منصة غرفة جدة
للتدريب الإلكتروني
JEDDAH CHAMBER E-TRAINING PLATFORM

الأمن السيبراني

المستوى المتقدم

المدرب :عبدالعزيز الشيباني

خطة التدريب اليومي :

- **مدخل الأمن السيبراني :**

- تعريف الأمن السيبراني

- مقدمة للأمن السيبراني

- مثلث الأمان

- **نظرة عامة للفيروسات .**

- أنواع الفيروسات
- طرق انتشارها
- طرق الحد منها
- أختيار الطرق المناسبة لبرامج الحماية

ما هو الأمن السيبراني (Cybersecurity)؟

أصبحت شبكة المعلومات الإلكترونية المتصلة جزءًا لا يتجزأ من حياتنا اليومية.
جميع أنواع المؤسسات تستخدم هذه الشبكة للعمل بفعالية ونشاط مثل المؤسسات الطبية
والمالية والتعليمية .
وهي تستخدم الشبكة عن طريق جمع كميات كبيرة من المعلومات الرقمية ومعالجتها وتخزينها ومشاركتها.
ومع جمع المزيد من المعلومات الرقمية وتقاسمها ، أصبحت حماية هذه المعلومات أكثر أهمية لأمننا الوطني واستقرارنا الاقتصادي.

ماهو الأمن السيبراني (Cybersecurity)

هو الجهد المستمر لحماية هذه الشبكات المتصلة بالشبكة وكافة البيانات من الاستخدام الغير المصرح به .

على المستوى الشخصي :
تحتاج إلى حماية هويتك وبياناتك وأجهزتك الحاسوبية.

على مستوى المنشئة :
يتحمل الجميع مسؤولية حماية سمعة المنظمة وبياناتها وعملائها.

على مستوى الدولة :
فإن الأمن الوطني وسلامة المواطنين ورفاهيتهم هي المحك.

بيـــانـــاتك

بياناتك

أي معلومات عنك يمكن اعتبارها بياناتك.
يمكن لهذه المعلومات الشخصية أن تعرّفك بشكل فريد كفرد.
تتضمن هذه البيانات الصور والرسائل التي تتبادلها مع عائلتك وأصدقائك عبر الإنترنت.
أما المعلومات الأخرى ، مثل الاسم ورقم السجل المدني وتاريخ ومكان الميلاد، فهي معروفة لك وتستخدم للتعرف عليك.
يمكن أيضًا استخدام معلومات أخرى لتحديد هويتك عبر الإنترنت مثل المعلومات الطبية والتعليمية والمالية والتوظيفية

أجهزة الكمبيوتر الخاصة بك

أجهزة الكمبيوتر الخاصة بك

لا تقوم أجهزة الكمبيوتر الخاصة بك بتخزين البيانات الخاصة بك فقط.
بل أصبحت الآن هذه الأجهزة البوابة إلى بياناتك وتوليد معلومات عنك.
ومع توفر كل هذه المعلومات عنك على الإنترنت ، أصبحت بياناتك الشخصية مربحة للمخترقين.

أنواع البيانات التنظيمية

أولًا : البيانات التقليدية Traditional Data :-

تشمل بيانات الشركة
- ✓ معلومات الموظفين
- ✓ الممتلكات الفكرية
- ✓ البيانات المالية.

ماذا تتضمن معلومات الموظفين ؟

مواد الطلب ، وكشوف الرواتب ، وخطابات العروض ، واتفاقيات الموظفين ، وأي معلومات تستخدم في اتخاذ قرارات التوظيف.

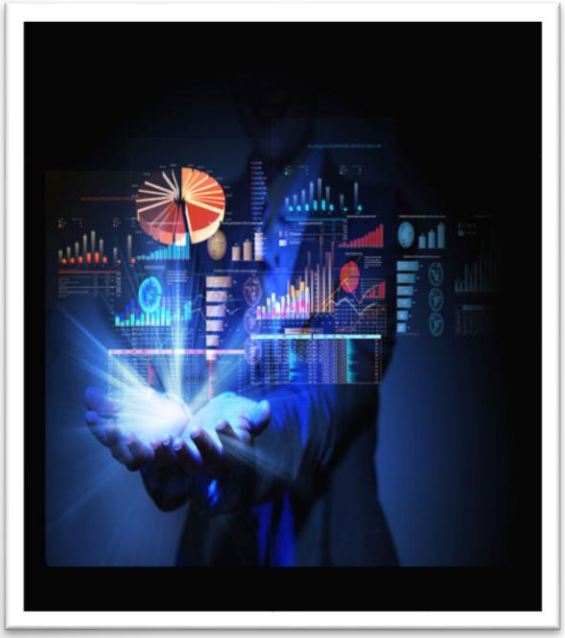
ماذا تتضمن الملكية الفكرية ،؟

براءات الاختراع والعلامات التجارية وخطط المنتجات الجديدة ، تتيح للأعمال التجارية اكتساب ميزة اقتصادية على منافسيها.يمكن اعتبار الملكية الفكرية سرًا تجاريًا.

فقدان هذه المعلومات قد يكون كارثًه على مستقبل الشركة.

البيانات المالية ،؟

مثل بيانات الدخل ، والميزانيات العمومية ،وبيانات التدفق النقدي (ملخص عن المبالغ والمصروفات الفعلية أو المتوقعة للنقد في الشركة خلال فترة معينة) للشركة تعطي نظرة ثاقبة على صحة مسار الشركة .

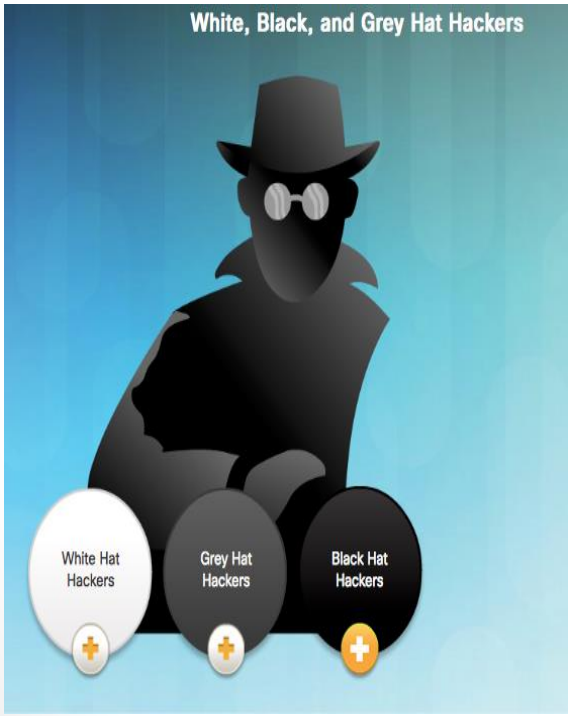


السرية والنزاهة والتوافر

تعد السرية والنزاهة والتوافر، المعروفة باسم مثلث CIA (الشكل ١) ، بمثابة دليل لأمن المعلومات لمنظمة ما.

- تضمن السرية خصوصية البيانات عن طريق تقييد الوصول بواسطة التشفير.
- تؤكد النزاهة أن المعلومات دقيقة وجديرة بالثقة.
- يضمن التوفر توافر المعلومات للأشخاص المرخص لهم.

أنواع المهاجمين



المهاجمون (Attackers)

هم أفراد أو مجموعات يحاولون استغلال(exploit) الضعف لتحقيق مكاسب شخصية أو مالية. يهتم المهاجمون بكل شيء ، بدءًا من بطاقات الائتمان وتصميمات المنتجات او أي شيء ذي قيمة.

الهواة (Amateurs) –

يطلق على هؤلاء الأشخاص أحيانًا اسم Kiddies Script. وهم عادة مهاجمون لديهم مهارات قليلة أو معدومة ، وغالبا ما يستخدمون الأدوات أو التعليمات الموجودة على الإنترنت لشن هجمات. البعض منهم مجرد فضول ، بينما يحاول آخرون إظهار مهاراتهم وإحداث الضرر. قد يستخدمون الأدوات الأساسية دون التعمق في الأدوات ، ولكن النتائج لا تزال مدمرة.

مخترقين (Hackers) –

هذه المجموعة من المهاجمين اقتحام أجهزة الكمبيوتر أو الشبكات للوصول.

يتم تصنيف هؤلاء المهاجمين على أنها قبعات بيضاء أو رمادية أو سوداء. اعتمادًا على الهدف.

أنواع المهاجمين

مخترقي القبعة البيضاء (white Hat Hackers)

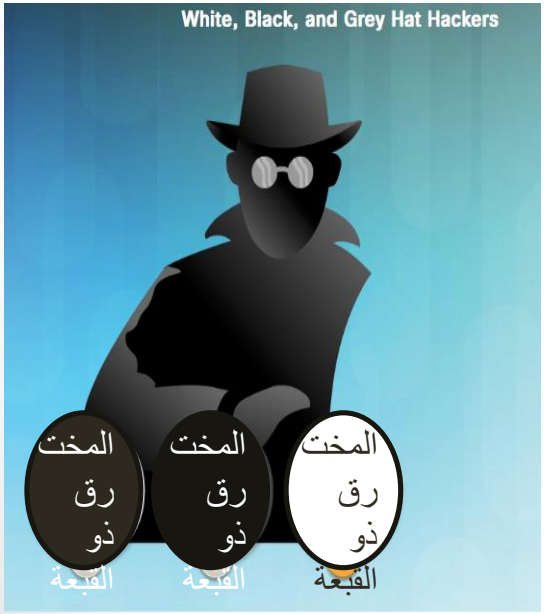
هؤلاء هم مخترقين أخلاقيون (Ethical hackers) يستخدمون مهاراتهم البرمجية لأغراض جيدة وأخلاقية وقانونية. قد يقوم مخترقي القبعة البيضاء بإجراء اختبارات اختراق الشبكات في محاولة لتهديد الشبكات والأنظمة عن طريق استخدام معرفتهم بأنظمة أمان الكمبيوتر لاكتشاف نقاط ضعف الشبكة. يتم الإبلاغ عن ثغرات أمنية للمطورين ليقوموا بإصلاحها قبل تهديد نقاط الضعف. بعض المنظمات تمنح الحوافز أو الجوائز لمخترقي القبعة البيضاء عندما يبلغونهم بالضعف.

