ج { وضع خطة حماية الأمن السيبراني لمؤسسة محددة

بعد الاطلاع على العديد من تهديدات الأمن السيبراني المختلفة التي يمكن أن تواجهها المنظمة، وطرق الحماية التي يمكن أن تستخدمها، ستدرس بعد ذلك كيفية تطوير خطة حماية الأمن السيبراني لتلبية احتياجات منظمة معينة.

تقييم الثغرات في أنظمة الحاسوب

المهارات

المهارات المعرفية/العمليات والإستراتيجيات المعرفية:

- التحليل
- التفكير الناقد

هناك عدد من الأدوات والأساليب المختلفة التي يمكن استخدامها لتقييم نقاط الضعف في أنظمة الحاسوب الخاصة بالشركة أو المنظمة.

أنواع الأدوات

فاحص المنفذ

تتيح المنافذ الشبكية لتطبيقات الحاسوب المختلفة الاتصال عبر الشبكة، إذا لم يكن المنفذ مطلوبًا (على سبيل المثال، إذا لم يتم تثبيت التطبيق الذي يستخدمه)، فيجب إغلاقه، ويتم ذلك عادةً بواسطة جدار الحماية. ومع ذلك، يمكن لفاحص المنافذ التحقق لمعرفة المنافذ المفتوحة والمغلقة. يوجد عدد من تطبيقات فاحص المنافذ المتاحة على الإنترنت، والتي تمكنك من فحص الشبكة باستخدام عنوان بروتوكول الإنترنت الخارجي أو فحص أجهزة الحاسوب الفردية داخل شبكة محلية.

مدقق السجل

سجل Microsoft Windows قاعدة بيانات تستخدمها كل تثبيتات نظام التشغيل Windows لتسجيل جميع الإعدادات المختلفة التي يستخدمها نظام التشغيل والتطبيقات. بعض أنواع البرمجيات الضارة تستخدم السجل. يمكن استخدام برامج فحص أو تنظيف السجل لاختبار سلامة السجل وتصحيح أي تناقضات.

ماسحات ثغرات المواقع الإلكترونية

تُستخدم هذه الأنواع من برامج الماسح الضوئي لفحص الخادم المستضيف لموقع إلكتروني والتأكد من أنه محمي بشكل صحيح. يمكنهم الكشف عن حقن SQL والعديد من الثغرات المعروفة في المواقع الإلكترونية. ويمكن العثور على العديد من ماسحات الثغرات المواقع الإلكترونية مجانًا على الإنترنت، على الرغم من أن التسجيل قد يكون مطلوبًا.

برنامج اكتشاف الثغرات الأمنية وإدارتها

تُعد هذه البرامج نوعًا متطورًا من برامج الأمان التي تراقب الشبكة الحاسوبية للشركة أو المنظمة وتبحث عن الثغرات والهجمات، حيث تُحلل البيانات التي تم جمعها بواسطة البرنامج بعدة طرق لمحاولة تحديد التهديدات وتنبيه مديري الأنظمة إليها. كما تقدم الاقتراحات المناسبة للإجراءات الواجب اتخاذها. يبحث البرنامج عادةً عن التكوينات الخاطئة عبر الشبكة والتي قد تسمح للمهاجمين باستغلال الثغرات الأمنية. ومن الأمثلة على هذا النوع من البرامج برنامج Microsoft Defender Advanced Threat Protection® (ATP).

تقييم ثغرات المستخدم

يمكن أن يكون المستخدمون سبب في تواجد ثغرة محتملة، ولا بد من تقديم تدريب منتظم لهم لتذكيرهم بالمخاطر المحتملة، وقد يلزم إجراء فحوصات (عمليات تدقيق) للتحقق من الامتثال. وتوجد عدة طرق يمكن للمستخدمين من خلالها أن يكونوا عرضة للخطر. يمكن أن تشمل الثغرات الأمنية الاقتصادية الابتزاز أو عروض المال لتوفير المعلومات، مثل كلمات المرور. بينما تشمل الثغرات المادية تدوين كلمة مرور على الورق أو فقدان بطاقة الهوية. وتشمل الثغرات الاجتماعية تقديم معلومات حساسة للأصدقاء.

مراجعة الطرف الثالث

كما هو الحال في العديد من التخصصات، قد يكون من الصعب اكتشاف الأخطاء في النظام أو الشبكة التي

صممتها أو أنشأتها بنفسك. ويتمثل النهج الأكثر فاعلية في الطلب من خبير خارجي أن يُراجع تصميم النظام أو الشبكة والتعليق حول مدى حمايتها من التهديدات الأمنية. ويجب أن يتم ذلك بشكل مثالي قبل تنفيذ النظام أو بدء تشغيله، بحيث يمكن حل أي مشكلات تم تحديدها قبل هذه النقطة.

مناقشة

ما نوع الهجمات التي يمكن أن يكون المستخدمون عرضة لها بشكل خاص؟

اختبار الاختراق

عند استخدام هذه الطريقة لاختبار النظام بحثًا عن الثغرات الأمنية، يحاول خبراء الأمن اختراق النظام باستخدام مجموعة من أساليب الهجوم الشائعة. ويُطلق على اختبار الاختراق أحيانًا اسم القرصنة الأخلاقية، نظرًا لأن القائم بالاختبار يستخدم التقنيات ذاتها التي يستخدمها المتسلل الخبيث لكن بهدف العثور على المشكلات حتى يمكن حلها. عادةً ما يجري خبراء أمن تكنولوجيا المعلومات التابعون لجهات خارجية اختبار الاختراق، وهم من يخططون أولًا لاختباراتهم بالاشتراك مع المنظمة قبل تنفيذها. وتستند الاختبارات في بعض الأحيان إلى سيناريوهات، مثل توصيل جهاز غير مصرح به بالشبكة. حيث تُجرى الاختبارات لمعرفة ما إذا تم تحديد الهجمات والإجراءات المتخذة في حال تم تحديدها. وبمجرد اكتمال الاختبار، يتم إعداد تقرير مفصل، ونظرًا لأن التهديدات تتغير طوال الوقت، من المهم أن يستخدم اختبار الاختراق أساليب الهجوم الأكثر شيوعًا في وقت الاختبار. يحافظ مشروع أمان تطبيقات الويب المفتوح (OWASP) على قائمة محدثة بأهم عشرة تهديدات أمنية على الويب بناءً على الهجمات الفعلية. كان الهجوم الأكثر شيوعًا في تقرير OWASP Top 10 لعام 2017 هو الهجمات من نوع الحقن مثل حقن SQL.

وقفة للتفكير

تصفح موقع OWASP (مشروع أمان تطبيقات الويب المفتوحة) الإلكتروني واطلع على أحدث قائمة لأكبر 10 تهديدات.

تلميح استخدم محرك بحث للبحث عن قائمة "OWASP top ten"

توسيع الأفق بالنسبة لكل نوع هجوم مدرج في قائمة أكبر 10 تهديدات، حدد الإجراءات التي يجب على المؤسسة اتخاذها لحماية نفسها من الهجوم.

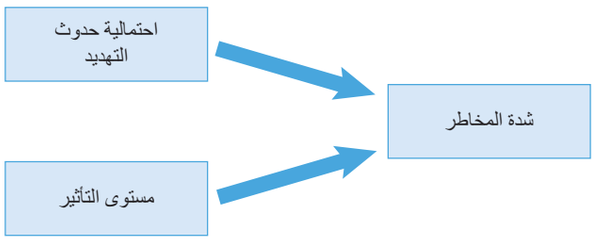
تقييم شدة المخاطر في كل تهديد

المهارات

المهارات المعرفية/العمليات والإستراتيجيات المعرفية:

- التحليل
- التفكير الناقد
- حل المشكلات

تعتبر المخاطر مفهومًا مهمًا عند النظر في خطة الأمن السيبراني، ويجب تقييم مدى خطورة كل خطر. وتجدر الإشارة إلى أن ليست كل التهديدات تستدعي القلق. كما يوضح الشكل 11.17، يمكن اعتبار شدة المخاطر مزيجًا من احتمالية حدوث التهديد والتأثير المتوقع في حالة حدوثه (أو قيمة الخسارة من الناحية المالية). ويمكن استخدام هذا لإنشاء مصفوفة مخاطر بناءً على احتمالية حدوث التهديد.



الشكل 11.17 تقييم شدة المخاطر

احتمالية حدوث التهديد

يُعد هذا التقييم بمنزلة تقييمًا تقريبيًا لمدى احتمالية حدوث التهديد، والذي يُقسم إلى "محتمل جدًا"، و"محتمل"، و"غير محتمل". ويمكن تقييم احتمالية الهجوم من خلال النظر في عاملين أساسيين:

الشخص أو المجموعة التي نفذت الهجوم

ما مستوى المهارة المطلوب للهجوم؟ وما الدافع وراء المكافأة؟ وما المكسب المالي؟ وما الموارد المطلوبة؟ وما حجم هذه المجموعة؟ إذا لم يكن استغلال التهديد مُمكنًا إلا من جانب المطورين أو مسؤولي النظام داخل الشركة، فإن المجموعة صغيرة. ومع ذلك، إذا كان التهديد يمكن لأي شخص على الإنترنت استغلاله، فإن المجموعة كبيرة. إذا كان التهديد لا يتطلب مهارات كبيرة، والدافع هو المكافأة المالية، ولا يتطلب معدات خاصة، ويمكن تنفيذه بواسطة أي مستخدم مصدق على النظام (مجموعة متوسطة الحجم)، فإن احتمالية حدوثه تكون "محتملة جدًا". وعلى الجانب الآخر، إذا كان التهديد يتطلب درجة عالية من المهارة، ولا يوجد مكسب مالي، ويتطلب إعدادًا معقدًا أو موارد، ولا يمكن استغلاله إلا من جانب مديري النظام، فحينها لا يُحتمل حدوثه.

