تعرُّف الوحدة

نظرًا لزيادة اعتمادنا على الإنترنت والأنظمة الحاسوبية في العديد من جوانب حياتنا، فقد أصبحت هذه الأنظمة هدفًا لمجرمي العصر، كما إنها صارت عرضة للاضطراب بسبب انقطاع التيار الكهربائي والحوادث والكوارث الطبيعية. يعد الحفاظ على أمان الأنظمة تحديًا كبيرًا؛ ولكن كلما تحسنت وسائل الأمان، كلما تطورت أساليب هجوم أكثر تعقيدًا.

بصفتك محترفًا في مجال تكنولوجيا المعلومات، يجب أن يكون لديك فهم جيد للتهديدات الأمنية الحالية والأساليب التي يجب عليك استخدامها للحفاظ على سلامة الأنظمة وأمانها؛ كما يجب أن تفهم أيضًا كيفية إنشاء خطة أمن سيبراني للمؤسسة. ونظرًا لأن أي تدابير حماية لا يمكن أن تكون فعّالة بنسبة 100%، يجب عليك أيضًا فهم الإجراءات التي يجب اتباعها لجمع الأدلة في حال وقوع حادث أمني.

ستتعرف في هذه الوحدة تهديدات الأمن السيبراني المختلفة الحالية وطرق الحماية التي يمكن استخدامها لمواجهتها، وستحقق أيضًا في الآثار الأمنية لأنظمة الحاسوب المتصلة بالشبكة. ستتعلم كيفية وضع خطة الأمن والحماية الإلكترونية لمؤسسة معينة، وستنظر في الإجراءات التي يجب استخدامها لجمع الأدلة الجنائية في حالة اكتشاف حادث أمني.

كيفية إجراء التقييم

ستجد في هذه الوحدة، أنشطة التمارين التقييمية التي ستساعدك على حل واجباتك، وإنجاز هذه الأنشطة لا يعني حصولك على درجة معينة، لكنك ستكون قد نفذت بحثًا أو تدريبًا مفيدًا في إطار استعدادك لواجبك النهائي.

لإنجاز المهام في واجبك بنجاح، لا بد من التأكد من استيفائك لجميع معايير درجة النجاح للمستوى، ويمكنك القيام بذلك إتمام الواجبات التي تُكلَّف بها. إذا كنت تهدف إلى تحقيق درجة التفوق أو الامتياز، عليك التأكد من تقديم المعلومات في واجبك بالأسلوب الذي تتطلبه معايير التقييم ذات الصلة، على سبيل المثال، تتطلب منك معايير التفوق التحليل والمناقشة، وتتطلب معايير الامتياز التقييم والتقويم.

سيتألف الواجب المحدد الخارجي من مهام بحثية وعملية مصممة لتلبية المعايير الواردة في جدول معايير التقييم، وسيتطلب منك هذا الواجب الاستجابة في سيناريو يفصِّل مؤسسة بعينها، وستحتاج إلى إعداد تقارير رسمية تتضمن:

- استكشاف تهديدات الأمن السيبراني وثغرات النظام والكيفية التي يمكن بها للمؤسسة تنفيذ تدابير أمنية لحماية نفسها منها
- تقييم أنواع الشبكات بالمؤسسة والثغرات الموجودة بها
- برنامج لتنفيذ خطة الأمن السيبراني وتقييمها لمؤسسة محددة
- فحص إجراءات جمع الأدلة الجنائية بعد وقوع الحادث الأمني

التقييم

سُتُقيَّم داخليًا باستخدام تقييمات Pearson المحددة.

معايير التقييم

يوضح لك هذا الجدول ما يجب عليك فعله من أجل الحصول على درجة النجاح أو التفوق أو الامتياز.

النجاح	التفوق	الامتياز
نتاج التعلم أ فهم تهديدات الأمن السيبراني وثغرات النظام وأساليب الحماية الأمنية		
A.P1 شرح تهديدات الأمن السيبراني المختلفة التي يمكن أن تؤثر في أنظمة تكنولوجيا المعلومات في المؤسسات. **تمرين تقييمي 11.1** **A.P2** شرح ثغرات النظام التي يمكن أن تؤثر في أنظمة تكنولوجيا المعلومات في المؤسسات. **تمرين تقييمي 11.1** **A.P3** شرح الكيفية التي يمكن بها للمؤسسات استخدام تدابير أمان البرامج والأجهزة لمواجهة التهديدات الأمنية. **تمرين تقييمي 11.1**	**A.M1** تقييم الأثر الذي يمكن أن تسببه تهديدات الأمن السيبراني في أنظمة تكنولوجيا المعلومات في المؤسسات مع مراعاة المتطلبات القانونية. **تمرين تقييمي 11.1**	**AB.D1** تقييم فعالية التدابير المستخدمة لحماية المؤسسات من تهديدات الأمن السيبراني مع مراعاة المتطلبات القانونية. **تمرين تقييمي 11.1** **تمرين تقييمي 11.2**
نتاج التعلم ب استكشاف الآثار الأمنية للأنظمة المتصلة بالشبكة		
B.P4 شرح الكيفية التي يمكن بها تأمين أنواع الشبكات ومكوناتها المختلفة. **تمرين تقييمي 11.2** **B.P5** شرح كيفية تأثير الأمن السيبراني في البنية التحتية للشبكات ومواردها. **تمرين تقييمي 11.2**	**B.M2** تحليل الآثار الأمنية لمختلف الأنظمة المتصلة بالشبكة. **تمرين تقييمي 11.2**	
نتاج التعلم ج وضع خطة حماية الأمن السيبراني لمؤسسة محددة		
C.P6 إجراء تقييم لمخاطر ثغرات النظام. **تمرين تقييمي 11.3** **C.P7** وضع خطة حماية الأمن السيبراني لنظام تكنولوجيا المعلومات في إحدى المؤسسات. **تمرين تقييمي 11.3**	**C.M3** تحديد أسباب اختيارات التدابير الأمنية المستخدمة للدفاع عن أنظمة تكنولوجيا المعلومات لإحدى المؤسسات. **تمرين تقييمي 11.3**	**CD.D2** تقييم خطة الأمن السيبراني، بما في ذلك أثرها في السياسات الداخلية ومزودي الخدمات الخارجية. **تمرين تقييمي 11.3** **تمرين تقييمي 11.4**
نتاج التعلم د فحص إجراءات جمع الأدلة الجنائية بعد وقوع الحادث الأمني		
D.P8 شرح الإجراءات الجنائية لجمع الأدلة بعد وقوع حادث أمني. **تمرين تقييمي 11.4**	**D.M4** تحليل كيفية تنفيذ الإجراءات الجنائية على نظام مشبوه. **تمرين تقييمي 11.4**	

بدء النشاط

بالتعاون في مجموعة صغيرة، ناقِش الأمن السيبراني بعبارات عامة، هل سبق لك أن واجهت أي مشكلة أمنية مع حاسوب استخدمته، مثل الإصابة بفيروس، أو هل تم اختراق حساب لك عبر الإنترنت؟ كيف اكتُشفت المشكلة وكيف تم التعامل معها؟ ما عواقب المشكلة الأمنية؟ كيف تحمي نفسك من الهجمات المستقبلية؟

نتاجات التعلم

ستتعلم في هذه الوحدة:

أ } فهم تهديدات الأمن السيبراني وثغرات النظام وأساليب الحماية الأمنية.

ب } استكشاف الآثار الأمنية للأنظمة المتصلة بالشبكة.

ج } وضع خطة حماية الأمن السيبراني لمؤسسة محددة.

د } فحص إجراءات جمع الأدلة الجنائية بعد وقوع الحادث الأمني.

أ } فهم تهديدات الأمن السيبراني وثغرات النظام وأساليب الحماية الأمنية

جميع أجهزة الحاسوب، بما فيها الأجهزة الرقمية مثل: الهواتف وأجهزة الحاسوب المحمولة والأجهزة اللوحية مُعرضة لمجموعة واسعة من تهديدات **الأمن السيبراني** والتهديدات الجديدة الناشئة بصفة دائمة. ومن الضروري حماية أجهزة الحاسوب والأجهزة الرقمية باستخدام مجموعة متنوعة من الطرق للحفاظ على أمانها قدر الإمكان.

المهارات

المهارات المعرفية/العمليات والإستراتيجيات المعرفية:

- التحليل
- التفسير

المصطلحات الرئيسة

الأمن السيبراني – حماية أجهزة وبرامج الحاسوب (بما في ذلك الأجهزة المحمولة مثل الهواتف الذكية) والبيانات التي تخزنها من خطر تلفها أو كشفها أو تعطيلها أو خسارتها، ويُعرف أيضًا باسم أمان الحاسوب أو تكنولوجيا المعلومات.

الوصول غير المصرح به – الوصول إلى أنظمة الحاسوب والبيانات المخزنة فيها من جانب الأشخاص الذين لا يُسمح لهم بالوصول إلى تلك الأنظمة والبيانات.

تهديدات الأمن السيبراني

يمكن أن تأتي التهديدات الأمنية من داخل المؤسسة (التهديدات الداخلية) أو من خارجها (التهديدات الخارجية).

التهديدات الداخلية

تشمل التهديدات الداخلية عادةً موظفي المؤسسة، الذين يتسببون في خرق أمني بإحدى الطرق الآتية:

- قد يقوم الموظفون غير الراضين عن الشركة أو المؤسسة لسبب ما بإتلاف أو تدمير البيانات أو المعدات المادية كشكل من أشكال الانتقام. على سبيل المثال، إذا فِصَل موظف أو سُرّح من عمله، فقد يحذف معلومات مهمة من أنظمة الحاسوب الخاصة بالشركة.
- قد يتمكن الموظفون من الحصول على **وصول غير مصرح به** إلى البيانات التي لا ينبغي لهم الوصول إليها، مثل: كشوف المرتبات أو المعلومات المالية. وقد يفعلون ذلك لتحقيق مكاسب شخصية؛ على سبيل المثال، قد يكونون قادرين على بيع معلومات المؤسسة السرية لأطراف خارجية، كمنافسي المؤسسة. وقد تسمح الإدارة غير الفعالة للمتعاقدين أو الشركاء أيضًا بالوصول إلى البيانات أو التدابير الأمنية التي لا ينبغي لهم أن يقدروا على الوصول إليها.
- قد تؤدي الإجراءات الأمنية الضعيفة أو الممارسات غير الآمنة إلى جعل المعدات عرضة للضياع أو السرقة. وقد يؤدي الفشل في الحفاظ على أمان غرف الحاسوب، كأن يكون ذلك عن طريق قفل الأبواب

M01_INFO_ST_55924_U11 Rev 3 FP 08 Aug_AR.indd 132 03/05/2025 12:17:51

وتقييد الوصول، إلى السماح للزوار أو الموظفين بسرقة الأجهزة. وتسمح الأجهزة المحمولة غير المؤمَّنة وغير المحمية بكلمة مرور للموظف بالوصول إلى البيانات السرية.

- قد يحذف الموظفون الذين لم يحصلوا على تدريب جيد على استخدام أنظمة تكنولوجيا المعلومات البيانات المهمة عن طريق الخطأ، كما يمكنهم الإفصاح عن المعلومات السرية الخاصة بالشركة لأشخاص خارج الشركة. على سبيل المثال، بعض معلومات التسعير (مثل سعر تكلفة المنتج وليس سعر البيع) تكون سرية في بعض الشركات. قد يُقدِم الموظف الذي لم يحصل على التدريب الكافي على الكشف عن هذه المعلومات عن طريق الخطأ إلى عميل خارجي أو منافس، كأن يكون ذلك عن طريق إرسال رسالة بريد إلكتروني مرفق بها معلومات التسعير.
- قد يقوم الموظفون عن غير قصد بتعريض الشركة لتهديدات أمنية خارجية بزيارة **مواقع إلكترونية غير موثوقة** أو فتح مرفقات لرسائل البريد الإلكتروني من مصادر غير موثوقة.
- يمكن لزوار المؤسسة أن يشكلوا تهديدًا. لذا، يجب وضع الإجراءات المناسبة للتحقق من أن الزوار لديهم سبب مشروع لوجودهم في المبنى وعدم تركهم بمفردهم. تحتاج المؤسسات -كالبنوك أو عيادات الأطباء- التي تتعامل مع الكثير من العملاء والمعلومات السرية إلى وضع احتياطات لمنع الإفصاح العرضي عن المعلومات. ويجب ترتيب شاشات الحاسوب الموجودة في مجال العرض العام بحيث لا يستطيع رؤية ما يُعرض على الشاشة سوى الموظفين والعملاء المعنيين فقط.

قد لا تكون بعض التهديدات الداخلية ناتجة عن تخريب الموظفين أو إهمالهم، ولكن بسبب قوى لا يمكنهم السيطرة عليها مثل: الحرائق والفيضانات والزلازل والكوارث الطبيعية الأخرى أو النشاط السياسي.

المصطلح الرئيس

المواقع الإلكترونية غير الموثوقة – المواقع الإلكترونية الضارة التي تدعوك لتنزيل برامج ضارة على حاسوبك أو تسعى للحصول على معلومات منك بخداعك.

التهديدات الخارجية

تُنفذ تهديدات الأمان الخارجية بأساليب مختلفة:

البرامج الخبيثة (أو الضارة)

وتشمل الآتي:

- **برامج التجسس** تجمع هذه البرامج المعلومات (عن عاداتك في تصفح الإنترنت غالبًا) دون موافقة المستخدم. ومن ثم تُستخدَم المعلومات التي جرى جمعها لاستهداف المستخدم بالإعلانات. تعتبر بعض أنواع برامج التجسس أكثر خطورة لأنها تتضمن برنامج مسجل نقرات المفاتيح (keylogger) والذي يسجل بالضبط ما يكتبه المستخدم على لوحة المفاتيح ويمرره إلى المجرمين. يمكن استخدام مسجلات المفاتيح لجمع أسماء المستخدمين وكلمات المرور.
- **البرامج الدعائية** – نوع من أنواع **البرامج الضارة** يعرض إعلانات منبثقة للمستخدم. ومثلها مثل برامج التجسس، قد تجمع بيانات عن عادات تصفح الإنترنت لتقديم إعلانات استهدافية. وعادةً لا يكون للبرامج الدعائية تأثير ضار في حاسوب المستخدم، ولكنها قد تكون مزعجة للمستخدم.
- **برامج الفدية** – يمكن أن يكون هذا النوع من البرامج ضارًا جدًّا ومدمرًا لنظام الحاسوب، وعادةً ما تصيب برامج الفدية الضارة جهاز حاسوب عبر مرفق بريد إلكتروني ثم تقفل ملفات المستخدم عن طريق **تشفيرها**. وبعد ذلك، يُطلب من المستخدم دفع فدية لتزويده بالمفتاح اللازم لفك تشفير الملفات.
- **الفيروسات** – تنتشر هذه الأنواع من البرامج الضارة عبر أنظمة الحاسوب والشبكات. ويمكن للعدوى الأولية التسلل للنظام بطرق مثل مرفقات البريد الإلكتروني أو من خلال زيارة المستخدم للمواقع الإلكترونية المصابة. ثم يقوم الفيروس بتكرار نفسه عبر أجهزة الحاسوب الأخرى على الشبكة. تتضمن أنواع الفيروسات ما يأتي.
  - الفيروس المتنقل: نوع من الفيروسات يستطيع نسخ نفسه عبر العديد من أجهزة الحاسوب، عادةً على شبكة.
  - فيروس الجذر: يختبئ هذا النوع من الفيروسات في حاسوب المستخدم ويسمح للمتسللين بالوصول إليه من بُعد.
  - فيروس حصان طروادة: برنامج يبدو أنه شرعي وغير ضار، ولكنه يخفي برنامجًا ضارًا.

المصطلحات الرئيسة

البرامج الضارة – برامج ذات مقصد ضار (سيئ) وقد تتسبب في تلف برامج حاسوبك أو بياناتك أو قد تجمع معلومات عنك.

التشفير – عملية ترميز البيانات حتى لا يمكن أن يقرأها أي شخص سوى الشخص الذي تُخصص له، وعادةً ما تُشفَّر البيانات باستخدام مفتاح يلزم توافره لفك تشفير البيانات.

M01_INFO_ST_55924_U11 Rev 3 FP 08 Aug_AR.indd 133 03/05/2025 12:17:51

دراسة حالة

برامج الفدية الضارة

CryptoLocker هو مثال معروف لبرامج الفدية التي كانت نشطة في المدة من سبتمبر 2013 حتى أبريل 2014. فقد انتشرت العدوى عن طريق مرفقات البريد الإلكتروني واستخدمت شيفرة Trojan التي استهدفت أجهزة الحاسوب التي تعمل بنظام Microsoft Windows. وعملت العدوى على تشفير ملفات الحاسوب وطالبت بدفع فدية بعملة البيتكوين لتوفير المفتاح لفك تشفير الملفات. وتشير التقديرات إلى إصابة نحو 250,000 جهاز حاسوب مكتبي. وفي عام 2017، حدث هجوم آخر من برنامج فدية يسمى Wannacry. واستخدم هذا الهجوم ثغرة أمنية في Microsoft Windows تم تصحيحها. أما المستخدمون الذين لم يطبقوا التصحيح، أو كانوا يستخدمون إصدارات غير مدعومة من Windows، مثل Windows XP، فقد أُصيبت أجهزة الحاسوب خاصتهم. وكانت هيئة الخدمات الصحية الوطنية (NHS) في المملكة المتحدة واحدة من أكبر المؤسسات التي تأثرت بالهجوم حيث أصيب ما يصل إلى 70,000 جهاز حاسوب والأجهزة المرتبطة به. وتم تتبع مصدر برامج الفدية إلى كوريا الشمالية.

اختبر معلوماتك

1 ما رأيك في تأثير مثل هذه العدوى في شبكات الحاسوب التي تستخدمها الخدمات الصحية الوطنية؟

2 لماذا تعتقد أنهم استُهدفوا؟

المصطلح الرئيس

المتسلل – شخص يحاول الحصول على وصول غير مصرح به إلى نظام حاسوب باستخدام مجموعة متنوعة من الأساليب المختلفة.

القرصنة

هي العملية التي يحاول فيها شخص ما (**المتسلل**) الوصول إلى نظام حاسوبي شبكي، ويمكن القيام بذلك لمجموعة من الأسباب. يحب بعض الأفراد محاولة اختراق الأنظمة كمغامرة فقط. ويعتزم البعض الآخر سرقة البيانات أو تدميرها. تُنفِّذ الحكومات أو الشركات أنشطة القرصنة أيضًا. القرصنة لأسباب تجارية هي محاولة لسرقة البيانات التي من شأنها أن تمنح المنافس ميزة، على سبيل المثال تفاصيل المنتج الجديد أو التسعير أو معلومات العملاء. وقد تستخدم الحكومات هجمات القرصنة لمحاولة جمع معلومات سرية من دول أخرى، مثل الأسرار العسكرية أو السياسية.

التخريب

يحدث هذا عندما لا تقوم البرامج الضارة أو المخترقة بالوصول إلى الأنظمة أو جمع البيانات فحسب، بل تسعى بنشاط إلى تعطيل الأنظمة بطريقة ما حتى لا تتمكن من العمل على النحو المنشود. ويمكن للأفراد تنفيذ هجمات التخريب، لأغراض الانتقام أو الابتزاز، أو أن تنفذها المؤسسات التجارية للحصول على ميزة تنافسية على الشركات المنافسة. ويمكن للحكومات شن حروب إلكترونية لتعطيل الأنظمة ذات الأهمية الإستراتيجية للبلدان الأخرى، كما يمكن تنفيذ هجمات التخريب لأغراض إرهابية، ما يتسبب في حدوث اضطراب وربما حتى الإصابة أو الوفاة عن طريق تعطيل الأنظمة المهمة.

دراسة حالة

هجوم قطع الخدمة (DoS)

هذا هجوم يهدف إلى تخريب موقع المؤسسة. فهو ينطوي على إغراق خادم الويب الخاص بالموقع بعدد كبير من الطلبات بحيث يصبح غير قادر على الاستجابة للطلبات الحقيقية. ما يؤدي إلى إيقاف الموقع وتحويله إلى وضع غير متصل بالإنترنت فعليًا. وتستخدم النسخة الشائعة من هذه الهجمات أعدادًا كبيرة من أجهزة الحاسوب (غالبًا ما تكون مصابة ببرامج ضارة في ما يُعرف باسم شبكة الروبوتات) لإغراق خادم الويب المستهدف. كما أن استخدام العديد من أجهزة الحاسوب المختلفة في الهجوم يجعل من الصعب على خادم الويب التمييز بين حركة المرور المشروعة والضارة. ويُطلق على هذه الهجمات أحيانًا اسم هجوم قطع الخدمة الموزع (DDoS). ونظرًا لأن العديد من المؤسسات مثل Amazon تعتمد بشكلٍ كبير على مواقعها الإلكترونية لإنجاز أعمال تجارية، فإن هجمات قطع الخدمة تشكل تهديدًا خطيرًا. ثمة عدد من الأسباب التي تدفع الأشخاص إلى القيام بهجمات قطع الخدمة.

اختبر معلوماتك

1 ماذا يمكن أن يكون الدافع لهجوم قطع الخدمة؟

2 لماذا يشن الأشخاص هجمات قطع الخدمة على الشركات الكبيرة مثل Amazon بدلًا من الشركات الصغيرة؟

M01_INFO_ST_55924_U11 Rev 3 FP 08 Aug_AR.indd 134 03/05/2025 12:17:51

دراسة حالة

التصيد الاحتيالي

يُعد التصيد الاحتيالي تهديدًا للهندسة الاجتماعية وهو شائع جدًّا وغالبًا ما يستهدف مستخدمي الخدمات المصرفية عبر الإنترنت. حيث يُعِد المجرمون صفحة ويب تشبه صفحة تسجيل الدخول لخدمة بنك شرعي عبر الإنترنت. ثم يرسلون رسالة بريد إلكتروني إلى أعداد كبيرة من الأشخاص (غالبًا ما يستخدمون قوائم رسائل البريد الإلكتروني التي تم جمعها من الهجمات الإلكترونية الأخرى) لإخبار هؤلاء المستخدمين أنهم بحاجة إلى تسجيل الدخول إلى حسابهم عبر الإنترنت باستخدام الرابط المقدم في رسالة البريد الإلكتروني. وينقل الرابط مستلم رسالة البريد الإلكتروني إلى الصفحة المزيفة، حيث يُدخِل معلوماته لتسجيل الدخول إلى الخدمات المصرفية عبر الإنترنت، والتي يجمعها المجرمون بعد ذلك. بعد ذلك، يمكنهم استخدام معلومات تسجيل الدخول للوصول إلى الموقع المصرفي الحقيقي وربما سرقة الأموال. وانخفض هذا التصيد الاحتيالي في السنوات الأخيرة بسبب الوعي بالتهديد والأساليب التي بدأت البنوك في استخدامها لمواجهته.

اختبر معلوماتك

1. هل سبق لك أن تعرضتَ لهجوم تصيد احتيالي؟
2. إذا تمكنتَ من اكتشاف أنه كان هجوم تصيد احتيالي، فكيف عرفتَ ذلك؟

وقفة للتفكير

ما الأسباب المختلفة التي تجعل الناس يحاولون اختراق الأنظمة؟ هل لدى المتسللين دائمًا نية خبيثة؟ ابحث عن معنى مصطلح «قرصان القبعة البيضاء» لمعرفة ماهيته ولماذا يتم هذه القرصنة أحيانًا.

تلميح

المكاسب المالية ليست الدافع الوحيد للقرصنة.

توسيع الأفق

فكّر في الطرق التي تختلف بها تهديدات الهندسة الاجتماعية عن الطرق الأخرى للتهديد الأمني. لماذا يصعب الدفاع عن تهديدات الهندسة الاجتماعية؟

تهديدات الهندسة الاجتماعية

يحدث هذا من خلال مجموعة من الوسائل الخارجية والداخلية. تتضمن هذه الهجمات محاولة مهاجم خارجي خداع موظف داخلي للإفصاح عن معلومات الشركة التي يجب أن تظل آمنة وسرية. ويمكن أن يكون هذا الهجوم بسيطًا مثل قيام المهاجم بالاتصال بالشركة، مدعيًا أنه من قسم دعم تكنولوجيا المعلومات وطلب اسم المستخدم وكلمة المرور. ويعتمد هذا النوع من الهجمات على الافتراض الطبيعي لدى الناس بأن الآخرين يقولون الحقيقة، ولذلك يمكن أن يكون فعالًا للغاية.