مخترقي القبعة الرماديه (Grey Hat Hackers)

هؤلاء هم أفراد يرتكبون جرائم ويقومون بأشياء غير أخلاقية (unethical)، ولكن ليس من أجل تحقيق مكسب شخصي أو للتسبب في ضرر. مثال على ذلك هو شخص يدخل الشبكة دون إذن ثم يكشف عن الضعف علانية. قد يكشف قراصنة القبعات الرمادية عن ثغرة أمنية للمنظمة المتأثرة بعد اختراق شبكتهم. هذا يسمح للمؤسسة بإصلاح المشكلة.

مخترقي القبعة السوداء (Black Hat Hackers)

هؤلاء هم مجرمون غير أخلاقيون ينتهكون أمن الكمبيوتر والشبكات من آجل مكسب شخصي ، أو لأسباب ضارة مثل مهاجمة الشبكات. يستغل قراصنة القبعة السوداء نقاط الضعف في اختراق أنظمة الكمبيوتر والشبكة.



السوداء

ما هو الحروب الإلكترونية؟

أصبح الفضاء السيبراني بعدًا هامًا آخر للحرب ، حيث يمكن للدول أن تنفّذ صراعات دون مواجهات القوات والآلات التقليدية. وهذا يسمح للبلدان ذات القوة العسكرية التقليدية الضعيفة أن يكون قوياً مثل الدول الأخرى في الفضاء السيبراني.

إن الحرب الإلكترونية هي صراع قائم على الإنترنت ينطوي على اختراق أنظمة الكمبيوتر وشبكات الدول الأخرى. يمتلك هؤلاء المهاجمون الموارد والخبرات اللازمة لشن هجمات ضخمة على الإنترنت ضد دول أخرى لإحداث ضرر أو تعطيل الخدمات ، مثل إغلاق شبكة الطاقة الكهربائية.

ومن الأمثلة على الهجوم الذي ترعاه الدولة برنامج "Stuxnet" الخبيث المصمم لإتلاف مصنع التخصيب النووي الإيراني.

الغرض من الحرب السيبرانية

الغرض من الحرب السيبراني

الهدف الرئيسي للحرب السيبرانية هو اكتساب ميزة على الاعداء، سواء كانوا دول أو منافسين.

يمكن لدولة أن تغزو البنية التحتية لدولة اخرى باستمرار ، وتسرق أسرار الدفاع ، وجمع المعلومات حول التكنولوجيا لتضييق الفجوات في صناعاتها في شتى المجالات وخاصة في المجال العسكري . إلى جانب التجسس الصناعي والعسكري ، يمكن للحرب السيبرانية أن تخرب البنية التحتية للدول الأخرى وتكلف الأرواح في الدول المستهدفة.

على سبيل المثال ، يمكن أن يؤدي الهجوم إلى تعطيل شبكة الطاقة في إحدى المدن الرئيسية.

حركة المرور قد تعطلت.

يتم إيقاف تبادل السلع والخدمات.

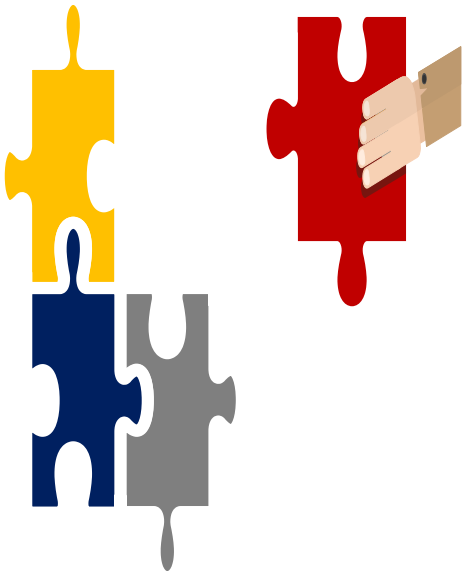
لا يمكن للمرضى الحصول على الرعاية اللازمة في حالات الطوارئ. تعطيل الوصول إلى الإنترنت.

من خلال التأثير على شبكة الطاقة ، يمكن أن يؤثر الهجوم على الحياة اليومية للمواطنين العاديين.

علاوة على ذلك ، يمكن للبيانات الحساسة المخترقة أن تعطي المهاجمين القدرة على ابتزاز الأفراد داخل الحكومة. قد تسمح المعلومات للمهاجم بالتظاهر بأنه مستخدم مصرح له بالوصول إلى معلومات أو الأجهزة الحساسة.

ماذا يحدث إذا لم تتمكن الحكومة من الدفاع ضد الهجمات الإلكترونية ، :

- يفقد المواطنون الثقة في قدرة الحكومة على حمايتهم.
- يمكن للحرب الإلكترونية أن تزعزع استقرار الدولة
- وتعطل التجارة
- وتؤثر على ثقة المواطنين في حكومتهم دون أن تغزو الدولة المستهدفة فعليًا.



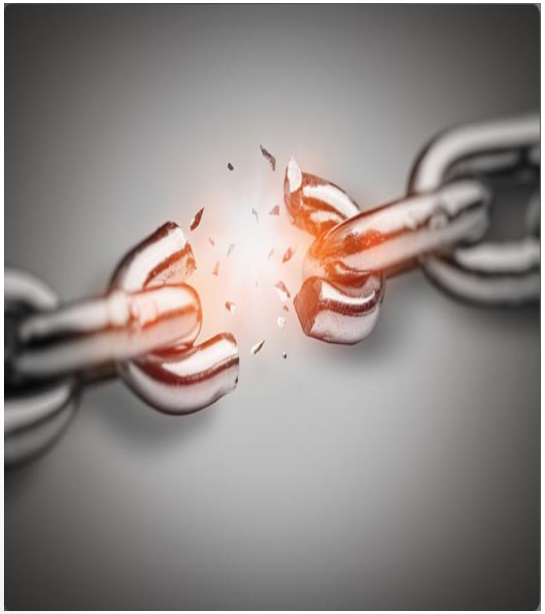
الهجمات والمفاهيم والتقنيات

Attacks, Concepts and Techniques

2.1.1.1

العثور على نقاط ضعف الأمن

ماهي الثغرات الأمنية (Security vulnerabilities)؟



هي أي نوع من أنواع العيوب في البرامج أو الأجهزة.

بعد اكتساب معرفة بالثغرة الأمنية ، يحاول المستخدمون الخبيثون استغلالها (exploit).

الاستغلال هو مصطلح يستخدم لوصف برنامج مكتوب للاستفادة من ثغرة معروفة.

ويشار إلى استغلال الثغرة على أنها هجوم.

الهدف من الهجوم هو الوصول إلى النظام أو البيانات الموجودة في النظام و إلى مصادر معينه.

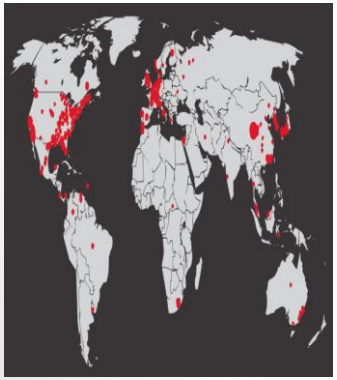
أنواع البرامج الضارة

أنواع البرامج الضارة(Types of Malware):

هي أي شفرة يمكن استخدامها لسرقة البيانات أو تجاوز عناصر التحكم على الوصول أو إلحاق الضرر بالنظام أو تعريضه للخطر. فيما يلي بعض الأنواع الشائعة من البرامج الضارة

برامج التجسس (Spyware) :

هذا البرنامج هو مصمم للتتبع والتجسس على المستخدم. غالبًا ما تتضمن برامج التجسس برامج تعقب النشاطات ، وجمع البيانات. في محاولة للتغلب على الإجراءات الأمنية ، تقوم برامج التجسس بتعديل إعدادات الأمان. غالبًا ما تجمع برامج التجسس نفسها مع البرامج الشرعية أو مع أحصنة طروادة (Trojan horses).



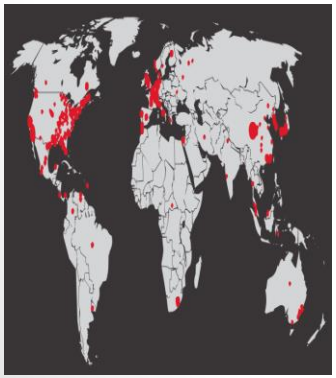
أنواع البرامج الضارة

الفدية (Ransomware):

تم تصميم هذا البرنامج الضار لعقد نظام الكمبيوتر أو البيانات التي تحتوي على أسير (رهينة) حتى يتم إجراء الدفع. عادةً ما يعمل Ransomware عن طريق تشفير البيانات في الكمبيوتر باستخدام مفتاح غير معروف للمستخدم. ينتشر الفدية بواسطة ملف تم تنزيله أو بعض ثغرات البرامج.

