراءات الأمان اللازمة للحماية من المخاطر.

التطبيق: تطوير خطط أمان شاملة تشمل جميع جوانب الأمان السيبراني.

الإجراءات التصحيحية: الإجراءات التصحيحية هي الخطوات التي تُتخذ لمعالجة المشاكل الأمنية التي تم اكتشافها وتحسين الأمان بعد وقوع الحوادث. تشمل:

تحليل الحوادث:

الوظيفة: فهم السبب الجذري للحوادث الأمنية لتجنب تكرارها.

التطبيق: إجراء تحقيقات وتحليلات شاملة بعد الحوادث الأمنية.

تحديث الأنظمة وإصلاح الثغرات

الوظيفة: تصحيح الثغرات والأخطاء التي أدت إلى الحادث الأمني.

التطبيق: تنفيذ التحديثات الأمنية والتصحيحات بعد تحليل الثغرات.

تقييم الأثر:

الوظيفة: تقييم الأضرار التي سببها الحادث وتحليل تأثيرها على النظام.

التطبيق: مراجعة الأثر المالي والتشغيلي للحوادث وتحليل الأضرار.

تحسين الإجراءات:

الوظيفة: تعديل السياسات والإجراءات الأمنية بناءً على دروس مستفادة من الحوادث.

التطبيق: تحديث السياسات الأمنية وإجراءات الاستجابة للحوادث لتحسين فعالية الأمان.

استعادة الأنظمة والبيانات:

الوظيفة: استعادة الأنظمة والبيانات المتأثرة بالحادث إلى حالتها الطبيعية.

التطبيق: استخدام النسخ الاحتياطية واستعادة الأنظمة والبيانات بعد الحادث.

التوثيق والتقارير:

الوظيفة: توثيق الحادث والإجراءات التصحيحية المتخذة.

التطبيق: إعداد تقارير تفصيلية حول الحادث، الإجراءات التصحيحية، والدروس المستفادة.

تطبيق نظام إدارة الأمن السيبراني

تطبيق نظام إدارة الأمن السيبراني يشمل تطوير وتنفيذ إطار عمل متكامل لإدارة الأمان السيبراني في المؤسسات. يهدف هذا النظام إلى حماية المعلومات والأنظمة من التهديدات، وضمان الامتثال للمعايير الأمنية، وتعزيز القدرة على التصدي للحوادث. فيما يلي الخطوات الأساسية لتطبيق نظام إدارة الأمن السيبراني:

1. تحديد نطاق النظام

تحديد الأصول: تحديد الأصول المعلوماتية التي تحتاج إلى حماية، بما في ذلك البيانات، الأنظمة، والشبكات.

تحديد التهديدات: التعرف على التهديدات المحتملة والضعف في الأنظمة.

2 .تطوير السياسات والإجراءات

تطوير السياسات الأمنية: وضع سياسات أمنية شاملة تشمل حماية البيانات، إدارة الوصول، واستجابة الحوادث.

إنشاء الإجراءات: تطوير إجراءات تشغيلية تتوافق مع السياسات وتحدد كيفية تنفيذها ومراقبتها.

3 .تقييم وإدارة المخاطر

تحديد المخاطر: إجراء تحليل للمخاطر لتحديد التهديدات والضعف المحتملة.

تقييم المخاطر: تقييم احتمالية وتأثير المخاطر وتحديد أولويات التعامل معها.

إدارة المخاطر: وضع استراتيجيات للتخفيف من المخاطر، بما في ذلك التدابير الوقائية والتصحيحية.

4 .تنفيذ التدابير الأمنية

تطبيق الضوابط: تنفيذ ضوابط الأمان مثل جدران الحماية، وأنظمة كشف التسلل، والتشفير.

تدريب الموظفين: توفير التدريب والتوعية للموظفين حول السياسات الأمنية وأفضل الممارسات.

5 .المراقبة والتدقيق

مراقبة الأنظمة: استخدام أدوات المراقبة لمتابعة النشاطات وتحليل السجلات للكشف عن الأنشطة غير الطبيعية.

التدقيق: إجراء تدقيقات دورية للتحقق من فعالية سياسات وإجراءات الأمان.

6 .استجابة الحوادث والتعافي

إعداد خطة استجابة للحوادث: تطوير خطة شاملة للاستجابة للحوادث الأمنية تشمل تحديد الأدوار والمسؤوليات والخطوات الواجب اتخاذها.

تنفيذ إجراءات التعافي: وضع خطة للتعافي من الكوارث لاستعادة الأنظمة والبيانات المتأثرة بالحوادث.

7 .مراجعة وتحسين النظام

مراجعة الأداء: تقييم فعالية نظام إدارة الأمن السيبراني بناءً على الأداء والتقارير.

تحسين مستمر: تحديث السياسات والإجراءات استنادًا إلى نتائج المراجعات والتدقيقات وأي تغييرات في البيئة أو التهديدات.

8 .ضمان الامتثال

الامتثال للمعايير: التأكد من أن النظام يتوافق مع المعايير والقوانين التنظيمية ذات الصلة.