تأثير التهديدات

يتسبب مصدر التهديد الذي ينجح في الحصول على وصول غير مصرح به إلى نظام الحاسوب في حدوث خسارة للمؤسسة بشكل أو بآخر. قد تتضمن الخسارة التي تكبدتها المؤسسة عدة أنواع مختلفة.

الخسارة التشغيلية

عندما تتعرض أنظمة المؤسسة **لهجوم سيبراني**، فمن المحتمل جدًّا أن تحدث بعض الأعطال، ما سيتسبب في عدم إتاحة الأنظمة لبعض الوقت أو على الأقل يضعف من أدائها. ويمكن أن يتراوح هذا من الاضطراب الطفيف الذي قد يسببه فيروس غير ضار نسبيًا، إلى الاضطراب الكبير الناجم عن هجوم برامج الفدية الذي يحجب كل بيانات المؤسسة أو جزء منها. يمكن أن تؤدي كارثة كبيرة مثل الحريق أو الفيضان إلى تدمير أنظمة الحاسوب الخاصة بالمؤسسة. وتعتمد معظم المؤسسات بشكل كبير على أنظمة الحاسوب، لذلك من المحتمل جدًّا أن يكون لتعطيلها تأثير كبير في قدرتها على إدارة عملياتها. على سبيل المثال، ستعاني شركة التصنيع التي تعتمد على أنظمة التصنيع المحوسبة من خسارةً في الإنتاج التصنيعي. وسيعاني الموقع الإلكتروني الذي يتعرض لهجوم حجب الخدمة (DoS) نقصًا في توافر الخدمة، أما الذي يتعرض لهجوم المتسللين فقد يعاني فقدان بيانات الخدمة المهمة.

M01_INFO_ST_55924_U11 Rev 3 FP 08 Aug_AR.indd 135 03/05/2025 12:17:51

الخسارة المالية

من المحتمل أن يكون للخسارة التشغيلية تأثير مالي. إذا كانت المؤسسة غير قادرة على تنفيذ عملياتها، مثل تقديم خدمة أو توزيع المنتجات، فلا يمكنها تقاضي رسوم من العملاء مقابل هذه العمليات. وقد تتكبد المؤسسة خسارة مالية إن اضطرت إلى توظيف خبراء متخصصين في الأمن السيبراني للتحقيق في المشكلات الأمنية وحلها واستبدال المعدات التي تعرضت للسرقة أو التلف أو التدمير. واعتمادًا على نوع الهجوم وتأثيره، قد تكون الشركة مسؤولة عن دفع تعويضات للعملاء الذين يعانون عدم توافر منتجاتها أو خدماتها. على سبيل المثال، يجبر القانون شركات خطوط الطيران والسكك الحديدية في بعض البلدان على دفع تعويضات للعملاء في حالة تأخر رحلاتهم. وقد تواجه الشركات أيضًا غرامات كبيرة في حالة فقدان البيانات الشخصية في هجوم بسبب التزامها القانوني بالحفاظ على أمان هذه البيانات.

خسارة السمعة

يُحتمل أن تخسر إحدى المؤسسات سمعتها إذا لم تتمكن من حماية معلومات الخدمة أو الموظف أو العميل في أثناء تعرضها **للهجوم السيبراني**. قد يتم الإبلاغ عن هجوم إلكتروني كبير في نطاق واسع، ومعرفة أن الشركة تعرضت لهجوم إلكتروني يضر بسمعتها بلا ريب. بل إن هذا قد يدفع الناس إلى رفض التعامل مع تلك الشركة، لأنه يثبت أن أنظمة الحاسوب لديها ليست محمية بشكل كافٍ. على سبيل المثال، تحتاج أي شركة تبيع المنتجات عبر الإنترنت إلى أن يقوم العملاء بإدخال أرقام بطاقات الائتمان أو الخصم على موقعها الإلكتروني. وقد لا يرغب العملاء في القيام بذلك إذا عرفوا أن الشركة كانت ضحية لهجوم سيبراني فقدت فيه البيانات. وقد لا يرغب الموظفون المحتملون في العمل لدى شركة إذا كانوا يعتقدون أن معلوماتهم الشخصية قد تكون في خطر.

خسارة الملكية الفكرية

قد تقع الشركة ضحية لهجمات لها دوافع تجارية؛ وقد تفقد الشركة تصميمات المنتجات الجديدة أو الأسعار السرية أو بيانات العملاء أو الأسرار التجارية، مثل تفاصيل مكونات المنتجات الغذائية أو تركيبات الطلاء.

مستويات التأثير

يعتمد مدى تأثير الهجوم الناجح في المؤسسة بقدر كبير على قيمة الخسارة التي تتكبدها. فقد يتسبب الهجوم في خسارة مالية مباشرة، كأن يتمكن الهجوم من الوصول إلى الحساب البنكي للشركة وسرقة أموالها. أو قد يكون له تأثير مالي غير مباشر، مثل خسارة الإنتاجية لأن الموظفين غير قادرين على تنفيذ المهام في أثناء حل المشكلات الناجمة عن الهجوم.

تهديدات الأمن السيبراني عبر الزمن

الأمن السيبراني يتغير باستمرار والتهديدات الأمنية تتفاوت. لذا تحافظ مؤسسات الأمن السيبراني على مواكبة أحدث التهديدات والحلول، وتقدم تحديثات منتظمة لعملائها.

المصطلحات الرئيسة

الهجوم السيبراني – محاولة خبيثة لتعطيل أجهزة الحاسوب أو سرقة البيانات أو استخدام جهاز حاسوب لشن هجوم بطريقة أخرى.

الملكية الفكرية – "الملكية" التي تترتب على الإبداع في الأعمال مثل: الاختراعات والأعمال المكتوبة (الكتب) والعمل الفني (الأعمال الفنية) وأعمال الموسيقى والرموز والأسماء والصور.

وقفة للتفكير

ماذا يمكن أن يكون تأثير الهجوم عبر الإنترنت عليك؟

ماذا سيحدث في حالة تدمير جميع البيانات الموجودة على الحاسوب المحمول أو الحاسوب الذي تستخدمه في المنزل أو في المدرسة/الكلية؟

ماذا لو تم اختراق حساب بريدك الإلكتروني؟ أو حساب وسائل التواصل الاجتماعي خاصتك (مثل فيسبوك)؟

تلميح راعِ الوقت والجهد اللازمين لاستبدال البيانات المفقودة.

توسيع الأفق ماذا لو تمت سرقة بعض البيانات المالية الخاصة بك في الهجوم، مثل أرقام الحسابات المصرفية أو بطاقات الائتمان؟ هل أنت على علم بسياسة بنكك بشأن الأموال المسروقة منك في هجوم إلكتروني؟

M01_INFO_ST_55924_U11 Rev 3 FP 08 Aug_AR.indd 136 03/05/2025 12:17:51

ثغرات النظام

يمكن للمتسللين والبرامج الضارة استغلال الثغرات الأمنية لخرق الإجراءات الأمنية للنظام الحاسوبي. ويتكون النظام الحاسوبي المتصل بالشبكة من مجموعة متنوعة من المكونات العتادية والبرمجية، والتي من المحتمل أن تحتوي جميعها على ثغرات.

توجد تهديدات مختلفة وثغرات مختلفة بحسب نوع الحاسوب أو النظام الحاسوبي.

ثغرات الشبكة

قد تحاول العديد من مصادر التهديد الخارجية، مثل المتسللين، الوصول إلى النظام الحاسوبي من خلال اتصاله الخارجي بالإنترنت، وعادةً ما تكون الاتصالات الخارجية محمية بواسطة **جدار الحماية**. وتوفر أجهزة التخزين الخارجية مثل شرائح ذاكرة الناقل التسلسلي العالمي (USB) طريقة أخرى يمكن للبرامج الضارة من خلالها دخول نظام الشبكة. فيمكن أن يؤدي استخدام شريحة ذاكرة USB مصابة إلى ظهور برامج ضارة، كالفيروسات المتنقلة، والتي يمكن أن تنتشر في جميع أنحاء الشبكة.

الثغرات التنظيمية

هناك عدة أنواع من الثغرات الأمنية المرتبطة بالطريقة التي تقوم بها المؤسسة بإعداد أنظمة الحاسوب المتصلة بالشبكة:

أذونات الملفات والمجلدات

تميل الشركات التي تقوم بتشغيل نظام حاسوب شبكي مع خادم ملفات عادةً إلى تقييد الوصول إلى الملفات باستخدام أنظمة أذونات الملفات والمجلدات المضمنة في أنظمة تشغيل الخادم مثل ويندوز سِرفر (Windows Server) ولينكس (Linux). باستخدام أذونات الملفات والمجلدات، يمكن منح مجموعات من المستخدمين مستويات مختلفة من الوصول إلى مجلدات محددة (مثل القراءة فقط والقراءة والكتابة وما إلى ذلك) أو عدم الوصول على الإطلاق. ويمكن أن يكون إعداد المجموعات والمجلدات أمرًا معقدًا وقد يكون محبطًا للمستخدمين إذا كانوا بحاجة إلى مجلد أو ملف لا يمتلكون إذن الوصول إليه.

الامتيازات

يمكن لمدير نظام الشبكة التحكم في مجموعة متنوعة من الأشياء التي يمكن لمستخدمي الأنظمة القيام بها، وتُعرف هذه بامتيازات نظام التشغيل. من الناحية المثالية، يجب تقييد المستخدم من القيام بأي شيء يشكل خطرًا أمنيًا للحصول على الحماية المُثلى. على سبيل المثال، يجب ألا يتمكن المستخدمون من الوصول إلى موجه الأوامر، أو أن يكونوا قادرين على استخدام مشغِّل الأوامر (run command)، أو أن يكونوا قادرين على تثبيت البرنامج. وإذا فشل مسؤول النظام في تطبيق هذه الإعدادات بشكل صحيح، فقد يشكل ذلك خطرًا أمنيًا.

سياسة كلمات المرور

يعيّن مدير النظام سياسة كلمات المرور باستخدام نظام تشغيل الخادم. ويتضمن ذلك تحديد طول كلمات مرور المستخدم، وعدد مرات تغييرها ودرجة تعقيدها (مثل الرموز التي يجب استخدامها، مثل الأرقام والأحرف الإنجليزية الكبيرة والصغيرة والرموز). وإذا لم يطبق مدير النظام سياسات كلمات مرور قوية، فقد يكون النظام عرضة للهجوم.

ثغرات البرامج

عادةً ما تكون البرامج المرخصة والمحدثة بشكل صحيح في خطر منخفض من الهجمات السيبرانية. أما البرامج غير المرخصة أو غير القانونية فتشكل خطرًا أمنيًا جسيمًا. إذا قام الموظفون بتنزيل برامج من مصادر غير موثوقة، فهناك خطر من أن تتضمن برامج ضارة. وقد يحاول المجرمون إغراء المستخدمين لتنزيل ما يبدو أنه نسخة مجانية من تطبيق برمجي باهظ التكلفة، ولكنه في الواقع يحتوي على برامج ضارة يتم تثبيتها بدلًا من ذلك. تشمل الثغرات الأخرى المتعلقة بالبرامج ما يأتي:

حقن لغة الاستعلام المهيكلة (SQL): هذه طريقة شائعة لمهاجمة مواقع التجارة الإلكترونية، إذ تحتوي هذه المواقع على خادم ويب يشغّل تطبيقات قواعد البيانات للحفاظ على معلومات حول المنتجات المعروضة

المهارات

المهارات المعرفية/العمليات والإستراتيجيات المعرفية
- التفكير الناقد
- التحليل

موضوعات ذات صلة

لمعرفة المزيد عن تشغيل جدار الحماية، راجع الجزء *تدابير الأمان المادي* في صفحة 145.

المصطلحات الرئيسة

ثغرة أمنية في النظام – نقطة ضعف في نظام التشغيل أو البرامج الأخرى التي يمكن أن يستغلها المهاجم.

جدار الحماية – برنامج أو جهاز يتولى تصفية البيانات الواردة والصادرة بين شبكة محلية والإنترنت بهدف حظر الوصول غير المصرح به أو الضار.

مناقشة

ناقش الأبعاد القانونية والأخلاقية للبرامج غير المرخصة أو غير القانونية والمخاطر التي يمكن أن تشكلها.

المصطلح الرئيس

لغة الاستعلام المهيكلة (SQL) – لغة الأمر المستخدمة لاستخراج البيانات من قاعدة بيانات.

M01_INFO_ST_55924_U11 Rev 3 FP 08 Aug_AR.indd 137 03/05/2025 12:17:51

دراسة حالة

بين عامي 2005 و2007، نفّذ المخترق الأمريكي ألبرت غونزاليس، إلى جانب العديد من المتسللين الروس، واحدة من أكبر عمليات سرقة أرقام بطاقات الائتمان والبيانات الشخصية الأخرى باستخدام إدخال لغة SQL جنبًا إلى جنب مع تقنيات أخرى. في سلسلة من الهجمات، سرق غونزاليس وشركاؤه أكثر من 170 مليون رقم بطاقة وأداروا موقعًا إلكترونيًا حيث تم بيع البيانات المسروقة. تم القبض على غونزاليس في عام 2008 وعثر بحوزته على 1.6 مليون دولار نقدًا. وحُكم عليه بالسجن لمدة 20 عامًا.

اختبر معلوماتك

1 كيف يمكن استخدام حقن لغة SQL للحصول على معلومات مثل أرقام بطاقات الائتمان والبيانات الشخصية من موقع إلكتروني؟

2 ما الذي يمكن أن تفعله الشركات لحماية نفسها من هذه الهجمات؟

للبيع والعملاء والطلبات وما إلى ذلك. على سبيل المثال، قد يبحث زائر موقع التجارة الإلكترونية عن منتج عن طريق إدخال وصف المنتج في مربع البحث في الصفحة الأولى للموقع، ومن ثم يُستخدم هذا الإدخال للبحث في قاعدة بيانات المنتجات عن المنتجات المطابقة. ويتم ذلك عن طريق إدراج سلسلة البحث التي أدخلها المستخدم في أمر بحث SQL. تتمثل ثغرة حقن SQL في إدخال المهاجم أمر SQL في مربع البحث على الموقع. في ظروف معينة، يمكن أن يؤدي ذلك إلى عرض قاعدة البيانات لمعلومات ينبغي أن تظل سرية، مثل تفاصيل بطاقات ائتمان العملاء. ويمكن لأوامر SQL أن تتسبب في إسقاط جداول من قاعدة بيانات الموقع الخلفية، ما يمنع خاصية البحث من العمل بشكل فعّال على الموقع. ننتقل إلى هجوم البرمجة النصية عبر المواقع (المعروف باسم XSS)، وهو شكل شائع آخر من الهجمات، حيث يقوم المخترق بحقن نص برمجي من جهة العميل في موقع إلكتروني، عادةً من خلال نموذج HTML. قد يعرض النص الضار رسائل منبثقة، أو يسرق ملفات تعريف الارتباط، أو يعيد توجيه المتصفح إلى موقع إلكتروني آخر.

الثغرات الأمنية غير المعروفة. يتولى مطور البرمجيات إصلاح أي ثغرات معروفة في تطبيق عن طريق تحديثات الأمان ولكن قد يكون هناك فارق زمني بين اكتشاف الثغرة وإصدار مطور البرمجيات للتحديث الذي يصلحها. يتيح هذا الفارق الزمني فرصة للمتسلل باستغلال هذه المدة المعروفة باسم "يوم الصفر" حيث لا تتوفر حماية بعد.

ثغرات نظام التشغيل

توجد ثغرات أمنية في برامج أنظمة التشغيل، ولكنها تُعالَج من خلال التحديثات. في نظام التشغيل ويندوز (Windows)، تكون تحديثات الأمان مفعلة بشكل افتراضي، على الرغم من أنه من الممكن إيقافها سواءً عن قصد أو عن طريق الخطأ. إذا كان جهاز الحاسوب يعمل بنظام تشغيل لم يتم تحديثه، أو بنسخة قديمة من نظام التشغيل التي لم يعد مطور النظام يدعمها، فقد تسمح هذه الثغرات للمهاجمين بالوصول إل النظام. على سبيل المثال، ما يزال نظام Windows XP مستخدمًا على العديد من أجهزة الحاسوب حول العالم، لكن تحديثات الأمان لم تعد تصله من شركة Microsoft®. وفي حال اكتُشِفَت ثغرة أمنية جديدة، لن تحصل أجهزة الحاسوب التي تعمل بنظام Windows XP على الحماية.

ثغرات الأجهزة المحمولة

بالنسبة للعديد من المؤسسات، توفر الأجهزة المحمولة فرصًا وتحديات. فيرغب العديد من الموظفين في استخدام أجهزتهم المحمولة للوصول إلى أنظمة الشركة، وهذا يسمح للموظفين بالعمل بمرونة. ومع ذلك، قد يكون لدى الشركة سيطرة محدودة جدًا على هذه الأجهزة ومدى أمانها وتواتر تحديثها وما يحدث إذا فُقدت أو سُرقت. تعتمد الأجهزة المحمولة أيضًا على التحديثات التي ينتجها صانعها الأصلي (OEM)؛ ويكون المستخدم الفردي هو المسؤول عن تطبيق هذه التحديثات أو توقيت تطبيقها. وعلى النقيض من ذلك، فإن التحديثات لأجهزة الحاسوب داخل النظام الحاسوبي المتصل بالشبكة لدى المؤسسة تكون تحت سيطرة مدير النظام.

M01_INFO_ST_55924_U11 Rev 3 FP 08 Aug_AR.indd 138 03/05/2025 12:17:51

الثغرات الأمنية المادية

بحسب نوع المؤسسة وأماكن تواجد الحواسيب، قد تكون الأنظمة عرضة للسرقة أو الفقدان. وينطبق هذا بشكل خاص على الأجهزة المحمولة وأجهزة الحاسوب المحمولة، والتي ربما تحتوي على معلومات حساسة تخص الشركة. بالإضافة إلى أجهزة الحاسوب، تمثل أجهزة USB وشرائح الذاكرة أيضًا خطرًا كبيرًا، فهي معرضة بسهولة للفقدان أو السرقة. وكما ذُكر سابقًا، يمكن استخدام مجموعة متنوعة من أساليب الهندسة الاجتماعية لجمع كلمات المرور من المستخدمين غير المشتبهين.

ثغرات عمليات المستخدمين

يمثل المستخدمون ثغرة رئيسة قد تؤدي إلى اختراق أمان النظام، إذ يمكن بسهولة تسريب بيانات تسجيل الدخول إما عن قصد وإما عن طريق الخطأ. على سبيل المثال، ربما يقوم المستخدم بعرض اسم المستخدم وكلمة المرور الخاصة به بشكل علني على ملصق ملاحظات على شاشة حاسوبه، ما يجعله مرئيًا للموظفين الآخرين وزوار المكتب. ولا يخفى أن مشاركة بيانات تسجيل الدخول ليست آمنة. قد يميل المستخدمون إلى القيام بذلك إذا كان زميل غير قادر على تسجيل الدخول، ربما بسبب نسيان كلمة المرور أو إذا كانت حساباته تفتقر إلى الأذون اللازمة للوصول إلى مجلد معين؛ ولكن يجب عليهم الامتناع عن ذلك.

ثغرات التقنيات الجديدة

توفر التقنيات الجديدة فرصًا جديدة لمجرمي الإنترنت.

الحوسبة السحابية

ترتبط العديد من الثغرات الأمنية التي تم النظر فيها حتى الآن بحوسبة خادم العميل التقليدية، حيث يتم الاحتفاظ بالخوادم وإدارتها داخل المؤسسة. ولكن، تتبنى المؤسسات بشكل متزايد نماذج الحوسبة السحابية، التي تُخزَّن فيها الملفات وتُنفَّذ فيها العمليات الحسابية خارج المؤسسة، ويقوم بتشغيلها وصيانتها مزود خدمة حوسبة سحابية خارجي. وأحد فوائد الحوسبة السحابية هو أن المسؤولية عن أمان النظام تقع على عاتق مزود خدمة الحوسبة السحابية. ومن المفترض أن يكون لديهم المهارات والموارد اللازمة للحفاظ على أمان النظام، ولكن من المهم أن تختار المنظمة مزود خدمة حوسبة سحابية يمكن الوثوق به للحفاظ على أمان بياناتهم.

إنترنت الأشياء (IoT)

نظرًا لقدرة العديد من الأجهزة على تبادل البيانات في ما بينها، توفر تقنية إنترنت الأشياء مزايا للمنازل أو المكاتب. على سبيل المثال، تتيح الكاميرات المتصلة بالإنترنت للأفراد مراقبة منازلهم أو مكاتبهم عن بُعد. وإن تمكن المجرمون من اختراق هذه الأجهزة، يمكنهم معرفة متى يكون المنزل أو المكتب خاليًا، وقد يكونون قادرين على تعطيل أي أنظمة إنذار أيضًا.

المصطلح الرئيس

إنترنت الأشياء (IoT) – مصطلح عام يشير إلى التكنولوجيا التي تسمح للأجهزة اليومية (مثل: كاميرا الفيديو أو ترموستات التدفئة أو المصابيح) بتضمين أجهزة الحوسبة فيها ما يتيح لها إرسال البيانات واستقبالها عبر الإنترنت.

بحث

ابحث عبر الإنترنت للعثور على معلومات الأمان المحدثة لموردي البرامج الرئيسين الآتيين.

Microsoft – https://support.microsoft.com.

Norton – https://uk.norton.com (أمن الإنترنت)

مركز تهديدات McAfee في المملكة المتحدة – www.mcafee.com (مركز التهديدات)

وقفة للتفكير

ابحث عن مشكلات أمن تكنولوجيا المعلومات الحديثة التي تواجهها الشركات الكبيرة. ماذا حدث بالفعل؟ ما أنواع الهجمات الموصوفة في هذا الجزء التي تم استخدامها؟ ما تأثير ذلك في الشركة؟ هل خسروا المال أم كانت هناك عواقب قانونية؟

تلميح

تُعد مواقع الأخبار أو الصحف مثل هذه أماكن ممتازة لبدء البحث.

- *New York Times*®: www.nytimes.com (التكنولوجيا)
- *The Australian*®: www.theaustralian.com (التكنولوجيا)
- *Telegraph*®: www.telegraph.co.uk (التكنولوجيا)
- *The Guardian*®: www.theguardian.com (التكنولوجيا في المملكة المتحدة)
- BBC News®: www.bbc.co.uk (الأخبار)

توسيع الأفق

فكّر كيف تمكنت الشركة من تجنب حدوث خرق أمني. هل هناك طرق حماية كان بالإمكان استخدامها؟ وإذا كان الأمر كذلك، فلماذا لم تُستخدم؟ وكيف يمكن للمؤسسات حماية نفسها في المستقبل من هذه المشكلات الأمنية؟

M01_INFO_ST_55924_U11 Rev 3 FP 08 Aug_AR.indd 139 03/05/2025 12:17:52

المسؤوليات القانونية

نواقل الهجوم

هي الطرق التي يمكن للمتسلل من خلالها الوصول إلى نظام لاستغلال ثغرة أمنية فيه. ويتم ذلك عادةً عبر اتصال شبكي. يوفر الوصول إلى الشبكة اللاسلكية، مثل Wi-Fi أو Bluetooth، طريقة واضحة للوصول إلى النظام بسبب طبيعتها البثية. والوصول عبر اتصال الإنترنت السلكي يكون أكثر صعوبة، بينما يتطلب الوصول عبر الشبكة المحلية الداخلية (LAN) وجود مهاجم داخلي.

حماية البيانات

أرست العديد من البلدان حول العالم قوانين تحمي البيانات الموجودة المتعلقة بالأفراد الأحياء على أنظمة الحاسوب. ففي أوروبا على سبيل المثال، يُعرف التشريع الخاص بحماية البيانات الذي ينطبق على جميع الدول الأعضاء في الاتحاد الأوروبي باسم اللائحة العامة لحماية البيانات (GDPR). وتوجد ستة مبادئ رئيسة بهذه اللائحة تتعلق بالبيانات الشخصية:

- يجب معالجتها بشكل قانوني.
- يجب جمعها لأغراض محددة فقط.
- يجب أن تكون ذات صلة وتقتصر على ما هو ضروري لهذا الغرض.
- يجب الاحتفاظ بها للمدة التي تكون فيها ضرورية فقط.
- يجب الحفاظ على أمانها.