برامج الرعب (Scareware)

: هذا هو نوع من البرامج الضارة المصممة لإقناع المستخدم باتخاذ إجراء محدد بناء على الخوف. تقوم برامج الرعب بتكوين نوافذ منبثقة تشبه نوافذ حوار نظام التشغيل. تنقل هذه النوافذ رسائل مزورة تفيد بأن النظام في خطر أو يحتاج إلى تحميل برنامج أو أمر معين للعودة إلى التشغيل العادي. في الواقع لم يتم تقييم أو اكتشاف أي مشكلات ، وإذا وافق المستخدم على البرنامج المذكور وتم تنفيذه ، فسيتم إصابة نظامه ببرامج ضارة.



الفيروس(Virus):

هو عبارة عن شفرة تنفيذية خبيثة متصلة بملفات قابلة للتنفيذ ، وغالبًا برامج مشروعة.

تنتشر معظم الفيروسات الآن بواسطة محركات أقراص USB أو الأقراص الضوئية أو مشاركات الشبكة أو البريد الإلكتروني.

أنواع البرامج الضارة

حصان طروادة(Trojan horse) :

حصان طروادة هو برنامج خبيث يقوم بعمليات خبيثة تحت غطاء العملية المطلوبة. يستغل هذا الرمز الخبيث صلاحيات المستخدم الذي يشغله. في كثير من الأحيان ، يتم العثور على أحصنة طروادة في ملفات الصور والملفات الصوتية أو الألعاب. حصان طروادة يختلف عن الفيروس لأنه يربط نفسه إلى الملفات غير القابلة للتنفيذ.

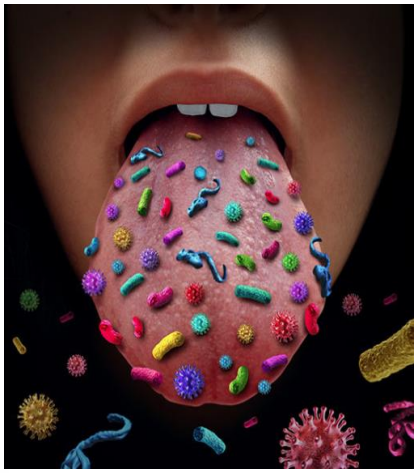
-الديدان (Worms):

الديدان هي شفرة خبيثة مستقله تقوم بتكرار نفسها من خلال استغلال الثغرات في الشبكات. الديدان عادة تبطئ الشبكات. تستطيع الدودة أن تنتشر بسرعة كبيرة عبر الشبكة.

أعراض البرامج الضارة

أعراض البرامج الضارة(Symptoms of Malware):

بغض النظر عن نوع البرامج الضارة التى أصيب بها النظام ، فهناك أعراض شائعة للبرامج الضارة (لمعرفة هل جهازك مصاب أم لا):



١- زيادة في استخدام وحدة المعالجة المركزية.
٢- انخفاض في سرعة الكمبيوتر.
٣- الكمبيوتر يتجمد أو يتعطل في كثير من الأحيان.
٤- انخفاض في سرعة تصفح الإنترنت.
٥أ- مشاكل غير قابلة للتفسير (غير مفهومة)مع اتصالات الشبكة.
٦- تعديل الملفات الإلكتروني دون علم المستخدم و موافقته.
٧- حذف الملفات الإلكتروني دون علم المستخدم أو موافقته.
٨- وجود ملفات غير معروفة أو برامج أو رموز سطح المكتب.
٩- إيقاف البرامج أو إعادة تكوين نفسها.
١٠- إرسال البريد الإلكتروني دون علم المستخدم أو موافقته.

الهندسة الاجتماعية

ماهي الهندسة الاجتماعية(Social Engineering)؟

الهندسة الاجتماعية هي هجوم يحاول استغلال الأفراد في القيام بأعمال أو إفشاء معلومات سرية. غالبًا ما يعتمد المهندسون الاجتماعيون على رغبة الأشخاص في أن يكونوا مساعدين ولكن أيضًا يفترسون نقاط ضعف الأشخاص. على سبيل المثال ، يمكن للمهاجم الاتصال بموظف مفوض (لديه صلاحيات) والتظاهر بإن لديه مشكلة ملحة تتطلب الوصول إلى الشبكة بشكل فوري. او يمكن للمهاجم الطعن في الغرور الخاص بالموظف باستخدام بعض العبارات مثلا(انت لا تستطيع فعل ذلك ، أنت شخص لا تحب المساعدة) ، أو استدعاء السلطة باستخدام أساليب إسقاط الأسماء (ذكر أسماء الأشخاص النافذين في الإدارة، او الصراخ بصوت عالي)، أو استدعاء سلوك العاطفة البشرية بالتوسل للمساعدة.

هذه بعض أنواع هجمات الهندسة الاجتماعية:

1- التقليد (Pretexting) :

هذا عندما يتصل المهاجم بشخص ما ويكذب عليه في محاولة للوصول إلى البيانات المميزة. مثال على ذلك وجود مهاجم يدعي أنه يحتاج إلى بيانات شخصية أو مالية من أجل تأكيد هوية المستلم.

2- التتبع أو الذيل (Tailgating):

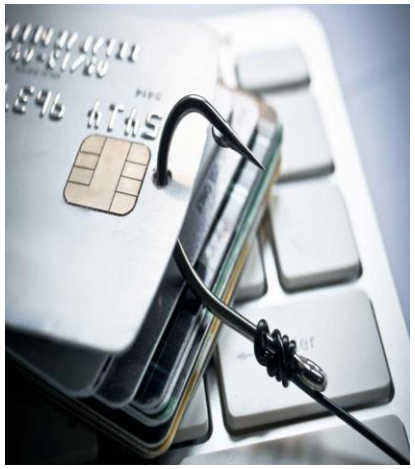
هذا هو عندما يتبع المهاجم بسرعة الشخص المصرح له في مكان آمن والدخول خلفه.

٣- شيء ما لأجل شيء ما (Quid pro quo)(Something for **Something**) :

عندما يطلب المهاجم معلومات شخصية مقابل شيء ما ، كهدية مجانية.

التصيد الإحتيالي

ماهو التصيد الإحتيالي(Phishing)؟



التصيد الاحتيالي هو عندما يرسل الطرف الخبيث بريدًا إلكترونيًا مخادعًا متنكراً على أنه مصدر شرعي وموثوق به. هدف الرسالة هو خداع المستلم إلى تثبيت برامج ضارة على أجهزته أو مشاركة معلومات شخصية أو مالية.

مثال على التصيّد الاحتيالي هو رسالة بريد إلكتروني مزورة لتبدو وكأنها مرسلة من متجر بيع بالتجزئة تطلب من المستخدم النقر فوق رابط للمطالبة بالجائزة التي فاز بها . قد ينتقل الرابط إلى موقع مزيف يطلب معلومات شخصية ، أو قد يقوم بتثبيت فيروس.

ما هو الهجوم المخلوط

ما هي الهجمات الممزوجة(Blended attacks)؟

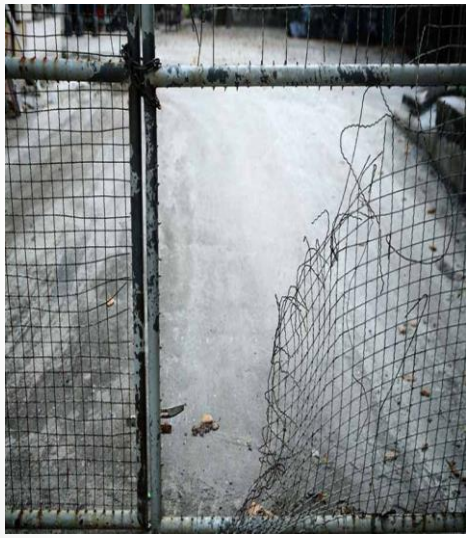
هي هجمات تستخدم تقنيات متعددة لخرق هدف. عن طريق استخدام العديد من تقنيات الهجوم المختلفة في وقت واحد ، يكون لدى المهاجمين برامج ضارة هي مزيج من الديدان ، وأحصنة طروادة ، وبرامج التجسس ، ومخططات التصيّد الاحتيالي.

هذا الاتجاه من الهجمات المخلوطة يكشف عن برامج ضارة أكثر تعقيدًا ويعرض بيانات المستخدم لخطر كبير.

النوع الأكثر شيوعًا في الهجمات الممزوجة يستخدم رسائل البريد الإلكتروني غير المرغوب فيها والرسائل الفورية والمواقع الشرعية لتوزيع الروابط حيث يتم تنزيل البرامج الضارة و برامج التجسس سراً إلى الكمبيوتر.

ما هو الحد من الأثر

ما هو الحد من الأثر(What is Impact Reduction)؟



في حين أن غالبية الشركات الناجحة اليوم تدرك القضايا الأمنية المشتركة وتضع جهدا كبيرا في منعها ، لا توجد مجموعة من الممارسات الأمنية ذات كفاءة ١٠٠٪.

الاستجابة لخرق البيانات هي عملية ديناميكية للغاية.

فيما يلي بعض التدابير الهامة التي يجب على الشركة اتخاذها عند تحديد الاختراق الأمني ، وفقًا لكثير من خبراء الأمن:

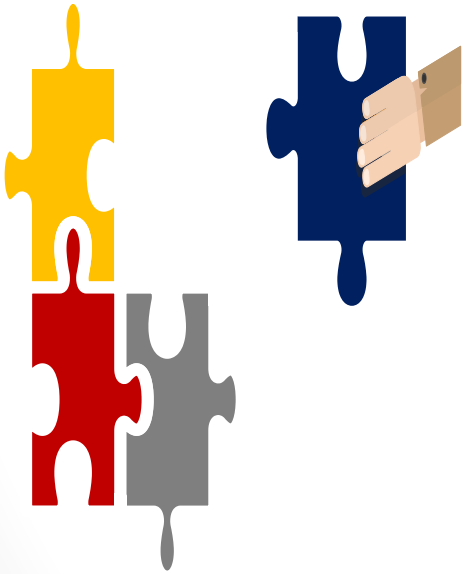
1-التواصل مع القضية. يجب إبلاغ الموظفين داخليا بالمشكلة،و يجب إخطار العملاء من خلال الاتصال المباشر والإعلانات الرسمية.

