## 9-0 مقدمة

يتعين على الفنيين فهم أمان جهاز الكمبيوتر والشبكات. إذ قد يكون للفشل في تطبيق إجراءات الأمان الصحيحة تأثيره على المستخدمين وأجهزة الكمبيوتر والجمهور العام .وفي حالة عدم اتباع إجراءات الأمان السليمة فإن المعلومات السرية وأسرار الشركات والبيانات المالية وأجهزة الكمبيوتر وعناصر الأمن القومي تكون عرضة للخطر.

وبعد الانتهاء من هذه الوحدة، سيكون بمقدورك تحقيق الأهداف التالية:

- شرح أهمية عامل الأمان .
- وصف تهديدات الأمان .
- تحديد إجراءات الأمان .
- تحديد طرق الصيانة الوقائية الشائعة للأمان .
- استكشاف أخطاء الأمان وتصحيحها.

## 9-1 شرح أهمية الأمان

يساعد أمان الكمبيوتر والشبكة في استمرار البيانات والمعدات في أداء وظيفتها وتوفير إمكانية الوصول للأشخاص المناسبين. ويتعين على كل شخص في أي مؤسسة أن يولي اهتمامًا كبيرًا لقضية الأمان إذ قد يصاب الجميع بانخفاض في مستوى الأمان .

وتعد السرقة والفقد واقتحام الشبكات والتلف المادي بعضًا من الطرق التي يمكن أن تتعرض من خلالها الشبكة أو جهاز الكمبيوتر للضرر. حيث يمكن أن يتسبب تلف الأجهزة أو فقدها في فقد الإنتاج. ومن ثم فإن إصلاح الأجهزة أو استبدالها قد يكلف الشركة الكثير من الوقت والمال. ويمكن أن يؤدي الاستخدام غير المرخص للشبكة إلى الكشف عن معلومات سرية وتقليل موارد الشبكة.

كما يمكن أن يتسبب الهجوم الذي يتعمد الحد من أداء جهاز الكمبيوتر أو الشبكة في إلحاق الضرر بإنتاج المؤسسة. وتشير معايير الأمان التي يتم تطبيقها تطبيقًا غير دقيق على أجهزة الشبكة اللاسلكية إلى أن الاتصال المادي ليس شرطًا للوصول غير المرخص من قِبل المتطفلين.

ويعتبر أمان البيانات والشبكة من بين المسئوليات الرئيسية الملقاة على عاتق الفني. فقد يعتمد عليك عميل أو مؤسسة لضمان أمان البيانات وأجهزة الكمبيوتر الخاصة بهم. وبناءً على ذلك ستقوم بأداء بعض المهام الأكثر حساسية من تلك التي يتم إسنادها إلى الموظف العادي. وقد تقوم بإصلاح المعدات وضبطها وتركيب الأجهزة. وسيتعين عليك معرفة كيفية تكوين الإعدادات للحفاظ على أمان الشبكة وفي نفس الوقت إتاحتها لمن يريدون الوصول إليها. ويتعين عليك أيضًا ضمان أنه يتم تطبيق تصحيحات البرامج وتحديثاتها وتثبيت برامج مكافحة الفيروسات (anti-virus) مع استخدام برامج مكافحة برامج التجسس .(anti-spyware) وقد يطلب منك أيضًا إرشاد المستخدمين إلى كيفية الحفاظ على ممارسات الأمان الجيدة مع أجهزة الكمبيوتر .

## 9-2 وصف تهديدات الأمان

لحماية أجهزة الكمبيوتر والشبكة بنجاح، يتعين على الفني فهم كلا نوعي التهديدات التي يتعرض لها أمان الكمبيوتر وهما:

- التهديدات المادية: وهي الأعمال أو الهجمات التي من شأنها الاستيلاء على الأجهزة أو إتلافها أو تدميرها، مثل الخوادم والمحولات والأسلاك
- تهديدات البيانات: وهي الأعمال أو الهجمات التي من شأنها إزالة المعلومات أو إتلافها أو رفض الوصول للمعلومات أو السماح بالوصول لها أو الاستيلاء عليها

يمكن أن تأتي تهديدات الأمان من داخل المؤسسة أو من خارجها، وقد يتفاوت مستوى التلف المحتمل بصورة كبيرة وفقًا لما يلي:

- داخليًا: حيث يتمتع الموظفون بإمكانية الوصول إلى البيانات والمعدات والشبكة
  - o وتحدث التهديدات الضارة عندما يقوم أحد الموظفين بإحداث التلف عن عمد .

- أما التهديدات العرضية فتحدث عندما يقوم المستخدم بإتلاف البيانات أو المعدات من دون قصد منه .
- خارجيًا: حيث لا يتمتع المستخدمون خارج المؤسسة بوصول مرخص للشبكة أو الموارد
  - غير منظم: حيث يستخدم المهاجمون الموارد المتاحة، مثل كلمات المرور أو البرامج النصية، للحصول على وصول وتشغيل البرامج المصممة خصيصًا للتخريب
  - منظم: وفيه يستخدم المهاجمون الكود للوصول إلى أنظمة التشغيل والبرامج

قد تكون الخسارة أو التلف المادي الذي يصيب الأجهزة عالي التكلفة، وقد يلحق الفقد في البيانات الضرر بشركة أعمالك وسمعتها. والتهديدات التي تتعرض لها البيانات دائمة التغير حيث يجد المهاجمون أساليب جديدة للحصول على دخول وارتكاب جرائمهم.

بعد إكمال هذا القسم سيكون بمقدورك تحقيق الأهداف التالية:

- تعريف الفيروسات والفيروسات المتنقلة (worm) وأحصنة طروادة .(Trojans)
- شرح أمان الويب .
- تعريف برامج الإعلانات المتسللة (adware) وبرامج التجسس (spyware)والبرامج غير المرغوب فيها .(grayware)
- شرح رفض الخدمة .(Denial of Service)
- وصف البريد العشوائي (spam) والإطارات المنبثقة .(popup)
- شرح الهندسة الاجتماعية .
- شرح هجمات .TCP/IP
- شرح إحلال مكونات الكمبيوتر المادية وإعادة تصنيعها .