التوثيق: الحفاظ على توثيق دقيق لجميع السياسات والإجراءات والتقارير لمراجعات الامتثال.

الوحدة السابعة

- تحليل الأداء الأمني.
- تحديد معايير التقييم.
- جمع البيانات يجب جمع البيانات اللازمة لتقييم الأداء الأمني.
- تحليل البيانات.
- تقييم الأداء الأمني.
- تطبيق الخطط اللازمة.
- مراقبة الأداء الأمني.
- توثيق الأداء الأمنى.

تحليل الأداء

تحليل الأداء الأمني هو عملية تقييم فعالية أنظمة الأمان السيبراني والإجراءات المتبعة في المؤسسة. يهدف هذا التحليل إلى ضمان أن تدابير الأمان تعمل كما هو متوقع، وتحديد أية نقاط ضعف، وتحسين استراتيجيات الأمان. فيما يلي الخطوات الأساسية لتحليل الأداء الأمني:

1 .تحديد مؤشرات الأداء الرئيسية(KPIs)

تحديد المؤشرات: اختر مؤشرات الأداء الرئيسية التي تعكس فعالية نظام الأمان السيبراني، مثل عدد الحوادث الأمنية، مدة الاستجابة للحوادث، وعدد الاختراقات الناجحة.

تحديد الأهداف: ضع أهدافًا محددة لكل مؤشر أداء لضمان تحقيق الأداء الأمثل.

2 .جمع البيانات

تجميع البيانات: جمع البيانات المتعلقة بالأداء الأمني من مختلف المصادر مثل أدوات المراقبة، سجلات الأنظمة، وتقارير الحوادث.

تحديث البيانات: تأكد من أن البيانات التي تجمعها حديثة وذات صلة.

3 .تحليل البيانات

تحليل الاتجاهات: مراجعة البيانات لتحديد الاتجاهات والأنماط، مثل زيادة في عدد الحوادث أو تغييرات في أوقات الاستجابة.

تحديد الثغرات: الكشف عن الثغرات في نظام الأمان التي قد تؤثر على الأداء، مثل نقاط الضعف في الضوابط الأمنية.

4 .تقييم فعالية التدابير الأمنية

مراجعة التدابير: تقييم فعالية التدابير الأمنية المطبقة مثل التشفير، وأنظمة كشف التسلل، وجدران الحماية.

تحليل التكاليف والفوائد: مقارنة تكلفة التدابير الأمنية بفوائدها لضمان فعالية الاستثمار في الأمان.

5 .تقييم استجابة الحوادث

مراجعة الحوادث السابقة: تحليل كيفية التعامل مع الحوادث السابقة وتقييم فعالية استجابة الفريق.

تقييم التحسينات: التحقق من تنفيذ أي تحسينات أو تغييرات تم إدخالها بناءً على الحوادث السابقة.

6 .إعداد تقارير الأداء

تقرير الأداء: إعداد تقارير مفصلة تلخص نتائج التحليل، بما في ذلك المؤشرات، الاتجاهات، والتوصيات.

تقديم التقارير: مشاركة التقارير مع الإدارة العليا وأصحاب المصلحة الرئيسيين للحصول على الموافقة على الخطوات التالية.

7 .اتخاذ إجراءات تصحيحية وتحسينية

تطوير خطة تحسين: بناءً على نتائج التحليل، وضع خطة لتحسين الأداء الأمني، بما في ذلك تحديث السياسات، تعزيز التدابير الأمنية، أو تحسين التدريب.

تنفيذ التحسينات: تنفيذ التغييرات والتحديثات اللازمة لضمان تعزيز فعالية الأمان السيبراني.

8 .المراجعة الدورية

مراجعة دورية: إجراء مراجعات دورية لأداء الأمان لضمان استمرار فعاليته في مواجهة التهديدات المتغيرة.

التحديث والتحسين المستمر: التكيف مع التغيرات في البيئة الأمنية والتكنولوجيا.

تحديد معايير التقييم

تحديد معايير التقييم هو خطوة أساسية لضمان أن نظام الأمان السيبراني يتم قياسه بفعالية وفهم أدائه بشكل دقيق. تشمل المعايير عادةً مؤشرات أداء رئيسية (KPIs) وسمات تقييمية يمكن قياسها بموضوعية. فيما يلي بعض المعايير التي يمكن استخدامها لتقييم الأداء الأمني:

1 .عدد الحوادث الأمنية

الوصف: عدد الحوادث الأمنية المسجلة خلال فترة زمنية معينة.

الأهمية: يساعد في تقييم مدى فعالية تدابير الأمان الحالية في منع الحوادث.

2 .وقت الاستجابة للحوادث

الوصف: الوقت المستغرق من اكتشاف الحادث إلى اتخاذ إجراء أولي.

الأهمية: يعكس سرعة وفعالية استجابة الفريق الأمني للحوادث.

3 .مدة التوقف عن الخدمة

الوصف: الفترة الزمنية التي تكون فيها الأنظمة أو الخدمات غير متاحة بسبب الحوادث الأمنية.

الأهمية: يقيس تأثير الحوادث الأمنية على استمرارية العمل والأداء التشغيلي.