الاتصال يخلق الشفافية ، وهو أمر حاسم في هذا النوع من الحالات.

2- كن صادقًا ومتقبلاً للمساءلة في حال كانت الشركة على خطأ.

3- زود بالتفاصيل.، اشرح سبب حدوث القضية وما تم اختراقه.

ومن المتوقع أيضًا أن تهتم الشركة بتكاليف خدمات حماية سرقة الهوية للعملاء المتأثرين.



حماية بياناتك وخصوصيتك

حماية أجهزة الكمبيوتر الخاصة بك

لماذا يجب علينا حماية أجهزة الكمبيوتر الخاصة بنا ؟

تخزن أجهزة الكمبيوتر الخاصة بك بياناتك وهي البوابة إلى حياتك على الإنترنت.

حماية أجهزة الكمبيوتر الخاصة بك

استخدم برامج مكافحة الفيروسات وبرامج مكافحة التجسس –

يتم تثبيت البرامج الضارة ، مثل الفيروسات وأحصنة طروادة والديدان وبرامج الفدية وبرامج التجسس ، على أجهزة الكمبيوتر الخاصة بك دون إذن منك ، من أجل الوصول إلى جهاز الكمبيوتر الخاص بك والبيانات الخاصة بك. يمكن للفيروسات أن تدمر بياناتك ، أو تبطئ جهاز الكمبيوتر ، أوتتحكم بجهازك .

إحدى الطرق التي يمكن للفيروسات السيطرة على جهازك

هو السماح لمرسلي الرسائل غير المرغوب (spammers) فيها بإرسال رسائل البريد الإلكتروني باستخدام حسابك .

يمكن لبرامج التجسس

مراقبة أنشطتك على الإنترنت ، أو جمع معلوماتك الشخصية ، أو إنتاج إعلانات منبثقة غير مرغوب فيها على متصفح الويب أثناء اتصالك بالإنترنت

حماية أجهزة الكمبيوتر
الخاصة بك

.الإجراء الجيد لحماية أجهزتك من هذه المشكلة

هو فقط تنزيل البرامج من المواقع الموثوق بها لتتجنب التجسس على جهازك

.

ماهو الغرض من تصميم برنامج مكافحة الفيروسات ؟

لفحص جهاز الكمبيوتر الخاص بك والبريد الإلكتروني الوارد بحثًا عن الفيروسات وحذفها .في بعض الأحيان ، يتضمن برنامج مكافحة الفيروسات أيضًا برامج مكافحة التجسس .

حافظ على تحديث برامج الحماية باستمرار لحماية جهاز الكمبيوتر الخاص بك من الاصابة بأحدث البرامج الضارة.

3.1.1.3

استخدم كلمة مرور مختلفة لكل حساب على الإنترنت

من المحتمل أن يكون لديك أكثر من حساب واحد على الإنترنت ، لذا يجب أن يكون لكل حساب كلمة مرور مختلفة. ستصبح كلمات مرور كثيرة لتتذكرها. ومع ذلك ، فإن عدم استخدام كلمات مرور قوية وفريدة من نوعها يتركك وبياناتك عرضة للمجرمين السيبرانيين (مجرمي الإنترنت).

إن استخدام نفس كلمة المرور لجميع حساباتك على الإنترنت يشبه استخدام نفس المفتاح لجميع أبوابك المغلقة ، إذا حصل لص ما على هذا المفتاح، فسيكون لديه القدرة على الوصول إلى كل شيء تملكه.

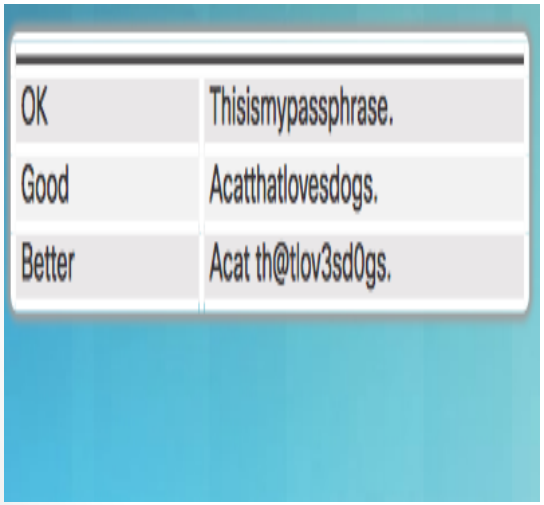
OK	Good	Better
allwhitecat	a11whitecat	A11whi7ec@t
Fblogin	1FBLogin	1.FB.L0gin$
amazonpass	AmazonPa55	Am@z0nPa55
ilikemyschool	ILikeMySchool	!Lik3MySch00l
Hightidenow	HighTideNow	H1gh7id3Now

استخدم عبارة المرور بدلًا من كلمة المرور

لمنع الوصول الفعلي غير المصرح به إلى أجهزة الكمبيوتر الخاصة بك ، استخدم عبارات المرور (سلسلة من الكلمات passphrases) بدلاً من كلمات المرور .

من الأسهل والأفضل إنشاء عبارة مرور طويلة بدلاً من كلمة مرور ، لأنها تتكون بشكل عام من جملة بدلاً من كلمة .

كون عبارة المرور أطول يجعلها أقل عرضة للتفسير و التخمين أو هجمات الإختراق .علاوة على ذلك قد تكون عبارة المرور أسهل في التذكر خاصة إذا كنت مطالبًا بتغيير كلمة المرور بشكل متكرر .



استخدم عبارة المرور بدلًا من كلمة المرور

مؤخراً قام المعهد الوطني الأمريكي للمعايير والتقنية (NIST) بنشر بعض المتطلبات لتحسين كلمات المرور.

ملخص الإرشادات الجديدة:.

1- ثمانية أحرف كحد أدنى في الطول ، ولكن لا يزيد عن 64 حرفًا.

2-لا تستخدم كلمات مرور عامة يسهل تخمينها ، مثل كلمة المرور:abc123

3-لا تستخدم قواعد التركيب ، (مثلاً إجبار المستخدم على خليط من الأحرف الصغيرة والكبيرة أو حظر الأحرف المتكررة على التوالي).

4-طور دقة إدخال كلمة المرور عن طريق السماح للمستخدم برؤية كلمة المرور أثناء الكتابة

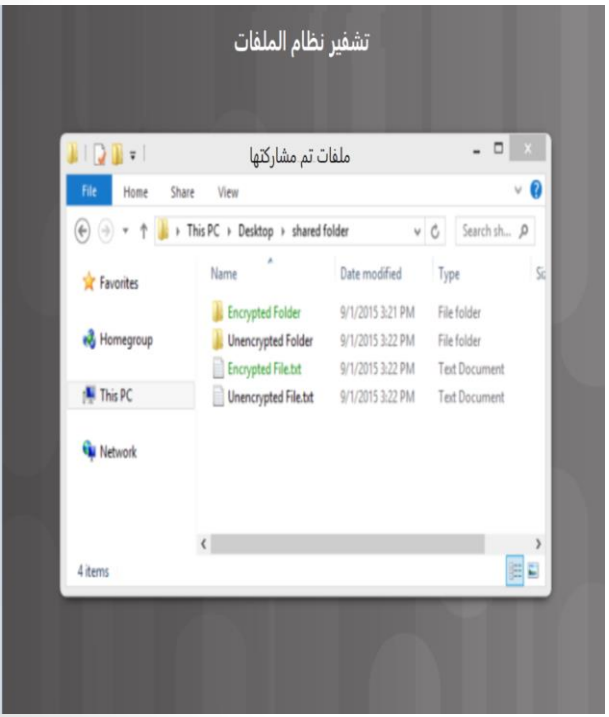
تشفير البيانات

ما هو التشفير (encryption)؟

التشفير هو عملية تحويل البيانات من نص عادي إلى نموذج مشفر لا يمكن التعرف عليه حيث لا يستطيع الطرف الغير مصرح له قراءتها. ويمكن فقط لشخص موثوق به ومصرح له لديه المفتاح السري أو كلمة المرور لفك تشفير البيانات والدخول إليها في شكلها الأصلي.

لا يمنع التشفير نفسه أي شخص من اعتراض البيانات. ولكن يمنع أي شخص غير مصرح له من عرض المحتوى أو الوصول إليه.

يتم استخدام البرامج لتشفير الملفات والمجلدات وحتى محركات الأقراص بالكامل.



حذف بياناتك نهائيًا

ماذا يحدث عند نقل ملف إلى سلة المحذوفات أو المهملات وحذفه نهائيًا ،

- لا يمكن الوصول إلى الملف إلا من نظام التشغيل.
- لكن لا يزال بإمكان أي شخص يمتلك أدوات التحليل الجنائي الصحيحة استعادة الملف نظرًا لوجود أثر مغناطيسي على القرص الصلب.

ماذا يجب أن أفعل من أجل مسح البيانات بحيث لا يمكن استردادها ، ؟

يجب أن تتم الكتابة فوق البيانات عدة مرات. لمنع استعادة الملفات المحذوفة ،

- تحتاج إلى استخدام أدوات مصممة خصيصًا للقيام بذلك.
- مثل برنامج SDelete من (Microsoft) لنظام تشغيل فيستا Vista و ما بعده ، حيث أنه قادر على إزالة الملفات الحساسة تمامًا.