التهديد نفسه

إلى أي مدى يمكن استغلاله بسهولة؟ وما مدى شهرته؟ وما مدى احتمالية اكتشافه؟ على سبيل المثال، بعض الثغرات الأمنية توجد لها أدوات قرصنة مؤتمتة متاحة عبر الإنترنت، ما يجعل من السهل استغلالها، كما يجعل احتمالية حدوثها "محتملة جدًا".

أثر حدوث التهديد

هناك نوعان من التأثيرات التي يجب مراعاتها، التأثير الفني والأثر التجاري، وهما مرتبطان ببعضهما البعض.

- **التأثير الفني** يشمل مقدار البيانات السرية المفقودة أو التالفة أو المدمرة. هل تأثر توفر الخدمة؟
- **الأثر التجاري** مثل مقدار الخسارة المالية المحتملة والأضرار المحتملة على السمعة وكمية البيانات الشخصية المفقودة.

يوضح الجدول 11.6 مثالًا لمصفوفة المخاطر.

الجدول 11.6 مثال على مصفوفة المخاطر

احتمالية الحدوث	تأثير التهديد		
	طفيفة	معتدلة	كبيرة
محتمل للغاية	متوسطة	مرتفع	شديدة
محتمل	منخفضة	متوسطة	مرتفع
غير محتمل	منخفضة	منخفضة	متوسطة

يمكن استخدام مصفوفة المخاطر هذه لمساعدتك على تقييم المخاطر في نظام معين.

متى يجب إجراء تقييمات المخاطر؟

يجب أن يتم تقييم المخاطر في البداية في أثناء مرحلة التصميم أو التخطيط للنظام. ويرجع السبب وراء ذلك إلى أن عملية المراجعة تسمح لك بالتحقق من أن النظام مصمم بطريقة توفر حماية كافية، لا سيما من تلك المخاطر التي تتمتع بدرجات خطورة أعلى. بمجرد تشغيل النظام، يجب إجراء تقييم المخاطر مرة أخرى على مدد منتظمة (على سبيل المثال، سنويًا) بوصفه أحد أشكال **التدقيق**. ويُعد هذه الإجراء ضروريًا لأن التهديدات تتغير، إضافة إلى أن التهديدات الجديدة تتطور طوال الوقت. كما قد يتطور النظام نفسه ويتغير، على سبيل المثال مع إدخال برامج جديدة أو إصدارات جديدة من البرامج الحالية.

طريقة تقييم المخاطر

تظهر خطوات إجراء تقييم المخاطر في الشكل 11.18.

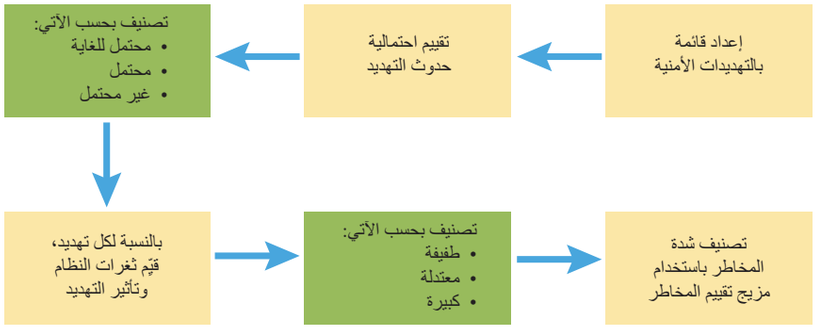
ويجب أن تكون النتيجة النهائية على شكل قائمة بالتهديدات، ولكل منها تصنيف خطورة، ما يوفر قائمة ذات أولوية من الأمور التي يجب التعامل معها. يجب معالجة طرق الحماية للتهديدات ذات الشدة القصوى أولًا،

بحث

غالبًا ما تُصنّف المخاطر باستخدام الطريقة الموضحة في مشروع أمان تطبيقات الويب المفتوحة (OWASP). ابحث عن ما تتضمنه المنهجية، بدءًا من هنا: https://owasp.org (منهجية تصنيف المخاطر)

المصطلح الرئيس

التدقيق – تقييم دوري للشؤون المالية لنظام ماء أو موارده أو كفاءته.



الشكل 11.18 خطوات تقييم المخاطر

ويمكن تحديد أسباب أي تكاليف مرتبطة بطرق الحماية بناءً على مستوى الشدة.

خطة الأمن السيبراني للنظام

بعد الانتهاء من تصنيف مخاطر الأمن السيبراني لمساعدتك على تحديد أولويات طرق الحماية، فإن الخطوة التالية هي وضع خطة مفصلة لتنفيذ الحماية. وقد تحتاج الخطة إلى موافقة إدارة المنظمة، ونظرًا لأنه من المحتمل أن تكلف هذه الخطة المال، فهم بحاجة إلى معرفة أن النفقات المعنية مبررة.

يجب أن تتضمن الخطة قائمة بطرق الحماية التي من المقرر تطبيقها على جميع المخاطر في فئات الخطورة الشديدة والعالية والمتوسطة. وتشمل طرق الحماية ما يأتي:

- **الأجهزة** - مثل جدران الحماية وأجهزة التوجيه ونقاط الوصول اللاسلكية
- **البرامج** - مثل مكافحة البرامج الضارة وجدار الحماية ومسح المنافذ وحقوق الوصول وتوافر المعلومات
- **الطرق المادية** - مثل الأقفال وكاميرات المراقبة (CCTV) وأجهزة الإنذار وتخزين البيانات والنسخ الاحتياطية.

إستراتيجيات إدارة المخاطر البديلة

بدلًا من الحماية من التهديد، يمكن تحديد خيار آخر مثل نقل المخاطر إلى شخص آخر، على سبيل المثال الاستعانة بمقاول جهة خارجية يعمل بوصفه مزود خدمة. ويحدث هذا عندما تستخدم المنظمة خدمات السحابة، حيث يتم نقل مسؤولية المخاطر المرتبطة بالخدمات إلى مزود الخدمة السحابية. وتشمل الاحتمالات الأخرى:

- إيقاف بعض الأنشطة لأنها تعتبر محفوفة بالمخاطر (على سبيل المثال حظر استخدام الذاكرة المحمولة USB) أو لأن تكلفة وسائل الحماية مرتفعة جدًّا.
- قبول المخاطر كما قد يتم في حالة المخاطر ذات الشدة المنخفضة.

مبررات طرق الحماية

يجب أن تتضمن كل طريقة حماية مخططة مبررًا لسبب الحاجة إلى الطريقة وكيفية حمايتها للنظام. ولا ينبغي أن يكون هذا المبرر تقنيًا صرف، وذلك نظرًا لأن الفئة المستهدفة للخطة هم على الأرجح مديرين كبار لا يُعدون خبراء تقنيين. ويعُد الأمر الأهم هو أن كل طريقة حماية مقترحة يتم تبرير استخدامها من خلال التهديد أو التهديدات التي تحمي منها.

القيود

يجب أن تتضمن كل طريقة حماية القيود الفنية والمالية المرتبطة بها، وتشمل القيود الفنية أي تأثير في تكوين أنظمة الأجهزة والبرامج الحالية وكفاءتها. كما تشمل أي قيود لطريقة الحماية مثل أنواع الهجمات

تطبيق النظرية

أجرِ تقييم أساسي للمخاطر على جهاز حاسوب تستخدمه أو تملكه مثل جهاز الحاسوب المحمول. وضع قائمة بأربعة أو خمسة تهديدات أمنية قد يتعرض لها جهاز الحاسوب المحمول (مثل فقده أو سرقته، أو تعرضه لهجوم برامج الفدية الضارة، وما إلى ذلك) ثم ضع تقديرًا لمدى احتمالية حدوث كل تهديد (على سبيل المثال، من المحتمل جدًّا سرقة جهاز حاسوب محمول أو فقده باستخدام المعايير الموضحة أعلاه). فكّر في تأثير هذا التهديد فيك (على سبيل المثال، إذا سُرق جهاز الحاسوب المحمول الخاص بك، فقد تفقد جميع أعمالك في المدرسة/الكلية) وحدد درجة شدة المخاطر لكل تهديد.

المهارات

المهارات المعرفية/العمليات والإستراتيجيات المعرفية:

- اتخاذ القرار
- التفكير الناقد
- التحليل

موضوعات ذات صلة

لمطالعة مزيد من المعلومات بشأن المسؤوليات القانونية، راجع **الوحدة 2: إنشاء أنظمة إدارة المعلومات**.

التي قد لا تحمي منها أو التحديثات اللازمة للحفاظ على مستوى الحماية بمرور الوقت. تشمل القيود المالية التكلفة التقديرية لتنفيذ طريقة الحماية.

المسؤوليات القانونية

يجب أن يشير هذا الجزء من الخطة إلى المسؤوليات القانونية للمنظمة بموجب تشريعات حماية البيانات.

قابلية الاستخدام

يمكن لبعض أنواع طرق الحماية أن يكون لها تأثير سلبي في قابلية استخدام النظام. على سبيل المثال، سياسات كلمات المرور الصارمة التي تتطلب كلمات مرور طويلة ومعقدة والتي يجب تغييرها بشكل متكرر، قد تكون آمنة جدًا لكنها صعبة جدًا للمستخدمين. وهذا ما قد يسفر عن ممارسات غير آمنة مثل تدوين كلمات المرور على وسائط مادية. كما تزيد سياسة كلمة المرور الصارمة من تكاليف دعم تكنولوجيا المعلومات عن طريق زيادة عدد المكالمات إلى قسم الدعم بسبب كلمات المرور المنسية. يمكن استخدام مشكلات قابلية الاستخدام هذه على أنها مبرر لإنفاق المزيد من الأموال لتنفيذ سياسة الحماية. ومع ذلك، فمن الأسهل استخدام أساليب المصادقة مثل المصادقة الثنائية.