4 .فعالية التدابير الأمنية

الوصف: مدى نجاح التدابير الأمنية مثل التشفير، جدران الحماية، وأنظمة كشف التسلل في حماية الأصول.

الأهمية: يساعد في تقييم مدى كفاءة الأدوات والتقنيات الأمنية المستخدمة.

5 .عدد الثغرات المكتشفة

الوصف: عدد الثغرات الأمنية التي تم اكتشافها خلال فحص الأمان أو اختبار الاختراق.

الأهمية: يقيم فعالية إجراءات الكشف والتصحيح المتعلقة بالثغرات.

6 .معدل الفشل في اختبارات الأمان

الوصف: نسبة الاختبارات الأمنية التي فشلت في كشف التهديدات أو الثغرات.

الأهمية: يوضح مدى فعالية أدوات وتقنيات اختبار الأمان المستخدمة.

7 .مستوى التوعية والتدريب

الوصف: مدى تدريب الموظفين وتوعيتهم حول سياسات الأمان والممارسات الجيدة.

الأهمية: يؤثر على قدرة الموظفين على التعرف على التهديدات والالتزام بالسياسات الأمنية.

8 .التوافق مع السياسات واللوائح

الوصف: مدى التزام المؤسسة بالمعايير والسياسات الأمنية المحددة.

الأهمية: يضمن الامتثال للمتطلبات القانونية والتنظيمية ذات الصلة.

9 .تكاليف الأمان

الوصف: التكاليف المرتبطة بتنفيذ وصيانة تدابير الأمان، بما في ذلك التحديثات والإصلاحات.

الأهمية: يساعد في تقييم فعالية التكلفة للعائد من الاستثمار في الأمان.

10 .معدل نجاح استعادة الأنظمة

الوصف: مدى سرعة وفعالية استعادة الأنظمة والبيانات بعد حادث أمني.

الأهمية: يقيم فعالية خطط التعافي من الكوارث والإجراءات التصحيحية.

11 .مستوى الأمان التشغيلي

الوصف: مدى الأمان الذي توفره العمليات اليومية، مثل إدارة الوصول ومراقبة الأنظمة.

الأهمية: يقيم مدى فعالية الأمان خلال العمليات اليومية العادية.

جمع البيانات

جمع البيانات اللازمة لتقييم الأداء الأمني هو خطوة حيوية لضمان أن التحليل يستند إلى معلومات دقيقة وموثوقة. البيانات التي يتم جمعها تساعد في قياس فعالية التدابير الأمنية وتحديد المناطق التي تحتاج إلى تحسين. إليك كيفية جمع البيانات بشكل منهجي:

1 .تحديد مصادر البيانات

سجلات الأنظمة: تشمل سجلات الخوادم، الشبكات، وقواعد البيانات، والتي توفر معلومات حول الأنشطة والأحداث.

أدوات المراقبة: بيانات من أنظمة المراقبة مثل جدران الحماية، وأنظمة كشف التسلل، وبرامج مكافحة الفيروسات.

تقارير الحوادث: توثيق شامل للحوادث الأمنية، بما في ذلك تفاصيل الحوادث، إجراءات الاستجابة، والتقارير النهائية.

نتائج اختبارات الأمان: بيانات من اختبارات الاختراق، تقييمات الثغرات، ومراجعات الأمان.

استطلاعات الموظفين: نتائج من استطلاعات الرأي أو الاستبيانات التي تقيس مستوى الوعي والتدريب الأمني بين الموظفين.

سجلات الاستجابة للحوادث: بيانات حول الوقت المستغرق للاستجابة، وإجراءات التعافي، وتكاليف التعامل مع الحوادث.

2 .جمع البيانات بشكل دوري

التجميع المستمر: جمع البيانات بشكل مستمر من أدوات المراقبة والسجلات لضمان الحصول على أحدث المعلومات.

الجمع الدوري: إجراء تقييمات دورية وتحليل النتائج من اختبارات الأمان والتقارير الأمنية لتحديث البيانات.

3 .تنظيم البيانات

تصنيف البيانات: تنظيم البيانات إلى فئات مثل أحداث الأمان، استجابة الحوادث، والتدابير الأمنية للتسهيل على التحليل.

تنسيق البيانات: التأكد من تنسيق البيانات بشكل موحد لتسهيل عملية التحليل والمقارنة.

4 .التحقق من جودة البيانات

التدقيق: التحقق من دقة البيانات وصحتها للتأكد من أنها تعكس الوضع الحقيقي للأداء الأمني.

التحقق من الاتساق: التأكد من أن البيانات متسقة مع المصادر الأخرى ولا تحتوي على تناقضات.

5 .استخدام أدوات جمع البيانات

أدوات المراقبة: استخدام أدوات لرصد الشبكات، الأنظمة، والتطبيقات لجمع البيانات بشكل تلقائي.

برامج تحليل الأمان: استخدام برامج تحليل الأمان لجمع وتفسير بيانات الأمان السيبراني.

6 .حماية البيانات

تأمين البيانات: ضمان حماية البيانات المجمعة من الوصول غير المصرح به أو التلاعب.