لا تشارك معلومات كثيرة على شبكات التواصل الاجتماعي

لا تشارك معلومات كثيرة على شبكات التواصل الاجتماعي

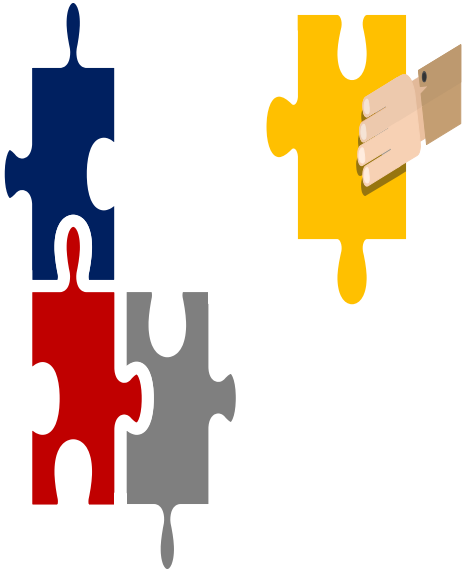
إذا كنت ترغب في الحفاظ على خصوصيتك على الشبكات الاجتماعية ، شارك أقل قدر ممكن من المعلومات. يجب ألا تشارك معلومات مثل تاريخ ميلادك أو عنوان بريدك الإلكتروني أو رقم هاتفك في ملفك الشخصي.

الأشخاص الذين يحتاجون إلى معرفة معلوماتك الشخصية سيتواصلون معك.

- لا تملأ ملفك الشخصي على وسائل التواصل الاجتماعي بالكامل ، فقط قم بتوفير الحد الأدنى من المعلومات المطلوبة علاوة على ذلك ،
- تحقق من إعدادات الوسائط الاجتماعية الخاصة بك للسماح فقط للأشخاص الذين تعرفهم برؤية أنشطتك أو المشاركة في محادثاتك.

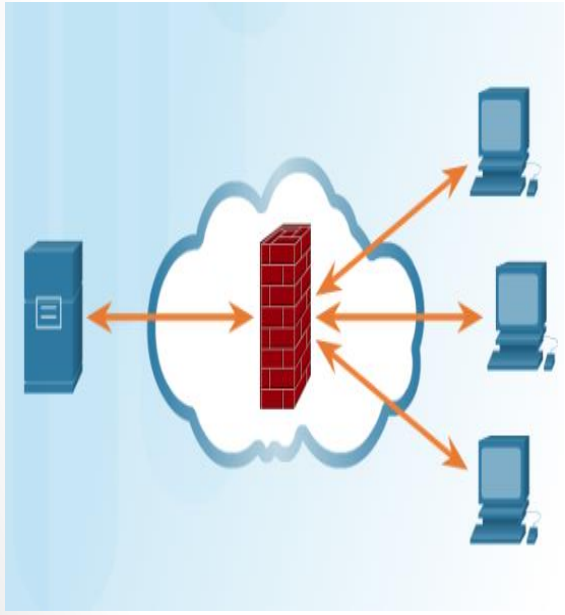
كلما زادت المعلومات الشخصية التي تشاركها عبر الإنترنت ، أصبح من السهل على شخص ما إنشاء ملف تعريف عنك واستغلالك في الحياة الواقعية.

المحور الرابع



حماية المنظمة

حماية الأنظمة



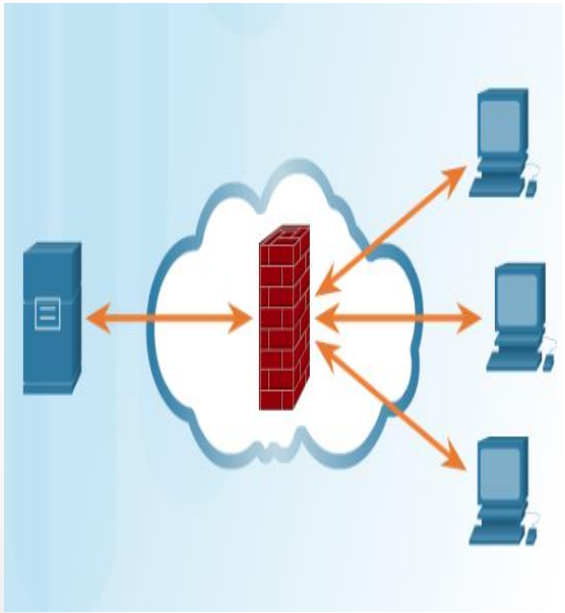
ماهو جدار الحماية؟؟؟

فكرة جدار الحماية في حياتنا الواقعية هو عبارة عن جدار أو قسم مصمم لمنع الحريق من الانتشار من جزء من المبنى إلى أخر.

اما في شبكات الحاسب صُمم للتحكم و تصفية (فلترة) الاتصالات الداخلة و الخارجة والتي يسمح بها داخل او بين الشبكات و الاجهزة ، كما هو موضح بالشكل.

حماية الأنظمة

أين يمكن تثبيت جدار الحماية؟؟؟؟



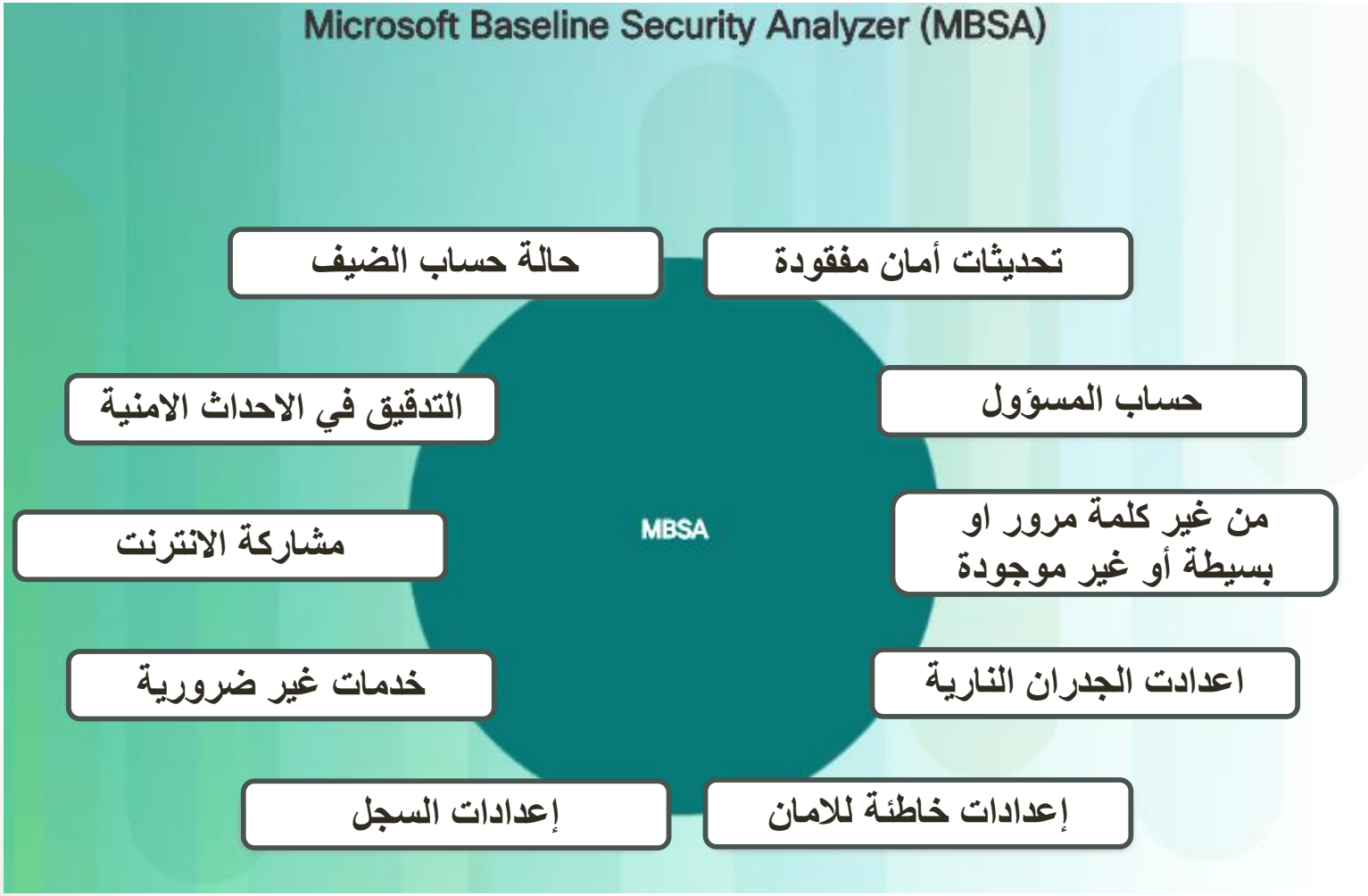
يمكن تثبيت جدار الحماية على جهاز حاسب واحد بغرض حمايته (host-based firewall)

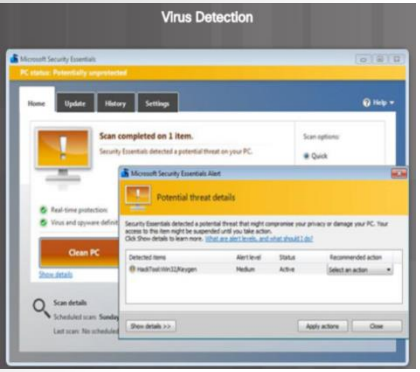
يمكن أن يكون جهاز شبكة قائم بذاته (stand-alone) يحمي شبكة كاملة مكونة من عدة أجهزة حاسب وجميع الأجهزة المستضيفة على تلك الشبكة (network-based firewall).