تمنح اللائحة العامة لحماية البيانات (GDPR) الأفراد عدة حقوق تتعلق بالبيانات الخاصة بهم المخزنة على أنظمة الحاسوب، وتشمل هذه الحقوق ما يأتي:

- الحق في أن يتم إبلاغهم بجمع بياناتهم.
- الحق في الوصول إلى البيانات المخزنة عنهم عند الطلب.
- الحق في محو البيانات (يمكن للأفراد طلب محو البيانات المسجلة عنهم).
- الحق في الاعتراض على استخدام بياناتهم لأغراض معينة، مثل رسائل البريد الإلكتروني الترويجية.

إساءة استخدام الحاسوب

يُستخدم هذا التشريع لجعل عمليات الاختراق ونشر الفيروسات والإجراءات ذات الصلة غير قانونية. في المملكة المتحدة، يحدد قانون إساءة استخدام الحاسوب، الذي تم تمريره في عام 1990، عددًا من الإجراءات المختلفة على أنها غير قانونية، وهي كالآتي:

- الوصول غير المصرح به إلى بيانات الحاسوب
- الوصول غير المصرح به بقصد ارتكاب جرائم أخرى
- إتيان أعمال غير مصرح بها بقصد تعطيل نظام الحاسوب
- إتيان أعمال غير مصرح بها بقصد إحداث أضرار جسيمة
- تنفيذ تعديل غير مصرح به لبيانات الحاسوب
- صنع أو توريد أو الحصول على أدوات لاستخدامها في جرائم إساءة استخدام الحاسوب

وقد تم استخدام هذا القانون كنموذج لسياسات مماثلة في دول أخرى حول العالم.

تشريعات الاتصالات

في المملكة المتحدة، يسمح القانون لأصحاب العمل باعتراض الاتصالات المرسلة عبر شبكاتهم الخاصة. ويأتي ذلك في إطار لوائح الاتصالات (الممارسات التجارية المشروعة) (اعتراض الاتصالات) (2000). على سبيل المثال، يمكن للشركة اعتراض رسائل البريد الإلكتروني لموظفيها بشكل قانوني وتسجيل محادثاتهم الهاتفية (إذا كانوا يستخدمون شبكة الشركة). ويجب أن يكون الموظفون على دراية بأن اتصالاتهم قد يتم اعتراضها، وعادة ما يتم تضمين ذلك في عقد عملهم.

المهارات

المهارات المعرفية/العمليات والإستراتيجيات المعرفية

- التفكير الناقد
- التحليل

فكِّر مليًّا

لمَ تمثل حماية البيانات أهمية للفرد برأيك؟ فكر في ظروفك الخاصة. لمَ تُعد حماية البيانات ذات أهمية بالنسبة لك؟ لماذا تعتبر قضية مهمة لشركة أو مؤسسة؟ ما العواقب التي قد تترتب على انتهاك شركة أو مؤسسة لقوانين حماية البيانات؟ ما قوانين حماية البيانات في بلدك؟ هل تختلف عن تلك المدرجة هنا؟

بحث

تعرّف قوانين حماية البيانات التي تؤثر فيك. ما مبادئها الرئيسة؟ ما الحقوق التي تمنحها هذه القوانين للأفراد؟

M01_INFO_ST_55924_U11 Rev 3 FP 08 Aug_AR.indd 140 03/05/2025 12:17:52

دراسة حالة

في فبراير 2014، اتُهم مواطن بريطاني يعاني حالات طبية معقدة بما في ذلك متلازمة أسبرجر باختراق أنظمة الحاسوب الأمريكية، بما في ذلك مكتب التحقيقات الفيدرالي والجيش الأمريكي ووكالة الدفاع الصاروخي. ويُزعم أنه كان يحاول العثور على أدلة بشأن الأجسام الطائرة المجهولة (UFos). وقد وجهت إليه اتهامات في الولايات المتحدة بخرق أعداد كبيرة من أنظمة الحاسوب وقد يواجه عقوبة سجن طويلة. فلم تنجح محاولات تسليمه من المملكة المتحدة إلى الولايات المتحدة، ويرجع ذلك في الأساس إلى المشكلات الصحية التي يواجهها.

اختبر معلوماتك

ابحث عبر الإنترنت للعثور على حالات أخرى مماثلة. لماذا برأيك ينجذب القراصنة إلى مؤسسات مثل مكتب التحقيقات الفيدرالي أو وكالة الدفاع الصاروخية؟

تشريعات مكافحة الاحتيال

الهجمات السيبرانية التي تتضمن الحصول على المال عن طريق الخداع قد تكون مشمولة ضمن تشريعات الاحتيال. ويحدث الاحتيال عندما يحاول شخص ما عمدًا تحقيق فوائد مالية أو غيرها بوسائل غير قانونية. على سبيل المثال، قد يستخدم المجرمون طرقًا متنوعة للحصول على معلومات (مثل اسم الفرد، أو عنوانه، أو رقم حسابه البنكي) والتي يمكنهم استخدامها للتقدم بطلب للحصول على قرض بنكي باسم شخص آخر.

الصحة والسلامة

تفرض معظم الدول تشريعات متعلقة بالصحة والسلامة تهدف إلى حماية أصحاب العمل والموظفين في مكان العمل، كما تفرض هذه التشريعات متطلبات على الموظفين لأداء واجباتهم بطريقة لا تعرض الآخرين للخطر.

تدابير الأمان المادي

يمكن استخدام تدابير الأمان المادي للمساعدة على منع السرقة والحفاظ على أمان البيانات.

أمان الموقع

يعد الحفاظ على أمان أجهزة الحاسوب والتحكم في من يمكنه الوصول إليها جزءًا مهمًا من حماية أنظمة الحاسوب. يجب أن تبقى غرف الحاسوب، حيث توجد الخوادم والمعدات الحساسة الأخرى، مقفلة ويتم التحكم في الوصول إليها، على سبيل المثال من خلال استخدام نظام دخول باستخدام بطاقات المفتاح، حيث يتم تسجيل وقت واسم الشخص الذي يدخل الغرفة. وقد تكون الأكبال عرضة للتنصت، خاصة في المساحات المكتبية المشتركة أو المباني. يجب الاحتفاظ بالأكبال والمعدات الشبكية الأخرى في خزائن مقفلة لمنع الوصول غير المصرح به.

هناك عدة طرق أخرى يمكن من خلالها الحفاظ على أمان هذه المواقع:

- **القياسات الحيوية**: يمكن استخدامها بدلًا من المفاتيح أو البطاقات. وتعتمد هذه التقنية على خصائص بشرية فريدة مثل بصمات الأصابع أو مسح قزحية العين لتحديد هوية الشخص الذي يدخل منطقة آمنة.
- **الدوائر التلفزيونية المغلقة (CCTV)** تسمح لموظفي الأمن بمراقبة مساحات واسعة من المبنى ويمكن تسجيل اللقطات لتكون دليلًا. يمكن أيضًا ربط أنظمة CCTV بأنظمة تعرُّف الوجوه لتتبع الحركة داخل المبنى.
- **أفراد الأمن**: يمكن استخدامهم لتفتيش الزوار عند وصولهم والقيام بدوريات في الموقع.
- **أجهزة الإنذار**: يمكن أن تكتشف دخول غير المصرح لهم إلى المبنى. ويمكن تركيبها على الأبواب والنوافذ أو تشمل أجهزة استشعار الحركة للكشف عن وجود شخص في جزء من المبنى في وقت لا ينبغي أن يكون فيه هناك.

المهارات

المهارات المعرفية/العمليات والإستراتيجيات المعرفية:

- التفكير الناقد
- التحليل

M01_INFO_ST_55924_U11 Rev 3 FP 08 Aug_AR.indd 141 03/05/2025 12:17:52

تخزين البيانات

البيانات هي أحد أهم الموارد التي تمتلكها المؤسسة، ولا يمكن استبدالها بسهولة حال فقدها، ويجب حماية البيانات من الضياع من خلال النسخ الاحتياطي المنتظم لها والذي يُشغَّل تلقائيًّا بواسطة نظام التشغيل بالمؤسسة. تقوم بعض المؤسسات بعمل نسخ احتياطية على وسائط خارجية (مثل محرك أقراص USB خارجي) وتخزين محرك الأقراص خارج الموقع. التخزين خارج الموقع مهم للحماية من الكوارث مثل الحرائق أو الفيضانات، ويُستخدم النسخ الاحتياطي السحابي بشكل متزايد، حيث تُنسخ الملفات عبر الإنترنت إلى موقع بعيد. تتشارك النسخ الاحتياطية السحابية التخوفات الأمنية نفسها مع الخدمات الأخرى القائمة على السحابة، حيث تنتقل مسؤولية أمان وسلامة البيانات إلى طرف ثالث (مزود الخدمة).

تدابير أمان البرامج والأجهزة

نظرًا لتعدد طرق الهجمات على الأنظمة، يتطلب الأمر مجموعة متنوعة من تدابير الأمان في البرمجيات والأجهزة للحفاظ على أمان النظام.

برامج مكافحة الفيروسات

تُستخدم للدفاع ضد مجموعة من التهديدات البرمجية الخبيثة تعتمد برامج مكافحة الفيروسات على عدد من التقنيات لمحاولة تعرُّف الفيروسات في الملفات.

- **توقيعات الفيروسات:** لكل ملف فيروسي معروف نمط يمكن تمييزه من خلاله؛ وتُعرف هذه الأنماط بتوقيعات الفيروسات. يقوم برنامج مكافحة الفيروسات بفحص كل ملف على الحاسوب ومقارنته بتوقيعات الفيروسات التي لديه، ليتمكن من تحديد ما إذا كان أي من الملفات يحتوي على فيروسات. ونظرًا لظهور فيروسات جديدة من حين لآخر، فمن المهم أن يتم تحديث قائمة توقيعات الفيروسات باستمرار.
- **الموجِّهات**: توقيعات الفيروسات تتعرف على الفيروسات المعروفة فقط. هنا يأتي دور الموجهات والتي تُستخدم للبحث في الملفات عن أنواع الأوامر أو التعليمات التي لا يمكن العثور عليها في التطبيقات غير الضارة والتي تشير إلى أن الملف مشبوه
- **التهديدات المحددة:** بمجرد تحديد فيروس أو ملف مشبوه، يحتاج برنامج مكافحة الفيروسات إلى التعامل معه بشكل مناسب. في بعض الحالات، قد يقوم برنامج مكافحة الفيروسات بحذف الملف ببساطة. وفي حالات أخرى، قد يضع الملف في مجلد "العزل" والذي يحد بشدة من تصرفات الملف ولكنه لا يحذفه. وقد تكون بعض إصابات الفيروسات صعبة الإزالة؛ وهذه قد تتطلب بدء تشغيل الحاسوب في الوضع الآمن أو استخدام قرص إنقاذ قادر على إعادة تشغيل الحاسوب باستخدام نظام تشغيل مختلف لإزالة ملفات الفيروسات بشكل دائم.

جدران حماية البرامج والأجهزة

إحدى الطرق التي يمكن من خلالها أن تحاول التهديدات الخارجية الوصول إلى أنظمة الحاسوب الخاصة بالمؤسسة هي عبر رابط خارجي إلى الإنترنت. تقوم جدران الحماية بتحليل البيانات الواردة والصادرة من وإلى شبكة المنطقة المحلية (LAN) الخاصة بالمؤسسة إلى شبكة الإنترنت ومنها بهدف حظر البيانات المشبوهة ويمكن تنفيذ جدران الحماية في البرامج وتشغيلها على أجهزة الحاسوب الفردية. في المؤسسات، تكون جدران الحماية عادةً جهازًا ماديًا واحدًا يقوم بتحليل البيانات لجميع أجهزة الحاسوب على الشبكة المحلية (LAN). وتستخدم جدران الحماية عددًا من التقنيات التحليلية المختلفة.

- **تصفية الحزم وفحصها:** تتضمن هذه التقنية النظر إلى كل **حزمة** من البيانات في أثناء مرورها عبر جدار الحماية، وبناءً على القواعد التي يحددها جدار الحماية أو مدير الشبكة، يُسمح بمرور الحزم عبر جدار الحماية أو يُحظر. يمكن أن تشمل القواعد أشياء مثل **عنوان بروتوكول الإنترنت (IP)** المصدر والوجهة، أو **منفذ** الشبكة، أو **البروتوكول** المستخدم أو إعدادات أخرى.
- **الوعي بطبقة التطبيقات:** تعمل هذه التقنية على مستوى التطبيق بدلًا من مستوى الحزمة، حيث تطبق القواعد لكل تطبيق وترفض أي اتصالات تخالف القواعد. على سبيل المثال، يمكنك إعداد جدار حماية لحظر تطبيقات الشبكة، مثل الاتصال عن بعد بجهاز طرفي.

المهارات

المهارات المعرفية/العمليات والإستراتيجيات المعرفية:

- حل المشكلات
- التفكير الناقد

المصطلحات الرئيسة

الحزمة – وحدة بيانات تم تحويلها إلى "حزمة" صغيرة أو "حزمة" تنتقل عبر مسار الشبكة.

عنوان بروتوكول الإنترنت (IP) – عنوان رقمي يعرّف جهاز الحاسوب تعريفًا فريدًا على إحدى الشبكات.

المنفذ – في سياق جدران الحماية، يعد منفذ الشبكة ميزة برمجية تسمح بتحديد التطبيقات المختلفة المتصلة بالشبكة.

البروتوكول – بروتوكول الشبكة هو مجموعة من القواعد التي تحكم كيفية إجراء نوع معين من الاتصالات عبر الشبكة.

M01_INFO_ST_55924_U11 Rev 3 FP 08 Aug_AR.indd 142 03/05/2025 12:17:52

- **قواعد الدخول والخروج:** تُوضع القواعد للتحكم في كيفية عمل تصفية الحزم والتطبيقات. يحتوي جدار الحماية على بعض القواعد الافتراضية، ولكن يمكن لمدير الشبكة تعديل هذه القواعد وإضافة قواعد جديدة. ويمكن وضع القواعد لكل من البيانات الصادرة (من الشبكة المحلية إلى الإنترنت) والبيانات الواردة (من الإنترنت إلى الشبكة المحلية).
- **عنوان الشبكة:** تخفي جدران الحماية عناوين IP الحقيقية للأجهزة الموجودة على الشبكة المحلية لمنع المتسللين من خارج الشبكة المحلية من تعرُّف عناوين الأجهزة الفردية. تُعرف هذه التقنية باسم ترجمة عنوان الشبكة (NAT)، وتعمل عن طريق الاحتفاظ بجدول لعناوين IP الداخلية المتعددة للأجهزة داخل الشبكة المحلية وربطها بعناوين IP العامة الخارجية المستخدمة على الإنترنت.

مصادقة المستخدم

الهدف من مصادقة المستخدم هو ضمان أن المستخدمين الشرعيين يمكنهم تسجيل الدخول إلى النظام والوصول إلى الملفات والتطبيقات الصحيحة. وينبغي أن تمنع إجراءات تسجيل الدخول الأشخاص غير المصرح لهم من الوصول إلى النظام دون أن تسبب إزعاجًا مفرطًا للمستخدمين المصرح لهم.

- **إجراءات تسجيل دخول المستخدم:** الطريقة القياسية لمصادقة المستخدم هي مزيج من اسم المستخدم وكلمة المرور. فيعرّف اسم المستخدم النظام بالمستخدم، وتُستخدم كلمة المرور السرية لحماية الحساب من الوصول غير المصرح به. في بعض المؤسسات، لا يُعتبر استخدام اسم مستخدم وكلمة مرور بسيطين آمنًا بما فيه الكفاية، لذا تُستخدم مجموعة من الطرق الأخرى.
- **كلمات المرور القوية:** لا تُعتبر كلمات المرور البسيطة التي تحتوي على رموز أحرف أبجدية فقط قوية لأنها عرضة لهجمات القاموس، والتي تجرّب جميع الكلمات الموجودة في قاموس عبر الإنترنت. كما تُعتبر كلمات المرور القصيرة (أقل من 8 رموز) ضعيفة لأنها سهلة الاختراق. يجب أن تكون كلمات المرور القوية طويلة –كلما كانت أطول كان ذلك أفضل– وأن تكون مزيجًا من رموز الأحرف الأبجدية والأرقام والرموز. كلما كانت كلمة المرور أكثر تعقيدًا، كلما كان من الصعب على المستخدمين تذكرها. يُنصح بتغيير كلمات المرور كل بضعة أشهر للحفاظ على أمانها، ولكن قد يكون ذلك مزعجًا للمستخدمين.
- **كلمات المرور النصية والرسومية:** تُعتبر كلمات المرور الرسومية بديلًا قويًا لكلمات المرور النصية، وهي جيدة بشكل خاص على الأجهزة التي تعمل باللمس، حيث يقوم المستخدم برسم نمط لفتح الجهاز.
- **المصادقة البيومترية:** تستخدم القياسات البيومترية سمات جسدية فريدة لمصادقة المستخدم الفردي، مثل بصمات الأصابع، أو مسح القزحية أو الشبكية، أو التعرُّف على الوجه والصوت. وتتمثل فائدة المصادقة البيومترية في أن المستخدم لا يحتاج إلى تذكر أي شيء، ولكنها قد تتطلب برامج وأجهزة إضافية، مثل ماسح ضوئي لقراءة بصمات الأصابع أو القزحية. وتتضمن أحدث الهواتف المحمولة ماسحًا لبصمات الأصابع يمكن استخدامه لفتح الهاتف. يقوم النظام بتخزين بيانات القياسات الحيوية للمستخدم بحيث يمكن مقارنتها بالبيانات المقدمة عند تسجيل الدخول. تعتبر المصادقة البيومترية آمنة بشكل عام، إلا أنه إذا تمكن المتسلل من الوصول إلى البيانات البيومترية أو سرقتها، فقد يتسبب ذلك في مشكلات كبيرة، إذ لا يمكن تغيير البيانات البيومترية مثل كلمة المرور.
- **التحقق بخطوتين:** يُعرف هذا النوع من المصادقة أيضًا بالمصادقة الثنائية (2FA)، ويُستخدم بشكل شائع حيث تتطلب المصادقة أمانًا أعلى من مجرد اسم المستخدم وكلمة المرور (التي تسمى أحيانًا المصادقة الأحادية). يتضمن التحقق بخطوتين إدخال المستخدم لكلمة مرور واستخدام طريقة ثانية للمصادقة مثل القياسات الحيوية أو زر أمان مميز. يوفر التحقق بخطوتين طبقة إضافية من الأمان.
- **رموز الأمان:** هي أجهزة صغيرة (تشبه أحيانًا بطاقة الائتمان أو سلسلة المفاتيح) توفر الخطوة الثانية في عملية التحقق بخطوتين. وتوجد عدة أنواع من هذه الرموز، على سبيل المثال، عندما يريد المستخدم تسجيل الدخول إلى النظام، يقوم الرمز بتوليد شفرة تُستخدم لمرة واحدة يجب إدخالها كجزء من عملية

M01_INFO_ST_55924_U11 Rev 3 FP 08 Aug_AR.indd 143 03/05/2025 12:17:52

المصادقة. بعض أنواع هذه الرموز يتصل بالحاسوب عبر مقبس USB، بينما تستخدم أنواع أخرى من الرموز تقنية **الاتصال قريب المدى (NFC)** حيث يكون الرمز عبارة عن بطاقة أو علامة لا تحتاج إلا إلى تقريبها من قارئ NFC المتصل بالحاسوب.

- **المصادقة القائمة على المعرفة:** تُستخدم هذه الطريقة بشكل شائع كجزء من عملية التحقق متعددة الأجزاء (كتلك المطلوبة عند تسجيل الدخول إلى موقع مصرفي) أو لاسترداد كلمة المرور المنسية، والتي تتطلب تقديم الإجابة الصحيحة عن سؤال معين. عند إعداد حساب، عادةً ما يقدم المستخدم إجابة عن بعض الأسئلة المُجهزة مسبقًا (مثل "ما اسم المدينة التي وُلدت فيها؟" أو "ما اسم أول حيوان أليف لديك؟" أو ما شابه). عندما يحتاج المستخدم إلى تسجيل الدخول (أو استعادة كلمة المرور)، يجب عليه تقديم الإجابة نفسها عن السؤال.
- **مصادقة كيربيروس:** بروتوكول المصادقة القياسي المستخدم في أنظمة العميل والخادم على نظام ويندوز، وتتوافر إصدارات منه أيضًا لأنظمة Linux وأنظمة التشغيل الأخرى. يضمن كيربيروس عدم إرسال كلمات المرور عبر الشبكة دون تشفيرها أولًا. في نظام مايكروسوفت ويندوز، يتم إنشاء حسابات المستخدمين على خادم وتخزينها في قاعدة بيانات تسمى أكتيف ديركتوري (AD)، والتي تعمل كمركز توزيع لمفاتيح كيربيروس (KDC). تحتوي حسابات المستخدمين على كلمة مرور مخزنة (في شكل مشفر) على KDC. وعندما يقوم المستخدم بتسجيل الدخول إلى جهاز عميل ويقوم بإدخال كلمة المرور الخاصة به، تُشفَّر باستخدام الطريقة نفسها التي تم استخدامها عند إنشاء الحساب على KDC. وفي حال تطابق المفتاحان المشفران، فهذا يعني أن المستخدم أدخل كلمة المرور الصحيحة.
- **المصادقة المستندة إلى الشهادات:** تُستخدم هذه الطريقة في المواقع الإلكترونية التي تحتاج إلى ضمان اتصالات آمنة وموثوقة، مثل عند القيام بعملية شراء عبر الإنترنت أو تسجيل الدخول إلى موقع مصرفي. تُستخدم الشهادة الرقمية ضمن بروتوكول HTTPS الآمن، الذي يضمن أن البيانات المرسلة بين المستخدم النهائي والموقع الإلكتروني مشفرة. يجب على المواقع الإلكترونية التي ترغب في استخدام هذا النوع من المصادقة الحصول على **شهادة رقمية**، والتي توفرها **هيئة الشهادات**. تعتمد هذه العملية على عملية التشفير بالمفتاح العام، التي سيتم شرحها في الجزء الآتي.

المصطلحات الرئيسة

الاتصال قريب المدى (NFC) – طريقة اتصال لاسلكية تستخدمها خدمات مثل آبل باي ومدفوعات البطاقات اللاتلامسية، إذ يجب وضع جهازين (مثل بطاقة الخصم وقارئ البطاقات) بالقرب من بعضهما (في نطاق بضعة سنتيمترات) ليتمكنا بعد ذلك من نقل كميات صغيرة من البيانات.

الشهادة الرقمية – يجب أن يتقدم الموقع الإلكتروني الآمن (الذي يستخدم بروتوكول HTTPS) بطلب الحصول على شهادة رقمية من سلطة شهادات الاعتماد لإثبات أنه موقع حقيقي.

هيئة الشهادات –هيئة الشهادات (CA) هي مؤسسة تتولى إصدار الشهادات الرقمية.

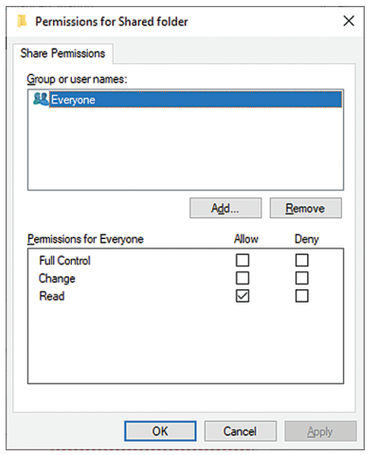
مناقشة

ناقش مزايا وعيوب استخدام المصادقة البيومترية للوصول إلى أحد المواقع الإلكترونية.

عناصر التحكم في الوصول

توفر أنظمة تشغيل الشبكات مثل مايكروسوفت ويندوز ولينكس ضوابط للوصول. ويمكن استخدام هذه العناصر لتنظيم المستخدمين الذين لديهم حق الوصول إلى الملفات والمجلدات المختلفة، وكذلك تحديد نوع الوصول الذي لديهم - سواء كان التحكم الكامل، أو الوصول للكتابة فقط، أو القراءة فقط. وتُعد أذونات الملفات في Windows موضوعًا معقدًا نسبيًا، حيث تختلف الأذونات قليلًا بين الملفات المخزنة محليًا وتلك الموجودة على الخوادم (تسمى أذونات ملفات NTFS)، وبين المجلدات المشتركة عبر الشبكة (تسمى أذونات المجلدات المشتركة). يوفر نظام التشغيل لينكس أدوات مشابهة تُعرف باسم أذونات ملفات لينكس، أو أحيانًا أذونات الملفات الثمانية في لينكس، لأنها تتضمن 8 مستويات تتراوح من 0 (عدم الوصول) إلى 8 (إذن القراءة/الكتابة والتنفيذ).