النسخ الاحتياطي: إجراء نسخ احتياطية للبيانات لضمان عدم فقدانها.

7 .تحليل البيانات

معالجة البيانات: تجهيز البيانات للتحليل باستخدام أدوات التحليل المناسبة.

التحليل والتفسير: تحليل البيانات لتحديد مؤشرات الأداء، الاتجاهات، ونقاط الضعف.

تحليل البيانات

تحليل البيانات هو عملية حيوية لتحويل المعلومات المجمعة إلى رؤى مفيدة حول فعالية نظام الأمان السيبراني. يهدف التحليل إلى تقييم الأداء، تحديد الثغرات، وتقديم توصيات للتحسين. إليك كيفية إجراء تحليل فعال للبيانات:

1 .إعداد البيانات

تنظيف البيانات: إزالة البيانات غير الدقيقة أو المكررة لضمان صحة التحليل.

تنظيم البيانات: تصنيف وتنظيم البيانات حسب الفئات مثل الحوادث الأمنية، الاستجابة، وكفاءة التدابير الأمنية.

2 .تحليل الاتجاهات

تحديد الاتجاهات: استخدم الأدوات التحليلية لتحديد الأنماط والاتجاهات في البيانات، مثل زيادة في عدد الحوادث أو تغييرات في أوقات الاستجابة.

تحليل الأنماط: تحليل الأنماط لتحديد الأسباب المحتملة للمشكلات أو النجاحات في النظام الأمني.

3 .تقييم فعالية التدابير الأمنية

مقارنة الأداء: قارن بين الأداء الفعلي والتوقعات أو الأهداف المحددة، مثل عدد الحوادث مقارنة بالأهداف أو فعالية أدوات الأمان.

تحليل الفجوات: تحديد أي فجوات بين الأداء الفعلي والنتائج المطلوبة لتقييم فعالية التدابير الأمنية.

4 .تحليل الحوادث الأمنية

تحليل الأسباب الجذرية: تحليل الأسباب الجذرية للحوادث الأمنية لتحديد الأسباب الأساسية وعدم الاكتفاء بالظواهر.

تقييم الاستجابة: مراجعة كيفية التعامل مع الحوادث وتقييم فعالية الاستجابة والإجراءات التصحيحية.

5 .تقييم الأداء المالي

تحليل التكاليف: تحليل تكاليف التدابير الأمنية مقارنة بالفوائد المحققة، مثل تكلفة التحديثات الأمنية مقابل تقليل الحوادث.

تحليل العائد على الاستثمار :(ROI) قياس العائد على الاستثمار لتحديد كفاءة الإنفاق على الأمان السيبراني.

6 .مقارنة الأداء مع المعايير

مقارنة بالمعايير: قارن أداء الأمان مع المعايير والممارسات الفضلى في الصناعة مثل إطار عمل NIST أو.ISO/IEC 27001

مراجعة التوافق: تحقق من مدى التزام الأداء بالسياسات واللوائح الداخلية والخارجية.

7 .إعداد تقارير الأداء

إعداد التقارير: إعداد تقارير مفصلة تلخص نتائج التحليل، بما في ذلك البيانات الرئيسية، الاتجاهات، والتوصيات.

تقديم التوصيات: تقديم توصيات بناءً على التحليل لتحسين الأمان، بما في ذلك تحديث السياسات، تعزيز التدابير الأمنية، أو تحسين التدريب.

8 .تنفيذ التحسينات

تطوير خطة تحسين: بناءً على نتائج التحليل، وضع خطة لتحسين الأداء الأمني تشمل التعديلات الضرورية والتحديثات.

مراقبة التقدم: متابعة تنفيذ التحسينات وقياس تأثيرها على الأداء الأمني.

9 .مراجعة وتحسين مستمر

التقييم الدوري: إجراء مراجعات دورية لتحليل الأداء لضمان التحسين المستمر وتحديث الاستراتيجيات.

تحديث البيانات: تحديث البيانات والمعايير بناءً على التغيرات في البيئة الأمنية والتقنية.

تقييم الأداء

تقييم الأداء الأمني هو عملية منهجية تهدف إلى قياس فعالية أنظمة الأمان السيبراني وتحديد مدى نجاحها في حماية الأصول المعلوماتية. يتضمن التقييم تحليل البيانات التي تم جمعها من مختلف المصادر ومقارنتها بالمعايير والأهداف المحددة. إليك كيفية إجراء تقييم شامل للأداء الأمني:

1 .مراجعة الأهداف والمعايير

تحديد الأهداف: مراجعة الأهداف الأمنية المحددة مسبقاً، مثل تقليل عدد الحوادث الأمنية أو تحسين وقت الاستجابة.

مقارنة المعايير: مقارنة الأداء الفعلي بالمعايير والمعايير المتفق عليها مثل مؤشرات الأداء الرئيسية (KPIs) ومعايير الصناعة.

2 .تحليل نتائج الأداء

مراجعة المؤشرات: تحليل نتائج مؤشرات الأداء مثل عدد الحوادث الأمنية، وقت الاستجابة، وفترة التوقف عن الخدمة.