## 9-2-1 تعريف الفيروسات والديدان(worm) وأحصنة طروادة(Trojan)

يتم تصميم فيروسات الكمبيوتر وإرسالها عن طريق المهاجمين بشكلٍ متعمد. حيث يتم إرفاق الفيروس بجزء صغير من تعليمات الكمبيوتر البرمجية (الكود code أو البرامج أو المستندات. ثم يبدأ الفيروس عمله فور تشغيل البرنامج على جهاز الكمبيوتر. فإذا انتشر الفيروس في أجهزة الكمبيوتر الأخرى، ستواصل هذه الأجهزة نشر هذا الفيروس .

فالفيروس عبارة عن برنامج قام المهاجمون بتصميمه وإرساله لغرض خبيث. وينتقل الفيروس من جهاز كمبيوتر لآخر عبر البريد الإلكتروني وعمليات نقل الملفات والمراسلة الفورية. ويخفي الفيروس نفسه عن طريق إلحاق نفسه بملف على الكمبيوتر. وعند وصول المستخدم لهذا الملف، يباشر الفيروس عمله ويصيب جهاز الكمبيوتر. وللفيروس القدرة على إتلاف ملفات أو حتى حذفها من الكمبيوتر، أو استخدام البريد الإلكتروني الخاص بك لنشر نفسه على أجهزة الكمبيوتر الأخرى أو حتى محو كافة محتويات محرك الأقراص الثابتة .

وقد تمثل بعض الفيروسات خطورة شديدة. وأكثر أنواع الفيروسات ضررًا ما يستخدم في تسجيل ضغطات المفاتيح على لوحة المفاتيح. حيث يمكن أن يستخدم المهاجمون هذه الفيروسات لجمع بيانات حساسة، مثل كلمات المرور وأرقام بطاقات الائتمان. حتى أن هناك فيروسات يمكن أن تقوم بتبديل أو تدمير المعلومات التي على الكمبيوتر. ويمكن للفيروسات الضارة إصابة جهاز الكمبيوتر وتظل خاملة إلى أن يتم استدعاؤها من قِبل المهاجم.

والديدان (worm) هي عبارة عن برنامج يتضاعف ذاتيًا ويسبب الضرر للشبكات. وتقوم ديدان (worm) باستخدام الإنترنت لتكرار الكود الخاص به على المضيفين الموجودين على الشبكة، وبدون تدخل من أي مستخدم في الغالب. وتختلف ديدان worm عن الفيروسات في كونها لا تحتاج إلى أن يتم إرفاقها ببرنامج لإصابة الجهاز المضيف. حتى وإن لم تقم الديدان (worm) بإتلاف البيانات أو التطبيقات على المضيفين الذين تصيبهم، فإنها تتسبب في الإضرار بالشبكات حيث إنها تستهلك جزءًا من النطاق الترددي.

يعتبر حصان طروادة (Trojan) من الناحية التقنية من نوع ديدان .(worm) حيث لا يحتاج حصان طروادة (Trojan)إلى أن يتم إرفاقه ببرنامج آخر. بل عوضًا عن ذلك، يتم إخفاء تهديد حصان طروادة (Trojan) في برنامج يبدو وكأنه يقوم بعمل واحد، ولكنه يقوم بعمل آخر في الخفاء. ويتنكر حصان طروادة (Trojan)

في العادة في شكل برنامج مفيد .ويمكن لحصان طروادة (Trojan) التكاثر كفيروس virus والانتشار في أجهزة كمبيوتر أخرى. وقد يبلغ تلف بيانات الكمبيوتر وفقد الإنتاج مبلغًا كبيرًا. وقد يُطلب من الفني القيام بالإصلاحات، وربما يفقد الموظفون البيانات أو يضطرون إلى استبدالها .يمكن أن يقوم جهاز كمبيوتر مصاب بإرسال بيانات هامة للمنافسين، ويقوم في الوقت نفسه بإصابة أجهزة الكمبيوتر الأخرى على الشبكة.

برامج الحماية ضد الفيروسات - والتي تعرف ببرامج مكافحة الفيروسات - عبارة عن برامج صممت خصيصًا لاكتشاف الفيروسات والديدان (worm) وبرامج حصان طروادة (Trojan) وتعطيل عملها وإزالتها قبل إصابة الكمبيوتر. وعلى الرغم من ذلك، فإن برامج مكافحة الفيروسات سريعًا ما تصبح قديمة، ويتحمل الفنيون مسئولية تطبيق أحدث التحديثات والتصحيحات وتعريفات الفيروسات كجزء من جدول الصيانة المنتظمة. وتقوم العديد من المؤسسات بتأسيس نهج أمان مكتوب ينص على أنه لا يُسمح للموظفين بتثبيت أية برامج غير مقدمة من قِبل الشركة. كما تقوم المؤسسات أيضًا بتوعية الموظفين بمخاطر فتح مرفقات بريد إلكتروني نظرًا لأنها قد تحتوي على فيروس أو دودة.(worm)

## 9-2-2 شرح أمان الويب

يعد أمان الشبكة من الأمور الهامة حيث إن العديد من الأشخاص يزورون شبكة الويب العالمية يوميًا. وبعض الميزات التي تجعل الشبكة مفيدة ومسلية يمكن أيضًا أن تجعلها ضارة لجهاز الكمبيوتر.

فالأدوات التي تستخدم لجعل صفحات الويب أكثر قوة ومتعددة الاستعمالات
-كما هو موضح في الشكل رقم 1 - يمكن أيضًا أن تجعل الكمبيوتر أكثر عرضة للهجمات. وإليك بعض الأمثلة على أدوات الويب :

- **ActiveX** - وهي تقنية أنشأتها شركة Microsoft للتحكم في التفاعل على صفحات الويب. في حالة وجود ActiveX على أحد الصفحات، يتعين تنزيل تطبيق صغير أو برنامج صغير للوصول إلى الوظيفة الكاملة .
- **Java** - وهي لغة برمجة تتيح للتطبيقات الصغيرة إمكانية التشغيل في مستعرض ويب. ومن أمثلة التطبيقات الصغيرة الآلة الحاسبة أو العدّاد .
- **JavaScript** - لغة برمجة تم تطويرها لتتفاعل مع كود مصدر لغة HTML لمواقع الويب التفاعلية. ومن أمثلته الشعار الدوار أو الإطار المنبثق .

قد يستخدم المهاجمون أيًا من هذه الأدوات لتثبيت برنامج على الكمبيوتر .وللحيلولة دون حدوث هذه الهجمات، فإن غالبية المستعرضات تحتوي على إعدادات تجبر مستخدم جهاز الكمبيوتر على السماح بتنزيل ActiveX أو Java أو JavaScript واستخدامها، كما هو موضح في الشكل رقم 2.