يمكنك بسهولة مشاركة مجلد على جهاز حاسوب يعمل بنظام ويندوز من خلال الوصول إلى خصائص المجلد واختيار مشاركة المجلد. ويمكنك التحكم في نوع الوصول الذي يمتلكه المستخدمون الآخرون إلى المجلد المشترك عن طريق ضبط الأذونات. يعرض الشكل 11.1 مربع الحوار الخاص بالأذونات لمجلد يحمل اسم "مجلد مشترك" (Shared folder). في هذه الحالة، يمتلك جميع المستخدمين (مجموعة "الجميع") إذن الوصول للقراءة فقط إلى المجلد، وبالتالي لا يمكنهم تغيير أي ملفات في المجلد.



الشكل 11.1 أذونات المجلد المشترك

الحوسبة الموثوقة

هذا مصطلح عام يشير إلى محاولات حل المشكلات الأمنية من خلال تطوير الأجهزة والبرامج المرتبطة بها. أنشأت عدد من الشركات المصنعة للأجهزة (بما في ذلك HP وIBM وMicrosoft) مشروع تعاوني تحت اسم "مجموعة الحوسبة الموثوقة". وحدة الأنظمة الأساسية الموثوقة (TPM) عبارة عن شريحة يمكن تضمينها في جهاز، مثل اللوحة الأم للحاسوب. تُستخدم شريحة TPM لدعم تشفير القرص بالكامل.

M01_INFO_ST_55924_U11 Rev 3 FP 08 Aug_AR.indd 144 03/05/2025 12:17:52

الغرض من التشفير واستخداماته

الغرض من التشفير هو إخفاء البيانات حتى يتمكن المستخدم أو المستلم المقصود فقط من قراءتها. وهناك العديد من التقنيات المختلفة لتشفير البيانات، وتستخدم لأغراض مختلفة، بعضها مذكور أدناه. وتعتمد معظم تقنيات التشفير على مفتاح -والذي يكون عبارة عن رقم ثنائي- لتشفير البيانات وفك تشفيرها.

تخزين كلمات المرور

تحتاج أجهزة حاسوب الخادم عادةً إلى تخزين كلمات مرور المستخدمين المعتمدين. وإذا تمكن المتسللون من الوصول إلى قاعدة بيانات كلمات مرور المستخدمين، فقد تكون العواقب وخيمة. لذلك، يجب دومًا تشفير كلمات المرور المخزنة للحفاظ على أمانها حتى إذا تمكن المتسلل من الوصول إلى النظام.

إدارة الحقوق الرقمية (DRM)

باستخدام الأنظمة المستندة إلى الحاسوب، يمكن نسخ الوسائط الرقمية مثل البرامج والأفلام والألعاب والموسيقى بسهولة من حاسوب إلى آخر. وإدارة الحقوق الرقمية هي اسم عام للتقنيات المستخدمة لحماية الأعمال المحمية بحقوق التأليف والنشر، وبعض هذه التقنيات يستخدم التشفير. أحد أبسط أشكال DRM هو مفتاح المنتج المطلوب لتثبيت التطبيقات البرمجية مثل Microsoft Windows أو FairPlay، الذي يستخدم للوصول إلى خدمات الموسيقى والأفلام عبر الإنترنت مثل Spotify وApple® iTunes.

تشفير الملفات والمجلدات والأقراص

تسمح أنظمة التشغيل مثل Microsoft Windows للمستخدمين بتشفير الملفات أو المجلدات (المعروف بنظام الملفات المشفرة أو EFS). يتم تشفير مفتاح التشفير (الذي يحتاجه المستخدم لفك تشفير الملفات) باستخدام كلمة مرور المستخدم. وعندما يكون المستخدم مسجل الدخول، يكون مفتاح التشفير متاحًا بحيث يمكن الوصول إلى الملفات؛ بينما لا يمكن للمستخدمين الآخرين الوصول إلى المفتاح، وبالتالي لا يمكنهم فك تشفير المجلد أو الملفات. بشكل عام، في نظام الحاسوب المتصل بالشبكة، يتم حماية الملفات والمجلدات من مجموعات مختلفة من المستخدمين باستخدام ميزة الأذونات. إذا سُرق جهاز حاسوب محمول وأُزيل القرص الصلب وتم توصيله بجهاز حاسوب آخر، فمن الممكن تجاوز نظام الأذونات والوصول إلى الملفات (وهو ما يُعرف **بالهجوم غير المتصل بالإنترنت**). ينطبق هذا أيضًا على الأقراص الصلبة المسروقة من أجهزة الحاسوب المكتبية والخوادم. يؤدي استخدام تشفير الملفات أو المجلدات إلى حماية البيانات من هذا النوع من السرقة لأنه لا يمكن فك تشفير الملفات إلا على يد المستخدم الذي شفرها. وإذا نسي المستخدم كلمة المرور الخاصة به واضطر إلى إعادة تعيينها، فلن تكون الملفات المشفرة الخاصة به متاحة بعد ذلك.

الحل الأفضل، خاصة لأجهزة الحاسوب المحمولة (التي تكون عرضة للفقدان أو السرقة)، هو تشفير القرص الصلب بالكامل. يمكن القيام بذلك في نظام Microsoft Windows باستخدام ميزة تسمى BitLocker، وهي متاحة في إصدارات Enterprise أو Pro من Windows، ولكنها غير متاحة في إصدارات Home. تعمل ميزة BitLocker بالتعاون مع شريحة TPM الموجودة في اللوحة الأم للحاسوب. لتشفير القرص الصلب على جهاز حاسوب، يجب إدخال كلمة مرور ستكون مطلوبة في كل مرة تقوم فيها بتشغيل الجهاز، قبل الوصول إلى شاشة تسجيل الدخول إلى Windows. يمكنك استخدام كلمة مرور مكتوبة أو شريحة ذاكرة USB كمفتاح. إذا نسيت كلمة المرور الخاصة بك، ستفقد الوصول إلى حاسوبك، لذا يتم إنشاء مفتاح استرداد أيضًا. ويمكنك حفظ مفتاح الاسترداد في عدة أماكن مختلفة وطباعته إذا رغبت في ذلك. وبمجرد تشفير محرك الأقراص، لا يمكنك الوصول إليه إلا عن طريق إدخال المفتاح عند بدء تشغيل الجهاز.

تشفير الاتصالات

عند نقل البيانات عبر الشبكات، تتعرض البيانات لاعتراض الآخرين، وينطبق هذا الأمر بشكل خاص على الإنترنت، حيث قد تمر البيانات عبر العديد من أنواع معدات الاتصالات الوسيطة في طريقها من المرسل إلى المستلم. لذلك، يجب تشفير البيانات الحساسة (مثل البيانات الشخصية أو المالية) عند إرسالها. يرد في ما يأتي أمثلة على طرق تشفير الاتصالات.

المصطلح الرئيس

هجوم غير متصل بالإنترنت – عندما يسرق مهاجم جهاز حاسوب أو قرص صلب ويقوم إما بتوصيل القرص الصلب بجهاز حاسوب مختلف وإما بتشغيل جهاز الحاسوب من نظام تشغيل مختلف (مثل Linux على شريحة ذاكرة USB)، تتخطى هذه الطرق الميزات الأمنية العادية لنظام Windows.

M01_INFO_ST_55924_U11 Rev 3 FP 08 Aug_AR.indd 145 03/05/2025 12:17:52

المصطلحات الرئيسة

المصدر المفتوح – نوع من برامج الحاسوب التي تتوافر فيها شفرة المصدر للمستخدمين لعرضها وتعديلها إذا رغبوا في ذلك، ويتناقض هذا الأمر مع البرامج التي لا تتوافر فيها شفرة المصدر، والتي تسمى البرمجيات الاحتكارية.

البروتوكول النفقي – بروتوكول شبكة ينشئ شبكة خاصة داخل الإنترنت من خلال تغليف البيانات المراد إرسالها وتشفيرها، قبل إدراجها في حزم البيانات القياسية. ويقوم البروتوكول أيضًا بالمصادقة على مستخدمي الاتصال والتفاوض على مفاتيح التشفير التي ستستخدم لتشفير البيانات المرسلة وفك تشفيرها.

- **مضمنة في الأجهزة:** تُنقَل محادثات الهواتف المحمولة باستخدام بيانات رقمية مشفرة، وتُشَفَّر هذه المحادثات في نظام الاتصالات المتنقلة العالمي (GSM) باستخدام خوارزمية تشفير A5/1. ولكن، لم تعد خوارزمية A5/1 آمنة؛ حيث ثبت أنه من الممكن كسر التشفير وفك تشفير بيانات الهاتف المحمول، ما يسمح بالتنصت على المحادثات في الوقت الحقيقي.
- **الموجه أونيون (تور):** أداة مجانية و **مفتوحة المصدر** مصممة لحماية خصوصية المستخدمين عند استخدام الإنترنت؛ وذلك عن طريق إخفاء مواقع المستخدمين واستخدامهم (بما في ذلك المواقع التي يزورونها، والمشاركات عبر الإنترنت، والمراسلات الفورية) من أي شخص يراقب الشبكة أو يحلل حركة البيانات.

الشبكات الافتراضية الخاصة (VPN): بشكل عام، توجد الشبكات الخاصة -التي لا يمكن أن يصل إليها إلا فرد أو مؤسسة- داخل مبنى أو موقع معين، وتُعرف عادةً بشبكة المنطقة المحلية (LAN)، في حين أن الإنترنت هو شبكة واسعة النطاق (WAN) مفتوحة للجمهور. لذلك، إذا كانت هناك مؤسسة تمتلك مكتبين أو موقعين منفصلين جغرافيًا، وكل منها يحتوي على شبكة LAN خاصة به، يمكن ربطهما عبر الإنترنت. ولكن حركة البيانات بينهما تسير عبر شبكة عامة وليست خاصة، ما يجعلها عرضة للاعتراض. تتيح شبكة VPN للمؤسسة تحويل الاتصالات التي تتم عبر شبكة الإنترنت العامة إلى اتصالات خاصة باستخدام التشفير. وغالبًا ما تسمح المؤسسات للعاملين عن بُعد بالاتصال الآمن بشبكة المؤسسة عند العمل من المنزل أو موقع بعيد آخر، وتستخدم المؤسسة شبكات VPN لضمان أمان اتصالاتها، إذ تعتمد شبكات VPN على **البروتوكولات النفقية** لإنشاء اتصالات افتراضية من نقطة إلى نقطة عبر الإنترنت.

بروتوكول نقل النص التشعبي الآمن (HTTPS): هو النسخة الآمنة من بروتوكول HTTP الذي يُستخدم لطلب وتقديم صفحات الويب على الإنترنت. ويُستخدم بروتوكول HTTPS الشهادات الرقمية لضمان أن صفحة الويب التي تزورها آمنة. ويقوم بتشفير البيانات التي يتم نقلها بينك وبين صفحة الويب حتى لا يتمكن الآخرون من اعتراضها باستخدام طريقة **المفتاح العام/الخاص**.

المفتاح العام/الخاص: تُستخدم هذه التقنية في المعاملات الآمنة عبر الإنترنت باستخدام بروتوكول HTTPS. وتتضمن إنشاء زوج من المفاتيح المرتبطة رياضيًا، مفتاح عام ومفتاح خاص. ويُعرف هذا

دراسة حالة

هجوم سان برناردينو

في ديسمبر 2015، لقيَ أربعة عشر شخصًا حتفه في هجوم إرهابي في مقاطعة سان برناردينو، كاليفورنيا، الولايات المتحدة الأمريكية. وقد استرد مكتب التحقيقات الفيدرالي جهاز آيفون 5C يخص أحد الإرهابيين، وأراد مكتب التحقيقات فتح الهاتف لمعرفة ما إذا كان هناك أشخاص آخرون متورطين في الهجوم. (قُتل الإرهابيان اللذان نفذا الهجوم برصاص الشرطة).

ومع ذلك، كُشف النقاب في عام 2014 عن أن مكتب التحقيقات الفيدرالي وأجهزة الأمن البريطانية كان لديها طرق للوصول إلى جميع المعلومات على أجهزة آبل والهواتف الذكية الأخرى. وردًا على ذلك، قامت شركة آبل بتحسين تشفيرها في الإصدار 8 من نظام تشغيل iOS، ما منع مكتب التحقيقات الفيدرالي من الوصول إلى هاتف الإرهابي. فطلب مكتب التحقيقات الفيدرالي من شركة آبل فتح الهاتف. ورفضت الشركة ذلك، مشيرةً إلى أن سياسة الشركة تقضي بعدم تقويض الميزات الأمنية لمنتجاتها؛ لأن القيام بذلك لن يكون في مصلحة عملائها. وأصدر مكتب التحقيقات الفيدرالي أمرًا قضائيًا يجبر شركة آبل على فتح الهاتف. ومع ذلك، قبل إحالة القضية إلى المحكمة، أسقط مكتب التحقيقات الفيدرالي القضية لأنهم ذكروا أن طرفًا خارجيًا (يُقال إنه شركة Cellebrite®) قد مكنتهم من الوصول إلى جميع البيانات الموجودة على الهاتف.

وأثارت القضية العديد من الأسئلة التقنية والأخلاقية حول ما إذا كان ينبغي لشركات التكنولوجيا إنشاء "منفذ خلفي" في منتجات التشفير الخاصة بها بغرض السماح للوكالات الحكومية بالوصول إليها في حالات مثل إطلاق النار في سان برناردينو، وما إذا كان من مصلحة عملائها حماية طرق التشفير الخاصة بهم بأي ثمن.

اختبر معلوماتك

1. هل تعتقد أن رغبة مكتب التحقيقات الفدرالي في الوصول إلى المعلومات على هاتف الإرهابي هو أمر صائب؟
2. هل يجب أن يكون للحكومة الحق في الوصول إلى بياناتنا؟ إذا كنت لا تفعل شيئًا يخالف القانون، فما الذي لديك لتخفيه؟
3. لماذا تريد شركة آبل حماية طرق التشفير الخاصة بها؟ هل تعتقد أن الشركة كانت محقة في حجب المعلومات؟

M01_INFO_ST_55924_U11 Rev 3 FP 08 Aug_AR.indd 146 03/05/2025 12:17:52

الشكل 11.2 العملية عند الوصول إلى موقع إلكتروني باستخدام بروتوكول HTTPS

بالتشفير غير المتماثل لأن مفاتيح مختلفة تُستخدم لتشفير وفك تشفير البيانات. يتوافر المفتاح العام لأي شخص، في ما يبقى المفتاح الخاص سريًا على خادم الويب. ولا يمكن فك تشفير البيانات المشفرة بالمفتاح العام إلا باستخدام المفتاح الخاص.

عندما يريد المستخدم الوصول إلى موقع إلكتروني باستخدام بروتوكول HTTPS، يتم اتباع العملية الموضحة في الشكل 11.2.

إن عملية تشفير كميات كبيرة من البيانات باستخدام تشفير المفتاح غير المتماثل ليست فعالة. ولذلك لا تُستخدم إلا في نقل مفتاح جلسة العمل بين العميل والخادم. يتم تشفير بقية بيانات جلسة العمل وفك تشفيرها باستخدام مفتاح جلسة العمل.

وقفة للتفكير

يسبق التشفير عصر الحاسوب؛ إذ استخدم للعديد من الأغراض المختلفة التي تتطلب الحفاظ على سرية المعلومات.

- كيف يحافظ التشفير على أمن البيانات؟
- يستخدم نظام المفاتيح العامة/الخاصة مفاتيح غير متماثلة، حيث تُستخدم المفاتيح المختلفة لتشفير البيانات وفك تشفيرها. ما تشفير المفتاح المتماثل وكيف يختلف؟

تلميح يمكنك البحث عن هذه المصطلحات على الإنترنت.

توسيع الأفق في الوقت الذي باتت فيه أجهزة الحاسوب أكثر قوة، فقد أصبح اختراق طرق التشفير التي تستخدم طول المفتاح القصير فقط أسهل. ما سبب ذلك؟

M01_INFO_ST_55924_U11 Rev 3 FP 08 Aug_AR.indd 147 03/05/2025 12:17:53

حماية الشبكة المحلية اللاسلكية

الشبكات المحلية اللاسلكية (WLAN)، المعروفة باسم شبكات Wi-Fi، معرضة بشكل خاص لاعتراض البيانات لأنها، على عكس الشبكة السلكية، تبث البيانات على شبكة قائمة على الراديو حتى يتمكن أي شخص في النطاق من اعتراض الرسائل. هناك العديد من التقنيات المستخدمة للمساعدة على حماية شبكات Wi-Fi.

إخفاء معرف مجموعة الخدمة (SSID)

كل شبكة WLAN تحتوي على واحدة أو أكثر من نقاط الوصول اللاسلكية التي توفر رابطًا بين الشبكة اللاسلكية القائمة على الراديو والشبكة المحلية السلكية والإنترنت. في الشبكة المنزلية، غالبًا ما تُعرف هذه النقاط باسم أجهزة التوجيه ذات النطاق العريض. معرف SSID هو اسم شبكة Wi-Fi، وعندما يبحث المستخدم عن شبكات Wi-Fi المتاحة للاتصال على جهازه، يتم عرض معرفات SSID للشبكات في النطاق. يمكنك ضبط نقطة الوصول بحيث لا تبث معرف SSID؛ حيث يحتاج أي شخص يرغب في استخدام الشبكة إلى معرفة معرف SSID. وهذه الطريقة توفر مستوى أساسي جدًّا من الأمان، إذ يمكن للمهاجم الذي يمتلك الأدوات الصحيحة العثور بسهولة على معرف SSID حتى إذا لم يتم بثه.

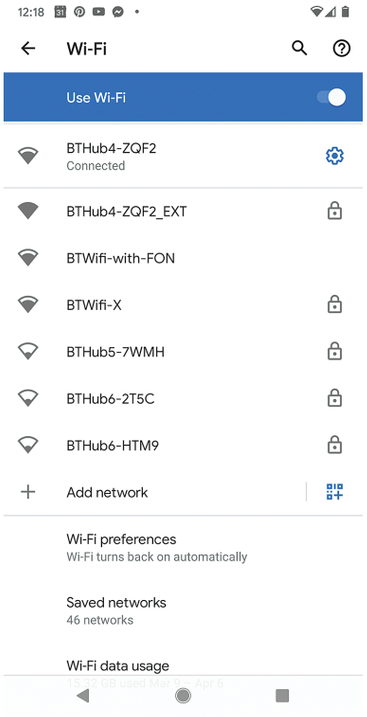
تصفية عناوين MAC

كل جهاز شبكة لديه عنوان مادي فريد يُعرف باسم عنوان التحكم في الوصول إلى الوسائط (MAC). ويتم تضمين هذا العنوان في الجهاز ولا يمكن تغييره بسهولة. لتحسين أمان شبكة WLAN، يمكنك تكوينها بحيث تقبل الاتصالات من أجهزة معينة بناءً على عنوان MAC الخاص بها. وعلى الرغم من أن هذا يزيد من أمان الشبكة، لأن الأجهزة المعتمدة فقط يمكنها الاتصال، إلا أنه قد يكون غير مناسب نظرًا إلى أنه يجب تحديد وإدخال عنوان MAC لأي جهاز جديد يرغب في الانضمام إلى الشبكة في قائمة الأجهزة المسموح بها في نقاط الوصول. ولن تمنع تصفية عناوين MAC مهاجمًا مصممًا وذو معرفة، إذ باستخدام الأدوات المناسبة لن يكون من الصعب تحديد عناوين MAC المسموح بها على النظام ثم تزوير هذا العنوان على جهاز للوصول إلى الشبكة.

التشفير اللاسلكي

الطريقة الأساسية لحماية البيانات المرسلة عبر شبكة WLAN هي تشفير هذه البيانات، يتم ذلك باستخدام كلمة مرور Wi-Fi لتشفير جميع البيانات المرسلة عبر الشبكة اللاسلكية. تم تطوير معايير مختلفة للتشفير اللاسلكي على مر الزمن.

- **WEP** (سياسة المكافئ السلكي) كان المعيار الأصلي لتشفير شبكات Wi-Fi، لكنه يمكن كسره خلال دقائق باستخدام أدوات متاحة بشكل شائع، إذ يستخدم WEP مفاتيح قصيرة نسبيًّا (64 أو 128 بت) ويُستخدم المفتاح نفسه لكل حزمة بيانات.
- **WPA** (الوصول المحمي عبر Wi-Fi) هو معيار تم تقديمه حوالي عام 2003 لمعالجة نقاط الضعف في WEP، واستخدم مفاتيح 256 بت ومفاتيح مختلفة لكل حزمة. ونظرًا لحقيقة أن WPA صُمِّم للسماح بترقية أجهزة WEP إلى WPA، فقد ظهرت أيضاً إمكانية كسره بسهولة نسبية.
- **WPA2** (الوصول المحمي عبر Wi-Fi 2) عالج نقاط الضعف في WPA وأصبح معيارًا رسميًّا في عام 2006، وهو يستخدم نظام التشفير المتقدم (AES) القوي ويعتبر أكثر معايير الأمان اللاسلكي المتاحة حاليًّا أمانًا، وهو المعيار الذي يجب أن تستخدمه جميع شبكات Wi-Fi المنزلية والمؤسسية.
- **WPS** (إعداد الحماية عبر Wi-Fi) ليس معيارًا للتشفير ولكنه طريقة وضعت للسماح للمستخدمين المنزليين بإضافة الأجهزة بسهولة إلى شبكة Wi-Fi. وعادةً ما يسمح هذا المعيار للمستخدمين بالضغط على زر في جهاز التوجيه اللاسلكي وعلى الجهاز الذي يرغبون في توصيله، أو يمكن للمستخدم إدخال رقم PIN مكون من 8 أرقام للانضمام إلى الشبكة. وعلى الرغم من أن WPS معيار مناسب، إلا أنه يحتوي على ثغرة أمنية، إذ يمكن كسر رقم PIN باستخدام **هجمات القوة الغاشمة** في مدة لا تزيد عن أربع ساعات، ويُوصى بتعطيل هذه الميزة على أجهزة التوجيه التي تدعم WPS.



الشكل 11.3 معرّفات مجموعة الخدمة (SSIDs) المدرجة على الجهاز

المصطلح الرئيس

هجوم القوة الغاشمة – هجوم يجرّب فيه المهاجم جميع كلمات المرور أو أرقام التعريف الشخصية الممكنة حتى يعثر على الرقم الصحيح، وكلما كانت كلمة المرور أو رقم التعريف الشخصي أطول، زادت المدة التي قد يستغرقها هجوم القوة الغاشمة.

M01_INFO_ST_55924_U11 Rev 3 FP 08 Aug_AR.indd 148 03/05/2025 12:17:53

جانب آخر يجب مراعاته في ما يتعلق بأمان Wi-Fi هو موقع جهاز التوجيه اللاسلكي، إذ تحتوي معظم أجهزة التوجيه المنزلية على مفتاح Wi-Fi مطبوع على ملصق موجود في الجزء الخلفي من جهاز التوجيه. إذا كان جهاز التوجيه سهل الوصول إليه، يمكن لأي شخص (مثل العمال أو عمال النظافة) الحصول بسهولة على كلمة المرور لشبكة WLAN.

يجب مراعاة المسائل الأمنية في مرحلة تصميم تثبيت شبكة Wi-Fi كبيرة لضمان دمجها من مرحلة التطوير. تشمل بعض الأمثلة على الأمور التي يجب مراعاتها:

- هل ستكون شبكة WLAN مخصصة لموظفي الشركة فقط، أم سيسمح للزوار بالوصول؟
- إذا سُمح للزوار بالوصول إلى Wi-Fi، هل سيشاركون شبكة WLAN نفسها مع الموظفين؟
- هل ستستخدم شبكة WLAN كلمة مرور ثابتة أم ستستخدم كلمات مرور فردية لكل مستخدم؟
- من سيتولى مراقبة الأجهزة المتصلة في أي وقت معين؟

وقفة للتفكير أحيانًا تكون "نقاط اتصال" Wi-Fi "مفتوحة" ولا تستخدم أي تشفير.

- كيف يمكنك معرفة ما إذا كانت نقطة اتصال Wi-Fi تستخدم التشفير أم لا؟
- ما نوع الأنشطة التي يجب ألا تشارك فيها في أثناء استخدام نقطة اتصال Wi-Fi مفتوحة؟

تلميح عندما تتصل بنقطة اتصال Wi-Fi، سيوفر جهازك معلومات عن الاتصال.