الحاجة إلى تقليل الاصابة بالفيروسات في المنزل
ومنها مشاركة جهاز الطابعة من خلال الشبكة
وهذا الجزء يقلل من الاصابة بالفيروسات التي تنقل
بواسطة الفلاش ميموري

طريقة ارسال البريد الالكتروني بطريقة مجدولة
تساعدك في تنظيم اعمالك ووقتك

7.1.1.1
أمان نظام التشغيل





7.1.1.2
Antimalware
مكافحة البرامج الضارة

مكافحة البرامج الضارة (Antimalware)

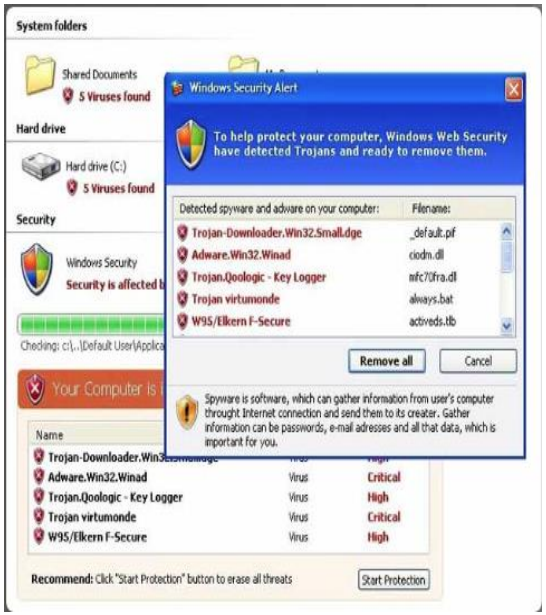
تشتمل البرامج الضارة على الفيروسات (viruses) والفيروسات المتطفلة (worms) وأحصنة طروادة (Trojan horses) و مراقبة لوحة المفاتيح (keyloggers) وبرامج التجسس (spyware) والإعلانات المتسللة (adware) ، جميعهم يعتبروا برامج غزو للخصوصية وسرقة المعلومات وتلف النظام أو حذف البيانات أو تخريبها .

من المهم حماية أجهزة الكمبيوتر والأجهزة المحمولة باستخدام برنامج مكافحة البرامج الضارة.
تتوفر الأنواع التالية من برامج مكافحة البرامج الضارة:

- الحماية من الفيروسات : البرنامج يراقب باستمرار للفيروسات ، وعندما يكتشف البرنامج فيروسًا يحذر المستخدم ويحاول عزل الفيروس أو حذفه ، كما هو موضح في الشكل ١ .
- حماية برامج الإعلانات المتسللة : يبحث البرنامج باستمرار عن البرامج التي تعرض الإعلانات على جهاز الكمبيوتر.
- حماية التصيد الاحتيالي : يقوم البرنامج بحظر عناوين الانترنت الخاصة بمواقع التصيد المعروفة ويحذر المستخدم من المواقع المشبوهة.
- الحماية من برامج التجسس : يقوم البرنامج بمسح لوحة المفاتيح (keyloggers) وبرامج التجسس الأخرى.
- مصادر موثوق بها / وغير موثوق بها : يحذر البرنامج المستخدم من البرامج غير الآمنة التي تحاول تثبيت مواقع ويب أو غير آمنة قبل قيام المستخدم بزيارتها.

7.1.1.2
Antimalware
مكافحة البرامج الضارة

مكافحة البرامج الضارة



قد يستغرق الأمر عدة برامج مختلفة وعمليات مسح متعددة لإزالة جميع البرامج الضارة تمامًا "قم بتشغيل برنامج واحد للحماية من البرامج الضارة في كل مرة.

توفر العديد من المؤسسات الأمنية الشهيرة مثل (McAfee) و (Symantec) و (Kaspersky) الحماية من البرامج الضارة الشاملة لأجهزة الكمبيوتر والأجهزة المحمولة.

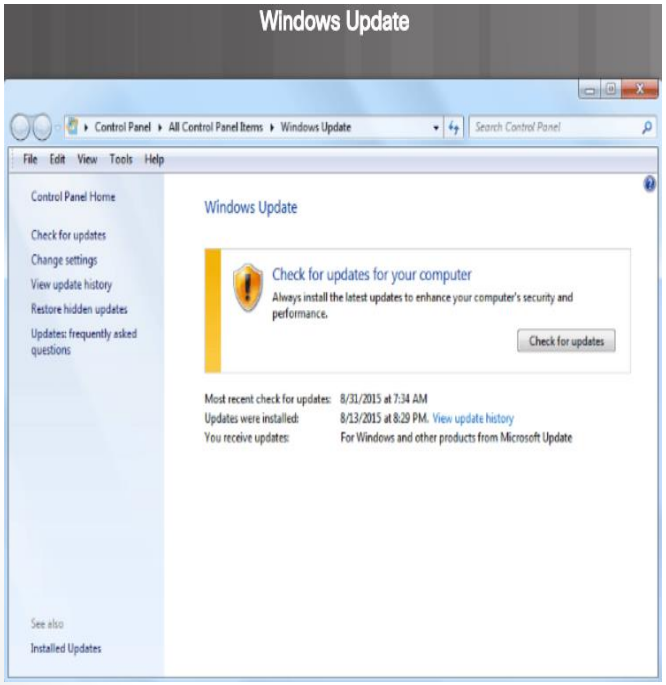
كن حذرًا من منتجات مكافحة الفيروسات الخبيثة المحتالة التي قد تظهر أثناء تصفحك للإنترنت ، تعرض هذه المنتجات مكافحة الفيروسات المحتالة إعلانًا أو نافذة منبثقة تشبه نافذة تحذير النظام الفعلية كما هو موضح في الشكل رقم ٢ ، وتدعي عادةً أن هناك برامج الضارة أصابة الكمبيوتر وتحث المستخدم على تنظيفه ، ويؤدي النقر على أي مكان داخل النافذة إلى بدء تنزيل البرامج الضارة وتثبيتها.

البرامج غير المعتمدة أو غير المتوافقة ليست مجرد برامج يقوم مستخدم بتثبيتها دون قصد على جهاز كمبيوتر فقط ، ولكن يمكن أن تأتي أيضًا من المستخدم الذي أراد تثبيتها ، والتي قد لا تكون ضارة ، ولكنها ما زالت تنتهك السياسة الأمنية ، يمكن أن يتدخل هذا النوع من النظام غير المتوافق مع برامج الشركة أو خدمات الشبكة ، فيجب على المستخدمين إزالة البرامج غير المعتمدة على الفور.

7.1.1.3
Patch Management
إدارة التصحيح

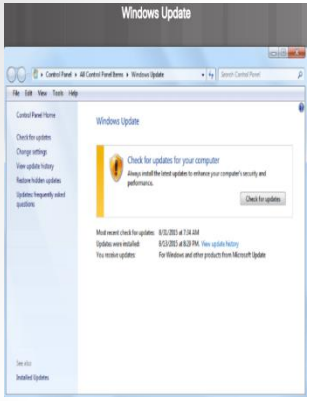
إدارة التصحيح

التصحيحات هي تحديثات التعليمات البرمجية التي يوفرها المصنعون لمنع فيروسات أو المتطفلات تم اكتشافها حديثًا من القيام بهجوم ناجح ، من وقت لآخر تجمع الشركات المصنعة بين التصحيحات والتحديثات في تطبيق تحديث شامل يسمى الحزمة الخدمية (service pack) ، يمكن أن يكون العديد من هجمات الفيروسات المدمرة أقل حدة بكثير إذا قام مستخدمون آخرون بتنزيل أحدث حزمات الخدمية وتثبيتها.



يقوم النظام (Windows) بشكل روتيني بالتحقق من موقع (Windows Update) على الويب للتحديثات ذات الأولوية العالية التي يمكن أن تساعد في حماية جهاز الكمبيوتر من أحدث تهديدات الأمان ، وتتضمن هذه التحديثات تحديثات الأمان والتحديثات الهامة والحزمات الخدمية.

استنادًا إلى الإعدادات التي تم تكوينها ، يقوم النظام تلقائيًا بتنزيل التحديثات ذات الأولوية العالية وتثبيتها والتي يحتاج إليها الكمبيوتر أو يقوم بإشعار المستخدم عند توفر هذه التحديثات.



7.1.1.3
Patch Management
إدارة التصحيح

إدارة التصحيح

قد ترغب بعض المؤسسات في اختبار التصحيح قبل تطبيقه على مستوى المؤسسة ، ستستخدم المؤسسة خدمة لإدارة التصحيحات محليًا بدلاً من استخدام خدمة التحديث عبر الإنترنت من المزود .

تتضمن فوائد استخدام خدمة تحديث التصحيح التلقائي ما يلي:

- ✓ يمكن للمسؤولين الموافقة على التحديثات أو رفضها.
- ✓ يمكن للمسؤولين تحديد وفرض تحديث للأنظمة في تاريخ محدد.
- ✓ يمكن للمسؤولين الحصول على تقارير حول التحديث اللازم لكل نظام.
- ✓ لا يتعين على كل كمبيوتر الاتصال بالمزود لتنزيل التحديثات ، فقط يحصل النظام على التحديث من خادم محلي.
- ✓ لا يمكن للمستخدمين تعطيل أو التحايل على التحديثات.

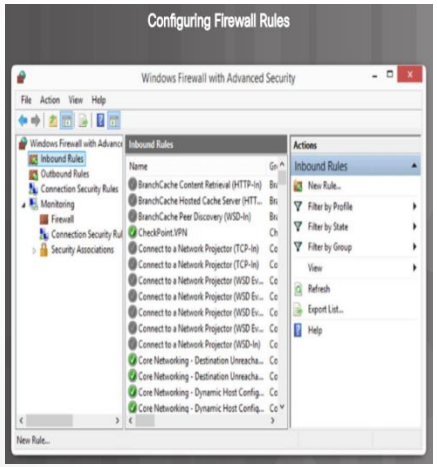
توفر خدمة التصحيح التلقائي للمسؤولين ضبطًا أكثر تحكمًا.