## 9-2-3 تعريف برامج الإعلانات المتسللة وبرامج التجسس والبرامج غير المرغوب فيها

عادةً ما يتم تثبيت برامج الإعلانات المتسللة (Adware) وبرامج التجسس (spyware)والبرامج غير المرغوب فيها (grayware) على الكمبيوتر دون علم المستخدم. وتقوم هذه البرامج بجمع المعلومات المخزنة على جهاز الكمبيوتر أو تغيير تكوين الكمبيوتر أو فتح إطارات إضافية على جهاز الكمبيوتر بدون رضا المستخدم .

أما برامج الإعلانات المتسللة (Adware) فهي عبارة عن برامج تقوم بعرض الإعلانات على جهاز الكمبيوتر. وعادةً ما يتم توزيع برامج الإعلانات المتسللة مع ما يتم تنزيله من برامج. وفي كثير من الأحيان، يتم عرض برامج الإعلانات المتسللة في إطار منبثق. ويصعب أحيانًا التحكم في الإطارات المنبثقة لبرامج الإعلانات المتسللة مما يمكنِها من فتح إطارات جديدة بسرعة تفوق قدرة المستخدم على إغلاقها .

وبرامج grayware أو) malware برامج ضارة) عبارة عن ملف أو برنامج يختلف عن الفيروس ويمكن أن يحدث ضررًا. والعديد من هجمات برامج grayware عبارة عن هجمات تهدف إلى الخداع وتحاول إقناع القارئ بتزويد المهاجم ـ دون علمه ـ بإمكانية الوصول إلى المعلومات الشخصية. وبمجرد قيامك بملء النموذج المقدم إليك عبر الإنترنت، يتم إرسال البيانات إلى المهاجم. ويمكن إزالة برامج grayware باستخدام أدوات إزالة برامج التجسس وبرامج الإعلانات المتسللة .

وتشبه برامج التجسس - (Spyware) وهي أحد أنواع برامج - grayware برامج الإعلانات المتسللة (adware).حيث يتم توزيعها دون أي تدخل من المستخدم أو علمه. وبمجرد تثبيتها، تقوم برامج التجسس بمراقبة نشاط الكمبيوتر. ثم يرسل برنامج التجسس بعد ذلك هذه المعلومات إلى الجهة المسئولة عن تشغيل برنامج التجسس .

ويعد الخداع (phishing) شكلاً من أشكال الهندسة الاجتماعية التي يقوم فيها المهاجم بالتظاهر بتمثيل مؤسسة شرعية خارجية، كالبنك على سبيل المثال. ويتم الاتصال بالضحية المحتملة عن طريق البريد الإلكتروني. وربما يطلب المهاجم التحقق من المعلومات - مثل كلمة المرور أو اسم المستخدم - زاعمًا منع حدوث بعض العواقب الوخيمة.

**ملاحظة :**من النادر جدًا الحاجة إلى الكشف عن معلومات شخصية أو مالية حساسة عبر الإنترنت. فكن حذرًا حيال مثل هذه الأمور. استخدم خدمة مكتب البريد لمشاركة المعلومات الحساسة.

## 9-2-4 شرح رفض الخدمة(DoS)

رفض الخدمة (DoS) هو إحدى أشكال الهجمات التي تمنع المستخدمين من الوصول إلى الخدمات العادية، مثل البريد الإلكتروني وخادم الويب، نظرًا لكون النظام مشغولاً بالاستجابة لقدر كبير من الطلبات يفوق المعتاد. يعمل رفض الخدمة DoS من خلال إرسال طلبات كافية لمورد النظام، مما ينتج عنه تحميل الخدمة المطلوبة بحمل زائد عن طاقتها وتوقفها عن العمل.

ومن هجمات DoS الشائعة ما يلي :

- الأمر - Ping of death عبارة عن سلسلة من أوامر ping المتكررة والأكبر من المعدل الطبيعي تعمل على تعطيل جهاز الكمبيوتر الذي يستقبلها
- قنبلة من رسائل البريد الإلكتروني - كمية كبيرة جدًا من البريد الإلكتروني غير الهام التي تملأ خادم البريد الإلكتروني عن آخره مما يمنع المستخدمين من الوصول إليه

ويعد Distributed DoS اختصاره (DDoS شكلاً آخر من أشكال الهجوم يستخدم العديد من أجهزة الكمبيوتر المصابة - والتي تسمى مسلوبة الإرادة - (zombie) لبدأ الهجوم .مع استخدامDDoS ، تكون النية هي اعتراض طريق الوصول إلى الخادم المستهدف أو ملأه عن آخره. تقع أجهزة الكمبيوتر مسلوبة الإرادة (zombie)في مواقع جغرافية مختلفة الأمر الذي يجعل من الصعب تعقب مصدر الهجوم.

## 9-2-5 وصف البريد العشوائي والإطارات المنبثقة

البريد العشوائي - والمعروف أيضًا بالبريد غير الهام - هو بريد إلكتروني غير مرغوب فيه، كما هو موضح في الشكل رقم 1. وفي غالبية الحالات، يستخدم البريد العشوائي كأسلوب للإعلانات. وعلى الرغم من ذلك، يمكن استخدام البريد العشوائي لإرسال ارتباطات ضارة أو محتوى مضلل، كما هو موضح في الشكل رقم 2.

وعند استخدامه كأسلوب للهجوم، قد يحتوي البريد العشوائي على ارتباطات لمواقع ويب مصابة أو على مرفق من شأنه إصابة جهاز الكمبيوتر. قد ينتج عن هذه الارتباطات أو المرفقات أعداد وافرة من الإطارات صممت لجذب انتباهك ونقلك إلى مواقع إعلانات .وتسمي هذه الإطارات بالإطارات المنبثقة. وكما هو موضح في الشكل رقم 2، يمكن للإطارات المنبثقة غير المتحكم بها تغطية شاشة المستخدم بسرعة وإعاقته عن إنجاز عمله.