توسيع الأفق كيف تختلف شبكة Wi-Fi عن اتصال بيانات الهاتف المحمول 4G؟

تمرين تقييمي 11.1 A.P.1, A.P2, A.P3, A.M1, AB.D1

وظفتك إحدى الشركات لتقديم الدعم والتوجيه في مجال أمن تكنولوجيا المعلومات. ويتعين عليك كتابة دليل لجميع مستخدمي تكنولوجيا المعلومات يقدم شرحًا لما يأتي:

- تهديدات الأمن السيبراني المختلفة التي يمكن أن تؤثر في أنظمة الشركة.
- ثغرات النظام التي يمكن أن تؤثر في أنظمة الشركة.
- الإجراءات الأمنية (بما في ذلك المادية والبرامج ومكونات الحاسوب) التي يمكن اتخاذها لحماية أنظمة المؤسسة من التهديدات الأمنية.

التخطيط

- ضع خطة لإنجاز المهمة، ذاكرًا فيها جميع الأشياء التي تحتاج إلى القيام بها ومتى ستقوم بها.

التنفيذ

- تأكد من تغطية جميع أنواع التهديدات الأمنية المختلفة.

المراجعة

- اقرأ ما كتبته للتأكد من أنه واضح ومعقول.

M01_INFO_ST_55924_U11 Rev 3 FP 08 Aug_AR.indd 149 03/05/2025 12:17:53

ب استكشاف الآثار الأمنية للأنظمة المتصلة بالشبكة

إنَّ استخدام أنظمة الحاسوب الشبكية من جانب الأفراد وداخل المؤسسات منتشر في نطاق واسع، وتستمر تقنيات الشبكات الجديدة في التطور. ولكن، للشبكات آثار أمنية ويساعد فهم طبيعة الشبكات ومشكلات الأمان على اختيار الشبكات لأغراض مختلفة والتقنية اللازمة لحمايتها.

أنواع الشبكات

استعمالات الشبكات وخصائصها

توجد عدة أنواع مختلفة من الشبكات، وتختلف في نطاقها الجغرافي:

- **شبكة المنطقة المحلية (LAN):** هذا النوع من الشبكات له نطاق جغرافي محدود، عادة داخل مبنى واحد أو مجموعة صغيرة من المباني في الموقع نفسه، وعادة ما تكون شبكة LAN خاصة، بمعنى أنه لا يستخدمها سوى مؤسسة واحدة. عادةً، تتصل شبكات LAN بواسطة أكبال نحاسية أو أكبال الألياف الضوئية. نظرًا لأنها عادة ما تكون داخلية ولا تستخدمها سوى مؤسسة واحدة، فهي أقل عرضة للتهديدات الخارجية، على الرغم من أن الاحتياطات الأمنية ضرورية لحماية اتصالات شبكة LAN بالإنترنت.
- **شبكة المنطقة الواسعة (WAN):** هذا النوع من الشبكات له نطاق جغرافي واسع، وأكثر شبكات WAN شيوعًا هي الإنترنت، الذي يكون مفتوحًا للجمهور. تتصل شبكات WAN عبر أكبال سلكية. ونظرًا لأنها مفتوحة للجمهور، فإن الإنترنت هو المصدر الرئيس للتهديدات الأمنية الخارجية.
- **الشبكة المحلية اللاسلكية (WLAN):** هي شبكة تعتمد على Wi-Fi وعادةً ما يستخدمها المستخدمون في المنازل والمؤسسات. هناك أيضًا شبكات WLAN عامة، وتوجد هذه الشبكات في العديد من الأماكن العامة مثل المحلات التجارية والمقاهي ومحطات السكك الحديدية والمطارات. تتيح هذه الشبكات لأفراد الجمهور الوصول إلى الإنترنت من الأجهزة المحمولة. ونظرًا للطبيعة البثية لشبكة WLAN، يجب اتخاذ الاحتياطات لتجنب اعتراض البيانات من جانب أشخاص غير مقصودين.
- **شبكة منطقة التخزين (SAN):** هي شبكة متخصصة عالية السرعة لأجهزة التخزين، وعادةً ما تُوصَّل عبر أكبال الألياف الضوئية أو أكبال **إيثرنت** عالية السرعة، لكنها لا تشارك عادةً حركة البيانات مع الشبكة المحلية (LAN). تتيح شبكة SAN للخوادم المتعددة الوصول إلى أجهزة التخزين نفسها (عادة الأقراص)، وعادةً ما تستخدمها المؤسسات الكبيرة التي تحتاج إلى تخزين والوصول إلى كميات كبيرة جدًّا من البيانات.
- **الشبكة الشخصية (PAN):** هي شبكة تربط الأجهزة في مساحة العمل الشخصية للمستخدم. على سبيل المثال، يتم توصيل الأجهزة باستخدام معيار Bluetooth. هذه طريقة اتصال لاسلكية قصيرة المدى وذات استهلاك منخفض للطاقة، تُستخدم لتوصيل الأجهزة مثل الهواتف المحمولة بسماعات الرأس الصوتية ولوحات المفاتيح والفأرة بأجهزة الحاسوب والأجهزة الأخرى.

تصنيف الشبكات

يمكن تصنيف الشبكات التي تستخدم تقنية الإنترنت من حيث من يمكنه الوصول إليها.

- **شبكة الإنترانت:** هذه شبكة خاصة داخلية للمؤسسة تستخدم تقنية الإنترنت. وباستخدام متصفحات الإنترنت، يمكن للمستخدمين الوصول إلى المعلومات الخاصة بالمؤسسة والتفاعل مع أنظمة المؤسسة.
- **الشبكة الخارجية:** هذه شبكة إنترانت تشاركها المؤسسة مع شركاء محددين مثل العملاء والموردين وما إلى ذلك. وهذا يسمح لشركاء المؤسسة بالوصول إلى بعض أنظمة المؤسسة. ومع ذلك، يجب اتخاذ الاحتياطات لضمان عدم تمكن المؤسسات الخارجية من الوصول إلى الأنظمة المخصصة للاستخدام الداخلي فقط.

المهارات

المهارات المعرفية/العمليات والإستراتيجيات المعرفية:

- التحليل
- التفسير

المصطلح الرئيس

الإيثرنت – مجموعة من معايير التكنولوجيا التي تطورت في الثمانينيات والتي تحدد طريقة لأجهزة الحاسوب للتحدث مع بعضها بعضًا في الشبكات السلكية واللاسلكية.

M01_INFO_ST_55924_U11 Rev 3 FP 08 Aug_AR.indd 150 03/05/2025 12:17:53

- **الإنترنت:** تصف هذه الكلمة أي شبكة عامة يمكن لأي شخص الوصول إليها.
- **السحابة:** تتعلق تقنية السحابة باستخدام الأنظمة القائمة على الإنترنت لتقديم خدمات كانت تُقدم محليًا في السابق. وأحد الاستخدامات الشائعة لتقنية السحابة هو تخزين الملفات. في السابق، كانت المؤسسات تحتفظ بملفاتها على خادم ملفات موجود في مكاتب المؤسسة. والبديل القائم على السحابة هو تخزين الملفات بواسطة مزود تخزين سحابي (مثل Dropbox) في مكان ما على الإنترنت.

الدمج بين الشبكات السلكية واللاسلكية

يحتاج كل من المستخدمين في المنازل والمؤسسات إلى دمج الشبكات السلكية واللاسلكية. ويتم تزويد المستخدمين المنزليين عادةً بجهاز يُعرف عادةً باسم الموجه اللاسلكي (router)، والذي يقوم بعدة وظائف. يوفر هذا الجهاز رابطًا سلكيًا باستخدام الإنترنت عبر كبل هاتف أو كبل تلفزيون. كما يتضمن نقطة وصول لاسلكية حتى يتمكن المستخدمون من الاتصال لاسلكيًا بالإنترنت، وعادةً ما يتضمن أيضًا عددًا من وصلات الشبكة المحلية السلكية (LAN) بحيث يمكن لجهاز ثابت مثل الحاسوب المكتبي الحصول على اتصال سلكي بالإنترنت.

الشكل 11.4 الجزء الخلفي من جهاز التوجيه اللاسلكي

في المؤسسات، يتم توفير وصلات سلكية للحواسيب المكتبية على مكاتب الموظفين داخل مكاتبهم، كما قد يتم توفير شبكة لاسلكية لتوصيل الأجهزة المحمولة مثل الحواسيب المحمولة والهواتف المحمولة.

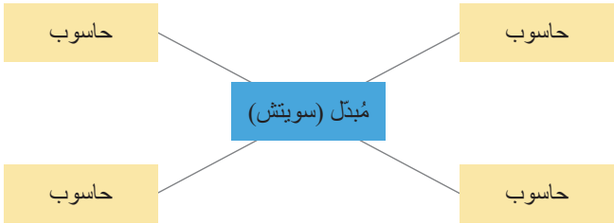
استعمالات مخططات الشبكات وخصائصها

يُقصد بمخططات الشبكة طريقة تنظيم وتوصيل الشبكة، وهي تنقسم إلي قسمين مادي أو منطقي.

المخططات المادية

تصف هذه المخططات كيفية توصيل الأكبال بالأجهزة المختلفة، وتوجد مجموعة متنوعة من المخططات المادية الشائعة الاستخدام:

- **المخطط النجمي** يُستخدم لتكوينات الشبكة المحلية السلكية البسيطة. وفيه، يتم توصيل جميع الأجهزة بمحول مركزي. انظر الشكل 11.5.

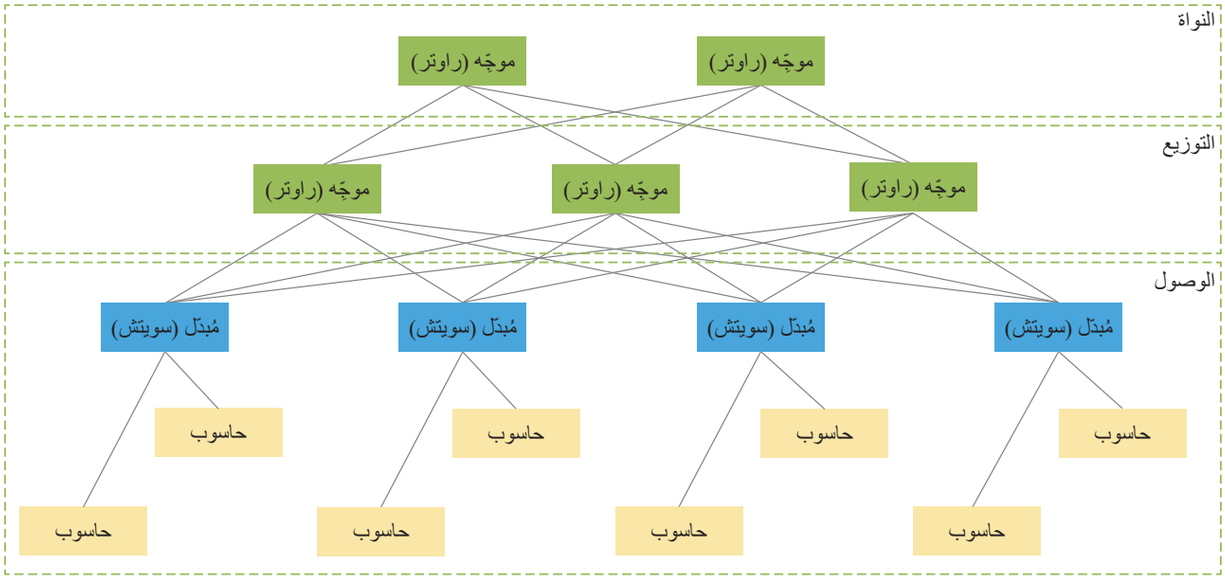


الشكل 11.5 الهيكل النجميّ

- **المخطط النجم الممتد** يستخدم هذا المخطط مفهوم المخطط النجمي نفسه، ولكن يتم تمديده بواسطة مفاتيح إضافية لتوفير المزيد من الاتصالات المتاحة للأجهزة. انظر الشكل 11.6.

الشكل 11.6 الهيكل النجميّ الموسّع

M01_INFO_ST_55924_U11 Rev 3 FP 08 Aug_AR.indd 151
03/05/2025 12:17:57



الشكل 11.7 هيكل الشبكة الهرمي

- **المخطط الهرمي:** يُستخدم هذا المخطط عندما تكون هناك حاجة لإنشاء شبكة كبيرة، وفيه تُقسَّم الشبكة إلى ثلاث طبقات مختلفة. توفر طبقة الوصول (Access Layer) الوصول الفردي للأجهزة إلى الشبكة، وتتحكم طبقة التوزيع (Distribution Layer) في الروابط بين طبقة الوصول وطبقة النواة، وتوفر طبقة النواة (Core Layer) الروابط بين أجهزة التوجيه في طبقة التوزيع. انظر الشكل 11.7.
- **الشبكة اللاسلكية المتشابكة:** يُستخدم هذا المخطط اللاسلكي لتغطية مناطق أكبر مما يمكن أن تغطيه نقطة وصول لاسلكية واحدة. تحتوي الشبكات اللاسلكية المتشابكة على عدد من العقد اللاسلكية التي توفر التغطية على مناطق مثل مكتب أو مستودع. تحتاج إحدى العقد فقط إلى اتصال سلكي بالإنترنت، حيث تشارك كل عقدة اتصالها مع أقرب عقدة إليها.
- **المخطط المخصص:** يستخدم هذا النوع من الشبكات مزيجًا من الشبكات السلكية واللاسلكية. ويمكن العثور على هذا النوع في المكاتب والمباني حيث يتمتع بعض الموظفين بالوصول إلى أجهزة الحاسوب المكتبية السلكية بينما يستخدم آخرون أجهزتهم الخاصة (الهواتف الذكية والأجهزة اللوحية وما إلى ذلك). عندما يتصل الموظفون بشبكة WLAN الخاصة بالشركة باستخدام أجهزتهم الخاصة، يُعرف هذا بمفهوم "إحضار جهازك الشخصي" (BYOD). راجع الجزء الآتي لمزيد من التفاصيل.

المخططات المنطقية

تصف المخططات المنطقية كيفية تواصل الأجهزة على مخطط معين. تنقل الشبكات المحلية السلكية (LAN) البيانات باستخدام تقنية الإيثرنت، بينما تستخدم الشبكات المحلية الحديثة أكبال مزدوجة غير محمية (UTP) وتربط الأجهزة (أجهزة الحاسوب والمفاتيح) باستخدام موصلات RJ45. تصل سرعات نقل البيانات إلى مستويات عالية جدًا (حتى 400 غيغابت في الثانية، اعتمادًا على نوع كبل UTP المستخدم). تعتبر مفاتيح الشبكة التي تربط أجهزة الحاسوب على شبكة الإيثرنت (LAN) أجهزة ذكية، حيث تقوم بفحص حزم البيانات الواردة لتحديد عنوان الشبكة الخاص بها، وترسل الحزمة فقط إلى المنفذ أو المنافذ التي يُقصد بها أن تصل إليها بدلًا من إرسالها إلى جميع المنافذ. تمتد الأكبال في شبكة الإيثرنت إلى طول نظري أقصى يبلغ 100 متر، على الرغم من أن ذلك يمكن أن يعتمد على نوع كبل UTP المستخدم وسرعة الاتصال. يُعد الإيثرنت معيارًا دوليًا يعرف بـ IEEE802.3.

تستخدم الشبكات اللاسلكية معيار اتصال يُعرف بـ IEEE802.11 الذي يشترك في بعض الأوجه مع معيار الإيثرنت السلكي من حيث التحكم في الوصول. تم تطوير إصدارات مختلفة من معيار IEEE802.11 على مر السنين مع زيادة سرعات نقل البيانات وتحسينات أخرى. كان المعيار الأصلي المستخدم في نطاق

M01_INFO_ST_55924_U11 Rev 3 FP 08 Aug_AR.indd 152 03/05/2025 12:17:57

واسع هو 802.11b الذي كان لديه معدل بيانات يبلغ 11 ميغابت في الثانية. وتدعم العديد من الأجهزة الحالية معيار 802.11n الذي يصل معدل بياناته إلى 600 ميغابت في الثانية، وتوجد إصدارات أسرع قيد التطوير حاليًا.

استعمالات بنية الشبكة وخصائصها

- **شبكات النظير إلى النظير:** هذه الشبكات غير منظمة ولا تحتوي على خادم مركزي يتحكم في الشبكة. وفيها يسجل المستخدمون الدخول إلى الحواسيب الفردية، ويمكنهم مشاركة الملفات والموارد مثل الطابعات. تُعد شبكات النظير إلى النظير مثالية للمستخدمين المنزليين أو المكاتب الصغيرة التي تحتوي على عدد محدود من المستخدمين، فهي سهلة الإعداد والإدارة ولا تتطلب أجهزة إضافية. ومع ذلك، تصبح هذه الشبكات صعبة الإدارة عند زيادة حجم الشبكة. ونظرًا لعدم وجود تحكم مركزي، يجب إدارة كل حاسوب بشكل منفصل، ويمكن للمستخدمين تسجيل الدخول فقط إلى الأجهزة التي لديهم حساب عليها.
- **شبكات الخادم والعميل:** تحتوي هذه الشبكات على خادم مركزي، ويسجل المستخدمون الدخول إلى الشبكة بدلًا من حاسوب فردي، لذلك إذا كان لديهم حساب شبكة، يمكنهم تسجيل الدخول في أي حاسوب. تتم إدارة جميع أجهزة الحاسوب في الشبكة مركزيًا على الخادم. وهذا يعني أن التحديثات وإنشاء الحسابات والقيود الأمنية وأذونات الملفات والمجلدات والنسخ الاحتياطية والعديد من الأمور الأخرى يمكن إدارتها مركزيًا على الخادم.
- **العميل منخفض الأداء (الحاسوب الرقيق):** يكون جهاز المستخدم النهائي (العميل في حوسبة العميل والخادم) عادةً قويًا بما يكفي لتشغيل التطبيقات محليًا ولديه سعة تخزين لتخزين الملفات محليًا أيضًا. ولكن مع التقدم الأخير في الشبكات عالية السرعة والمرافق السحابية، يمكن استخدام أجهزة ذات مواصفات أقل تُعرف بالعميل منخفض الأداء. تشغل هذه الأجهزة تطبيقات مستندة إلى الويب (مثل مجموعة تطبيقات Google® Office) وتخزن الملفات على السحابة. نظرًا لأن هذه الأجهزة تحتوي على مواصفات أجهزة أقل، فهي أقل تكلفةً من أجهزة الحاسوب المحمولة أو المكتبية التقليدية. سلسلة أجهزة الحاسوب المحمولة "Chromebook" هي مثال على هذا النوع من التكنولوجيا.

الاتجاهات الحديثة

تميل تكنولوجيا الحوسبة إلى التقدم بمعدل سريع جدًّا؛ وتشمل بعض التقنيات الناشئة الحالية ما يأتي:

- **المحاكاة الافتراضية:** في السابق، كانت الشركات أو المؤسسات الكبيرة تمتلك عددًا من خوادم الحاسوب المختلفة، كل منها يقوم بمهمة معينة. ومع ذلك، من الشائع اليوم أن يستخدم خادم حاسوب قوي برنامجًا افتراضيًّا لتشغيل عدة **أجهزة حواسيب افتراضية** لتنفيذ مهام محددة. وإنشاء عدة خوادم على جهاز حاسوب مادي واحد يجعل إدارة أعباء العمل أسهل ويحسن من قابلية التوسع، كما أنه يستخدم الأجهزة بشكل أكثر كفاءة.
- **الحوسبة السحابية:** سبق ذكر الحوسبة السحابية في سياق التخزين السحابي، ولكن هناك عدة طرق أخرى يمكن من خلالها استخدام تقنية السحابة:
  - **التطبيقات السحابية**: هي تطبيقات برمجية تعمل على خادم في السحابة بدلًا من تشغيلها على جهاز المستخدم المحلي، ويتم الوصول إليها عبر برامج متصفحات الويب. مثال على هذا النوع من التطبيقات هو Google Docs، ويُطلق أحيانًا على هذا النوع من خدمات السحابة "البرمجيات كخدمة" (SaaS).
  - **منصة تطوير البرمجيات السحابية**: هي خدمة تُقدم لمطوري البرمجيات حيث يقوم مزود خدمة السحابة بإنشاء بيئة تطوير تشمل أدوات تطوير البرامج وقواعد البيانات وخدمات الويب. ويُعرف هذا أحيانًا باسم "المنصة كخدمة" (PaaS).

تثير الحوسبة السحابية تخوفات أمنية للمؤسسات، حيث تنتقل مسؤولية حماية بيانات المؤسسة إلى مزود خدمة السحابة، وتشمل الآتي:

- **إحضار جهازك الشخصي (BYOD):** السماح للموظفين باستخدام أجهزتهم المحمولة الشخصية (مثل الهواتف الذكية) له مزايا لكل من أصحاب العمل والموظفين؛ فهو يوفر درجة أكبر من المرونة في

المصطلح الرئيس

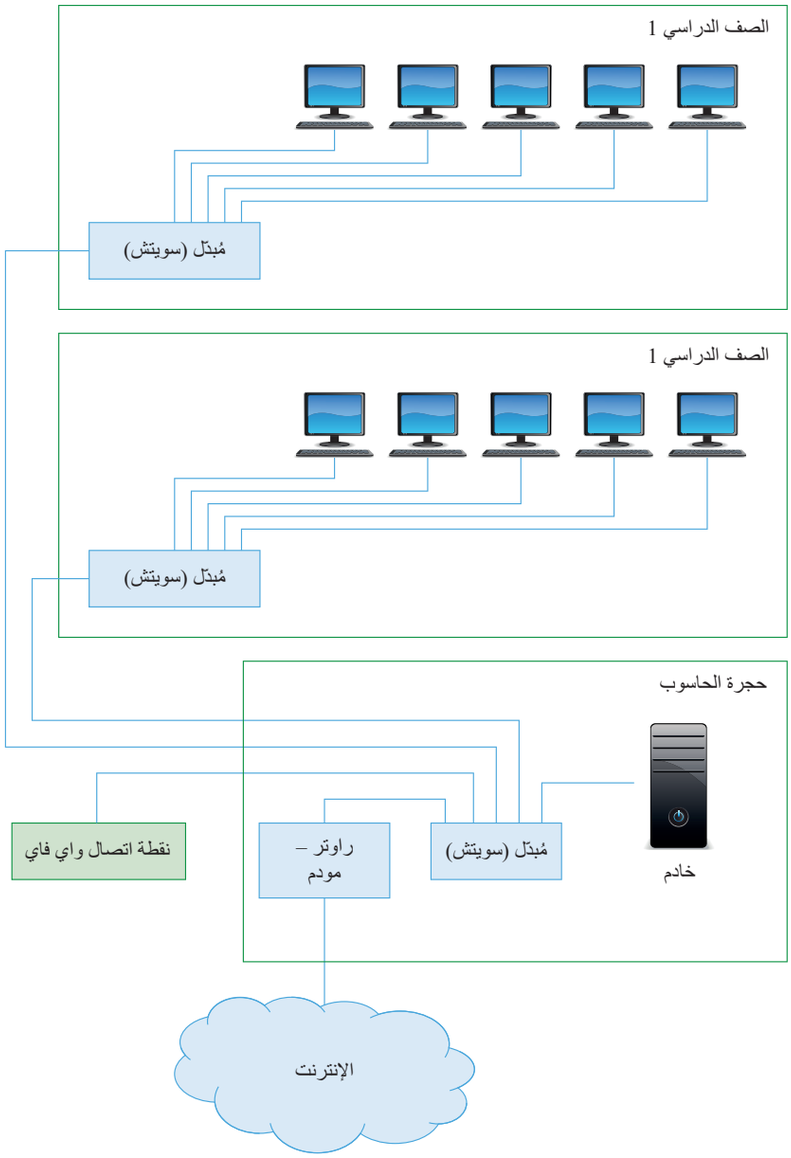
الحاسوب الافتراضي – محاكاة برمجية لمكونات الحاسوب تسمح باستضافة نسخة منفصلة من نظام التشغيل والتطبيقات المرتبطة به على جهاز حاسوب مادي موجود. وهذا الأمر من شأنه أن يسمح لحاسوب مادي واحد باستضافة عدد من أجهزة الحواسيب الافتراضية المختلفة التي يحتمل أن تشغِّل أنظمة تشغيل وتطبيقات مختلفة.

M01_INFO_ST_55924_U11 Rev 3 FP 08 Aug_AR.indd 153 03/05/2025 12:17:57

تطبيق النظرية

عُرضت بعض مخططات هيكل الشبكة سابقًا ويرد مثال آخر في الشكل 11.8.

أنشئ مخطط هيكل شبكة بسيط للشبكة في مدرستك أو كليتك باستخدام أدوات Microsoft Word Drawing أو برامج الرسم الأخرى مثل Visio أو استخدم أحد المخططات وأضف رابط إنترنت حاسوب خادم ورابط Wi-Fi.