دراسة حالة

عادةً ما تستخدم أنظمة المصادقة القياسية عاملًا واحدًا؛ وهو كلمة المرور. فكلمة المرور لا يعرفها إلا المستخدم. وتتطلب المصادقة الثنائية (2FA) من المستخدم إدخال عاملي مصادقة. حيث يوفر هذا مستوى أعلى من الأمن؛ لأن كلمة المرور وحدها لا تكفي للوصول إلى النظام. ويمكن أن يكون العامل الثاني عددًا من الأشياء المختلفة. فعلى سبيل المثال:

شيء يعرفه المستخدم - مثل رقم التعريف الشخصي.

شيء ما في حوزة المستخدم - مثل بطاقة الهوية أو الهاتف المحمول أو رمز الأمان

شيء شخصي - يُعرف باسم العامل البيومتري مثل بصمة الإصبع أو الوجه أو تعرف الصوت (يُسمى أحيانًا عامل الوراثة).

يُعد سحب الأموال من حسابك المصرفي باستخدام ماكينة الصراف الآلي مثالًا على المصادقة الثنائية، إذ يجب أن تعرف رقم التعريف الشخصي وأن تكون البطاقة المصرفية في حوزتك.

والطريقة الشائعة الأخرى التي تستخدمها البنوك لمصادقة أنواع معينة من المعاملات هي إرسال رمز في رسالة نصية SMS إلى رقم هاتف محمول مسجل. حيث يجب على صاحب الحساب المصرفي تسجيل رقم هاتفه المحمول قبل استخدام هذه الطريقة.

تصدر بعض المؤسسات رموز أمان للموظفين أو تستخدم تطبيق هاتف يقوم بإنشاء كلمات مرور للاستخدام الفردي (تسمى أحيانًا كلمات المرور المستخدمة لمرة واحدة (OTP)) والتي لا يمكن استخدامها إلا مرة واحدة، حيث يتم إدخالها مع كلمة مرور المستخدم لتسجيل الدخول إلى أنظمة المؤسسة.

اختبر معلوماتك

1 لماذا لا تُستخدم طريقة المصادقة الثنائية في نطاقٍ أوسع عند تسجيل الدخول إلى الحسابات عبر الإنترنت؟

2 ما طرق القرصنة التي يمكن أن تستهدف المصادقة الثنائية؟

تحليل التكلفة والمنفعة

سيرغب المدير الذي ستُعرض عليه الخطة في معرفة ما سيحصل عليه مقابل الأموال التي سيتعين إنفاقها. فينبغي أن تكون التكاليف واضحة بشكلٍ معقول من خلال الأجهزة والبرامج المطلوبة، ولكن قد يكون من الصعب تحديد الفوائد بدقة لأنها تتعلق بشكلٍ أساسي بتقليل المخاطر. كما يجب الإشارة إلى تقييم تأثير المخاطر المختلفة.

خطة الاختبار

ينبغي أن تتضمن خطة الأمان خطة اختبار. حيث يحدد هذا كيفية اختبار كل طريقة حماية للتأكد من عملها بشكلٍ صحيح. فعادةً ما تُقدَّم خطة الاختبار على أنها جدول، على النحو الموضح أدناه. تم تضمين بعض الاختبارات بالفعل في الخطة.

الجدول 11.7 مثال على خطة الاختبار

سيناريو الاختبار: اختبار إعدادات سياسة كلمة المرور عند إنشاء كلمة مرور جديدة				
رقم الاختبار	وصف الاختبار	النتيجة المتوقعة	النتائج الفعلية	الإجراءات
1	كلمة المرور = "welcome"	مرفوضة (قصيرة)		
2	كلمة المرور = "mypassword"	مرفوضة (غير معقدة)		
3	كلمة المرور = "?Gfh12nB"	قُبلت		
4				

لاحظ أن النتيجة الفعلية والإجراءات لا تكتمل إلا عند الانتهاء من الاختبار بالفعل.

فبمجرد الموافقة على الخطة وتنفيذ طرق الحماية المتفق عليها، تُستخدم خطة الاختبار لإجراء اختبارات فعلية على النظام المحمي.

السياسات الداخلية

لدى معظم المؤسسات، وخاصةً الكبيرة منها، عدد من السياسات والإجراءات المكتوبة التي تحدد ما يمكن للشركة والموظفين فعله وما لا يمكنهم فعله، وكيف ينبغي إنجاز مختلف المهام. ومن ثم ينبغي تضمين السياسات والإجراءات المتعلقة بالأمن السيبراني للتأكد من أن الموظفين على دراية بمسؤولياتهم في هذا المجال.

المهارات

العمليات والإستراتيجيات المعرفية:

- التحليل
- التفسير

متطلبات سياسة الأمن السيبراني

أنشأت المنظمة الدولية للمعايير (ISO) معيارًا لأنظمة إدارة أمن المعلومات يُعرف باسم ISO 27001. ويتضمن ذلك ضرورة أن يكون لدى المؤسسة سياسة لأمن المعلومات. ويتطلب معيار ISO 27001 أن تكون السياسة خاضعة لطريقة تحسين مستمر مثل **حلقة "خطط - نفّذ - تحقق - تصرف" (PDCA)**، وتشمل خطوات نهج PDCA ما يأتي:

- **خطط** – قبل إجراء أي تغييرات، تحتاج إلى تحديد ما تحاول تحسينه وكيف ستقيس التحسن. على سبيل المثال، قد ترغب في تغيير قواعد سياسة كلمة المرور. فسيتم قياس أي تحسن من خلال تقليل عدد المكالمات المتعلقة بكلمات المرور إلى إدارة تكنولوجيا المعلومات.
- **نفّذ** – تنفيذ التغيير.
- **تحقق** – استخدم المقياس المحدد في مرحلة التخطيط للتحقق مما إذا كان التحسين المتوقع قد تحقق أم لا.
- **تصرف** – إذا كانت نتيجة مرحلة التحقق هي نجاح التغيير، وقد لاحظت التحسين الذي حددته في مرحلة التخطيط، فإن التغيير يصبح دائمًا.

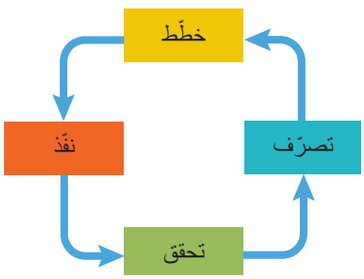
المصطلح الرئيس

حلقة "خطط - نفّذ - تحقق - تصرف" (PDCA) – نموذج متكرر مكون من أربع مراحل يُستخدم لإدخال تحسينات مستمرة في العملية أو النظام.

حلقة PDCA هي حلقة مستمرة، لذا بمجرد الوصول إلى مرحلة التصرف، ينبغي أن تكون هناك تحسينات إضافية على السياسة في مرحلة التخطيط.

ففي العديد من المؤسسات، قد تكون هناك العديد من السياسات المختلفة المتعلقة بالأمن السيبراني. ويمكن أن يشمل ذلك ما يأتي:

- **سياسة استخدام الإنترنت**: تحدد هذه السياسة ما يمكن للموظفين استخدام الإنترنت من أجله في أثناء الاتصال بشبكة LAN الخاصة بالشركة. كما ستدرج أنواعًا مختلفة من المواقع غير الملائمة التي يجب على الموظفين عدم زيارتها. وقد تحدد أيضًا قواعد تنزيل الملفات.



الشكل 11.19 حلقة "خطط نفّذ تحقق تصرف"

- **سياسة استخدام البريد الإلكتروني**: تنص هذه السياسة على قواعد آداب البريد الإلكتروني عند استخدام البريد الإلكتروني للشركة مثل المحتوى الذي ينبغي أن يكون احترافيًا ومهذبًا ومحترمًا. كما تحدد قواعد استخدام البريد الإلكتروني للشركة للرسائل الشخصية. وأخيرًا، فإنها تغطي إرشادات بشأن التعامل مع مرفقات البريد الإلكتروني والروابط واكتشاف رسائل البريد الإلكتروني المخادعة.
- **سياسة كلمة المرور وإجراءات الأمان**: تحدد هذه السياسة متطلبات كلمة المرور، بما في ذلك الطول والتعقيد وعدد المرات التي ينبغي تغييرها فيها وما إلى ذلك. كما تتضمن قواعد بشأن الحفاظ على أمان كلمات المرور مثل عدم مشاركتها وعدم كتابتها، وقد تشمل أيضًا إجراءات أمنية أخرى مثل استخدام المصادقة البيومترية أو المصادقة الثنائية. وقد تحدد هذه السياسات أو غيرها أيضًا قواعد لتدابير الأمان المادية المختلفة المستخدمة.
- **تدريب الموظفين**: من المهم أن يكون الموظفون على دراية بمحتوى سياسات أمن تكنولوجيا المعلومات الخاصة بالشركة. وعادةً ما يبدأ هذا بجلسة تدريبية كجزء من تعريفهم أو تأهيلهم عندما يبدؤون مع الشركة. وينبغي تحديث التدريب بانتظام، ربما سنويًا أو عندما يكون هناك تغيير في الإجراءات الأمنية، أو تحديد مشكلات جديدة أو وجود خرق أمني.
- **عمليات التدقيق**: تتمثل إحدى مشكلات السياسات والإجراءات المكتوبة في أنه يمكن حفظها ونسيانها بسهولة. ولضمان الامتثال المستمر بمرور الوقت، هناك حاجة إلى إجراء عمليات تدقيق. فيمكن لنظام التشغيل تطبيق بعض السياسات مثل سياسة كلمة المرور لكن قد تحتاج السياسات الأخرى إلى التحقق يدويًا من حينٍ لآخر.