تقوم العديد من برامج مكافحة الفيروسات وبرامج البريد الإلكتروني باكتشاف البريد العشوائي وإزالته من علبة البريد الإلكتروني الوارد. إلا أن هناك رسائل بريد عشوائي يمكنها الاختراق والتسلل، لكن يمكنك التعرف عليها من خلال العلامات الآتية:

- لا يوجد سطر موضوع
- عناوين الإرجاع غير مكتملة
- رسائل بريد إلكتروني يقوم الكمبيوتر بإنشائها
- إرجاع رسائل بريد إلكتروني لم يرسلها المستخدم

## 9-2-6 شرح الهندسة الاجتماعية

المهندس الاجتماعي المحتال (social engineer) هو الشخص الذي لديه القدرة على الوصول إلى الأجهزة أو إلى شبكة عن طريق خداع الأشخاص لتقديم معلومات الوصول الضرورية. وعادةً ما يكتسب المهندس الاجتماعي المحتال ثقة الموظف ويقنعه بإفشاء معلومات تتعلق باسم المستخدم وكلمة المرور.

وقد يتظاهر هذا المحتال بأنه فني محاولاً الدخول إلى إحدى الشركات، كما هو موضح في الشكل رقم 1. وبمجرد دخول هذا المحتال، قد يقوم خفية بجمع المعلومات أو يقوم بالبحث في الأوراق الموجودة على المكاتب بحثًا عن كلمات المرور وأرقام الهواتف الداخلية أو يحصل على دليل الشركة الذي يضم عناوين البريد الإلكتروني. يوضح الشكل رقم 2 قائمة بالأشياء التي قد يستعين بها المحتال.

وفيما يلي بعض التدابير الوقائية لمساعدتك في الحماية من الهندسة الاجتماعية:(social engineering)

- لا تكشف أبدًا عن كلمة المرور الخاصة بك
- اسأل دائمًا عن بطاقة الهوية الخاصة بالأشخاص غير المعروفين
- قلل من وصول الزوار غير المتوقعين
- قم بمرافقة كافة الزوار
- لا تقم مطلقًا بنشر كلمة المرور الخاصة بك في منطقة العمل
- قم بتأمين جهاز الكمبيوتر عند مغادرة المكتب
- لا تدع أي شخص يتبعك عبر باب يتطلب المرور منه استخدام بطاقة وصول

## 9-2-7 شرح هجماتTCP/IP

إن TCP/IP هو مجموعة من البروتوكولات التي تُستخدم للتحكم في كافة الاتصالات عبر الإنترنت. ولسوء الحظ، فإن TCP/IP من الممكن أن يتسبب أيضًا في جعل الشبكة عرضة للمهاجمين.

وإليك بعض الهجمات الأكثر شيوعًا:

- فيض حزم التزامن - (SYN Flood) والذي يفتح منافذ TCP عشوائيًا، وربط أجهزة الشبكة أو الكمبيوتر بقدرٍ كبير من الطلبات الزائفة، الأمر الذي يتسبب في رفض الجلسات للآخرين .
- رفض الخدمة - (DoS) يرسل قدرًا كبيرًا يفوق المعتاد من الطلبات للنظام مما يمنع الوصول إلى الخدمات .
- DDoS - يستخدم "أجهزة الكمبيوتر مسلوبة الإرادة" ليجعل من الصعب تحديد مكان هجمات DoS ومنشئها .
- انتحال الهوية - (Spoofing) يحصل على صلاحية وصول إلى الموارد الموجودة على الأجهزة وذلك بالتظاهر بأنه كمبيوتر موثوق به .
- الدخيل - (Man-in-the-Middle) يعترض سبيل حركة مرور البيانات أو يدرج معلومات زائفة إليها بين اثنين من المضيفين .
- إعادة التشغيل - (Replay) يستخدم أداوت استشعار الشبكة لاستخراج أسماء المستخدمين وكلمات المرور لاستخدامها في وقتٍ لاحق للحصول على صلاحية وصول .
- هدم DNS بالإنجليزية - (DNS Poisoning) يغير سجلات DNS على نظام للإشارة إلى خوادم زائفة حيث يتم تسجيل البيانات .

## 9-2-8 شرح إحلال مكونات الكمبيوتر المادية وإعادة تصنيعها

إن عملية إحلال مكونات الكمبيوتر المادية هي إزالة البيانات الحساسة من مكونات الكمبيوتر المادية والبرمجية قبل إعادة تصنيعها أو التخلص منها. يجب محو محتويات الأقراص الثابتة بالكامل لمنع إمكانية الاستعادة باستخدام برامج متخصصة. فلا يكفي حذف الملفات أو حتى تهيئة محرك الأقراص. استخدم أدوات من جهة أخرى لاستبدال البيانات عدة مرات لجعل البيانات غير قابلة للاستخدام. والطريقة الوحيدة للتأكد تمام التأكد أنه لا يمكن استعادة البيانات من محرك الأقراص الثابتة هي كسر الأسطوانات المعدنية الداخلية (platters)بحذر باستخدام مطرقة والتخلص من الأجزاء بأمان.

كما يجب تدمير وسائط مثل الأقراص المضغوطة والأقراص المرنة. استخدم آلة قطع مخصصة لهذا الغرض.

## 9-3 تحديد إجراءات الأمان

يجب استخدام خطة أمنية لتحديد ما ينبغي القيام به في المواقف الحرجة. ويجب تحديث نهج الخطة المبنية باستمرار لصد أحدث التهديدات التي تتعرض لها الشبكة. والخطة الأمنية التي تتبع إجراءات أمان واضحة تعد هي الأساس الذي ينبغي على الفني اتباعه .وتجب مراجعة الخطط الأمنية سنويًا.

وجزء من عملية ضمان الأمان يتمثل في إجراء اختبارات لتحديد المناطق التي يكون فيها مستوى الأمان ضعيفًا. ويجب القيام بالاختبارات دوريًا. حيث تظهر وتصدر تهديدات جديدة كل يوم. توفر الاختبارات الدورية تفاصيل حول أية نقاط ضعف محتملة في خطة الأمان الحالية والتي يجب التعامل معها .

وهناك العديد من طبقات الأمان في الشبكة، بما في ذلك الطبقة المادية واللاسلكية وطبقة البيانات. وكل طبقة من هذه الطبقات عرضة لهجمات الأمان. ويتعين على الفني فهم كيفية تطبيق إجراءات الأمان لحماية الأجهزة والبيانات.

بعد إكمال هذا القسم سيكون بمقدورك تحقيق الأهداف التالية:

- شرح مستلزمات نهج الأمان المحلي الأساسي .
- شرح المهام اللازمة لحماية الأجهزة المادية .
- وصف طرق حماية البيانات .
- وصف تقنيات الأمان اللاسلكي .