الشكل 11.8 مثال لهيكل الشبكة

M01_INFO_ST_55924_U11 Rev 3 FP 08 Aug_AR.indd 154 03/05/2025 12:17:59

العمل، وغالبًا ما يشعر الموظفون براحة أكبر عند استخدام أجهزتهم الشخصية. ومع ذلك، فإن السماح لهذه الأجهزة بالوصول إلى أنظمة الشركة يثير مسألة أمنية كبيرة. فهذه الأجهزة ليست تحت سيطرة الشركة بالكامل، وقد لا تحتوي على إعدادات أمان قوية بما يكفي.

- **الشبكات المحددة بالبرامج (SDN):** هذه طريقة أكثر مرونة للشبكات مقارنة بالبُنى التقليدية للشبكات؛ توفر شبكات SDN قدرات شبيهة بالسحابة داخل شبكة الشركة الداخلية؛ إذ تحتوي على وحدات تحكم تتيح لمديري الشبكات طريقة لإدارة وتكوين الشبكة. تمتلك شبكة SDN أيضًا اتصالات بأجهزة وتطبيقات الشبكات.
- **الشبكات المعرفة بالتخزين:** هذه طريقة لتوصيل أجهزة التخزين مباشرةً بشبكة لتكون متاحة لجميع مستخدمي الشبكة للوصول إليها. وتُستخدم هذه الشبكات عادةً في المؤسسات الكبيرة حيث يمكن أن يستفيد المستخدمون من الوصول السهل إلى كميات كبيرة من البيانات.
- **إنترنت الأشياء (IoT):** هذا المفهوم يتعلق بتوصيل أي جهاز إلكتروني (طالما يمكن تشغيله وإيقافه) بالإنترنت والأجهزة الإلكترونية الأخرى.

وقفة للتفكير

تشهد تكنولوجيا الحوسبة تطورًا متسارعًا، حيث باتت الميزات والمرافق الجديدة متاحة طوال الوقت. ومع ذلك، تأتي كل تقنية جديدة بمشكلات أمنية وفرص يمكن للمجرمين من خلالها استغلال نقاط الضعف المحتملة.

ما الآثار الأمنية المترتبة على إنترنت الأشياء؟

لماذا تشعر المؤسسات بالقلق إزاء تأثير استخدام الجهاز الشخصي في العمل (BYOD)؟ ما المشكلات الأمنية المحتملة؟

تشمل الاتجاهات الحالية الأخرى الذكاء الاصطناعي والروبوتات. تعرّف الآثار الأمنية المترتبة على استخدام هذه التقنيات.

تلميح

نظرًا لأن قضايا التكنولوجيا والأمن تتطور وتتغير طوال الوقت، فإن أفضل مكان للبحث في هذه الموضوعات هو الإنترنت.

توسيع الأفق

ما الاتجاهات أو التطورات الأخرى أو الحديثة في مجال تكنولوجيا المعلومات؟ استكشفها وآثارها الأمنية.

مكونات الشبكة

تتكون الشبكات من مجموعة متنوعة من الأجهزة المختلفة، ولكل منها وظائف مختلفة.

المهارات

المهارات المعرفية/العمليات والإستراتيجيات المعرفية:

- التحليل
- حل المشكلات

المكونات من الأجهزة

- **أجهزة المستخدم النهائي.** هذه هي الأجهزة التي توفر واجهة للمستخدمين البشريين وتشمل أجهزة الحاسوب المكتبية والمحمولة والأجهزة المحمولة مثل الأجهزة اللوحية والهواتف الذكية.
- **أجهزة الاتصال:**
  - **المحولات:** تُستخدم داخل شبكة LAN السلكية لتوصيل الأجهزة. وتقوم المحولات بتوجيه البيانات إلى الجهاز النهائي الذي تم توجيهها إليه.
  - **أجهزة التوجيه:** تعمل مثل تقاطع طريق حيث تقوم بإرسال حزم البيانات إلى شبكات أو أجزاء مختلفة من الشبكات بناءً على عنوان IP الخاص بالوجهة.
  - **نقاط الوصول:** توفر رابطًا بين شبكة LAN السلكية والشبكة اللاسلكية.
  - **موزعات USB:** الأجهزة التي تسمح بتوصيل أجهزة USB متعددة (مثل الطابعات والأقراص الصلبة الخارجية وما إلى ذلك) بجهاز حاسوب.
  - **أجهزة المودم:** تُستخدم لتوصيل شبكة LAN بالإنترنت، ويوجد نوعان من أجهزة المودم يُستخدمان في نطاق واسع، إذ يتصل مودم ADSL بالإنترنت عبر خط هاتف تقليدي، بينما يتصل مودم الكبل عبر تلفزيون الكبل حيثما كان متاحًا.

M01_INFO_ST_55924_U11 Rev 3 FP 08 Aug_AR.indd 155 03/05/2025 12:17:59

- **الأجهزة متعددة الوظائف**: يُزوّد مزود خدمة الإنترنت (ISP) معظم المستخدمين المنزليين بجهاز متعدد الوظائف يجمع بين المودم والموجه ونقطة الوصول اللاسلكية والمحول السلكي.

- **وسائط الاتصال**:
  - **الأكبال**: يُعد الكبل الأكثر شيوعًا في الشبكات المحلية هو الكبل الثنائي المجدول غير المعزول، والذي يحتوي على أربعة أزواج من الأكبال النحاسية المجدولة معًا لتقليل التداخل. توجد عدة "فئات" من الأكبال الثنائية المجدولة غير المعزولة، وأدنى فئة مناسبة للشبكات الحاسوبية هي الفئة 5، والمعروفة باسم Cat 5. ويوضح الجدول 11.1 أدناه الفئات المختلفة من الأكبال الثنائية المجدولة غير المعزولة ومميزاتها.

الجدول 11.1 فئات الكبل الثنائي المجدول غير المعزول ومميزاته

فئة الكبل الثنائي المجدول غير المعزول	السرعة القصوى	طول المقطع
5	100 ميجابت/ثانية	100 متر
5e	1 جيجابت/ثانية	100 متر
6	10 جيجابت/ثانية	55 م
7	10 جيجابت/ثانية	100 متر

في حالات وجود تداخل كهربائي كبير (مثل المستودعات أو المصانع)، يمكن استخدام الكبل الثنائي المجدول المعزول، حيث يحتوي هذا النوع من الأكبال على عازل من الألومنيوم حول الأكبال المجدولة.

- **الكبل الليفي الضوئي**: عندما تكون هناك حاجة إلى روابط عالية السرعة، يمكن استخدام الكبل الليفي الضوئي، حيث تستخدم هذه الأكبال الضوء لنقل البيانات بدلًا من الإشارات الكهربائية. ويمكن تشغيل كبل الألياف الضوئية عبر مسافات أكبر بكثير من الأكبال الثنائية المجدولة غير المعزولة، ما يعني أنه يمكن استخدامه في اتصالات شبكة الاتصال واسعة النطاق من الشبكات المحلية فقط. تستخدم شركات الهاتف والإنترنت واسع النطاق كبلات الألياف الضوئية بديلًا لكبل الهاتف النحاسي التقليدي لتوفير اتصالات إنترنت ذات سرعة أكبر مما يمكن توفيره عبر كبلات الهاتف. تقليديًا، كانت كبلات الألياف الضوئية تتمتع بمعدلات نقل بيانات أسرع من الأكبال الثنائية المجدولة غير المعزولة ولكن أحدث إصدارات الأكبال الثنائية المجدولة غير المعزولة (Cat 7) تتمتع بنفس سرعة النقل التي توفرها كبلات الألياف. تعتبر كبلات الألياف الضوئية أكثر أمانًا من الأكبال الثنائية المجدولة غير المعزولة (UTP) نظرًا لأنه لا يوجد تسرب للإشارة خارج الكبل ومن الصعب جدًّا التلاعب بكبل الألياف دون التسبب في تسرب الضوء.
- **الوسائط اللاسلكية**: مثل Wi-Fi تستخدم موجات الراديو بدلًا من أي نوع من الأكبال. ويُمثل هذا الأمر ميزتها الرئيسة وكذلك عيبها. حيث لا تحتاج إلى تركيب كبلات لتوصيل الأجهزة، ما يعد فائدة كبيرة لكل من المستخدمين المنزليين والمستخدمين في المنظمات إذ يمكنهم التنقل بحرية بالأجهزة دون تكاليف أو اضطراب في تركيب الأكبال. ومع ذلك، نظرًا لبث الإشارة للجميع، فمن السهل جدًّا التجسس على الشبكة اللاسلكية وقد تمتد الإشارة لمسافة خارج المنزل أو المكتب حيث يُقصد استخدامها. عندما تكون مسألة الأمان مهمة، يجب الحرص على استخدام الشبكة البيانات المشفرة وإعدادها بشكل صحيح. وقد تعاني الشبكات اللاسلكية وجود نقاط ميتة حيث لا تكون هناك إشارة متاحة، خاصة في المنازل أو المكاتب التي تحتوي على جدران وأرضيات داخلية. ودون استخدام أجهزة إعادة الإرسال أو أنظمة الشبكات اللاسلكية، يكون النطاق محدودًا.
- **البلوتوث والأشعة تحت الحمراء**: البلوتوث هو نظام لاسلكي قصير المدى يستهلك طاقة منخفضة ويُستخدم عادةً لتوصيل الأجهزة الصغيرة (مثل سماعات الرأس ولوحات المفاتيح/ الفأرة) بأجهزة الحاسوب أو الأجهزة المحمولة. أما الأشعة تحت الحمراء فهي وسيلة للاتصال اللاسلكي تستخدم الإشعاع الكهرومغناطيسي ذات طول موجي أطول بقليل من الضوء الأحمر (ولكن أقصر من موجات الراديو). الاتصال بالأشعة تحت الحمراء قصير المدى وخط الرؤية فقط (لا يمكن أن تكون هناك عوائق بين المرسل والمستقبل). وتُستخدم الأشعة تحت الحمراء بكثرة في أجهزة التحكم عن بُعد الخاصة بالتلفزيون.

M01_INFO_ST_55924_U11 Rev 3 FP 08 Aug_AR.indd 156 03/05/2025 12:17:59

– وتُعد تقنية **Li-Fi** تقنية مشابهة لتقنية Wi-Fi لكنها تستخدم الضوء بدلًا من موجات الراديو، كما أن لديها القدرة على توفير نطاق ترددي أعلى وسرعات نقل أسرع. ويمكن استخدامها أيضًا في المناطق التي لا يمكن فيها استخدام Wi-Fi بسبب التداخل الكهرومغناطيسي، مثل مقصورات الطائرات. التكنولوجيا قيد التطوير حاليًا.

الجدول 11.2 مقارنة بين أنواع الوسائط المختلفة

	الكبل الثنائي المجدول غير المعزول	الألياف الضوئية	الاتصال اللاسلكي
المسافة	متوسط (الشبكة المحلية فقط)	طويل	قصير
السرعة	مرتفع (بحسب نوع الكبل)	مرتفع	منخفض/ متوسط (يعتمد على الإصدار)
سهولة التثبيت	صعبة	صعبة	سهل
الأمان	يمكن اعتراضها	يصعب اعتراضها	يسهل اعتراضها
التكلفة	متوسطة	مرتفع	منخفضة

- **الوسائط الخارجية والتخزين**: قبل انتشار التخزين السحابي، كان استخدام الوسائط الخارجية للتخزين غير المتصل بالإنترنت ونقل ملفات البيانات شائعًا. ويشمل الآتي:

– **محركات أقراص USB المحمولة**: (المعروفة أيضًا باسم محركات فلاشة التخزين أو الذاكرة المحمولة): يتم توصيل هذه الأجهزة الصغيرة بمنفذ USB للحاسوب وتخزين الملفات بسعة تصل إلى حوالي 64 جيجابايت. وهي مفيدة لنقل الملفات بين الحواسيب التي قد تكون كبيرة جدًّا بحيث لا يمكن إرسالها على أنها مرفقًا لرسالة بريد إلكتروني. ومع ذلك، فهي تمثل مصدر قلق أمني كبير حيث يمكن فقدها بسهولة ويمكن استخدامها لنشر الفيروسات من حاسوب إلى آخر. ولهذا السبب، تحظر العديد من المنظمات استخدامها. وفي معظم الحالات، يوفر التخزين السحابي خيارًا أفضل باستثناء حالة عدم وجود اتصال بالإنترنت. ويمكن أن توفر محركات أقراص USB المحمولة أيضًا طريقة بسيطة للمستخدمين المنزليين لنسخ ملفاتهم احتياطيًا.

– **الوسائط البصرية**: كانت الأقراص المضغوطة (CDs) وأقراص الفيديو الرقمية (DVDs) تستخدم في نطاق واسع أيضًا، خاصة لتوزيع البرمجيات، ومع ذلك، يتم الآن تنزيل جميع تطبيقات البرامج تقريبًا عبر الإنترنت بدلًا من توزيعها على قرص مضغوط (CD) أو أقراص الفيديو الرقمية (DVD).

وقفة للتفكير ما نوع الشبكة الموجودة في مدرستك أو كليتك؟

- ما الهيكل الذي تستخدمه؟
- ما نوع الأكبال أو شبكة Wi-Fi التي تستخدمها؟
- ما أجهزة الاتصال التي تستخدمها؟
- ما طرق حماية الأمن السيبراني المطبّقة لديها؟

تلميح قد يتمكن معلمك أو مدير تكنولوجيا المعلومات من مساعدتك على ذلك.

توسيع الأفق كيف يمكن ترقية الشبكة وطرق حمايتها؟

أنظمة التشغيل

يحتاج كل حاسوب إلى نظام تشغيل للتحكم في الأجهزة وتوفير واجهة مستخدم. يمكن تقسيم أنظمة التشغيل إلى أنظمة تدعم الأجهزة الفردية وأنظمة تدعم النظام المتصل بالشبكة.

- **أنظمة تشغيل الهواتف المحمولة**: تُشغل هذه الأنظمة الأجهزة المحمولة مثل الهواتف الذكية والأجهزة اللوحية، وهي مُصممة لدعم مستخدم واحد لكل جهاز، ومن الأمثلة على ذلك أندرويد وأبل iOS.

M01_INFO_ST_55924_U11 Rev 3 FP 08 Aug_AR.indd 157 03/05/2025 12:17:59

- **أنظمة تشغيل الحاسوب المكتبي والحاسوب المحمول**: صُممت هذه الأنظمة لتكون بمنزلة أنظمة التشغيل للمستخدم النهائي للعمل على الأجهزة ذات الشاشات الكبيرة وتوفر مجموعة كاملة من الوظائف. ومن الأمثلة على ذلك Microsoft Windows وMacOS. وتدعم هذه الأنظمة حسابات مستخدمين متعددة على جهاز واحد، ولكن يُمكن لمستخدم واحد فقط العمل على جهاز الحاسوب في وقت واحد. يأتي نظام Microsoft Windows بإصدارين: إصدار "Home" وهو مُخصص للاستخدام المنزلي ويعمل في شبكة نظير إلى نظير، ونسخة "Enterprise" (أحيانًا تُسمى "Professional") التي يمكنها العمل في كل من شبكات النظير إلى نظير وشبكات العميل/الخادم.
- **أنظمة تشغيل الخادم**: وتشمل هذه الأنظمة الميزات التي لا تركز على المستخدمين النهائيين لكنها توفر بدلًا من ذلك أدوات للسماح لمدير النظام بدعم شبكة خادم العميل. وتتيح أنظمة تشغيل الخوادم للمستخدمين عن بُعد الوصول إلى الخدمات التي تُقدمها بشكل متزامن. ومن أمثلة أنظمة تشغيل الخادم Microsoft Windows ولينوكس.

أدوات الشبكة

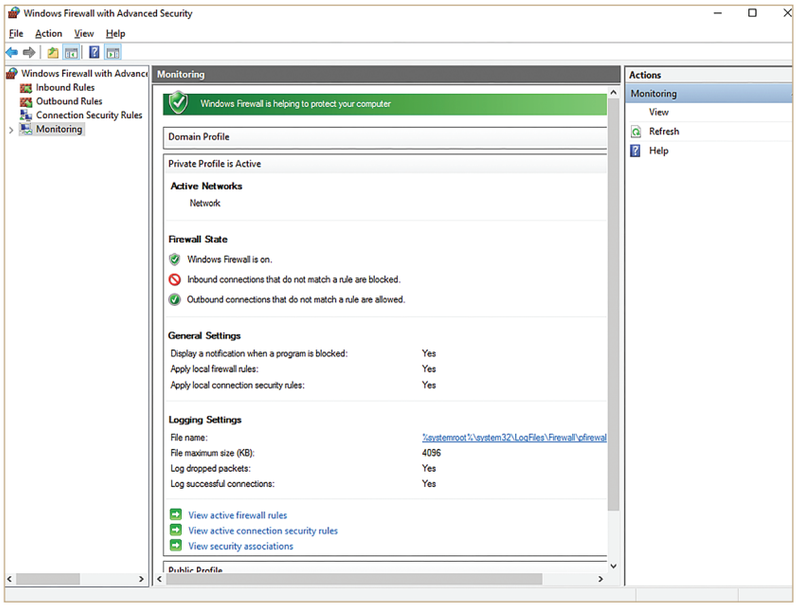
تُوفر أدوات الشبكات لمديري النظام الإمكانات اللازمة لإعداد الشبكة وإدارتها واستكشاف الأخطاء فيها، كما يمكن استخدامها أيضًا لحماية النظام والتحقيق في مشكلات الأمان. وتوجد العديد من أدوات الشبكة المتاحة.

- **مراقبة الشبكة**: يستخدم مديرو النظام هذا البرنامج لمراقبة أداء الشبكة والتأكد من عدم وجود اتصالات معطلة.

تطبيق النظرية

أدوات إدارة الشبكة

ينشئ جدار حماية Windows سجل. وإذا فتحت تطبيق إدارة جدار الحماية واخترت رابط المراقبة على اليمين، سترى رابطًا ينقلك إلى قسم التسجيل، انظر الشكل 11.10. وعليك التحقق من أن خاصية التسجيل تسجل الحزم المرفوضة (المحظورة) وإلا فلن يحتوي ملف السجل على شيء.



الشكل 11.9 عرض المراقبة لجدار حماية Windows

M01_INFO_ST_55924_U11 Rev 3 FP 08 Aug_AR.indd 158 03/05/2025 12:17:59

تطبيق النظرية متابعة

وسيؤدي النقر فوق الرابط إلى فتح السجل. يوضح الشكل 11.10 أحد الأمثلة على ذلك.

```
pfirewall.log - Notepad
File  Edit  Format  View  Help
#Version: 1.5
#Software: Microsoft Windows Firewall
#Time Format: Local
#Fields: date time action protocol src-ip dst-ip src-port dst-port size tcpflags tcpsyn tcpack tcpwin icmptype icm


2016-04-04 21:22:40 ALLOW UDP fe80::14e8:178e:a946:9a55 ff02::1:2 546 547 0 - - - - - - - SEND
2016-04-04 21:22:51 ALLOW UDP 192.168.1.162 192.168.1.255 137 137 0 - - - - - - - SEND
2016-04-04 21:22:51 ALLOW UDP fe80::61f7:e8a7:9312:af77 ff02::1:3 59860 5355 0 - - - - - - - SEND
2016-04-04 21:22:51 ALLOW UDP 192.168.1.162 224.0.0.252 59860 5355 0 - - - - - - - SEND
2016-04-04 21:22:51 ALLOW UDP fe80::61f7:e8a7:9312:af77 ff02::1:3 55634 5355 0 - - - - - - - SEND
2016-04-04 21:22:51 ALLOW UDP 192.168.1.162 224.0.0.252 55634 5355 0 - - - - - - - SEND
2016-04-04 21:22:51 ALLOW TCP 192.168.1.162 40.127.129.109 50783 443 0 - 0 0 0 - - - SEND
2016-04-04 21:22:51 ALLOW TCP 192.168.1.162 40.127.129.109 50784 443 0 - 0 0 0 - - - SEND
2016-04-04 21:22:55 ALLOW UDP fe80::61f7:e8a7:9312:af77 ff02::1:2 546 547 0 - - - - - - - SEND
2016-04-04 21:22:56 ALLOW UDP fe80::14e8:178e:a946:9a55 ff02::1:2 546 547 0 - - - - - - - SEND
2016-04-04 21:23:06 ALLOW UDP 192.168.1.162 192.168.1.254 62219 53 0 - - - - - - - SEND
2016-04-04 21:23:06 ALLOW UDP 192.168.1.162 192.168.1.255 137 137 0 - - - - - - - SEND
2016-04-04 21:23:06 ALLOW UDP fe80::61f7:e8a7:9312:af77 ff02::1:3 62002 5355 0 - - - - - - - SEND
2016-04-04 21:23:06 ALLOW UDP 192.168.1.162 224.0.0.252 62002 5355 0 - - - - - - - SEND
2016-04-04 21:23:06 ALLOW UDP fe80::61f7:e8a7:9312:af77 ff02::1:3 51178 5355 0 - - - - - - - SEND
2016-04-04 21:23:06 ALLOW UDP 192.168.1.162 224.0.0.252 51178 5355 0 - - - - - - - SEND
2016-04-04 21:23:09 ALLOW TCP 192.168.1.181 192.168.1.162 50642 3389 0 - 0 0 0 - - - RECEIVE
2016-04-04 21:23:13 ALLOW TCP 192.168.1.181 192.168.1.162 50644 3389 0 - 0 0 0 - - - RECEIVE
2016-04-04 21:23:15 ALLOW UDP 192.168.1.181 192.168.1.162 55708 3389 0 - - - - - - - RECEIVE
2016-04-04 21:23:19 ALLOW TCP 192.168.1.162 131.253.61.98 50785 443 0 - 0 0 0 - - - SEND
2016-04-04 21:23:27 ALLOW UDP fe80::61f7:e8a7:9312:af77 ff02::1:2 546 547 0 - - - - - - - SEND
2016-04-04 21:23:28 ALLOW UDP 192.168.1.162 192.168.1.254 52808 53 0 - - - - - - - SEND
2016-04-04 21:23:28 ALLOW UDP fe80::14e8:178e:a946:9a55 ff02::1:2 546 547 0 - - - - - - - SEND
2016-04-04 21:23:28 ALLOW TCP 192.168.1.162 207.46.101.29 50786 80 0 - 0 0 0 - - - SEND
2016-04-04 21:23:41 ALLOW UDP 192.168.1.162 192.168.1.254 62123 53 0 - - - - - - - SEND
2016-04-04 21:23:41 ALLOW UDP 192.168.1.162 192.168.1.254 54112 53 0 - - - - - - - SEND
2016-04-04 21:23:41 ALLOW UDP 192.168.1.162 192.168.1.254 56627 53 0 - - - - - - - SEND
2016-04-04 21:23:41 ALLOW UDP 192.168.1.162 192.168.1.254 49706 53 0 - - - - - - - SEND
2016-04-04 21:23:41 ALLOW UDP 192.168.1.162 192.168.1.254 53170 53 0 - - - - - - - SEND
```

الشكل 11.10 سجل جدار الحماية

قد يساعد عرض السجل مدير النظام على تحديد إحدى المحاولات التي يقوم بها المتسلل للوصول إلى النظام.

تُعد هذه واحدة من أبسط أدوات استكشاف الأخطاء وإصلاحها وأكثرها استخدامًا في برنامج «ping». يمكن تشغيل Ping من موجه أوامر Windows، حيث يسمح لك بالتحقق من أن جهازك يمكنه الحصول على استجابة عبر الشبكة المحلية و/أو الإنترنت من جهاز بعيد، باستخدام عنوان IP الخاص به أو عنوان URL الخاص به. يعد هذا اختبارًا مفيدًا منخفض المستوى للتأكد من وجود الاتصال. يوضح الشكل 11.11 استخدام أمر ping لاختبار الارتباط بجهاز محلي بحسب عنوان IP (192.168.1.236) والخادم البعيد بحسب عنوان (www.google.com) URL.

```
Command Prompt
C:\Users\Alan>ping 192.168.43.5

Pinging 192.168.43.5 with 32 bytes of data:
Reply from 192.168.43.5: bytes=32 time=4ms TTL=64
Reply from 192.168.43.5: bytes=32 time=5ms TTL=64
Reply from 192.168.43.5: bytes=32 time=4ms TTL=64
Reply from 192.168.43.5: bytes=32 time=4ms TTL=64

Ping statistics for 192.168.43.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 4ms, Maximum = 5ms, Average = 4ms

C:\Users\Alan>ping www.google.com

Pinging www.google.com [2a00:1450:4009:809::2004] with 32 bytes of data:
Reply from 2a00:1450:4009:809::2004: time=49ms
Reply from 2a00:1450:4009:809::2004: time=60ms
Reply from 2a00:1450:4009:809::2004: time=62ms
Reply from 2a00:1450:4009:809::2004: time=57ms

Ping statistics for 2a00:1450:4009:809::2004:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 49ms, Maximum = 62ms, Average = 57ms

C:\Users\Alan>
```

الشكل 11.11 استخدام أمر Ping

ولاحظ أن بعض الأجهزة لن تستجيب لطلبات ping لأنها تعتبر خطرًا أمنيًا. فكّر في سبب اعتبار الاستجابة لطلبات ping خطرًا أمنيًا.