7.1.1.4
Host-Based Firewalls and Intrusion Detection Systems
الجدران النارية القائمة على المضيف وأنظمة كشف التسلل

الجدران النارية القائمة على المضيف وأنظمة كشف التسلل

الحل القائم على المضيف هو تطبيق برمجي يعمل على كمبيوتر مضيف محلي لحمايته ويعمل البرنامج مع نظام التشغيل للمساعدة في منع الهجمات.

الجدران النارية القائمة على المضيف:



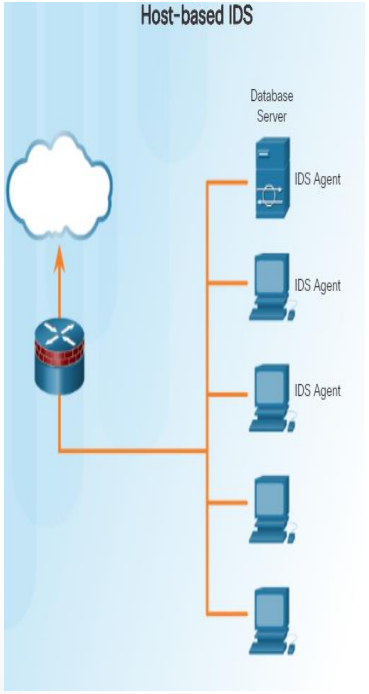
برنامج جدار الحماية هو برنامج يتم تشغيله على جهاز كمبيوتر للسماح أو رفض سير المعلومات بين الكمبيوتر وأجهزة الكمبيوتر أخرى متصلة به ، يقوم جدار حماية البرنامج بتطبيق مجموعة من القواعد على عمليات إرسال البيانات من خلال الفحص وتصفية حزم البيانات ، وعلى سبيل المثال يعد (Windows Firewall) مثالاً على برامج جدار حماية البرامج حيث يقوم نظام التشغيل (Windows) بتثبيته افتراضيًا أثناء التثبيت.

يمكن للمستخدم التحكم في نوع البيانات المرسلة من وإلى الكمبيوتر عن طريق فتح منافذ محددة أو حظرها ، دائمًا تحظر جدران الحماية اتصالات الشبكة الواردة والصادرة ما لم يتم تحديد استثناءات لفتح وإغلاق المنافذ التي يتطلبها البرنامج.

يحدد المستخدم قواعد الوارد (inbound rules) لتحديد أنواع حركة المعلومات المسموح لها بالمرور إلى النظام ، وسيساعد ضبط قواعد الوارد على حماية النظام من حركة المعلومات غير المرغوب فيها كما هو موضح في الشكل ١ .

الجدران النارية القائمة على المضيف وأنظمة كشف التسلل

7.1.1.4
Host-Based Firewalls and Intrusion Detection Systems
الجدران النارية القائمة على المضيف وأنظمة كشف التسلل



نظم كشف التسلل للمضيف

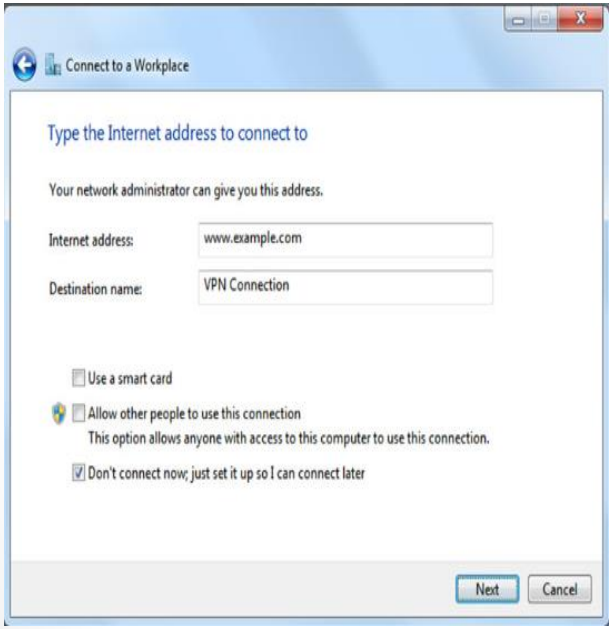
نظام كشف التسلل المضيف (HIDS) اختصارًا لـ(host intrusion detection system) هو برنامج يتم تشغيله على جهاز كمبيوتر المضيف يراقب النشاط المشبوه، سيتطلب على كل خادم أو نظام سطح مكتب يحتاج حماية إلى تثبيت البرنامج (HIDS) كما هو موضح في الشكل ٢ .

يراقب نظام (HIDS) الطلبات القادمة من النظام والدخول إلى ملفات النظام ؛ للتأكد من أن الطلبات ليست ناتجة عن نشاط ضار ، ويمكنه أيضًا مراقبة إعدادات السجل للنظام ، يحافظ السجل على معلومات التكوين حول الكمبيوتر.
يخزن (HIDS) كل بيانات السجل محليًا ويمكن أن يؤثر أيضًا على أداء النظام نظرًا لأنه يستهلك الكثير من الموارد.

لا يستطيع نظام (HIDS) مراقبة أي حركة معلومات شبكة لا تصل إلى النظام المضيف ، ولكنه مقتصر على مراقب نظام التشغيل وعمليات النظام الهامة الخاصة بهذا المضيف.

7.1.1.5
Secure Communications
تأمين الاتصالات

تأمين الاتصالات



عند الاتصال بالشبكة المحلية ومشاركة الملفات ، يبقى الاتصال بين أجهزة الكمبيوتر ضمن تلك الشبكة فقط ، كما تظل البيانات آمنة لأنها تكون خارج الشبكات الأخرى وخارج الإنترنت.
ولكن عندما التواصل ومشاركة الموارد عبر شبكات غير آمنة ، يستخدم المستخدمون شبكة افتراضية خاصة (Virtual Private Network) (VPN).
شبكة (VPN) هي شبكة خاصة تربط بين المواقع البعيدة أو المستخدمين معًا عبر شبكة عامة ، مثل الإنترنت.

يصل النوع الأكثر شيوعًا من (VPN) إلى شبكة خاصة تابعة لشركات ، تستخدم شبكة (VPN) اتصالات آمنة مخصصة يتم توجيهها عبر الإنترنت بين شبكة الشركات الخاصة والمستخدم البعيد ، عند الاتصال بشبكة الشركات الخاصة ، يصبح المستخدمون جزءًا من هذه الشبكة ويكون لهم حق الوصول إلى جميع الخدمات والموارد كما لو كانوا متصلين فعليًا بشبكة الشركة المحلية.

يجب أن يكون لدى مستخدمي الوصول عن بعد (Remote-access) عميل (VPN client) مثبت على أجهزة الكمبيوتر الخاصة بهم لتشكيل اتصال آمن مع شبكة الشركة الخاصة ، فيقوم برنامج عميل (VPN) بتشفير البيانات قبل إرسالها عبر الإنترنت إلى بوابة (VPN) على شبكة الشركة الخاصة ، تعمل بوابات الشبكة الافتراضية الخاصة (VPN) على إنشاء اتصالات (VPN) وإدارتها والتحكم فيها ، وتُعرف أيضًا باسم أنفاق (VPN tunnels).

تتضمن أنظمة التشغيل على عميل (VPN) الذي يقوم المستخدم بتكوينه من أجل اتصال (VPN).

7.1.2.1
(WEP)
(Wired Equivalent Privacy)
الخصوصية المكافئة للشبكات السلكية

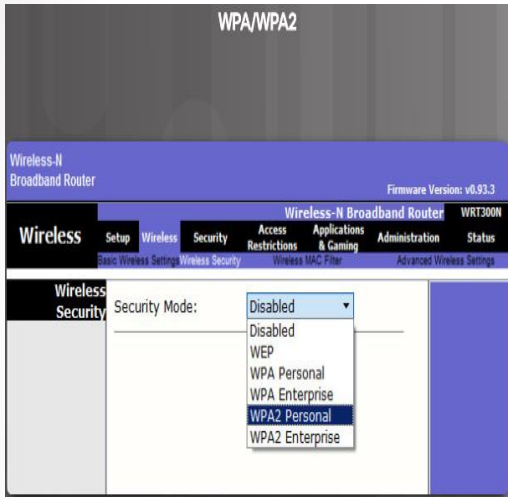
الخصوصية المكافئة للشبكات السلكية

واحدة من أهم مكونات الحواسب الحديثة هي الأجهزة المحمولة ، معظم الأجهزة الموجودة على شبكات اليوم هي أجهزة الكمبيوتر المحمولة والأجهزة اللوحية والهواتف الذكية والأجهزة اللاسلكية الأخرى ، تنقل الأجهزة المحمولة البيانات باستخدام إشارات لاسلكية يمكن لأي جهاز بهوائي متوافق معها باستلام هذه الاشارات ؛ ولهذا السبب طورت صناعة الكمبيوتر مجموعة من الشبكات اللاسلكية او معايير الأمن للهواتف المحمولة والمنتجات والأجهزة؛ لتقوم هذه المعايير بتشفير المعلومات المرسلة عبر موجات الأثير (airwaves)عن طريق الأجهزة المحمولة.

الخصوصية المكافئة للشبكات السلكية (WEP) هي واحدة من معايير أمن(Wi-Fi) الأولى والمستخدمة على نطاق واسع ، يوفر معيار (WEP) حماية للمصادقة والتشفير ، معايير **(WEP)** قديمة ولكن العديد من الأجهزة لا تزال تدعمه للتوافق مع الإصدارات السابقة. أصبح معيار (WEP) معيارًا للأمان **(Wi-Fi)** في عام ١٩٩٩ عندما كان الاتصال اللاسلكي في بدايته ، ولكن على الرغم من التنقيحات على المعيار وحجم المفتاح المتزايد عانى من العديد من نقاط الضعف الأمنية.