### 9-3-1 شرح مستلزمات نهج الأمان المحلي الأساسي

رغم اختلاف نهج الأمان المحلي من مؤسسة إلى أخرى، إلا أن هناك بعض الأسئلة التي ينبغي على كافة المؤسسات طرحها وهي:

- ما الأصول التي تتطلب حماية؟
- ما التهديدات المحتملة؟
- ما الإجراءات المتبعة في حالة خرق الأمان؟

**ملاحظة :**قد يشار لجهاز الكمبيوتر نفسه بأنه وحدة المعالجة المركزية أو CPU. وفي هذا المساق، سيشير المصطلح CPU إلى شريحة المعالج الدقيق فقط .

يجب أن يصف نهج الأمان كيفية تعامل الشركة مع المشاكل الأمنية:

- تعريف عملية معالجة حوادث أمان الشبكة
- تعريف عملية تدقيق أمان الشبكة الحالية
- تعريف إطار عمل الأمان العام لتطبيق أمان الشبكة
- تعريف السلوكيات المسموح بها
- تعريف السلوكيات الممنوعة
- وصف الأشياء التي ينبغي تسجيلها وكيفية تخزين السجلات: عارض الأحداث أو ملفات سجلات النظام أو ملفات سجلات الأمان
- تعريف وصول الشبكة إلى الموارد من خلال أذونات الحساب
- تعريف تقنيات المصادقة للوصول إلى البيانات مثل: أسماء المستخدمين وكلمات المرور وعمليات التعرف البيولوجي والبطاقات الذكية

## 9-3-2 شرح المهام اللازمة لحماية الأجهزة المادية

يحظى الأمان المادي بنفس أهمية أمان البيانات. فإن الاستيلاء على كمبيوتر يعني الاستيلاء على كل ما فيه من بيانات كذلك.

وهناك عدة طرق لتوفير الحماية المادية لأجهزة الكمبيوتر، كما هو موضح بالشكلين رقم 1 ورقم 2:

- التحكم في الوصول إلى المنشآت
- استخدام تأمين الكبلات مع الأجهزة
- الإبقاء على غرف أجهزة الاتصالات مغلقة
- تزويد الأجهزة بمسامير أمان
- استخدام أقفاص أمان حول الأجهزة
- وضع تسميات للمجسات وتثبيتها على الأجهزة؛ مثل علامات تعريف التردد اللاسلكي (RFID)

بالنسبة للوصول إلى المنشآت، توجد عدة طرق للحماية:

- المفاتيح ذات البطاقات التي تخزن بيانات المستخدم، بما في ذلك مستوى الوصول
- موصلات Berg للتوصيل بمحرك الأقراص المرنة
- مجسات التعريفات البيولوجية التي تقوم بتحديد السمات المادية للمستخدم، مثل بصمات الأصابع أو شبكية العين
- حارس الأمان المعين
- المجسات ـ مثل علامات RFID ـ لمراقبة الأجهزة

## 9-3-3 وصف طرق حماية البيانات

إن الأجهزة المادية لا ترقى قيمتها عادةً إلى مستوى قيمة البيانات التي تحتويها. فقد يكون فقد بيانات حساسة ووصولها إلى منافسي الشركة أو إلى المجرمين أمرًا مكلفًا جدًا. وقد تؤدي مثل هذه الخسائر إلى فقد الثقة في الشركة وفصل فنيي الكمبيوتر المسئولين عن أمان الكمبيوتر من العمل. وهناك العديد من طرق حماية البيانات التي يمكن تطبيقها.

**الحماية بكلمة المرور**
الحماية بكلمة المرور لها القدرة على منع الوصول غير المرخص إلى المحتوى، كما هو موضح في الشكل رقم 1. فبدونه يكون للمهاجمين القدرة على الوصول إلى بيانات الكمبيوتر غير المحمية. وتتعين حماية كافة أجهزة الكمبيوتر بكلمة مرور. ويُوصى باستخدام مستويين من الحماية بكلمة المرور وهما:

- مستوى - BIOS وهو يمنع تغيير إعدادات BIOS دون إدخال كلمة مرور صحيحة
- مستوى تسجيل الدخول - (Login) وهو يمنع الوصول غير المرخص إلى الشبكة

توفر تسجيلات الدخول إلى الشبكة وسائل تسجيل النشاط على الشبكة كما تقوم إما بمنع الوصول إلى الموارد أو السماح به. وهذا ما يجعل من الممكن تحديد الموارد التي يجري الوصول إليها. ويقوم مسئول النظام في العادة بتحديد اصطلاح تسمية لأسماء المستخدمين عند إنشاء تسجيلات الدخول إلى الشبكة. والمثال الشائع لاسم المستخدم هو الحرف الأول من اسم الشخص متبوعًا باسم العائلة بأكمله. يجب عليك جعل اصطلاح التسمية الخاص باسم المستخدم بسيطًا على الدوام بحيث لا يجد الأشخاص صعوبة في تذكره .

وعند تعيين كلمات المرور، يجب أن يتطابق مستوى التحكم في كلمة المرور مع مستوى الحماية المطلوب. يجب تطبيق نهج أمان جيد بكل دقة كما يجب أن يتضمن - على سبيل المثال لا الحصر - القواعد التالية:

- يجب أن تنتهي صلاحية كلمات المرور بعد فترة زمنية محدودة .
- يجب أن تتضمن كلمات المرور مزيجًا من الحروف والأرقام بحيث لا يمكن اختراقها بسهولة .
- يجب أن تكفل معايير كلمات المرور منع المستخدمين من تدوين كلمات مرورهم وتركها دون حماية خشية اطلاع الآخرين عليها .

- يجب تحديد قواعد بشأن انتهاء ومنع استخدام صلاحية كلمات المرور. يتم تطبيق قواعد منع الدخول عند القيام بمحاولة غير ناجحة للوصول إلى النظام أو عند اكتشاف حدوث تغيير معين في تكوين النظام .

ولتسهيل عملية إدارة الأمان، من الشائع تقسيم المستخدمين إلى مجموعات، ثم تقسيم المجموعات إلى موارد. وهذا الأمر يسمح بإمكانية تغيير قدرات وصول المستخدمين على الشبكة بسهولة من خلال تعيين ـ أو إزالة ـ المستخدم من مجموعات مختلفة. ويفيد هذا الأمر عند إعداد حسابات مؤقتة للعمال الزائرين أو المستشارين الضيوف، مما يمنحك القدرة على تقييد الوصول إلى الموارد .