تقييم الفعالية: تقييم فعالية التدابير الأمنية مثل جدران الحماية، والتشفير، وأنظمة كشف التسلل.

3 .تقييم فعالية استجابة الحوادث

مراجعة الاستجابة: تقييم كيفية تعامل الفريق الأمني مع الحوادث، بما في ذلك سرعة الاستجابة وكفاءة معالجة الحوادث.

تحليل الإجراءات التصحيحية: تحليل فعالية الإجراءات التصحيحية والتدابير المتخذة بعد الحوادث الأمنية.

4 .تقييم التكاليف والفوائد

تحليل التكاليف: تحليل التكاليف المرتبطة بتنفيذ وصيانة تدابير الأمان.

تقييم العائد على الاستثمار :(ROI) قياس الفوائد المحققة من الاستثمارات الأمنية مقارنةً بالتكاليف، مثل تقليل الخسائر بسبب الحوادث.

5 .مقارنة الأداء مع أفضل الممارسات

مراجعة المعايير: مقارنة الأداء مع أفضل الممارسات والمعايير المعترف بها في الصناعة مثل إطار عمل NIST أو معايير.ISO/IEC 27001

تقييم الامتثال: التأكد من أن الأداء يتماشى مع السياسات الداخلية والمتطلبات القانونية والتنظيمية.

6 .تحليل التغذية الراجعة

جمع التغذية الراجعة: جمع ملاحظات من موظفي الأمان والأطراف المعنية حول فعالية النظام الأمني وتجربة الاستجابة للحوادث.

تحليل الملاحظات: استخدام التغذية الراجعة لتحديد المجالات التي تحتاج إلى تحسين.

7 .تحديد نقاط القوة والضعف

تحديد نقاط القوة: تحديد الجوانب التي تعمل بشكل جيد وتساهم في تعزيز الأمان.

تحديد نقاط الضعف: الكشف عن الثغرات والمشكلات التي تؤثر على فعالية الأمان وتحليل أسبابها.

8 .إعداد تقارير الأداء

إعداد التقارير: تجهيز تقارير مفصلة تلخص نتائج التقييم، بما في ذلك نقاط القوة، ونقاط الضعف، والتوصيات.

مشاركة التقارير: تقديم التقارير للإدارة العليا وأصحاب المصلحة لتوجيه القرارات الإستراتيجية.

9 .تطوير خطة تحسين

وضع خطة تحسين: بناءً على نتائج التقييم، تطوير خطة لتحسين الأداء الأمني تشمل التعديلات الضرورية والتحديثات.

تنفيذ التحسينات: تنفيذ التغييرات المقترحة ومراقبة تأثيرها على الأداء.

10 .مراجعة وتحسين مستمر

التقييم الدوري: إجراء تقييمات دورية لضمان استمرار فعالية نظام الأمان وتحقيق التحسين المستمر.

تحديث المعايير: تحديث المعايير والأهداف بناءً على التغيرات في البيئة الأمنية والتقنية.

تطبيق الخطط اللازمة

بعد تقييم الأداء الأمني وتحليل النتائج، يأتي دور تطبيق الخطط اللازمة لتحسين نظام الأمان السيبراني. يتضمن ذلك تنفيذ الإجراءات والتدابير التي تم تحديدها في خطة التحسين. إليك كيفية تطبيق هذه الخطط بفعالية:

1 .تطوير خطة التحسين

تحديد الأولويات: بناءً على نتائج التقييم، حدد الأولويات في تنفيذ التحسينات. ركز على المجالات التي تحتاج إلى تحسين فوري وتأثير كبير.

تحديد الإجراءات: وضع إجراءات محددة لكل مجال يحتاج إلى تحسين، بما في ذلك التعديلات في السياسات، التحديثات التكنولوجية، أو تدريب الموظفين.

2 .تخصيص الموارد

تحديد الموارد المطلوبة: تحديد الموارد اللازمة لتنفيذ خطة التحسين، بما في ذلك التمويل، التقنية، والموظفين.

تخصيص الموارد: تخصيص الموارد بشكل فعّال لضمان تنفيذ الإجراءات المطلوبة.

3 .تنفيذ التعديلات

تحديث السياسات: تعديل السياسات الأمنية لتكون أكثر فعالية بناءً على نتائج التقييم. تحديث الإجراءات والضوابط الأمنية وفقًا للممارسات الجديدة.

تركيب الأدوات: تنفيذ التحديثات التقنية مثل تحسين الأنظمة الأمنية أو إضافة أدوات جديدة مثل أنظمة كشف التسلل أو حلول التشفير.

تنفيذ التدريبات: توفير التدريب والتوعية للموظفين بشأن السياسات والإجراءات الجديدة وأفضل الممارسات الأمنية.

4 .متابعة تنفيذ الإجراءات

مراقبة التقدم: متابعة تقدم تنفيذ الخطط للتحقق من أنها تُنفذ كما هو مخطط لها. استخدام أدوات المراقبة لمراقبة التعديلات التي تم إجراؤها.

تقييم التأثير: قياس تأثير التعديلات على الأداء الأمني باستخدام مؤشرات الأداء الرئيسية والبيانات المتاحة.