M01_INFO_ST_55924_U11 Rev 3 FP 08 Aug_AR.indd 159 03/05/2025 12:18:00

- **الإدارة واستكشاف الأخطاء وإصلاحها**: تُستخدم أدوات الإدارة واستكشاف الأخطاء وإصلاحها لمراقبة أداء الشبكة وضمان تشغيلها بكفاءة. على سبيل المثال:
  - **أداة مراقبة الأداء**: تُستخدم لتحديد أي روابط ذات أداء ضعيف وقد تحتاج إلى مزيد من التحقيق.
  - **عارض الأحداث والسجلات**: تقوم العديد من مكونات البرامج والأجهزة (مثل جدار الحماية) في الشبكة الكبيرة بإنشاء سجلات تحتوي على قائمة بالأحداث (مثل صعود أو هبوط رابط شبكة) ما يساعد مدير النظام على تحديد المشكلات.
  - **أدوات فحص الثغرات الأمنية**: يمكن أن تقوم بفحص جميع أجهزة الحاسوب على الشبكة للكشف عن الثغرات المحتملة (مثل جهاز الحاسوب بنظام تشغيل لم يتم تطبيق آخر التحديثات عليه).
  - **أدوات كشف الحزم**: تسمح بعرض محتويات حزم الشبكة الفردية، والذي بدوره قد يعد أمرًا مفيدًا لاستكشاف الأخطاء وإصلاحها والتحقيقات الأمنية. ومع ذلك، يمكن للمتسللين استخدام أدوات كشف الحزم لمحاولة الحصول على معلومات قد تساعدهم (مثل عناوين MAC أو IP).

تطبيقات الشبكة

- **أنظمة قواعد البيانات**: تُعتبر أنظمة قواعد البيانات من بين التطبيقات الأكثر استخدامًا على الشبكات. حيث تُمكن منتجات قواعد البيانات المتقدمة مثل Oracle وMicrosoft SQL Server وMySQL العديد من المستخدمين من البحث عن سجلات البيانات وتحريرها وإدراجها في قواعد البيانات العلائقية الكبيرة. كما تسمح أنظمة دعم التطبيقات هذه لعدة مستخدمين بالوصول إلى البيانات نفسها مع ضمان سلامة البيانات (على سبيل المثال من خلال ضمان عدم تمكن مستخدمين اثنين من تحديث سجل البيانات نفسه في الوقت ذاته). ونظرًا لأن أنظمة قواعد البيانات غالبًا ما تخزن كميات كبيرة من المعلومات الحساسة (مثل أسماء المستخدمين والعناوين وتفاصيل بطاقات الائتمان وما إلى ذلك)، فإنها غالبًا ما تكون هدفًا لهجمات الأمن السيبراني باستخدام حقن SQL وغيرها من التقنيات.
- **إدارة المستندات**: تتعامل العديد من المنظمات مع كميات كبيرة من المستندات، مثل شركات التأمين والبنوك التي تتعامل مع أعداد كبيرة جدًا من اتفاقيات وعقود العملاء. تسمح إدارة المستندات لعدة مستخدمين بإدارة كميات كبيرة من المستندات والبحث عنها والوصول إليها.

تطبيق النظرية

يرد في ما يأتي مثال بسيط يوضح كيفية عمل هجوم حقن SQL. فكّر في مربع البحث عن المنتج الذي يظهر على المواقع الإلكترونية مثل Amazon أو eBay. فعندما تكتب شيئًا ما في مربع البحث (مثل "Nike® أحذية")، فإن هذه القيمة تستخدم في استعلام SQL الذي يبحث في قاعدة بيانات Amazon أو eBay عن القيم المطابقة. وعادةً ما يكون نوع جملة SQL التي يمكن استخدامها كما يأتي:

SELECT * FROM Products WHERE description = ‘Nike trainers’

ويمكن للمهاجم الذي لديه معرفة بـ SQL استغلال استخدام SQL للفاصلة المنقوطة للإشارة إلى نهاية الجملة، ولذلك، لنفترض أن مهاجمًا أدخل ما يأتي في مربع البحث عن المنتج:

‘Nike trainers’;SELECT * FROM customers;

عندما يقرأ تطبيق الموقع الإلكتروني هذه الجملة يحولها إلى عبارتين (لأن الفاصلة المنقوطة تشير إلى نهاية العبارة الأولى)، فتظل الجملة الأولى كما هي، وتصبح الجملة الثانية:

SELECT * FROM customers

يمكن أن يوفر هذا قائمة بجميع السجلات على جدول العملاء، بما في ذلك الأسماء والعناوين وأرقام بطاقات الائتمان وما إلى ذلك.

M01_INFO_ST_55924_U11 Rev 3 FP 08 Aug_AR.indd 160 03/05/2025 12:18:00

- **أداة اكتشاف الشبكة** تُعد أداة اكتشاف الشبكة أداة تُستخدم للبحث في شبكة كبيرة عن الخدمات المتاحة، بما في ذلك خدمات تطبيقات البرمجيات والأجهزة مثل الطابعات المتصلة بالشبكة. تُعرض الخدمات المتاحة للمستخدمين، غالبًا بتنسيق رسومي، ما يسمح لهم برؤية كافة المعلومات المتاحة. ويمكن إيقاف تشغيل اكتشاف الشبكة على جهاز معين بحيث لا يظهر على قائمة خدمات الشبكة المتاحة التي يمكن للمستخدمين الآخرين رؤيتها.

إجراء بعض الأبحاث حول كيفية حماية الموقع الإلكتروني من هجمات حقن SQL

خدمات وموارد البنية التحتية للشبكات

تدعم خدمات الشبكات بناء الشبكات وتوفير الوظائف التي تحتاج إليها التطبيقات التي تستخدم هذه الشبكات.

المهارات

المهارات المعرفية/العمليات والإستراتيجيات المعرفية:

- التحليل
- التفسير

بروتوكول التحكم في الإرسال/بروتوكول الإنترنت (TCP/IP)

يتسم برنامج الشبكة بالتعقيد، ولذلك يُقسم إلى طبقات. في الطبقة الأدنى، توجد مكونات الأجهزة والإشارات الكهربائية، وفي الطبقة الأعلى توجد التطبيقات التي يستخدمها المستخدم مثل متصفح الويب. ويوضح الشكل 11.12 الطبقات الأربع لنموذج بروتوكول التحكم في الإرسال/ بروتوكول الإنترنت.

التطبيق
النقل
الإنترنت
الوصول إلى الشبكة

الشكل 11.12 طبقات نموذج بروتوكول التحكم في الإرسال/ بروتوكول الإنترنت

في طبقة النقل، يتم استخدام بروتوكول التحكم في الإرسال وفي طبقة الإنترنت يتم استخدام بروتوكول الإنترنت. وتعد هذه البروتوكولات الرئيسة المستخدمة في هذه الطبقات، إلا أنه تُستخدم البروتوكولات الأخرى أيضًا لأغراض معينة.

المنافذ وطبقة النقل

تُستخدم طبقة النقل لتتبع الاتصالات الفردية وتقسيم البيانات المرسلة إلى شرائح (وإعادة تجميعها عند الاستلام). ما لم يتم تقسيم البيانات على هذا النحو، فإن بعض التطبيقات التي تحتاج إلى إرسال كميات كبيرة من البيانات (مثل البث المباشر الفيديو) ستمنع التطبيقات الأخرى من إرسال البيانات أو استقبالها لفترات طويلة من الزمن. ونظرًا لأن الجهاز الفردي قد يحتوي على العديد من التطبيقات التي تتصل عبر الشبكة في الوقت نفسه، يجب أن تحدد طبقة النقل التطبيقات التي تعمل، وللقيام بذلك، يُعين **رقم منفذ** لكل تطبيق. وتُعد أرقام المنافذ للتطبيقات المستخدمة بشكل شائع ثابتة (تُعرف باسم "أرقام المنافذ المعروفة") ويحتوي الجدول الوارد أدناه على بعض أرقام المنافذ المعروفة هذه.

المصطلح الرئيس

رقم المنفذ – نقطة نهاية الاتصال.

الجدول 11.3 بعض أرقام المنافذ المعروفة

التطبيق	رقم المنفذ
بروتوكول نقل الملفات (FTP)	20
بروتوكول نقل البريد البسيط	25
بروتوكول نقل النصوص الترابطية (HTTP)	80
بروتوكول مكتب البريد (POP)	110
بروتوكول نقل النصوص الترابطية الآمن (HTTPS)	443

M01_INFO_ST_55924_U11 Rev 3 FP 08 Aug_AR.indd 161 03/05/2025 12:18:00

يُقسم بروتوكول التحكم في الإرسال البيانات إلى ما يسمى حزمة بيانات (رسالة بيانات)، وتحتوي على أجزاء من البيانات المراد إرسالها ومعلومات إضافية، بما في ذلك منفذ المصدر والوجهة ورقم التسلسل (قد لا تصل حزمة بيانات إلى وجهتها بالترتيب الذي تم إرسالها به، لذلك عند استلامها، يجب أن يكون بروتوكول التحكم في الإرسال قادرًا على إعادتها بالترتيب الصحيح).

الحزم وطبقة الإنترنت

عند إرسال البيانات، تستقبل طبقة الإنترنت أجزاء (أو حزمة بيانات بروتوكول التحكم) من البيانات من طبقة النقل، والتي تتمثل مهمتها في توفير معلومات العنونة. ويتم ذلك عن طريق إضافة عناوين بروتوكول الإنترنت المصدر والوجهة إلى المقطع في ما يعرف باسم عنوان بروتوكول الإنترنت. تُسمى عملية إضافة هذه المعلومات الإضافية إلى الشريحة باسم الكبسلة ومع إضافة معلومات العنوان إلى الشريحة، يُصبح اسمها "حزمة".

عنونة شبكة بروتوكول الإنترنت

تُستخدم عناوين بروتوكول الإنترنت لتحديد مكان إرسال الحزمة بشكل فريد، كما تعتمد عنونة بروتوكول الإنترنت على مفهوم الأجهزة المضيفة والشبكات. الأجهزة المضيفة هي أجهزة فردية، بينما الشبكات عبارة عن مجموعات من الأجهزة في موقع جغرافي واحد (مثل المنزل أو المكتب).

عنونة IPv4. عُرف هذا النظام في الثمانينيات ويستخدم تنسيق عنوان من 32 بت يظهر عادةً بتنسيق عشري، مع 4 مجموعات من 8 بت تُسمى أحيانًا "أوكتات (ثمانيات)" من الأرقام العشرية في النطاق من 0 إلى 255، على سبيل المثال 192.168.10.5. يُحدد الجزء الأول من العنوان الشبكة ويستخدم بواسطة أجهزة توجيه الإنترنت لإرسال الحزمة إلى المنزل أو المبنى الصحيح. أما الجزء الأخير من العنوان فهو عنوان الجهاز الفردي ويُستخدم داخل الشبكة لإرسال الحزمة إلى الجهاز الصحيح. يمكن تحديد عدد البتات الـ32 المخصصة للشبكة وأجزاء الجهاز من عنوان بروتوكول الإنترنت بعدة طرق مختلفة. وتُعد الطريقة الأبسط هي استخدام فئات عناوين بروتوكول الإنترنت، حيث تُستخدم الفئات A و B و C لعناوين الأجهزة. وتُعرف فئة عنوان بروتوكول الإنترنت بواسطة الأوكتات (الثمانيات) الأولى كما هو موضح في الجدول أدناه.

الجدول 11.4 فئات عناوين IP

	نطاق أول ثمانية	عنوان الشبكة	عنوان المضيف	عدد الشبكات المحتمل	عدد الأجهزة المحتملة (الأجهزة المضيفة)
الفئة أ	من 1 إلى 127	أول ثمانية	الثمانية الثانية والثالثة والرابعة	126	16 مليون (تقريبًا)
الفئة ب	من 128 إلى 191	الثمانية الأولى والثانية	الثمانية الثالثة والرابعة	16,384	65,534
الفئة ج	من 192 إلى 223	الثمانية الأولى والثانية والثالثة	الثمانية الرابعة	2,097,159	254

على سبيل المثال 129.10.30.16 هو عنوان من الفئة B، وعنوان الشبكة هو 129.10 وعنوان الجهاز هو 30.16. 200.20.15.68 هو عنوان من الفئة C، وعنوان الشبكة هو 200.20.15 وعنوان الجهاز هو 68. كانت الفكرة الأصلية وراء نظام العناوين هذا هي أن عناوين الفئة A ستكون مناسبة للمنظمات الكبيرة جدًّا التي يوجد بها عدد صغير جدًّا (بحد أقصى 126) لكن كل منظمة لديها عدد كبير جدًّا من الأجهزة التي تحتاج إلى الاتصال بها. تناسب عناوين الفئة B الشركات متوسطة الحجم وستناسب عناوين الفئة C الشركات الصغيرة التي لديها الكثير من عناوين الشبكة ولكن كل شبكة تحتوي فقط على عدد صغير من الأجهزة (بحد أقصى 254).

M01_INFO_ST_55924_U11 Rev 3 FP 08 Aug_AR.indd 162 03/05/2025 12:18:00

لم تعد الفئات تُستخدم بالطريقة المقصودة في الأصل، ومن الشائع اليوم الإشارة إلى مكان التقسيم بين الشبكة وقسم المضيف في العنوان عن طريق إضافة عدد بتات الشبكة التي يسبقها خط مائل، لذلك يتم عرض عنوان الفئة A على النحو الآتي:

88.100.35.88/

عنوان الفئة A يُظهر بهذا الشكل:

129.10.30.1616/

عنوان الفئة C يُظهر بهذا الشكل:

200.20.15.6824/

تتيح لك هذه الطريقة إنشاء تقسيم بين عنوان الشبكة وعنوان الجهاز المضيف في أي مكان ترغب فيه باستخدام عملية تسمى التقسيم الفرعي للشبكة (تقسيم نطاق عناوين بروتوكول الإنترنت).

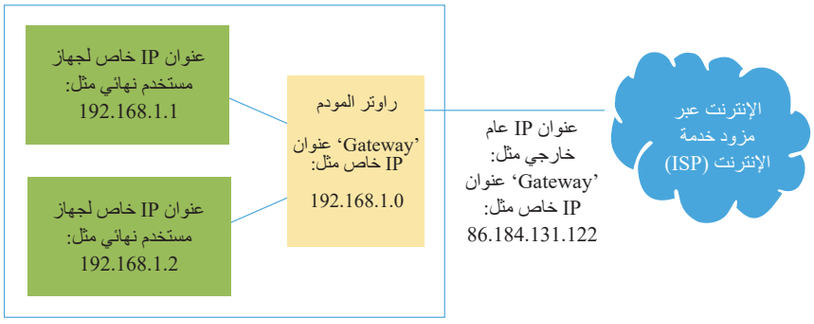
صُمم نظام العناوين هذا قبل مدة طويلة من تطور شبكة الإنترنت ونفدت العناوين الفريدة منذ سنوات عديدة، ما أدى إلى استبداله بعناوين IPv6. ومع ذلك، ما يزال IPv4 يستخدم في نطاق واسع للعنونة، خاصة في الشبكات المحلية.

عناوين بروتوكول الإنترنت الخاصة: في حين أن لكل جهاز يتصل بالإنترنت عنوان بروتوكول إنترنت (IP) فريد، فإن الأجهزة داخل الشبكة المحلية (LAN) (أو الشبكة المحلية اللاسلكية (WLAN)) تحتاج فقط إلى عنوان يكون فريدًا داخل الشبكة المحلية ذاتها. وهذا يعني أنه يمكن إعادة استخدام العناوين في كل شبكة محلية، وتُعرف عناوين بروتوكول الإنترنت خصيصًا لهذا الاستخدام وتسمى عناوين بروتوكول الإنترنت الخاصة. ولا يتم استخدام هذه العناوين مطلقًا على شبكة الاتصال واسعة النطاق العامة للإنترنت. تظهر عناوين بروتوكول الإنترنت الخاصة كما هو موضح في الجدول أدناه.

الجدول 11.5 نطاقات عناوين بروتوكول الإنترنت الخاصة

	بدء عنوان بروتوكول الإنترنت الخاص	إنهاء عنوان بروتوكول الإنترنت
تجميعة /8	10.0.0.0	10.255.255.255
تجميعة/ 12	172.16.0.0	172.31.255.255
تجميعة/ 16	192.168.0.0	192.168.255.255

يُحول العنوان العام الفريد لبروتوكول الإنترنت المستخدم للاتصال بالإنترنت وعناوين بروتوكول الإنترنت الخاصة المستخدمة داخل الشبكة المحلية بواسطة جهاز التوجيه اللاسلكي باستخدام عملية تُسمى ترجمة عناوين الشبكة (NAT). وتُعرف عناوين بروتوكولات الإنترنت الخاصة بمعيار RFC1918. يوضح الرسم التخطيطي في الشكل 11.13 كيفية استخدام عناوين بروتوكولات الإنترنت العامة والخاصة في تثبيت شبكة منزلية أو مكتبية. لاحظ أن عنوان بروتوكول الإنترنت العام يوفره مزود خدمة الإنترنت بينما يتم توفير عناوين المستخدم النهائي عادةً للأجهزة بواسطة بروتوكول التكوين الديناميكي للمضيف، والذي يتم تشغيله في التثبيت المنزلي على المودم/ جهاز التوجيه.



الشكل 11.13 عناوين IP العامة والخاصة

M01_INFO_ST_55924_U11 Rev 3 FP 08 Aug_AR.indd 163 03/05/2025 12:18:00

IPv6. ومع تطوير شبكة الإنترنت ونفاد عناوين IPv4، تم تطوير IPV6، IPv6 الذي يستخدم عناوين -128بت بدلًا من -32بت في IPv4، ما يوفر كمية هائلة من عناوين 2^{128}. يتم استخدام أول 64 بت كعنوان شبكة (يسمى بادئة التوجيه في IPv6) بينما تُستخدم الـ 64 بت الباقية كعنوان الجهاز. يتم عرض عناوين IPv6 على هيئة 8 مجموعات من أربعة أرقام من **أنظمة ست عشرية** مثل:

FE80:0000:B6F7:A1FF:FEA4:E211

عندما تكون هناك مجموعات من الأصفار فإنه يمكن حذفها بحيث يصبح العنوان أعلاه:

FE80::B6F7:A1FF:FEA4:E211

- يمكنك العثور على عنوان بروتوكول الإنترنت الخاص بالحاسوب الخاص بك عند الاتصال بشبكات مختلفة (مثل شبكة الـ Wi-Fi وشبكات الهاتف المحمول).
- يمكنك العثور على عنوان بروتوكول الإنترنت لجهاز حاسوب يعمل بنظام Windows من شاشة موجه الأوامر باستخدام الأمر IPCONFIG (قد يكون استخدام موجه الأوامر مقيدًا في مدرستك أو كليتك لأسباب أمنية).
- يمكن العثور على عنوان بروتوكول الإنترنت العام الخارجي المستخدم للاتصال بالإنترنت للشبكة التي تستخدمها عن طريق كتابة "ما عنوان بروتوكول الإنترنت الخاص بي" في محرك بحث مثل Google.
- ما فئة عنوان بروتوكول الإنترنت التي يتصل بها الجهاز على شبكات مختلفة؟

المصطلح الرئيس

نظام ست عشري – هو نظام عدّ مؤلف من 16 قيمة؛ يُمثَّل بالأرقام من 0 إلى 9 وبالحروف من A إلى F.

تطبيق النظرية

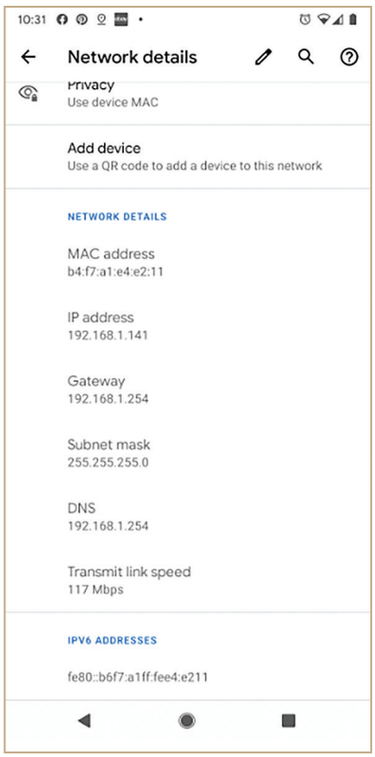
يعرض الشكل 11.14 صفحة إعداد الشبكة لهاتف Android المتصل بشبكة Wi-Fi عامة.

ويسرد عنوان MAC وعنوان IPv4 الخاصين بالجهاز. وفي هذه الحالة، تستخدم نقطة اتصال Wi-Fi العامة عنوانًا من نطاق عناوين IP الخاصة /8 وهو 10.0.0.158. وتحتوي البوابة الافتراضية، التي توفر رابطًا إلى الإنترنت، على عنوان 10.0.0.1. وعادةً ما يكون عنوان البوابة الافتراضية هو عنوان IP الأول (أو الأخير أحيانًا) في نطاق الشبكة. ويوفر خادم DHCP الذي ربما يكون مدمجًا في نقطة وصول Wi-Fi، هذه العناوين.

يعرض الشكل 11.15 الجهاز نفسه (لاحظ أن عنوان MAC هو نفسه) المتصل بشبكة Wi-Fi منزلية. تستخدم هذه الشبكة أيضًا نطاق عناوين خاص ولكن هذه المرة في نطاق /16، حيث يحتوي الجهاز على عنوان 192.168.1.141. وتكون البوابة الافتراضية في هذه الشبكة هي العنوان الأخير في هذا النطاق، 192.168.1.254.

يحدد قناع الشبكة الفرعية الموضح في كلا اللقطتين أي جزء من عنوان IP للجهاز يخص الشبكة وأي جزء يخص المضيف (جزء الجهاز الفردي). وفي كلتا الحالتين يُعين هذا إلى 255.255.255.0. حيث يشير هذا إلى استخدام الثمانية الأخيرة فقط من عنوان IP لتعريف الأجهزة الفردية بشكل فريد. ويُعين عنوان DNS (عنوان IP حيث يجب توجيه طلبات DNS) في كلتا الحالتين إلى عنوان البوابة الافتراضية.

الشكل 11.14 مثال لعناوين IP عند الاتصال بنقطة اتصال عامة



الشكل 11.15 مثال لعناوين IP عند الاتصال بشبكة منزلية

M01_INFO_ST_55924_U11 Rev 3 FP 08 Aug_AR.indd 164
03/05/2025 12:18:01

أنظمة تشغيل الشبكة

عادة ما تُقسم أنظمة تشغيل الشبكة مثل Windows Server إلى نطاقات (Windows Domains)، وهي عبارة عن مجموعة من المستخدمين وأجهزة الحاسوب (والأجهزة الطرفية مثل الطابعات) التي تشمل جميع المستخدمين المصرح لهم في منظمة واحدة. وتُخزن تفاصيل المستخدمين والأجهزة في خدمة دليل Windows وActive Directory، كما تتم إدارة صلاحيات المستخدمين وتطبيق سياسات الأمان عبر Active Directory. إضافة إلى ذلك، يمكن إنشاء نطاق فرعي (يسمى أيضًا المجال الفرعي) في شبكة Windows التي تعد جزءًا من النطاق الرئيس وقد يُستخدم في حالات مثل وجود مكتب فرعي لشركة يملك شبكة منفصلة.