**تشفير البيانات**

تشفير البيانات يستخدم الأكواد والشفرات. ويمكن حماية حركة مرور البيانات بين الموارد وأجهزة الكمبيوتر على الشبكة من مراقبة المهاجمين للعمليات أو تسجيلها وذلك من خلال تطبيق التشفير. وقد لا يكون من الممكن فك تشفير البيانات التي تم التقاطها على الفور للاستفادة منها .

وتستخدم الشبكة الظاهرية الخاصة (VPN) التشفير لحماية البيانات. حيث يتيح اتصال VPN للمستخدم البعيد إمكانية الوصول الآمن إلى الموارد كما لو كان جهاز الكمبيوتر متصلاً ماديًا بالشبكة المحلية.

**حماية المنفذ**

يقترن كل اتصال يستخدم برتوكول TCP/IP برقم منفذ. فعلى سبيل المثال، يستخدم اتصال HTTPS المنفذ رقم 443 بشكل افتراضي .جدار الحماية
-كما هو موضح في الشكل رقم 2 - عبارة عن طريقة لحماية الكمبيوتر
من التدخل عبر المنافذ. يمكن أن يتحكم المستخدم في نوع البيانات التي يتم إرسالها إلى الكمبيوتر عن طريق تحديد المنافذ التي سيتم فتحها وأيها سيتم تأمينه. وتعرف البيانات التي يتم نقلها عبر الشبكة بحركة مرور البيانات.

**النسخ الاحتياطية للبيانات**

يجب أن تتضمن خطة الأمان إجراءات النسخ الاحتياطي للبيانات. حيث يمكن أن تتعرض البيانات للفقد أو التلف في ظروف مثل السرقة أو فشل الأجهزة أو حدوث كارثة مثل اندلاع حريق أو فيضان. لذلك يعتبر النسخ الاحتياطي للبيانات أحد أكثر الطرق فاعلية للحماية من فقد البيانات .وفيما يلي بعض الاعتبارات التي تتعلق بالنسخ الاحتياطي للبيانات:

- **تكرار النسخ الاحتياطية** - قد تستغرق النسخ الاحتياطية وقتًا طويلاً. أحيانًا يكون من الأسهل القيام بعملية نسخ احتياطي شهريًا أو أسبوعيًا، ثم القيام بنسخ احتياطي جزئي بشكل متكرر لأي بيانات يطرأ عليها التغيير بعد القيام بآخر عملية نسخ احتياطي كاملة. وعلى الرغم من ذلك، فإن نشر النسخ الاحتياطية في العديد من السجلات يزيد من مقدار الوقت اللازم لاستعادة البيانات .
- **تخزين النسخ الاحتياطية** - يجب نقل النسخ الاحتياطية إلى موقع تخزين بعيد عن مكان العمل متفق عليه لمزيد من الأمان. يتم نقل وسائط النسخ الاحتياطي الحالية إلى الموقع البعيد عن العمل في دورة يومية أو أسبوعية أو شهرية حسب حاجة المؤسسة المحلية .
- **أمان النسخ الاحتياطية** - يمكن حماية النسخ الاحتياطية بكلمات مرور. ويجب إدخال كلمات المرور هذه قبل استعادة البيانات الموجودة على وسائط النسخ الاحتياطي .

**أمان نظام الملفات**

تتعقب كافة أنظمة الملفات مسارات الموارد، لكن أنظمة الملفات ذات دفاتر التسجيل هي فقط التي تستطيع الوصول حسب المستخدم والتاريخ والوقت. وتفتقر أنظمة الملفات FAT 32 ـ الموضحة في الشكل رقم 3 والتي تُستخدم في بعض إصدارات Windows ـ إلى قدرات كل من كتابة الدفاتر والتشفير .نتيجة لذلك، فإن المواقف التي تتطلب مستوى جيدًا من الأمان يتم نشرها غالبًا باستخدام نظام ملفات مثلNTFS ، والذي يعد جزءًا من Windows 2000 و .Windows XP أما في حالة الحاجة إلى مزيد من الأمان، فمن الممكن تشغيل أدوات مساعدة معينة مثل CONVERT لترقية نظام الملفات FAT 32 إلى .NTFS وعملية تحويل نظام الملفات عملية غير قابلة للعكس. فمن المهم تحديد أهدافك بوضوح قبل القيام بالنقل.

حيث أن حركة مرور البيانات تتدفق عبر الموجات اللاسلكية في الشبكات اللاسلكية، فمن السهل للمهاجمين مراقبة ومهاجمة البيانات دون حاجة إلى الاتصال بالشبكة بشكل مادي. ويحصل المهاجمون على وصول إلى الشبكة عن طريق دخول نطاق من الشبكة اللاسلكية غير محمي. ويتعين على الفني معرفة كيفية تكوين نقاط الوصول وبطاقات واجهة الشبكة اللاسلكية (NIC) إلى مستوى مناسب من الأمان .

عند تثبيت الخدمات اللاسلكية، ينبغي عليك تطبيق تقنيات الأمان اللاسلكية على الفور لمنع الوصول غير المرغوب إلى الشبكة كما هو موضح في الشكل رقم 1. ويجب تكوين نقاط الوصول اللاسلكية باستخدام إعدادات الأمان الأساسية التي تتوافق مع أمان الشبكة الحالية.

يمكن للمهاجم الوصول إلى البيانات أثناء انتقالها عبر الإشارة اللاسلكية. حيث يمكن استخدام نظام تشفير لاسلكي لمنع الالتقاط غير المرغوب فيه واستخدام البيانات عبر تشفير البيانات التي يتم إرسالها. فيجب أن يستخدم كلا طرفي الارتباط نفس معيار التشفير. ويوضح الشكل رقم 2 مستويات الأمان كالتالي:

- **الخصوصية السلكية المكافئة - (WEP)** وهي الجيل الأول من معيار الأمان للشبكات اللاسلكية. وسرعان ما اكتشف المهاجمون أنه يسهل فك تشفير WEP. حيث يمكن اكتشاف مفاتيح التشفير المستخدمة في تشفير الرسائل عن طريق برامج المراقبة. وبمجرد الحصول على المفاتيح، يصبح من السهل فك تشفير الرسائل .
- **الوصول المحمي بواسطة) Wi-Fi اختصارها - (WPA** إصدار محسَّن من WEP. تم إنشاؤه كحل مؤقت حتى تم تطبيق المعيار) i802.11 طبقة أمان للأنظمة اللاسلكية (بالكامل. وبما أنه قد تم التصديق الآن على المعيارi802.11 ، فقد تم إصدار WPA2. وهو يغطي معيار i802.11 بأكمله .
- **البروتوكول الخفيف للمصادقة القابلة للامتداد(LEAP)** ، يطلق عليه أيضًا **بروتوكول-EAP Cisco** - هو بروتوكول الأمان اللاسلكي أنشأته شركة Cisco لعلاج ما في بروتوكولي WEP و WPA من ضعف. يعد LEAP حلاً جيدًا عند استخدام أجهزة Cisco إلى جانب أنظمة تشغيل مثل Windows و .Linux