5 .مراجعة وتقييم فعالية التحسينات

مراجعة الأداء: بعد تنفيذ التحسينات، قم بمراجعة الأداء الأمني للتحقق من تحسين النتائج. استخدم البيانات المجمعة لتقييم مدى نجاح التعديلات.

تعديل الخطط: إذا لزم الأمر، قم بتعديل الخطط بناءً على نتائج المراجعة للتأكد من تحقيق الأهداف المطلوبة.

6 .توثيق العملية

توثيق التعديلات: سجل جميع التعديلات والإجراءات الجديدة المتخذة، بما في ذلك التعديلات على السياسات والإجراءات.

إعداد تقارير: إعداد تقارير تفصيلية حول تنفيذ الخطط والتأثيرات التي لوحظت. تقديم هذه التقارير للإدارة العليا وأصحاب المصلحة.

7 .تحسين مستمر

مراجعة دورية: إجراء مراجعات دورية لضمان استمرار فعالية التعديلات وتكييفها مع التغيرات في البيئة الأمنية.

تحديث الخطط: تحديث الخطط والإجراءات بانتظام بناءً على التغيرات في التهديدات والتقنيات وأفضل الممارسات.

مراقبة الأداء

مراقبة الأداء الأمني هي عملية مستمرة تهدف إلى التحقق من فعالية أنظمة الأمان السيبراني وضمان أنها تعمل بشكل جيد وتتصدى للتحديات الأمنية بفعالية. تشمل هذه العملية تتبع الأداء، جمع البيانات، وتحليل النتائج لضمان تحقيق الأهداف الأمنية. إليك كيفية تنفيذ مراقبة فعالة للأداء الأمني:

1 .تحديد مؤشرات الأداء الرئيسية(KPIs)

تحديد المؤشرات: حدد مؤشرات الأداء الرئيسية التي تعكس فعالية الأمان السيبراني، مثل عدد الحوادث الأمنية، وقت الاستجابة، وعدد الثغرات الأمنية.

تحديد الأهداف: وضع أهداف محددة لكل مؤشر أداء لضمان تحقيق الأداء الأمثل.

2 .استخدام أدوات المراقبة

تثبيت الأدوات: استخدم أدوات المراقبة الأمنية مثل أنظمة كشف التسلل(IDS) ، جدران الحماية، وبرامج تحليل السجلات لمراقبة الأنشطة والأحداث.

تحديث الأدوات: تأكد من أن الأدوات المستخدمة محدثة وتتناسب مع أحدث التهديدات والتهديدات الأمنية.

3 .جمع وتحليل البيانات

جمع البيانات: جمع البيانات من الأدوات المراقبة، سجلات الأنظمة، وتقارير الحوادث.

تحليل البيانات: استخدام التحليل لفهم الأنماط، الاتجاهات، وأية مشكلات أو ثغرات قد تظهر.

4 .مراجعة الأداء بانتظام

مراجعات دورية: إجراء مراجعات دورية للأداء الأمني باستخدام البيانات التي تم جمعها لتحديد مدى فعالية التدابير الأمنية.

تقييم الأداء: مقارنة الأداء الفعلي بالمعايير والأهداف المحددة لتحديد المجالات التي تحتاج إلى تحسين.

5 .التعامل مع الانحرافات والمشكلات

تحديد المشكلات: تحديد أية انحرافات عن الأداء المتوقع أو المشكلات التي تم اكتشافها أثناء المراقبة.

اتخاذ الإجراءات: تنفيذ الإجراءات التصحيحية لمعالجة المشكلات وتحسين الأداء الأمني.

6 .تحديث السياسات والإجراءات

مراجعة السياسات: تحديث السياسات والإجراءات الأمنية بناءً على نتائج المراقبة لضمان مواكبة التهديدات والتغيرات في البيئة الأمنية.

تحسين العمليات: تحسين العمليات والإجراءات الأمنية بناءً على الملاحظات والتقارير.

7 .إشراك الفرق ذات الصلة

التنسيق مع الفرق: العمل مع فرق الأمن، تقنية المعلومات، والإدارة لضمان تنفيذ الإجراءات التصحيحية بفعالية.

التواصل: تقديم تقارير دورية للفرق والإدارة حول حالة الأداء الأمني والإجراءات التي تم اتخاذها.

8 .توثيق العملية

تسجيل النتائج: توثيق نتائج المراقبة، بما في ذلك أي مشكلات تم اكتشافها والإجراءات المتخذة لمعالجتها.

إعداد التقارير: إعداد تقارير دورية وشاملة حول أداء الأمان لمشاركة المعلومات مع الإدارة العليا وأصحاب المصلحة.

9 .تحسين مستمر

التقييم المستمر: إجراء تقييمات مستمرة للأداء الأمني لضمان التكيف مع التغيرات في التهديدات والتقنيات.

تحديث استراتيجيات الأمان: تحديث استراتيجيات الأمان بانتظام بناءً على نتائج المراقبة لضمان فعالية مستمرة.