استخدام أجهزة الشبكة لتكوين الشبكات وتقسيمها

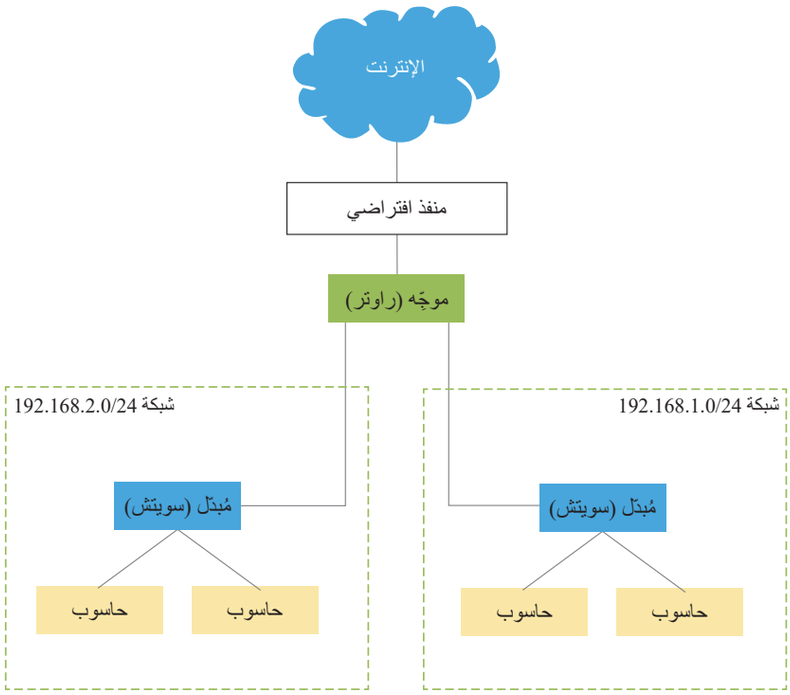
غالبًا ما تُقسم الشبكات المحلية الكبيرة إلى شبكات أصغر لتقليل حركة البيانات الشبكية عبر الشبكة بأكملها. هذه هي التقنية المستخدمة مع الهيكل الهرمي الموضح سابقًا.

وتُقسم الشبكات باستخدام أجهزة التوجيه، التي تكون دائمًا متصلة بشبكتين مختلفتين على الأقل. عندما تصل الحزم إلى جهاز توجيه، يفحص الجهاز عنوان بروتوكول الإنترنت الخاص بالوجهة ثم يقوم باستخدام معلومات التكوين (تسمى جداول التوجيه) بإرسال الحزمة إلى الوجهة الصحيحة.

يعرض المخطط الموضح في الشكل 11.16 الشبكة المحلية مقسمة إلى شبكتين مختلفتين، 192.168.1.0 و192.168.2.0. يحتوي جهاز التوجيه الذي يربط الشبكة على ثلاث واجهات. على سبيل المثال، سيتم فحص الحزم المرسلة إلى جهاز التوجيه من شبكة 192.168.1.0. إذا كان عنوان وجهتهم موجودًا في شبكة 192.168.2.0، فمن المقرر توجيهها إلى الواجهة المتصلة بهذه الشبكة. وإذا لم يكن الأمر كذلك، فسيتم توجيهها إلى الواجهة المعينة كبوابة افتراضية متصلة بالإنترنت الخارجي.

موضوعات ذات صلة

نوقشت الهياكل بمزيد من التفصيل سابقًا في هذه الوحدة، راجع الصفحتين 155-156.



الشكل 11.16 شبكة محلية (LAN) مجزأة إلى شبكتين

M01_INFO_ST_55924_U11 Rev 3 FP 08 Aug_AR.indd 165 03/05/2025 12:18:01

وظائف البنية التحتية للشبكة وتطبيقها

هناك عدد من خدمات الشبكة، والتي تعمل عادةً على خادم ضمن الشبكة. وهي تدعم وظائف الشبكة وتسهّل استخدام الشبكات.

خدمات أسماء النطاقات (DNS)

يتم توفير المواقع الإلكترونية بواسطة خوادم الويب ويتم تحديد خادم الويب من خلال عنوان بروتوكول الإنترنت الفريد الخاص به. ومع ذلك، يصعب تذكر عناوين بروتوكولات الإنترنت. تخيل لو كان عليك الانتقال إلى Amazon باستخدام أرقام. لحسن الحظ، نصل إلى المواقع الإلكترونية باستخدام اسم النطاق الخاص بها، مثل خدمات أسماء النطاقات www.facebook.com أو www.amazon.ae. تقدم أسماء النطاقات خدمة التحويل بين اسم المجال وعنوان بروتوكول الإنترنت للموقع الإلكتروني. تعمل حلول اسم خدمات أسماء النطاقات على النحو الآتي:

- تقوم بكتابة اسم نطاق (مثل dutchnews.nl) في متصفح الإنترنت الخاص بك على جهاز الحاسوب الخاص بك ويرسل متصفحك استعلامًا عبر الإنترنت يطلب مطابقة اسم النطاق مع عنوان بروتوكول الإنترنت الخاص بخادمه. يصل الاستعلام إلى المحلل التكراري والذي غالبًا ما يتم تشغيله بواسطة مزود خدمة الإنترنت الخاص بك.
- يقوم المحلل التكراري بالتواصل مع خادم أساسي (Root Server)، وهذه الخوادم تحتوي على معلومات حول نطاقات المستوى الأعلى (مثل org. و jp.).
- تم يتصل الخادم الأساسي بخادم نطاق المستوى الأعلى (TLD). وتخزن هذه الخوادم معلومات حول النطاقات الثانوية (مثل nytimes.com)، ويوفر خادم نطاق المستوى الأعلى عنوان بروتوكول الإنترنت الخاص بخادم الأسماء لهذا النطاق.
- بعد العثور على خادم الأسماء للنطاق، يرسل المحلل التكراري طلبًا إلى خادم الأسماء الذي يقوم بإعادة عنوان بروتوكول الإنترنت الخاص بخادم النطاق.
- إذا كان المحلل التكراري يعرف عنوان بروتوكول الإنترنت لخادم النطاق، فإنه يُعيد هذه المعلومات إلى المتصفح.
- يمكن للمتصفح الآن الاتصال بخادم المجال باستخدام عنوان بروتوكول الإنترنت المُقدم، ويطلب منه إرسال صفحته الرئيسة باستخدام بروتوكول نقل النصوص الترابطية.

خدمات الدليل

تُستخدم خدمات الدليل لتحديد تفاصيل الموارد المختلفة وتخزينها على الشبكة مثل المستخدمين وأنظمة الحاسوب والخدمات والتطبيقات. حيث تعمل هذه الخدمات على تحويل عناوين الشبكة إلى أسماء يمكن للمستخدمين الوصول إليها بسهولة دون الحاجة إلى معرفة عنوان بروتوكول الإنترنت الخاص بها. وتُقدم خدمة الدليل عبر خادم دليل على الشبكة. ويعتبر بروتوكول الوصول الخفيف إلى أدلة الدليل (LDAP) بروتوكول التطبيق القياسي في الصناعة للوصول إلى خدمات الدليل والحفاظ عليها. يُعتبر نظام أسماء النطاقات (DNS)، كما هو موضح أعلاه، نوعًا من خدمات الدليل لعناوين المواقع الإلكترونية. تُستخدم خدمة الدليل في خوادم Microsoft Windows للاحتفاظ بسجل لجميع المستخدمين وأجهزة الحاسوب في نطاق Windows ويُطلق عليها Active Directory. تنتج شركة Apple خدمة دليل بروتوكول الوصول الخفيف إلى أدلة الدليل لخادم MacOS يُطلق عليها Open Directory. كما يوجد تطبيق مجاني مفتوح المصدر لبروتوكول الوصول الخفيف إلى أدلة الدليل يُعرف باسم Open LDAP ويعمل على مجموعة واسعة من أنظمة التشغيل بما في ذلك Windows وLinux وMacOS وAndroid.

خدمات المصادقة

تُستخدم هذه الخدمات لمصادقة المستخدمين داخل الشبكة، وفي شبكة Windows، يتم مصادقة المستخدمين بواسطة خادم تم إعداده للعمل بوصفه وحدة تحكم في النطاق، ويستخدم Active Directory وطريقة مصادقة Kerberos الموضحة سابقًا.

بروتوكول التكوين الديناميكي للمضيف (DHCP)

يحتاج كل جهاز داخل شبكة محلية إلى الحصول على عنوان بروتوكول إنترنت فريد من نطاق عناوين بروتوكولات الإنترنت الخاصة بـ IPv4. ويمكن لمسؤول الشبكة تعيين هذا العنوان بشكل فردي، ولكن ذلك يتطلب الاحتفاظ بسجل للأجهزة التي لديها عنوان بروتوكول إنترنت معين. وقد يتسبب هذا في تعقيدات، على سبيل المثال، في حال انضمام أجهزة جديدة إلى الشبكة المحلية اللاسلكية وتطلبت تخصيص

M01_INFO_ST_55924_U11 Rev 3 FP 08 Aug_AR.indd 166 03/05/2025 12:18:01

عنوان بروتوكول الإنترنت. ويعتبر الحل الأفضل هو تخصيص عناوين بروتوكول إنترنت للأجهزة بشكل ديناميكي بحسب الحاجة. حيث يُعد هذا هو الغرض من بروتوكول التكوين الديناميكي للمضيف، الذي يخصص عناوين بروتوكول إنترنت للأجهزة بحسب الطلب. الأجهزة التي تصدر عناوين بروتوكول إنترنت تسمى خوادم بروتوكول التكوين الديناميكي للمضيف ويمكن أن تكون حاسوب خادم أو جهاز مثل جهاز توجيه عريض النطاق. عند تشغيل الجهاز، تظهر رسالة بروتوكول التكوين الديناميكي للمضيف تطلب عنوان بروتوكول الإنترنت. ويستقبل خادم بروتوكول التكوين الديناميكي للمضيف الطلب ويرد بعنوان بروتوكول إنترنت يمكن للجهاز استخدامه. يتم اختيار هذا العنوان من قائمة عناوين بروتوكول الإنترنت لدى خادم بروتوكول التكوين الديناميكي للمضيف، إضافة إلى معلومات أخرى مثل عنوان بروتوكول الإنترنت للبوابة الافتراضية وقناع الشبكة الفرعية الصحيح.

التوجيه

تستخدم أجهزة التوجيه جداول التوجيه التي يكونها مدير النظام لتحديد مكان إرسال كل حزمة من البيانات. في الشبكات الكبيرة جدًّا، مثل الإنترنت، يوجد العديد من أجهزة التوجيه المتصلة ببعضها البعض وقد تمر حزم البيانات عبر أجهزة توجيه متعددة (تُعرف باسم hops) في أثناء انتقالها من عنوان بروتوكول الإنترنت (IP) المصدر إلى عنوان بروتوكول إنترنت (IP) الوجهة.

خدمات الوصول عن بُعد

في بعض الحالات، من المفيد أن تكون قادرًا على الوصول عن بُعد إلى سطح مكتب حاسوب آخر. وتُعتبر هذه الخدمة مفيدة بشكل خاص في خدمات دعم تكنولوجيا المعلومات، حيث يمكن لفني تكنولوجيا المعلومات استخدام الوصول عن بعد لرؤية سطح مكتب مستخدم يعمل بنظام Windows أو Mac أو Linux والتفاعل معه للتحقق من مشكلة ما وتصحيحها أو إجراء تغيير في التكوين نيابة عنه. تسمى ميزة Microsoft Windows التي تدعم هذه الوظيفة Remote Desktop. كما توجد نسخ من جهات خارجية مثل GoToMyPC® التي تضيف ميزات إضافية مثل القدرة على الوصول إلى أجهزة سطح المكتب لنظامي Windows أو Mac من أنظمة أخرى مثل iOS وAndroid.

خدمات شبكة التطبيقات

- **خدمات الملفات والطباعة**: تعد الملفات والطابعات من أكثر الموارد المشتركة شيوعًا على الشبكة. باستخدام نظام Microsoft Windows، يمكن مشاركة المجلدات التي تحتوي على ملفات مع مستخدمي الشبكة من أي حاسوب (ليس بالضرورة خادمًا). ويمكن التحكم في الوصول إلى المجلدات المشتركة باستخدام أذونات المجلدات المشتركة. كما يمكن مشاركة الطابعات بحيث يمكن لأي شخص على الشبكة الوصول إليها بالأذونات الصحيحة.
- **خدمات الويب والبريد والاتصالات**: غالبًا ما تدير المنظمات الكبيرة خوادم الويب والبريد الإلكتروني الخاصة بها. ويمكن لخوادم الويب الداخلية توفير شبكة داخلية.

موضوعات ذات صلة

لمطالعة مزيد من التفاصيل بشأن أذونات المجلدات المشتركة، راجع صفحة 148.
ولمطالعة مزيد من التفاصيل بشأن خوادم الموقع الإلكتروني الداخلية والشبكات الداخلية، راجع صفحة 154.

تمرين تقييمي 11.2 BP.4, B.P5, B.M2, AB.D1

أنت تعمل في شركة تكنولوجيا معلومات وترغب في إنشاء أكاديمية "IT Academy" لتدريب الموظفين وغيرهم في مجال تكنولوجيا المعلومات والشبكات. وقد طُلب منك إعداد شرائح العرض التقديمي مصحوبةً بملاحظات المتحدثين لتغطية الموضوعات الآتية:

- شرح لأنواع الشبكات المختلفة ومكوناتها وكيفية تأمينها.
- شرح لكيفية تأثر البنية التحتية للشبكة ومواردها بالأمن السيبراني.

تحليل الآثار الأمنية للأنظمة المتصلة بالشبكة.

التخطيط

- هل تعرف ما يجب عليك فعله؟ من أين ستحصل على المعلومات التي تحتاج إليها؟

التنفيذ

- عند شرح الموضوعات، تأكد من تضمين تفاصيل كافية تتجاوز الوصف الأساسي للموضوع. فمن خلال تحليلك، تحتاج إلى التفكير في الجوانب الإيجابية والسلبية للآثار الأمنية.

المراجعة

- تحقق من أنك تناولت جميع أنواع الشبكات والمكونات المختلفة المدرجة في المواصفات.

M01_INFO_ST_55924_U11 Rev 3 FP 08 Aug_AR.indd 167 03/05/2025 12:18:02

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.

المهارات

المهارات المعرفية/العمليات والإستراتيجيات المعرفية:

- التحليل
- التفكير الناقد

تقييم الثغرات في أنظمة الحاسوب

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

M01_INFO_ST_55924_U11 Rev 3 FP 08 Aug_AR.indd 168 03/05/2025 12:18:02

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.

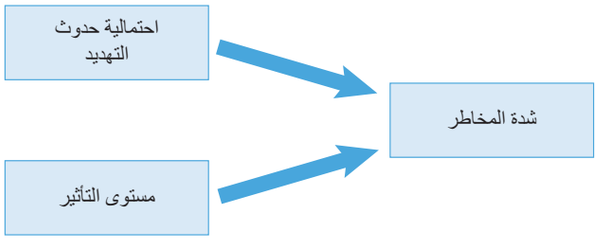
تقييم شدة المخاطر في كل تهديد

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.

المهارات

المهارات المعرفية/العمليات والإستراتيجيات المعرفية:

- التحليل
- التفكير الناقد
- حل المشكلات



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:

M01_INFO_ST_55924_U11 Rev 3 FP 08 Aug_AR.indd 169 03/05/2025 12:18:02

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 جدًّا". 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 جدًّا".

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، سنويًّا) بوصفه أحد أشكال **التدقيق**. ويُعد هذه الإجراء ضروريًّا 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،

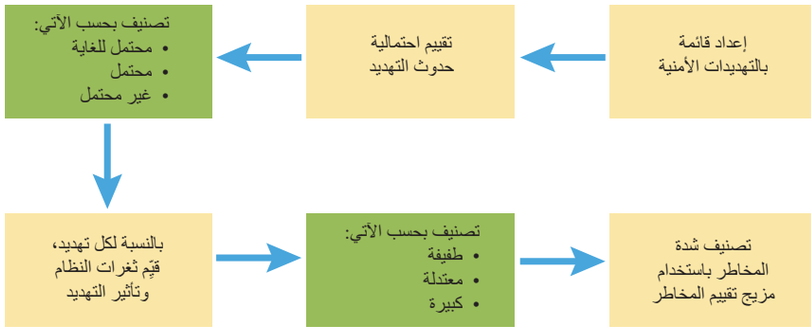
بحث

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.

M01_INFO_ST_55924_U11 Rev 3 FP 08 Aug_AR.indd 170 03/05/2025 12:18:02



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

M01_INFO_ST_55924_U11 Rev 3 FP 08 Aug_AR.indd 171
03/05/2025 12:18:02

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 جدًّا لكنها صعبة جدًّا 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.

موضوعات ذات صلة

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

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.

M01_INFO_ST_55924_U11 Rev 3 FP 08 Aug_AR.indd 172 03/05/2025 12:18:03

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.

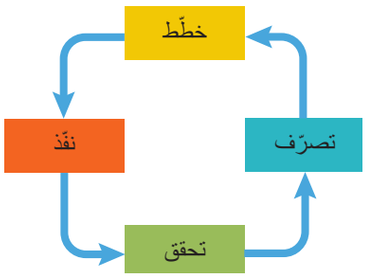
المصطلح الرئيس

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"

M01_INFO_ST_55924_U11 Rev 3 FP 08 Aug_AR.indd 173 03/05/2025 12:18:03

- **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.

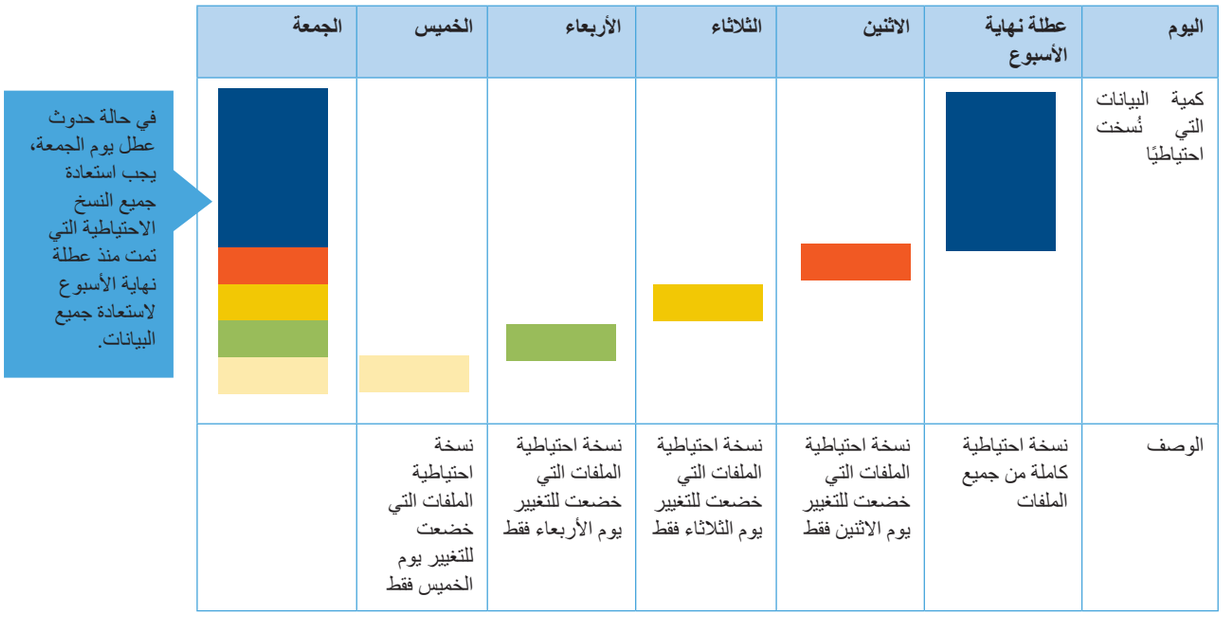
ويعتمد عدد المرات التي تحتاج فيها المؤسسة إلى نسخ بياناتها احتياطيًا على مقدار البيانات التي يمكنها تحمل فقدانها. فمع نظام النسخ الاحتياطي اليومي المشار إليه أعلاه، يجب أن تكون المؤسسة على استعداد لخسارة ما لا يقل عن يوم واحد من البيانات. ففي بعض المؤسسات، مثل البنك، لن يكون هذا مقبولًا. أخيرًا، تحتاج 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.

M01_INFO_ST_55924_U11 Rev 3 FP 08 Aug_AR.indd 174 03/05/2025 12:18:03



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).

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.

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.

M01_INFO_ST_55924_U11 Rev 3 FP 08 Aug_AR.indd 175 03/05/2025 12:18:03

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

M01_INFO_ST_55924_U11 Rev 3 FP 08 Aug_AR.indd 176 03/05/2025 12:18:03

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 جدًّا 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.

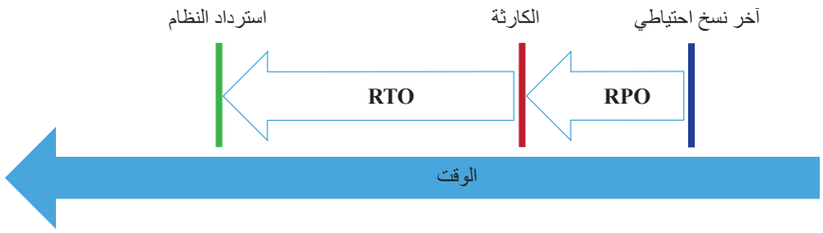
خطة التعافي من الكوارث

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 جدًّا موقع بديل متاح داخل الشركة يمكن استخدامه في حالة وقوع كارثة.

M01_INFO_ST_55924_U11 Rev 3 FP 08 Aug_AR.indd 177
03/05/2025 12:18:04

- 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.

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

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

M01_INFO_ST_55924_U11 Rev 3 FP 08 Aug_AR.indd 178 03/05/2025 12:18:04

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.

- أجر 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؟

M01_INFO_ST_55924_U11 Rev 3 FP 08 Aug_AR.indd 179 03/05/2025 12:18:04

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

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.

المهارات

المهارات المعرفية/العمليات والإستراتيجيات المعرفية:

- التحليل
- حل المشكلات
- اتخاذ القرار

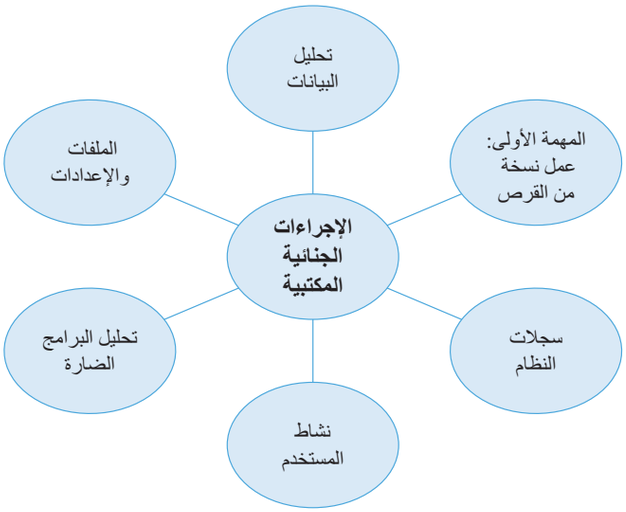
وقفة للتفكير

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؟

M01_INFO_ST_55924_U11 Rev 3 FP 08 Aug_AR.indd 180 03/05/2025 12:18:04



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؟

M01_INFO_ST_55924_U11 Rev 3 FP 08 Aug_AR.indd 181 03/05/2025 12:18:04

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

M01_INFO_ST_55924_U11 Rev 3 FP 08 Aug_AR.indd 182 03/05/2025 12:18:04

- **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

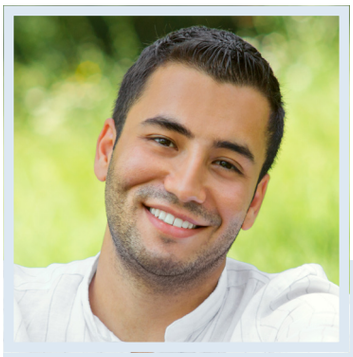
- عند كتابة الشرح الخاص بك عن الإجراءات الجنائية، تأكد من تضمين أكبر قدر ممكن من التفاصيل.
- تذكر أنه لا يمكنك النسخ واللصق مباشرة من الكتب أو المواقع الإلكترونية؛ إذ يجب عليك إعادة كتابة المعلومات بكلماتك.
- عند كتابة تحليلك لكيفية تنفيذ الإجراءات، تذكر تضمين المزايا وأي عيوب محتملة وأيضًا مراعاة أنواع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

M01_INFO_ST_55924_U11 Rev 3 FP 08 Aug_AR.indd 183 03/05/2025 12:18:05

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.

M01_INFO_ST_55924_U11 Rev 3 FP 08 Aug_AR.indd 184 03/05/2025 12:18:05