مناقشة

لماذا من المهم للشركات أن تخضع موظفيها لتدريب على سياسات البريد الإلكتروني والإنترنت الخاصة بالشركة؟ ما أفضل طريقة لتقديم هذا التدريب؟ هل أنت على علم بهذه السياسات في مدرستك أو كليتك؟ هل خضعت لأي تدريب بشأنها، ربما في بداية الدورة؟

وقفة للتفكير

ما سياسة استخدام الإنترنت وسياسة البريد الإلكتروني الخاصة بمدرستك أو كليتك؟ هل لدى مدرستك أو كليتك سياسة لكلمة مرور؟ هل هناك أي إجراءات أمنية أخرى يجب عليك اتباعها مثل ارتداء شارات هوية الطالب؟ كان يجب شرح هذه الأمور لك في الدورة التعريفية.

تلميح

يجب أن تكون هذه السياسات متاحة على موقع مدرستك أو كليتك أو في دليل الطالب الخاص بك.

توسيع الأفق

ألقِ نظرة فاحصة على إحدى السياسات وناقش مع زميلك الغرض من القواعد. هل يمكن إضافة أي شيء أو شرحه بمزيد من التفصيل؟

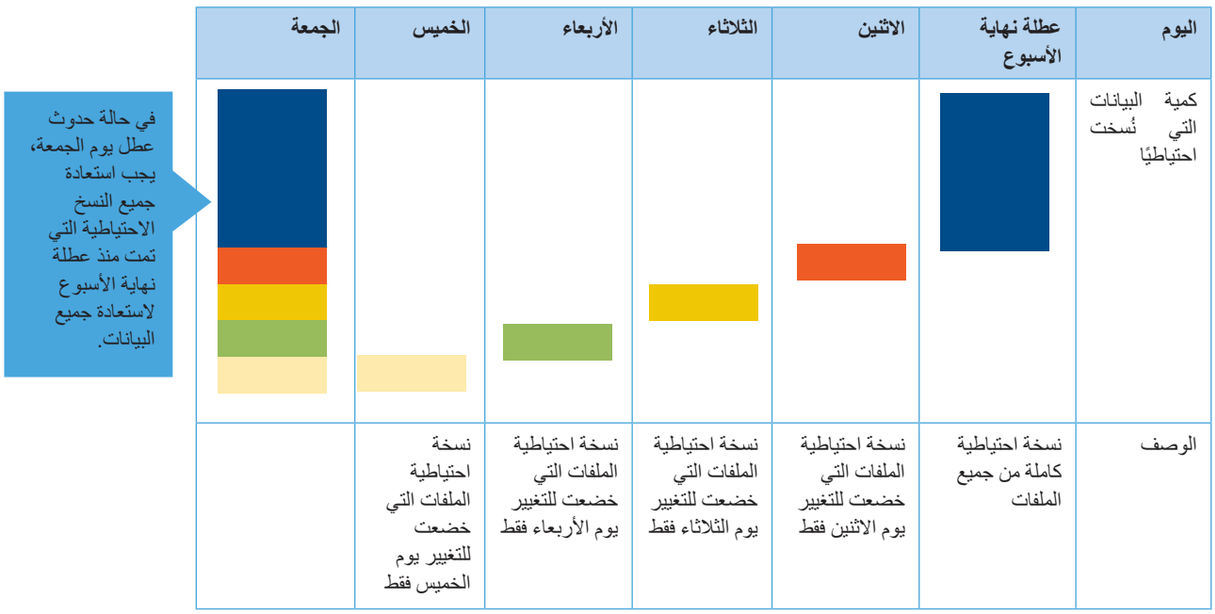
- **سياسة حماية البيانات**: يلزم توافر هذه السياسة لضمان امتثال المؤسسة لتشريعات حماية البيانات. فيجب أن تتوافق الإجراءات المدرجة في سياسة التعامل مع البيانات الشخصية مع المتطلبات الواردة في التشريعات ذات الصلة.
- **سياسة النسخ الاحتياطي**: يُعد النسخ الاحتياطي جزءًا أساسيًا من دفاع المؤسسة ضد فقدان البيانات، وبالتالي تستدعي الحاجة وجود سياسة واضحة لتحديد البيانات للنسخ الاحتياطي وطريقة النسخ الاحتياطي، إذ يتضمن **النسخ الاحتياطي الكامل** جميع بيانات المؤسسة. فرغم أنه يجب إجراء النسخ الاحتياطي الكامل في بعض الأحيان، نظرًا لأن نسبة كبيرة من البيانات لا تتغير كثيرًا، فإن النسخ الاحتياطي الكامل يُعد هدرًا ولذا عادةً ما يتم عمل نسخ احتياطي تزايدي بشكلٍ منتظم. حيث تأخذ عملية **النسخ الاحتياطي التزايدي** فقط نسخة احتياطية للبيانات التي تغيرت منذ النسخ الاحتياطي الأخير، وبالتالي يمكن فعل بذلك بسرعة أكبر من النسخ الاحتياطي الكامل على النحو الموضح في الشكل 11.20. وعادةً ما تجري المؤسسة نسخًا احتياطيًا كاملًا في عطلة نهاية الأسبوع ونسخًا احتياطيًا تزايديًا كل يوم من أيام الأسبوع. وتكمن المشكلة الوحيدة في هذا النهج، على سبيل المثال، في حالة فشل النسخ يوم الخميس. ومن أجل استعادة جميع البيانات، يجب استعادة النسخة الاحتياطية الكاملة لعطلة نهاية الأسبوع ثم جميع النسخ الاحتياطية التزايدية اليومية من الاثنين إلى الأربعاء.

ويعتمد عدد المرات التي تحتاج فيها المؤسسة إلى نسخ بياناتها احتياطيًا على مقدار البيانات التي يمكنها تحمل فقدانها. فمع نظام النسخ الاحتياطي اليومي المشار إليه أعلاه، يجب أن تكون المؤسسة على استعداد لخسارة ما لا يقل عن يوم واحد من البيانات. ففي بعض المؤسسات، مثل البنك، لن يكون هذا مقبولًا. أخيرًا، تحتاج السياسة إلى وصف مكان تخزين النسخ الاحتياطية. وكما ذكرنا سابقًا، لا يُقبل تخزين النسخ الاحتياطية في موقع البيانات نفسه، لأنه في حالة وقوع حدث خطير مثل نشوب حريق، يمكن فقد البيانات الأصلية والنُسخ الاحتياطية على حدٍ سواء.

المصطلحات الرئيسة

النسخ الاحتياطي الكامل – نسخة احتياطية كاملة من جميع الملفات الموجودة على القرص الصلب.

النسخ الاحتياطي التزايدي – نسخة احتياطية لجميع الملفات التي خضعت للتغيير منذ إجراء آخر نسخ احتياطي كامل.



الشكل 11.20 النسخ الاحتياطي التزايدي

سياسة الاستجابة للحوادث

عند وقوع حادث أمن سيبراني في مؤسسةٍ ما، فمن الطبيعي أن تكون هناك درجة من القلق ويلزم اتخاذ إجراءات عاجلة. ومن ثم يساعد وجود سياسة استجابة قبل وقوع الحادث على ضمان تنفيذ الإجراءات الصحيحة بطريقة سريعة وفعالة لمنع حدوث المزيد من الضرر للأنظمة والحفاظ على الأدلة على ما حدث. وينبغي أن تتضمن سياسة الحوادث ما يأتي:

- **فريق الاستجابة**: عند تحديد حادث، يتم تشكيل فريق الاستجابة لحوادث أمن الحاسوب (CSIRT) على الفور للتعامل مع الحادث. ويتضمن الفريق أدوارًا مختلفةً:
  - قائد الفريق: أحد كبار الموظفين الذي يمكنه الاتصال بأعضاء مجلس إدارة الشركة وإبقائهم على اطلاع دائم بالحادث.
  - قائد الحادث أو مديره: يتولى زمام المبادرة في الاستجابة التقنية التفصيلية والتحقيق، وعادةً ما يكون أحد أعضاء فريق تكنولوجيا المعلومات في الشركة، وغالبًا ما يكون مدير تكنولوجيا المعلومات.
  - الأعضاء المنتسبون: أعضاء فريق تكنولوجيا المعلومات في الشركة من أصحاب المهارات التقنية المطلوبة.
- **إجراءات الإبلاغ**: ينبغي أن يحدد هذا الجزء من السياسة نوع الحوادث التي ينبغي التعامل معها على أنها متعلقة بأمن الحاسوب وكيف يجب على الموظفين الإبلاغ عن حادثةٍ ما إذا اكتشفوها. كما تحدد هذه الفقرة أيضًا لمن يجب الإبلاغ عن الحادث.
- **التقييم الأولي**: يحدد هذا الإجراءات التي تُتخذ فور الإبلاغ عن الحادث، والخطوة الأولى هي التحقق مما إذا كان البلاغ يشير إلى حادث أمني حقيقي أم أنه **"إنذار كاذب"**.

فبمجرد تأكيد أن الحادث حقيقي، يتم تحديد نوع الهجوم وشدته (على سبيل المثال، عدد الأنظمة المتأثرة، وكيفية تأثرها، وما إلى ذلك).

الإبلاغ عن الحادث

بعد تأكيد وقوع الحادث، يجب التواصل مع فريق الاستجابة لحوادث أمن الحاسوب لبدء العمل على استجابتهم. كما ينبغي إخطار أعضاء مجلس إدارة الشركة بوقوع الحادث.