توثيق الأداء

توثيق الأداء الأمني هو عملية جمع وتسجيل معلومات حول كيفية أداء الأنظمة والتدابير الأمنية، والنتائج التي تم تحقيقها، والإجراءات المتخذة لتحسين الأمان. يشمل ذلك إنشاء سجلات دقيقة وشاملة لتتبع الأداء وتحليل النتائج. إليك كيفية توثيق الأداء الأمني بفعالية:

1. تحديد ما يجب توثيقه

مؤشرات الأداء: سجل مؤشرات الأداء الرئيسية (KPIs) مثل عدد الحوادث الأمنية، وقت الاستجابة، وكفاءة الأدوات الأمنية.

الأحداث والتقارير: توثيق الأحداث الأمنية، الحوادث، تقارير الاختراق، والتدابير التصحيحية المتخذة.

2. استخدام أنظمة التوثيق

أنظمة إدارة السجلات: استخدم أنظمة إدارة السجلات لتخزين البيانات وتوثيق الأداء بشكل منظم. تأكد من أن النظام يتيح الوصول السهل للبيانات والتقارير.

أدوات التوثيق: استخدم أدوات لإعداد التقارير والتوثيق مثل برامج التحليل وإعداد التقارير.

3. إعداد تقارير الأداء

تقارير دورية: إعداد تقارير دورية (أسبوعية، شهرية، أو ربع سنوية) تلخص الأداء الأمني، تشمل البيانات الرئيسية، نتائج التحليل، والإجراءات المتخذة.

تقارير حالة الطوارئ: توثيق الحوادث الأمنية الطارئة، الاستجابة، والإجراءات التصحيحية التي تم اتخاذها.

4. توثيق الإجراءات

إجراءات الأمان: تسجيل تفاصيل السياسات والإجراءات الأمنية المعتمدة، بما في ذلك التحديثات والتحسينات.

الإجراءات التصحيحية: توثيق الإجراءات التصحيحية المتخذة لمعالجة المشكلات أو الثغرات الأمنية المكتشفة.

5. تسجيل التعديلات والتحديثات

تحديث السياسات: سجل التعديلات التي تمت على السياسات والإجراءات الأمنية نتيجة للمراجعات أو التقييمات.

تحسينات الأنظمة: توثيق أي تحسينات أو تغييرات تم إدخالها على الأنظمة الأمنية أو الأدوات المستخدمة.

6 .مراجعة وتقييم الأداء

مراجعة البيانات: قم بمراجعة البيانات والتقارير بشكل دوري للتأكد من دقتها وشمولها.

تقييم الأداء: تقييم الأداء بناءً على البيانات الموثقة للتعرف على النجاح والإجراءات التي تحتاج إلى تحسين.

7 .ضمان الأمان والتوافر

حماية البيانات: تأكد من أن بيانات التوثيق محمية من الوصول غير المصرح به والتلاعب.

النسخ الاحتياطي: إجراء نسخ احتياطي منتظم للبيانات والوثائق لضمان عدم فقدانها.

8 .تدريب الفرق

تدريب الموظفين: توفير التدريب للموظفين حول أهمية التوثيق وكيفية استخدام أنظمة التوثيق بشكل فعال.

مراجعة السياسات: ضمان أن الموظفين على دراية بسياسات التوثيق والإجراءات المتعلقة بالأمان.

9 .التواصل مع أصحاب المصلحة

مشاركة التقارير: تقديم التقارير والبيانات إلى الإدارة العليا وأصحاب المصلحة لضمان الشفافية والتواصل الفعّال.

تلقي التغذية الراجعة: جمع التغذية الراجعة من الأطراف المعنية لتحسين عمليات التوثيق والأداء الأمني.

10 .تحسين مستمر

مراجعة الوثائق: إجراء مراجعات دورية للوثائق والتقارير للتأكد من استمرارها في تلبية الأهداف والمتطلبات.

تحديث العمليات: تحسين عملية التوثيق بناءً على التقييمات والتغذية الراجعة.

الوحدة الثامنة

- المراجعة.

المراجعة الشاملة لجميع الوحدات التي تناولت إدارة المخاطر السيبرانية تتيح لنا فهمًا عميقًا وشاملاً للمفاهيم والأدوات والإجراءات التي يجب اعتمادها للحفاظ على أمان الأنظمة والمعلومات في العالم الرقمي. تبدأ رحلتنا مع فهم المخاطر السيبرانية، حيث تعرفنا على ماهية المخاطر السيبرانية وأشكالها المختلفة، مثل الفيروسات، والبرامج الضارة، والقرصنة الإلكترونية، والاحتيال الإلكتروني، والتجسس الإلكتروني، والهجمات الموزعة على الخدمة. هذه المخاطر تمثل تحديات يومية تواجه أي مؤسسة أو فرد يتعامل مع التكنولوجيا الرقمية.