أمان طبقة النقل اللاسلكي (WTLS) عبارة عن طبقة أمان تستخدم في الأجهزة المحمولة التي تستخدم بروتوكول التطبيقات اللاسلكية.(WAP)
لا تحتوي الأجهزة المحمولة على قدر كبير من النطاق الترددي الاحتياطي لتخصيصه لبروتوكولات الأمان. وقد تم تصميم طبقة WTLS لتوفير الأمان لأجهزة WAP بطريقة فعالة من ناحية النطاق الترددي.

## 9-4 تحديد طرق الصيانة الوقائية الشائعة للأمان

إن الأمان عملية وتقنية دائمة التغير. فكل يوم يتم اكتشاف ثغرات أمنية جديدة .حيث يبحث المهاجمون باستمرار عن أساليب جديدة لاستخدمها في شن هجوم. لذلك يتعين على الجهات المصنعة للبرامج إنشاء التصحيحات وإصدارها بانتظام لإصلاح الأخطاء والثغرات الأمنية في المنتجات. فإذا ما تُرك جهاز الكمبيوتر دون حماية أحد الفنيين، عندئذ يمكن للمهاجم بسهولة الحصول على الوصول. وقد تصاب أجهزة الكمبيوتر غير المحمية المتصلة بالإنترنت في غضون دقائق معدودة .

ونظرًا لطبيعة تهديدات الأمان دائمة التغير، يتعين على الفنيين فهم كيفية تثبيت التصحيحات والتحديثات. كما يجب أن تكون لديهم القدرة على معرفة الوقت الذي تتوفر فيه التحديثات والتصحيحات الجديدة. وتقوم بعض الجهات المصنعة بإصدار التحديثات في نفس اليوم من كل شهر، لكنها تقوم أيضًا بإرسال تحديثات هامة عند الضرورة. بينما توفر بعض الجهات الأخرى خدمات التحديثات التلقائية التي من شأنها تصحيح البرامج في كل مرة يتم فيها تشغيل جهاز الكمبيوتر، أو بالإخطار عن طريق البريد الإلكتروني في حالة صدور تصحيح أو تحديث جديد.

بعد إكمال هذا القسم سيكون بمقدورك تحقيق الأهداف التالية:

- شرح كيفية تحديث ملفات التوقيع للبرامج المضادة للفيروسات وبرامج التجسس .
- شرح كيفية تثبيت حزم خدمات أنظمة التشغيل وتصحيحات الأمان .

## 9-4-1 شرح كيفية تحديث ملفات التوقيع للبرامج المضادة للفيروسات وبرامج التجسس

دائمًا ما يكون الأمان عرضة للتهديدات من الفيروسات والبرامج التخريبية (worm).ويسعى المهاجمون دومًا للتوصل إلى طرق جديدة للتسلل إلى أجهزة الكمبيوتر والشبكات. وحيث أنه يتم تطوير فيروسات جديدة دائمًا، يجب إذن تحديث برامج الأمان باستمرار. يمكن القيام بهذه العملية تلقائيًا، لكن يتعين على الفنيين معرفة كيفية التحديث اليدوي لأي نوع من برامج الحماية وكافة برامج تطبيقات العميل.

تبحث برامج اكتشاف الفيروسات وبرامج التجسس وبرامج الإعلانات المتسللة عن أنماط معينة في الأكواد البرمجية الخاصة بالبرامج على الكمبيوتر. يتم تحديد أنواع هذه الأنماط من خلال تحليل الفيروسات التي يتم اعتراضها على الإنترنت أو على شبكات LAN) الشبكات المحلية). وتعرف أنماط الأكواد هذه باسم التوقيعات. حيث تقوم الجهات الناشرة لبرامج الحماية بتجميع التوقيعات في جداول تعريف الفيروسات. ولتحديث ملفات التوقيعات للبرامج المضادة للفيروسات وبرامج التجسس، ينبغي أولاً التحقق لمعرفة ما إذا كانت ملفات التوقيع هي أحدث الملفات أم لا. يمكن القيام بذلك بالانتقال إلى الخيار "حول (About) "من برنامج الحماية، أو من خلال تشغيل أداة التحديث لبرنامج الحماية. فإذا كانت ملفات التوقيع قديمة، يتعين القيام بتحديثها يدويًا باستخدام الخيار "التحديث الآن (Update Now) "الموجود في غالبية برامج الحماية.

ويجب عليك دائمًا الحصول على ملفات التوقيع من موقع الويب التابع للجهة المصنعة للتأكد من أن التحديث موثوق به وأنه غير تالف بفعل الفيروسات. وهذا الأمر قد يزيد من الطلب بصورة كبيرة على موقع الويب الخاص بالجهة المصنعة لاسيما عند صدور فيروسات جديدة. ولتجنب التسبب في ازدحام مروري للبيانات على موقع ويب واحد، تقوم بعض الجهات المصنعة بتوزيع ملفات التوقيع الخاصة بها ليتم تنزيلها من خلال عدة مواقع ويب خاصة بالتنزيل. وتعرف مواقع التنزيل هذه باسم) mirrors أي المرايا .)

**تحذير :**عند تنزيل ملفات التوقيع من على موقع مثيل(mirror) ، تأكد أن الموقع المثيل موقع شرعي. قم بالارتباط بالموقع المثيل من خلال موقع الويب التابع للجهة المصنعة دائمًا.

## 9-4-2 شرح كيفية تثبيت حزم خدمات أنظمة التشغيل وتصحيحات الأمان

قد يصعب إزالة الفيروسات أو البرامج التخريبية المسماة بالدودة (worm) من الكمبيوتر. وينبغي توفر أدوات برمجية لإزالة الفيروسات وإصلاح كود جهاز الكمبيوتر الذي قام الفيروس بتعديله. ويتم توفير هذه الأدوات البرمجية من قِبل الجهات المصنعة لأنظمة التشغيل وشركات برامج الأمان. تأكد من قيامك بتنزيل هذه الأدوات من موقع شرعي .