المصطلح الرئيس

إنذار كاذب – تحدث عندما يبلغ النظام عن مشكلة بشكل غير صحيح، مثل إبلاغ برنامج مكافحة الفيروسات عن نشاط مريب وهو في الواقع غير ضار.

إجراءات فريق الاستجابة لحوادث أمن الحاسوب

ينبغي أن تحدد السياسة الإجراءات التي يتعين على فريق الاستجابة لحوادث أمن الحاسوب اتباعها بالنسبة لأنواع مختلفة من الحوادث، بما في ذلك سرقة المعدات وسرقة بيانات الشركة والإصابة بالبرامج الضارة والوصول غير المصرح به إلى أنظمة الشركة وتلف الأنظمة أو فقدانها بسبب الحوادث المادية مثل الحريق أو الفيضانات. ومن المرجح أن تتضمن الإجراءات ما يأتي:

- **حماية سلامة الأشخاص**: في حالة نشوب حريق أو وقوع فيضان، ينبغي اتباع إجراءات إخلاء الشركة. فإذا كانت الأنظمة المعنية ضرورية للسلامة مثل الأنظمة الطبية بالمستشفيات أو مراقبة الحركة الجوية، تأتي سلامة المرضى أو الركاب على رأس الأولويات. ومع ذلك، غالبًا ما تكون أنظمة السلامة الحيوية محمية بترتيبات مختلفة وأكثر تعقيدًا من أنظمة الأعمال.
- **احتواء الضرر والحد من المخاطر**: وفقًا لنوع الحادث، قد يلزم إيقاف تشغيل الأنظمة وتعطيل الوصول إلى الشبكة وتعطيل حسابات المستخدمين وتغيير كلمات المرور.
- **حماية البيانات**: ينبغي أن تحدد السياسة الإجراءات التي يلزم اتباعها لحماية البيانات، على سبيل المثال عن طريق جعل محركات الأقراص غير متصلة بالإنترنت، بما في ذلك الأولوية من حيث ضمان حماية البيانات الأكثر حساسية وقيمة أولًا.
- **حماية الأجهزة والبرامج**: في حالة وقوع حادث مادي وكان من الآمن فعل ذلك، يمكن حماية أجهزة الحاسوب والبرامج الموجودة عليها عن طريق فصلها ونقلها إلى مكان آمن.
- **تقليل التعطيل**: بمجرد تحديد الأنظمة المتأثرة وعزلها، قد لا تتأثر الأنظمة الأخرى ولكن ربما تكون الخدمات التي تقدمها قد توقفت. كإجراء احترازي، ينبغي إعادتها إلى وضع الاتصال بالإنترنت لتقليل التعطيل في الشركة.
- **تحديد الحادث**: رغم أنه سيتم تحديد طبيعة الحادث في وقتٍ مبكر، إلا أنه ستكون هناك حاجة إلى مزيدٍ من التحقيق المفصل لتحديد الطبيعة الدقيقة للهجوم والغرض منه (على سبيل المثال، سرقة البيانات لتحقيق مكاسب مالية، أو تشفير البيانات للحصول على فدية، وما إلى ذلك) ومصدر الهجوم (على سبيل المثال، إذا كان داخليًا أو خارجيًا)، وكيف تم الوصول إلى الأنظمة وما الملفات التي تم اختراقها.
- **حماية الأدلة**: لدعم التحقيق الجنائي في الحادث، ينبغي الحفاظ على جميع البيانات ذات الصلة، والتي قد تشمل إنشاء نسخ احتياطية لصورة القرص للأقراص بأكملها بما في ذلك البيانات وأنظمة التشغيل للحفاظ على إعدادات التكوين وأي ملفات ربما استُخدِمت في الحادث.
- **إخطار الجهات الخارجية**: اعتمادًا على نوع الحادث، هناك مجموعة متنوعة من الجهات الخارجية التي قد يتعين عليك التواصل معها. ففي حالة سرقة المعدات أو البيانات، فقد يكون من المناسب التواصل مع جهة إنفاذ القانون (الشرطة). وفي حالة فقدان البيانات الشخصية، قد تواجه المؤسسة نفسها الملاحقة القضائية بموجب تشريعات حماية البيانات. وهذا يعني أنه قد تكون هناك حاجة للتمثيل القانوني والمشورة. فإذا حدثت مشكلة أمنية معقدة أو إصابة بالبرامج الضارة، فقد تحتاج الشركة إلى الاستعانة بخبراء الأمان والبرامج الضارة الخارجيين.
- **تعافي الأنظمة**: بمجرد التعامل مع الحادث بشكلٍ كامل وجمع جميع الأدلة المطلوبة والحفاظ عليها، يجب استعادة الأنظمة المتأثرة باستخدام النسخ الاحتياطية إذا لزم الأمر.

بعد الحادث

بمجرد الانتهاء من الإجراءات العاجلة لحماية الأنظمة واستعادتها، هناك بعض المهام المهمة الأخرى التي يلزم إنجازها وينبغي تضمينها في وثيقة السياسة.

توثيق الحوادث

ينبغي كتابة التقارير بشأن الحادث بأكبر قدر ممكن من التفاصيل. وينبغي أن تتضمن الوثائق تفاصيل الحادث، وما فعله فريق الاستجابة لحوادث أمن الحاسوب، وجميع

الإجراءات المتخذة لتحديد الحادث وحله. تُعد تفاصيل الحادث مهمة بشكلٍ خاص لأنها قد تكون ضرورية لمحاكمة الأشخاص الذين نفذوا الهجوم، لذا من المهم أن تكون دقيقة ومفصلة ومدعومة بالأدلة مثل الملفات والسجلات وما إلى ذلك.

جمع الأدلة

ينبغي جمع الأدلة عند الحاجة إليها لأسباب قانونية.

نتائج المراجعة

هناك جزء آخر مهم جدًا من سياسة الحوادث وهو أنها تتطلب مراجعة بعد الحادث. فيمكن أن يساعد ذلك على ضمان عدم وقوع حادث آخر مماثل مرة أخرى وتعلّم الدروس. كما ينبغي أن تقدم المراجعة توصيات لمنع وقوع المزيد من الحوادث مثل تغيير الإجراءات الأمنية، وزيادة الأمن وتحسين آلية تدريب الموظفين.

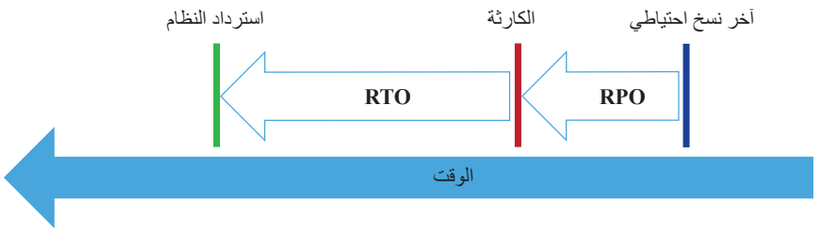
خطة التعافي من الكوارث

تشارك خطة التعافي من الكوارث بعض الميزات مع سياسة الحوادث الأمنية. ومع ذلك، يختلف الغرض منها قليلًا من حيث إنه تم إنشاؤها استعدادًا لكارثة مادية تدمر أنظمة الحاسوب أو تعطلها في المؤسسة، مثل حدوث حريق أو فيضان.

وينبغي أن تحدد خطة التعافي من الكوارث الأنظمة الحرجة. فلا تُعد جميع الأنظمة في الشركة بالغة الأهمية لعملياتها اليومية. ومن المحتمل أن تكون الأنظمة الحرجة عبارة عن أجهزة حاسوب خادم تُستخدم لإدارة أعمال الشركة. ويمكن تحديد مدى أهميتها للأعمال من خلال اتخاذ قرار بشأن السرعة التي ستحتاج بها إلى تشغيل الأنظمة مرة أخرى بعد وقوع كارثة.

- **هدف وقت التعافي (RTO)** هو مصطلح يُستخدم في التعافي من الكوارث لتحديد مقدار الوقت الذي يمكن أن تستغرقه الشركة دون خدمة بعد وقوع كارثة.
- **هدف نقطة التعافي (RPO)** هو مقدار البيانات (عادةً من حيث المعاملات) التي يمكن فقدها في حالة وقوع كارثة. وهذا هو مقدار الوقت منذ آخر عملية نسخ احتياطي. حيث يتم فقد جميع سجلات المعاملات الجديدة التي تم إنشاؤها بين آخر عملية نسخ احتياطي والكارثة.

الشكل 11.21 يوضح أهداف التعافي.



الشكل 11.21 هدف نقطة الاسترداد (RPO) وهدف وقت الاسترداد (RTO)

ينبغي أن تتضمن خطة التعافي من الكوارث أيضًا إستراتيجيات الوقاية والاستجابة والتعافي. فبالنسبة لكل نظام مهم، ستحتاج خطة التعافي من الكوارث إلى ذكر ما يأتي:

- مَن المسؤول عن إدارة تعافي النظام وتنفيذه.
- كيف سيتم تحقيق التعافي. عادةً ما يتضمن التعافي من الكوارث إعداد نظام مكرر للنظام الذي تم تدميره في موقع مختلف. فهناك عدد من الشركات التي تقدم خدمة التعافي من الكوارث ومقابل رسوم يمكن للشركة إعداد برامجها على الأنظمة الموجودة في مراكز البيانات الخاصة بها في حالة وقوع كارثة. وقد يكون لدى الشركات الكبيرة جدًا موقع بديل متاح داخل الشركة يمكن استخدامه في حالة وقوع كارثة.