عند تحديد وفهم هذه المخاطر، ننتقل إلى مرحلة تحليل وتقييم المخاطر السيبرانية. هنا نبدأ بتحديد الأصول السيبرانية التي تحتاج إلى حماية، مثل البيانات الحساسة، الأنظمة الحيوية، والشبكات. بعد ذلك، نقوم بتحليل التهديدات السيبرانية المحتملة التي قد تستهدف هذه الأصول، مثل الهجمات الإلكترونية أو استغلال الثغرات الأمنية. يعد تقييم الثغرات الأمنية جزءا مهمًا من هذه المرحلة، حيث يساعدنا على تحديد نقاط الضعف في أنظمتنا. بعد تحليل التهديدات وتقييم الثغرات، يتم تحديد المخاطر السيبرانية بناءً على مدى تأثير هذه التهديدات على الأصول المحددة. في نهاية هذه المرحلة، نقوم بتحديد الإجراءات الوقائية والتصحيحية التي يجب اتخاذها لتقليل هذه المخاطر وتطبيق نظام إدارة المخاطر السيبرانية بفعالية.

بعد التقييم، نأتي إلى الوحدة التي تتناول تقنيات تحليل المخاطر السيبرانية. في هذه الوحدة، ندرس تقنيات متنوعة مثل تقنية تحليل المخاطر الكمومية، التي تعتمد على تقنيات متقدمة مثل الحوسبة الكمومية، وتقنية تحليل المخاطر الإحصائية التي تستفيد من البيانات التاريخية والنماذج الإحصائية للتنبؤ بالمخاطر. تقنية تحليل المخاطر العكسية تركز على البحث في الأحداث السلبية السابقة لفهم كيفية وقوعها ومنع تكرارها، في حين أن تقنية تحليل المخاطر المعرفية تعتمد على فهم وتحليل السلوك البشري ودوره في المخاطر السيبرانية.

عند اكتمال فهم تقنيات التحليل، نصل إلى إدارة المخاطر السيبرانية، حيث نقوم بتطبيق كل ما تعلمناه حتى الآن. نبدأ بتحديد الأصول السيبرانية ثم نتابع بتحليل التهديدات وتقييم الثغرات، وصولًا إلى تحديد المخاطر الفعلية التي تواجهنا. من هنا، نحدد الإجراءات الوقائية والتصحيحية المناسبة ثم نطبق نظام إدارة المخاطر السيبرانية لضمان حماية مستمرة.

بمجرد إنشاء النظام الإداري، نبدأ في تنفيذ تطبيقات إدارة المخاطر السيبرانية من خلال استخدام أدوات مخصصة لتحليل المخاطر، وتصميم الأمن السيبراني، وإدارة المخاطر، وتنفيذ الأمن السيبراني، وتقييم المخاطر بشكل دوري لضمان فعالية النظام واستجابته للتحديات الجديدة.

ثم تأتي الوحدة التي تركز على القوانين واللوائح الخاصة بالأمن السيبراني. معرفة القوانين المعمول بها في البلدان المختلفة والمؤسسات سواء كانت حكومية أو خاصة هو أمر حيوي

لضمان الامتثال والالتزام بالمعايير الأمنية. تحليل المتطلبات الأمنية المفروضة من هذه القوانين يساعد على توجيه جهود الأمن السيبراني، وتطبيق معايير الأمن السيبراني بشكل يتماشى مع هذه المتطلبات. يتم كذلك تحديد الإجراءات الوقائية والتصحيحية لضمان التزام الأنظمة بالمعايير القانونية، وأخيرًا، نطبق نظام إدارة الأمن السيبراني الذي يضمن أن جميع الإجراءات تتماشى مع القوانين واللوائح المعمول بها.

أخيرا، نختتم بمراقبة الأداء الأمني. هنا نحدد معايير التقييم ونقوم بجمع البيانات اللازمة لتقييم الأداء الأمني بفعالية. تحليل هذه البيانات يتيح لنا فهم كيفية استجابة الأنظمة والممارسات الأمنية للمخاطر الفعلية، ويتم تقييم الأداء الأمني بشكل دوري لضمان فعاليته. بمجرد تحديد مجالات القوة والضعف، نقوم بتطبيق الخطط اللازمة لتعزيز الأمان ومن ثم مراقبة الأداء باستمرار. لا ننسى أهمية توثيق الأداء الأمني لضمان الشفافية والدقة، ما يعزز من القدرة على المراجعة والتحسين المستمر.

ختامًا، يمكننا القول إن إدارة المخاطر السيبرانية هي عملية متكاملة تبدأ بفهم المخاطر، مرورًا بتحليلها وتقييمها، ثم تطبيق أدوات وتقنيات الإدارة الفعالة، وصولًا إلى الامتثال للقوانين والمراقبة المستمرة للأداء. هذه المراحل مترابطة بشكل يعزز حماية الأصول السيبرانية ويضمن استجابة فعالة للتحديات الأمنية المتزايدة.

المراجع	١-	Risk Management in the Digital Era: A Guide to Mitigating "، "Cybersecurity Threats تاليف Gautam Kumawat النشر Apress : العام ٢٠٢١
	٢-	Cybersecurity Risk Management: A Complete Guide to " "Planning and Implementation٢٠١٩ :العام ،: Auerbach Publications الناشر : تاليف Donald L. Pipkin
	٣-	Andrea C. و: Merritt Maxim تأليف ،" Introduction to Simmons"Cybersecurity Risk Management"، الناشر Syngress : العام: ٢٠١٩