قد تقوم الجهات المصنعة لأنظمة التشغيل وتطبيقات البرامج بتوفير تحديثات للأكواد البرمجية تعرف بالتصحيحات ومن شأنها منع الفيروسات والبرامج التخريبية المكتشفة حديثًا من شن هجوم ناجح. ومن حين لآخر، تقوم الجهات المصنعة بدمج التصحيحات والتحديثات في تطبيق تحديثي شامل يعرف بحزمة الخدمة. وقد يكون تأثير هجمات الفيروسات المشينة والمدمرة أقل حدة بكثير وذلك في حالة قيام العديد من المستخدمين بتنزيل أحدث حزم الخدمات وتثبيتها .

ويقوم نظام التشغيل Windows دوريًا بالبحث في موقع ويب Windows Update عن التحديثات ذات الأولوية العليا والتي يمكن أن تساعد على حماية الكمبيوتر من أحدث تهديدات الأمان. وقد تحتوي هذه التحديثات على تحديثات أمان وتحديثات هامة وحزم خدمات. استنادًا للإعداد الذي تقوم بتحديده، يقوم Windowsتلقائيًا بتنزيل التحديثات ذات الأولوية العليا التي يحتاج إليها الكمبيوتر وتثبيتها أو إعلامك بمجرد توفر هذه التحديثات .

ويجب تثبيت هذه التحديثات ولا يُكتفى فقط بتنزيلها. في حالة استخدام الإعداد" تلقائي (Automatic) "فيمكنك جدولة الوقت والتاريخ. وإلا فسيتم تثبيت التحديثات الجديدة عند الساعة الثالثة ظهرًا بشكل افتراضي. في حالة إيقاف تشغيل الكمبيوتر أثناء عملية التحديث المجدول، سيتم تثبيت التحديثات في المرة القادمة التي تقوم فيها بتشغيل الكمبيوتر. كما يمكنك أن تختار أن يقوم Windows بإعلامك في حالة توفر تحديث جديد وتثبيت البرنامج بنفسك.

اتبع التعليمات الموضحة في الشكل رقم 1 لتحديث نظام التشغيل باستخدام إحدى حزم الخدمات أو تصحيح الأمان.

## 9-5 استكشاف أخطاء الأمان وتصحيحها

تُستخدم عملية استكشاف الأخطاء وإصلاحها للمساعدة في حل مشكلات الأمان. وتتراوح خطورة هذه المشكلات بين مشكلات بسيطة - مثل منع شخص من متابعة سير العمل - إلى مشكلات أكثر تعقيدًا؛ مثل حذف الملفات المصابة يدويًا. استخدم خطوات استكشاف الأخطاء وإصلاحها كإرشادات لمساعدتك في تشخيص المشاكل وعلاجها .

بعد إكمال هذا القسم سيكون بمقدورك تحقيق الأهداف التالية:

- مراجعة لعملية استكشاف الأخطاء وإصلاحها .
- التعرف على المشاكل الشائعة وحلولها .

### 9-5-1 مراجعة لعملية استكشاف الأخطاء وإصلاحها

يجب أن يتمتع فنيو الكمبيوتر بالقدرة على تحليل تهديدات الأمان وتحديد الأسلوب الأمثل لحماية الأصول وإصلاح التلف. ويطلق على هذه العملية استكشاف الأخطاء وإصلاحها .

أول خطوة في عملية استكشاف الأخطاء وإصلاحها هي جمع البيانات من العميل. يعرض الشكلان 1 و 2 أسئلة مفتوحة الإجابة وأسئلة إجاباتها "نعم" أو "لا" لطرحها على العميل.

بعد أن تتحدث مع العميل، يجب أن تتحقق من المشاكل الواضحة. يعرض الشكل رقم 3 المشاكل التي تنطبق على الكمبيوتر المحمول.

بعد التحقق من المشاكل الواضحة، حاول تجربة بعض الحلول السريعة. يعرض الشكل رقم 4 بعض الحلول السريعة لمشاكل الكمبيوتر المحمول.

إذا لم تفلح الحلول السريعة في حل المشكلة، فهذا وقت جمع البيانات من الكمبيوتر .يعرض الشكل رقم 5 طرقًا مختلفة لجمع معلومات حول المشكلة من الكمبيوتر المحمول.

عند هذه النقطة، سيكون لديك معلومات كافية لتقييم المشكلة وبحثها وتنفيذ الحلول الممكنة. يعرض الشكل رقم 6 موارد للحلول الممكنة.

بعد أن تقوم بحل المشكلة، ستقوم بختام الحل مع العميل. يعرض الشكل
رقم 7 قائمة بالمهام المطلوبة لإكمال هذه الخطوة.

### 9-5-2 التعرف على المشاكل الشائعة وحلولها

قد يرجع سبب مشاكل أجهزة الكمبيوتر إلى مشاكل في المكونات المادية أو البرمجية أو الاتصال أو اجتماع الأسباب الثلاثة في آن واحد. وبعض أنواع مشكلات الكمبيوتر ستقوم بحلها بشكل متكرر أكثر من غيرها. يوضح الشكل رقم 1 جدولاً يضم مشاكل الأمان الشائعة وحلولها .

تم تصميم ورقة العمل لتعزيز مهاراتك في الاتصال للتحقق من المعلومات من العميل.

## 9-6 ملخص

تناولت هذه الوحدة أمان الكمبيوتر وسبب أهميته لحماية أجهزة الكمبيوتر والشبكات والبيانات. ولقد تم وصف التهديدات والإجراءات والصيانة الوقائية ذات الصلة بأمان البيانات والأمان المادي وذلك لمساعدتك على المحافظة على أمان أجهزة الكمبيوتر والبيانات. ويعمل الأمان على حماية أجهزة الكمبيوتر وأجهزة الشبكة والبيانات من الفقد والخطر المادي. فيما يلي بعض المفاهيم المهمة التي يجب تذكرها من هذه الوحدة :

- قد تأتي تهديدات الأمان من داخل المؤسسة أو من خارجها .
- تعد الفيروسات والبرامج التخريبية المسماة بالدودة (worm) تهديدات شائعة تهاجم البيانات .

- ينبغي تطوير خطة أمنية وصيانتها لحماية كل من البيانات والأجهزة المادية من الفقد .
- ينبغي الحفاظ على أنظمة التشغيل والتطبيقات محدثة وآمنة دائمًا باستخدام التصحيحات وحزم الخدمات .