- أين سيتم تخزين النُسخ الاحتياطية وبأي صيغة (على سبيل المثال، الأشرطة والأقراص الصلبة الخارجية والنُسخ الاحتياطية عبر الإنترنت). بالإضافة إلى النسخ الاحتياطي للبيانات، ستكون هناك حاجة إلى نسخ احتياطية كاملة من أحدث نظام مع تثبيت جميع التطبيقات والبرامج المرتبطة بها حتى يمكن تثبيت النظام الكامل في الموقع البديل.
- كيف سيتم توصيل الشبكة بالأنظمة البديلة. سيكون هذا عادةً عبر الإنترنت وستكون لدى شركات التعافي من الكوارث اتصالات إنترنت ذات سرعات أعلى متاحة للاستخدام.
- أين سيتم الحصول على أي معدات إضافية ضرورية (يتم شراؤها أو تأجيرها)، وكيف يمكن لأشخاص إضافيين مثل المقاولين المساعدة على إعداد النظام، ومن أين سيتم الحصول عليها.

سيحتاج كل نظام مهم إلى إجراءات مفصلة تصف كيفية إجراء التعافي.

تُطبِّق المنظمة الدولية للمعايير (ISO) معيارًا لأمن تكنولوجيا المعلومات، يُعرف باسم ISO 27031 (المعيار السابق ISO 24762)، والذي يتضمن قسمًا عن التخطيط للتعافي من الكوارث. الأجزاء المدرجة في الخطة:

- **مقدمة** – أهداف الخطة.
- **الأدوار والمسؤوليات** – مَن يفعل ماذا عندما تقع كارثة. ينبغي أن تتضمن الخطة مخططًا تنظيميًا وأوصافًا وظيفية لكل عضو من أعضاء فريق خطة الكوارث.
- **إجراءات الاستجابة للحوادث** – إدراج جميع الأجهزة والبرامج ومرافق الشبكة المضمنة في خطة الكوارث.
- **كيفية تنشيط الخطة** – إجراءات البدء في العمليات المحددة ضمن الخطة
- **الإجراءات** – إستراتيجيات التعافي لكل نظام مهم.

تشجع المنظمة الدولية للمعايير استخدام نهج "خطط-نفّذ-تحقق-تصرف" في خطة الكوارث.

مزودو الخدمة الخارجية

كما ناقشنا سابقًا، فإن أحد الخيارات لتجنب بعض المشكلات المرتبطة بالأمن السيبراني و التعافي من الكوارث هو استخدام طرف خارجي (يسمى مزود الخدمة الخارجية (ESP)) لتوفير خدمة الحوسبة الخاصة بالمؤسسة. ومع ذلك، فإن استخدام طرف خارجي لا يخلو من المشكلات، ولضمان حماية حقوق المؤسسة، يجب وضع اتفاقية بين المؤسسة ومزود الخدمة الخارجية تغطي الجوانب الآتية:

- **الخدمات السحابية** – مثل النسخ الاحتياطي السحابي والتخزين
- **الأجهزة** – توفر خدمات مثل Amazon Web Services وMicrosoft Azure أجهزة قائمة على السحابة يمكن للمؤسسات تشغيل تطبيقاتها عليها
- **البرامج** – يوفر مزودو الخدمة الخارجية عمومًا برامج لدعم تشغيل تطبيقات المؤسسة. على سبيل المثال، ستوفر شركة استضافة الويب عادةً خدمة Apache على الويب وقاعدة بيانات MySQL ولغة برمجة PHP إلى جانب خدمات البرامج الأخرى.

الآثار المترتبة على اتفاقيات مزود الخدمة الخارجية

هناك العديد من الآثار المترتبة على اتفاقيات مزود الخدمة الخارجية.

الملكية القانونية والولاية القضائية

أولًا، عليك التفكير في من يملك البيانات الموجودة على أجهزة حاسوب مزود الخدمة الخارجية. فنظرًا لأن البيانات قد توجد في بلد مختلف عن البلد الذي تعمل فيه المؤسسة، فمن المهم تحديد قوانين البلد المطبقة. كما تنص تشريعات حماية البيانات، على سبيل المثال، على أنه لا ينبغي نقل البيانات إلى بلد ليس لديه تشريعات

بحث

أجرِ بعض الأبحاث عن المعيار ISO 27031 لمعرفة المزيد عنه وما يجب تضمينه في خطة أمن تكنولوجيا المعلومات.

موضوعات ذات صلة

لمطالعة مزيد من المعلومات بشأن حلقة PDCA، راجع صفحة 177.

المهارات

المهارات المعرفية/العمليات والإستراتيجيات المعرفية:

- التحليل

مناسبة لحماية البيانات. وينبغي أيضًا الاتفاق على الإجراءات التي يلزم اتباعها عند انتهاء الاتفاقية. على سبيل المثال، هل سيتم إرجاع جميع بيانات المؤسسة وحذفها من أنظمة مزود الخدمة الخارجية؟

الحماية الأمنية

تحتاج المؤسسة إلى التأكد من أن مزود الخدمة الخارجية يدرك مسؤوليته عن الحفاظ على أمان بياناتها وخاصةً باستخدام الطرق المناسبة بما في ذلك التشفير. ويجب أن توضح الاتفاقية المبرمة بين مزود الخدمة الخارجية والمؤسسة مَن المسؤول عن أي انتهاكات للبيانات والمسؤولية القانونية التي سيتحملها مزود الخدمة الخارجية عن فقدان البيانات أو تلفها، سواء كان ذلك متعمدًا أو عرضيًا. على سبيل المثال، هل سيلتزم مزود الخدمة الخارجية بتعويض المؤسسة في حالة فقدان البيانات؟

حل النزاعات

يجب أن تتضمن الاتفاقية طريقة لحل النزاعات بين مزود الخدمة الخارجية والمؤسسة. فيجب أن يشمل ذلك المتطلبات القانونية (التشريعية) وأي مشكلات تحدث بسبب البيانات الموجودة في الولاية القضائية للعديد من البلدان المختلفة.

بموجب تشريعات حماية البيانات في الاتحاد الأوروبي، تُعرَّف المؤسسة التي تستخدم التخزين السحابي للبيانات الشخصية على أنها "وحدة التحكم في البيانات"، وبعبارة أخرى فهي مسؤولة عن كيفية التعامل مع البيانات حتى لو لم يكن لديها سيطرة كاملة عليها لأن مزود الخدمة الخارجية خزَّنها على السحابة. لذا، يجب على المؤسسة التأكد من أن مزود الخدمة الخارجية يأخذ مسؤوليات حماية البيانات على محمل الجد وأن هناك اتفاقية مكتوبة مع مزود الخدمة الخارجية للحفاظ على أمان البيانات.

مناقشة

ناقش مزايا وعيوب استخدام المؤسسة لمزودي الخدمة الخارجيين.

تمرين تقييمي 11.3 C.P6, C.P7, C.M3, CD.D2

حدد إحدى المؤسسات التي تعرفها جيدًا. ويمكن أن تكون كلية أو مدرسة التحقت بها أو شركة محلية.

- أجرِ تقييمًا للمخاطر يشمل التهديدات ونقاط الضعف التي يمكن أن تؤثر في المؤسسة.
- استنادًا إلى تقييم المخاطر، اكتب خطة الأمن السيبراني للمؤسسة، بما في ذلك طرق الحماية المقترحة لجميع المخاطر الشديدة والمرتفعة والمتوسطة الخطورة.
- برر اختيارك لكل طريقة تختارها لحماية المؤسسة من حيث قدرتها على الدفاع عن الأنظمة.
- اكتب تقييمًا لخطة الأمن السيبراني التي أعددتها للمؤسسة، ذاكرًا فيه الكيفية التي ستؤثر بها الخطة في سياسات الأمن الداخلي للمؤسسة وأيضًا كيفية تأثيرها في أيٍ من مزودي الخدمة الخارجية الذي تستعين به المؤسسة.

التخطيط

- ما المؤسسة التي ستختارها لإجراء تقييم المخاطر؟
- كيف ستجمع معلومات عن المؤسسة التي اخترتها؟
- ضع خطة زمنية تتضمن جميع المهام التي تحتاج إلى القيام بها لإنجاز المهمة، محددًا المدة التي ستستغرقها كل مهمة. تأكد من إنجاز المهمة بحلول تاريخ الموعد النهائي.

التنفيذ

- عند تبرير طرق الحماية التي اخترتها، تأكد من ذكر سبب اختيارك للطريقة، وعدم الاكتفاء بذكر الطريقة وكيفية عملها. وعليك أن تشرح **كيف** ستسهم في حماية النظام.
- عند كتابة التقييم، يجب عليك مناقشة مزايا وعيوب خطتك واستخلاص بعض الاستنتاجات عن كيفية تحسينها أو تطويرها بشكل أكبر.

المراجعة

- هل التزمت بالخطة الزمنية التي وضعتها؟ إذا لم يكن الأمر كذلك، فما المهام التي استغرقت وقتًا أطول من ما خططت له؟ كيف ستنشئ خطة زمنية أكثر دقة في المرة القادمة؟
- هل راجعت مهمتك لتصحيح أي أخطاء، مثل أخطاء الكتابة أو الأخطاء الإملائية أو النحوية؟

د فحص إجراءات جمع الأدلة الجنائية بعد وقوع الحادث الأمني

كما ناقشنا سابقًا، عند وقوع حادث أمني، من المهم أن يتم جمع الأدلة على ما حدث بشكلٍ صحيح.

جمع الأدلة الجنائية

المهارات

المهارات المعرفية/العمليات والإستراتيجيات المعرفية:

- التحليل
- حل المشكلات
- اتخاذ القرار

يلزم توافر دليل على وقوع حادث أمني لسببين رئيسين. أولًا، قد تكون هناك حاجة لدعم مقاضاة المتورطين. ثانيًا، إن الفهم الكامل لما حدث بالضبط سيساعد على تقليل احتمالية حدوثه مرة أخرى.

الإجراءات الجنائية المكتبية

يتضمن ذلك جمع الأدلة من الملفات الموجودة على جهاز حاسوب تعرض لخرق أمني. وسيتم أولًا عزل الحاسوب وإزالته، أو في حالة الحاسوب المحمول الفردي، ستتم مصادرته من الفرد. بعد ذلك، يمكن تطبيق العديد من التقنيات:

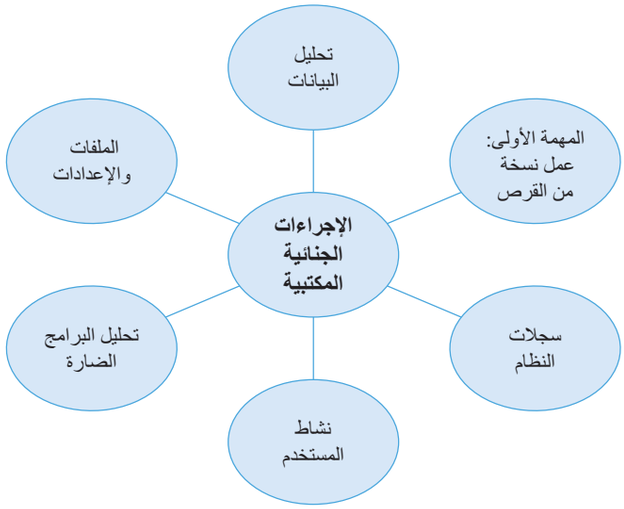
- **التقاط صورة** – هذه نسخة منخفضة المستوى من القرص بأكمله. يُعرف هذا باسم النسخة المكررة الجنائية. حيث يُوضع القرص الأصلي في وحدة تخزين آمنة. ويتم ذلك لإثبات أن عملية التحقيق لم تغير أي شيء على القرص.
- **تحليل البيانات** – يمكن فعل ذلك باستخدام عدد من الأدوات، والتي يمكنها، من بين أمور أخرى، استعادة الملفات المحذوفة. يمكن أيضًا إجراء عمليات البحث عبر جميع الملفات الموجودة على القرص للحصول على عبارة معينة ذات صلة أو لتصفية أنواع معينة من الملفات التي لا علاقة لها بالموضوع. على سبيل المثال، إذا كان يُعتقد أن الحاسوب متورط في هجوم حقن لغة SQL، فمن الممكن إجراء بحث عن أوامر SQL المختلفة ذات الصلة.
- **الملفات والإعدادات** – يتم التحقيق في إعدادات التكوين على الحاسوب. على سبيل المثال، قد يتم التحقق من وقت تثبيت آخر تحديثات نظام التشغيل وآخر تحديث لبرنامج مكافحة الفيروسات. كما يمكن إجراء عمليات التحقق من الملفات التي تم تنزيلها ورسائل البريد الإلكتروني، بما في ذلك المرفقات التي تم استلامها وفتحها.
- **سجلات النظام** – تحتفظ سجلات نظام التشغيل بالكثير من المعلومات بشأن الأحداث على الحاسوب. وتحتفظ سجلات أحداث Windows بتفاصيل زمنية للمستخدمين، عند تسجيل الدخول وعند حدوث محاولات تسجيل دخول غير ناجحة. كما أن أدوات تحليل سجل النظام متاحة أيضًا.
- **نشاط المستخدم** – يمكن تتبع نشاط المستخدم الفردي بعدة طرق. فيمكن تحديد الوقت الذي سَجّل فيه المستخدم الدخول والخروج من سجلات النظام. ويمكن تحديد الملفات التي قاموا بإنشائها وحذفها، بما في ذلك الملفات التي تم تنزيلها من الإنترنت. ويمكن أيضًا عرض البريد الإلكتروني وسجل تصفح الويب.
- **تحليل البرامج الضارة** – تحتفظ برامج مكافحة الفيروسات بسجلات التشغيل عندما يُجري المستخدم عمليات مسح للبرامج الضارة وعند تنزيل أحدث ملفات تعريف الفيروسات.

وقفة للتفكير

أنت تحقق في حادث أمني تضمن الوصول غير المصرح به إلى النظام. ما نوع المعلومات التي ستبحث عنها عند البحث في سجل الأحداث لعمليات تسجيل دخول المستخدم؟ ما الذي يمكن أن تخبرك به الكثير من محاولات تسجيل الدخول غير الناجحة؟

تلميح تكون إدخالات سجل الأحداث مختومة زمنيًا.

توسيع الأفق بخلاف أحداث تسجيل الدخول، ما الأدلة الأخرى التي قد تبحث عنها في موقف قد ينطوي على وصول غير مصرح به إلى النظام؟



الشكل 11.22 مراحل التحقيق الجنائي المكتبي

الإجراءات الجنائية المباشرة

الإجراءات الجنائية المباشرة هي عملية جمع المعلومات على جهاز حاسوب قيد التشغيل. وقد يكون هذا ضروريًا لأنه بمجرد إيقاف تشغيل الحاسوب يتم فقدان محتويات ذاكرة الوصول العشوائي (RAM). على سبيل المثال، يمكن فقدان البرامج الضارة التي تعمل في ذاكرة الحاسوب والتي قد تحتوي على أدلة مهمة (مثل عنوان IP الذي يتم الاتصال به) في حالة إيقاف تشغيل الحاسوب. بالإضافة إلى ذلك، تنشئ العديد من التطبيقات ملفات مؤقتة في أثناء تشغيلها (على سبيل المثال، Microsoft Word) والتي يتم حذفها عند إغلاق التطبيق. ومن ثم يتم فقدان العديد من المعلومات المهمة الأخرى مثل مفاتيح التشفير ورسائل الدردشة ومحتويات الحافظة واتصالات الشبكة المفتوحة من ذاكرة الوصول العشوائي عند إيقاف تشغيل الحاسوب. ويمكن استخدام برنامج التقاط ذاكرة الوصول العشوائي المباشر لتسجيل محتوى ذاكرة الوصول العشوائي لتحليله لاحقًا.

على سبيل المثال، إذا تم تشفير بيانات محرك أقراص حاسوب باستخدام أداة مثل Bitlocker، فلن يمكن قراءة بياناته (لأنها مشفرة) ما لم يتم تسجيل دخول مستخدم معتمد.

الإجراءات الجنائية للشبكة

من المحتمل أن تكون شبكة المؤسسة مصدرًا للاختراق الأمني، حيث يجد المتسللون طريقًا إلى شبكة LAN من الإنترنت. للتحقيق في كيفية التمكن من تنفيذ الهجوم، يجب اختبار الشبكة لتحديد التقنية الدقيقة المستخدمة. فقبل إجراء أي اختبار، ينبغي الاتفاق على منهجية اختبار الشبكة التي سيتم استخدامها مع الفريق الجنائي القائم بالإشراف والتحقيق في الحادث للتأكد من أنها مناسبة ومن الحصول على الإذن لإجراء الاختبارات. وهذا أمرٌ مهم لأن الاختبارات من المحتمل أن تحاكي الهجوم. ومن المهم أيضًا ألا يؤدي الاختبار إلى تعطيل النظام المباشر. على سبيل المثال، لا يُعد اختبار نظام مباشر من خلال محاكاة هجوم قطع الخدمة فكرة جيدة لأنه قد يمنع النظام المباشر من العمل. فيمكن جمع البيانات بشأن الاختبار باستخدام كل من الأدوات السلبية (جمع الأدلة من خلال مراقبة ما يحدث) والأدوات النشطة (إجراء التغييرات بنشاط وجمع النتائج).

كما يمكن فحص أجهزة البنية التحتية المختلفة على الشبكة وتحليلها، إذ يتم تكوين جدران الحماية بشكلٍ عام لإنشاء سجلات الاتصالات التي تقبلها وترفضها، وقد تعمل أجهزة التوجيه أيضًا على تجميع سجلات

مناقشة

ما نوع المعلومات التي قد تجدها في سجل جدار الحماية أو جهاز التوجيه وكيف يمكن أن تساعدك على معرفة المزيد عن الحادث الأمني؟

النشاط. ويمكن أيضًا مراجعة الإعدادات على الأجهزة مثل المحولات ونقاط الوصول اللاسلكية وستعرض سجلات تطبيقات مكافحة البرامج الضارة أي ملفات مشبوهة تم تحديدها. ستحتفظ بعض نقاط الوصول اللاسلكية بسجل للأجهزة المرفقة وستحتوي أيضًا على قائمة بعناوين MAC المسموح بها في حالة تمكين تصفية عناوين MAC.

المهارات

المهارات المعرفية/العمليات والإستراتيجيات المعرفية:

- التحليل
- حل المشكلات
- التفسير

التحليل الجنائي المنهجي لنظام مشبوه

لكي يكون من الممكن استخدام الأدلة الجنائية في مقاضاة الأشخاص المتورطين في هجوم ما، فلابد من جمع الأدلة بطريقة منهجية دقيقة مع تسجيل كل خطوة في تقرير مفصل.

وينبغي تدوين تفاصيل الحادث في أقرب وقت ممكن بعد وقوعه لتجنب احتمال نسيان الأشياء. حيث يحتاج فريق الاستجابة لحوادث أمن الحاسوب إلى تدوين الكثير من الملاحظات (التي يمكن كتابتها أو تسجيلها صوتيًا) بشأن كل ما يفعلونه ليتم كتابتها في تقريرهم في وقتٍ لاحق.

وينبغي جمع أكبر قدر ممكن من الأدلة في ما يتعلق بلقطات النظام، مثل لقطات الشاشة ونسخ السجلات والملفات. مرة أخرى، ينبغي فعل ذلك في أقرب وقت ممكن والاحتفاظ به للتحليل لاحقًا.

إذا تسببت التحقيقات في الحادث في أي تغييرات في النظام، إما عن قصد كجزء من عملية التحقيق وإما عن طريق الخطأ، فينبغي أيضًا ملاحظة ذلك بعناية.

اعتمادًا على طبيعة الحادث، يمكن إنشاء أدلة مرئية مثل الصور ومقاطع الفيديو.

فمن المهم التحقق من أن الأدلة تتعلق بالحادث الفعلي الذي وقع وليست إنذارًا كاذبًا. ويمكن فعل ذلك بعدة طرق، على سبيل المثال التحقق من المواعيد لمعرفة ما إذا كانت الأدلة مرتبطة بوقت وقوع الهجوم. ففي المراحل الأولى من التحقيق، قد تجمع أدلة لست متأكدًا من صلتها بالحادث، ولكن من الأفضل جمعها ثم إجراء تحليل مفصل لاحقًا للتحقق مما إذا كانت ذات صلة أم لا.

تقييم الأدلة

بمجرد جمع كل الأدلة، ينبغي تقييم كل عنصر.

- هل يقدم ذلك بالفعل أدلة على الجريمة أو الحادث؟
- هل يوضح كيف تم اختراق النظام من الخارج (خارجيًا) أو من داخل المؤسسة (داخليًا)؟
- هل يُظهر أن الهجوم تم بطريقة معينة بدلًا من الاحتمالات الأخرى؟

كجزء من تقييم الأدلة، يحتاج التقرير إلى شرح ما يظهره وتقديم وصف تفصيلي خطوة بخطوة لكيفية تنفيذ الهجوم.

وقفة للتفكير

اقتحم شخص ما غرفة الخادم وسرق أحد محركات الأقراص القابلة للإزالة من حاسوب الخادم. ما نوع الأدلة التي ستجمعها عن هذا الحادث؟

تلميح ما تدابير الأمان المادي التي قد تكون ذات صلة بهذا النوع من الحوادث؟

توسيع الأفق ما الذي يتعين على المؤسسة القيام به لاستعادة النظام في مثل هذه الحالة؟

التوصيات

كما ذكرنا سابقًا، من المهم أن يقدم التقرير الخاص بالحادث توصيات للمساعدة على تجنب مشكلات مماثلة في المستقبل. يمكن أن تشمل الآتي:

- **قد يلزم إجراء تغييرات على السياسات والإجراءات** مثل سياسة استخدام الإنترنت وأيضًا الاتفاقيات مع المؤسسات الخارجية مثل مزودي الخدمات السحابية

- **تدريب الموظفين** للتأكد من أنهم يفهمون متطلبات سياسات الشركة المتعلقة بأمن تكنولوجيا المعلومات ويلتزمون بها
- **أساليب الحماية الإضافية** بما في ذلك أساليب الحماية المادية والبرامج والأجهزة.

تمرين تقييمي 11.4 D.P8, D.M4, CD.D2

أنت تعمل في قسم تكنولوجيا المعلومات في إحدى المؤسسات وقد طُلب منك إعداد دليل للإجراءات الجنائية في حالة وقوع حادث أمني. ويجب أن يتضمن دليلك:

- شرح للإجراءات الجنائية التي يمكن استخدامها لجمع الأدلة بعد وقوع حادث أمني.
- تحليل لكيفية تنفيذ جميع الإجراءات الجنائية المختلفة المذكورة أعلاه على نظام يشتبه في تعرضه للهجوم في حادث أمني.

التخطيط

- ضع قائمة مرجعية لجميع الإجراءات الجنائية التي ستغطيها.
- أجرِ بحثًا لمعرفة أكبر قدر ممكن عن كل إجراء.

التنفيذ

- عند كتابة الشرح الخاص بك عن الإجراءات الجنائية، تأكد من تضمين أكبر قدر ممكن من التفاصيل.
- تذكر أنه لا يمكنك النسخ واللصق مباشرة من الكتب أو المواقع الإلكترونية؛ إذ يجب عليك إعادة كتابة المعلومات بكلماتك.
- عند كتابة تحليلك لكيفية تنفيذ الإجراءات، تذكر تضمين المزايا وأي عيوب محتملة وأيضًا مراعاة أنواع مختلفة من الحوادث الأمنية.

المراجعة

- كيف تحسنت مهاراتك في كتابة المهام (البحث والتخطيط والكتابة والمراجعة وإدارة الوقت وما إلى ذلك)؟ ما المجالات التي ما تزال بحاجة إلى تحسين؟
- كيف يمكنك تحسين العمل الذي قمت به في هذا الواجب؟
- كيف ستتعامل مع تقييمك المباشر بشكل مختلف؟

فكِّر في المستقبل

عمران حسين

تقني تكنولوجيا المعلومات

تمكن عمران من الحصول على فرصة تدريب مهني في شركة متوسطة الحجم بعد دوامه المدرسي، حيث يعمل في قسم دعم تكنولوجيا المعلومات. وعلى الرغم من أنه كان يدرك أن الأمن يمثل مشكلة كبيرة، فقد تفاجأ جدًّا بكمية طلبات مكتب المساعدة التي تلقاها والتي تتعلق بالأمن. فمشكلات الأمن تسهم في خلق الكثير من المتاعب للمستخدمين بطرق عديدة ومتنوعة. ويتعين على قسم دعم تكنولوجيا المعلومات إجراء الكثير من عمليات إعادة تعيين كلمات المرور لأن المستخدمين نسوا كلمات المرور الخاصة بهم وهو أمر محبط لكل من الفنيين والمستخدمين، ولكن سياسة الشركة تنص على أنه يجب على المستخدمين تغيير كلمات المرور كل ثلاثة أشهر. ويشعر بعض المستخدمين أن موظفي تكنولوجيا المعلومات يعقدون الأمور عليهم، ولكن الشيء المهم لقسم دعم تكنولوجيا المعلومات هو حماية البيانات الحساسة وأنظمة الشركة. وبعد ستة أشهر، توقف عمران عن دعم الخط الأول يعني عدم إعادة تعيين كلمة المرور، ولكن كان عليه بعد ذلك التعامل مع مشكلات تقنية أكثر تعقيدًا. والشيء الوحيد الذي يشعر أنه تعلمه هو أن العديد من مشكلات الأمن مثل تكوين جدار الحماية وتعيين أذونات المجلد معقدة للغاية، وقد يتسبب الفرد في خلق كثيرٍ من المشكلات إذا لم يكن يعرف ما يفعله، وقد تعلم عمران الكثير لكن ما يزال أمامه الكثير ليتعلمه. وتنظر إدارة الشركة التي يعمل بها عمران بقلق شديد إلى مشكلات أمن تكنولوجيا المعلومات وتذكّر موظفي تكنولوجيا المعلومات بانتظام بأنه من المرجح ظهور تهديدات جديدة وأكثر تعقيدًا في المستقبل لأن الوضع سيزداد سوءًا، وعلى موظفي تكنولوجيا المعلومات أن يكونوا على استعداد دائم.

تركيز مهاراتك

التخطيط للعمل في مجال تكنولوجيا المعلومات

من المحتمل أن يمثل الأمن مشكلة في أي وظيفة تفكر في أن تشغلها في المستقبل في مجال تكنولوجيا المعلومات وإذا كنت تخطط أن تشغل وظائف فنية مثل البرمجة أو تطوير المواقع الإلكترونية أو كفني تكنولوجيا معلومات، فإن فهمك للمسائل الأمنية في مجال تكنولوجيا المعلومات يجب أن يتعدى جوانب تحقيق الأمن للمستخدمين، مثل كلمات المرور القوية وإجراءات مكافحة البرامج الضارة. وإذا كنت تعمل في مجال أمن المواقع الإلكترونية أو تطوير البرامج، فهذه مشكلة ذات أهمية خاصة؛ لأنك تحتاج إلى معرفة كيفية دمج الجوانب المتعلقة بالأمن في المنتجات التي تعمل على تطويرها.

- نظرًا لأن أمن تكنولوجيا المعلومات يُعد مجالًا شديد الديناميكية، فأنت بحاجة إلى أن تبقى على اطلاع دائم على أحدث المشكلات الأمنية. وتعد متابعة مدونات التكنولوجيا إحدى طرق تحقيق ذلك. وثمة العديد من المدونات التي تتناول القضايا التكنولوجية المختلفة، ومن أشهرها Techdirt و Guardian Technology و Techworld و Krebs on Security.
- أجرِ بحثًا بنفسك عن مشكلات الأمن، مستهدفًا منه اكتساب معرفة تقنية متعمق عن آلية عمل بعض التهديدات الشائعة، مثل حقن SQL. وهناك الكثير من المعلومات حول جميع التهديدات الشائعة المتاحة على الإنترنت.
- إذا كنت قادرًا على الحصول على خبرات عملية (أو متابعة العمل) فإن هذا له العديد من الفوائد وسيوفر تجربة مفيدة للغاية يصعب الحصول عليها بأي طريقة أخرى. وستساعدك على فهم مشكلات الأمن من منظور المستخدم والتقني. يمكن أن تسبب المشكلات الأمنية - كما لاحظ عمران في عمله كمتدرب في مجال تكنولوجيا المعلومات - إحباط شديد للمستخدمين في كثيرٍ من الأحيان، لذلك فأنت بحاجة إلى تطوير مهارات التعامل مع الآخرين المطلوبة للتعامل مع المستخدمين الذين قد يشعرون بالضيق والغضب.