يمكن للمجرمين السيبرانيين كسر كلمات السر (WEP) في دقائق باستخدام البرمجيات المتاحة مجانا على الرغم من التحسينات ، ولكن لا يزال بروتوكول (WEP) ضعيفًا للغاية ويجب على المستخدمين ترقية الأنظمة التي تعتمد على (WEP) .

7.1.2.2
WPA/WPA2
(Wi-Fi Protected Access)
نقطة وصول محمية للواي فاي



نقطة وصول محمية للواي فاي

كان التحسين الرئيسي التالي للأمن اللاسلكي هو إدخال (WPA) و (WPA2) ، الوصول المحمي باللاسلكيWi-Fi Protected Access (WPA) ظهر تجاوبًا من صناع الكمبيوتر لضعف معيار (WEP).

أكثر تكوين (WPA) شيوعًا هو المفتاح المشترك مسبقًا-Pre (WPA-PSK Shared Key).
المفاتيح التي تستخدمها (WPA) هي ٢٥٦ بت ، وهي زيادة كبيرة على مفاتيح ٦٤ بت و ١٢٨ بت المستخدمة في نظام (WEP).

قدم معيار (WPA) العديد من التحسينات الأمنية.
قدمت أولاً (WPA) اختبارات سلامة الرسائل **message integrity (MIC) (checks)** والتي يمكنها اكتشاف ما إذا كان المهاجم قد قام بالاستيلاء وتبديل البيانات التي تم تمريرها بين نقطة الوصول اللاسلكية وعميل اللاسلكي.

7.1.3.1
File Access Control
التحكم في الوصول للملف

التحكم في الوصول للملف

الأذونات (Permissions) عبارة عن قواعد تم تكوينها لتقييد الوصول إلى المجلد أو الملف لشخص ما أو لمجموعة من المستخدمين ، في الجدول أنواع الأذونات المتوفرة للملفات والمجلدات.

- **مبدأ الإمتياز المحدودة (Principle of Least Privilege):**

يجب أن يقتصر المستخدمون على الموارد التي يحتاجونها فقط على نظام الكمبيوتر أو على الشبكة على سبيل المثال يجب ألا يتمكنوا من الوصول إلى كافة الملفات الموجودة على الخادم إذا كانوا يحتاجون فقط إلى الوصول إلى مجلد واحد ، قد يكون من الأسهل تزويد المستخدمين بالوصول إلى محرك الأقراص بأكمله ، ولكن من الأكثر أمانًا تقييد الوصول إلى المجلد الذي يحتاجون إليه لأداء وظيفتهم فقط ، هذا هو مبدأ الإمتيازات المحدودة ؛ تقييد الوصول إلى الملفات سيمنع البرامج الضارة من الوصول إلى تلك الملفات إذا أصيب جهاز الكمبيوتر الخاص بالمستخدم.

مستوى الإذن	وصف
السيطرة الكاملة	يمكن للمستخدمين مشاهدة محتويات ملف أو مجلد ، وتغيير وحذف الملفات والمجلدات الموجودة ، وإنشاء ملفات ومجلدات جديدة ، وتشغيل البرامج في مجلد.
تعديل	يمكن للمستخدمين تغيير الملفات والمجلدات الموجودة وحذفها ، ولكن لا يمكنهم إنشاء ملفات ومجلدات جديدة.
قراءة وتنفيذ	يمكن للمستخدمين مشاهدة محتويات الملفات والمجلدات الموجودة ويمكنهم تشغيل البرامج في مجلد.
قراءة	يمكن للمستخدمين رؤية محتويات مجلد وفتح الملفات والمجلدات.
كتابة	يمكن للمستخدمين إنشاء ملفات ومجلدات جديدة وإجراء تغييرات على الملفات والمجلدات الموجودة.

7.1.3.1
File Access Control
التحكم في الوصول للملف

- **تقييد أذونات المستخدم(Restricting User Permissions):**

إذا رفض مسؤول أذونات مشاركة شبكة لفرد أو مجموعة فإن هذا الرفض يتخطى ويتجاوز أي إعدادات أذونات أخرى ، على سبيل المثال إذا رفض المسؤول السماح لأحد الأشخاص بمشاركة الشبكة فلن يتمكن المستخدم من الوصول إلى تلك المشاركة ، حتى إذا كان المستخدم هو المسؤول أو جزءًا من مجموعة المسؤولين.

يجب أن تحدد السياسة الأمنية المحلية للموارد ونوع الوصول المسموح به لكل مستخدم ومجموعة.

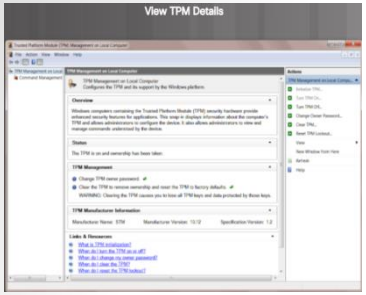
عندما يقوم أحد المستخدمين بتغيير أذونات لأحد المجلدات سيتوفر لديه خيار تطبيق نفس الأذونات على كافة المجلدات الفرعية.
وهذا يسمى بـ "انتشار الإذن" (permission propagation) ، يعد نشر الأذونات طريقة سهلة لتطبيق الأذونات على العديد من الملفات والمجلدات بسرعة ، بعد تعيين أذونات المجلد الأصل سيتم توارث أذونات المجلد الأصل إلى المجلدات والملفات التي تم إنشاؤها داخل المجلد الأصل.

أيضًا يحدد موقع البيانات والإجراء الذي تم تنفيذه على البيانات انتشار الأذونات:

- ✓ **البيانات التي تم نقلها إلى نفس وحدة التخزين ستحتفظ بالأذونات الأصلية.**
- ✓ **البيانات التي تم نسخها إلى نفس المجلد سوف ترث أذونات جديدة.**
- ✓ **نقل البيانات إلى وحدة تخزين مختلفة سوف ترث أذونات جديدة.**
- ✓ **البيانات التي تم نسخها إلى وحدة تخزين مختلفة ستنسخ إذنًا جديدًا.**

أنواع الاذونات

مستوى الإذن	وصف
السيطرة الكاملة	يمكن للمستخدمين مشاهدة محتويات ملف أو مجلد ، وتغيير وحذف الملفات والمجلدات الموجودة ، وإنشاء ملفات ومجلدات جديدة ، وتشغيل البرامج في مجلد.
تعديل	يمكن للمستخدمين تغيير الملفات والمجلدات الموجودة وحذفها ، ولكن لا يمكنهم إنشاء ملفات ومجلدات جديدة.
قراءة وتنفيذ	يمكن للمستخدمين مشاهدة محتويات الملفات والمجلدات الموجودة ويمكنهم تشغيل البرامج في مجلد.
قراءة	يمكن للمستخدمين رؤية محتويات مجلد وفتح الملفات والمجلدات.
كتابة	يمكن للمستخدمين إنشاء ملفات ومجلدات جديدة وإجراء تغييرات على الملفات والمجلدات الموجودة.

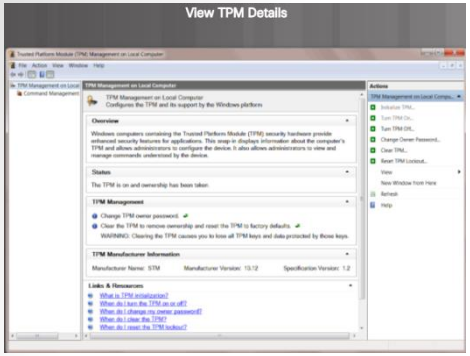


7.1.3.2
File Encryption
تشفير الملفات

تشفير الملفات

التشفير هو أداة تستخدم لحماية البيانات ، يحول التشفير البيانات باستخدام خوارزمية معقدة لجعلها غير قابلة للقراءة ، وعند استخدام المفتاح الخاص بإرجاع المعلومات غير القابلة للقراءة مرة أخرى إلى بيانات قابلة للقراءة ، تقوم برامج التشفير أيضًا بتشفير الملفات والمجلدات وحتى محركات الأقراص بالكامل.

تشفير نظام الملفات (Encrypting File System) (EFS) هو ميزة (Windows) التي يمكن تشفير البيانات ، يربط النظام (Windows) ملفات (EFS) مباشرة بحساب مستخدم محدد ، حيث أنه لن يتمكن سوى المستخدم الذي قام بتشفير البيانات من الوصول إلى الملفات أو المجلدات المشفرة.



7.1.3.2
File Encryption
تشفير الملفات

تشفير الملفات

يمكن للمستخدم أيضًا اختيار تشفير محرك أقراص ثابت بالكامل في النظام باستخدام ميزة تسمى (BitLocker) ، لاستخدام (BitLocker) يجب وجود وحدتين للتخزين على الأقل على قرص ثابت.

قبل استخدام (BitLocker)، يحتاج المستخدم إلى تمكين وحدة الموثوق به (Trusted Platform Module) (TPM) في نظام الإدخال والإخراج الأساسي وتسمى (BIOS) ، (BIOS) هي رقاقة متخصصة مثبتة على اللوحة الأم.

يقوم (TPM) بتخزين المعلومات الخاصة بالنظام المضيف ، مثل مفاتيح التشفير والشهادات الرقمية وكلمات المرور، كما يمكن للتطبيقات مثل (BitLocker) التي تستخدم التشفير باستخدام شريحة (TPM) ، ادخل وانقر فوق إدارة (TPM) لعرض تفاصيل (TPM) ، كما هو موضح في الشكل.

يقوم (BitLocker To Go) بتشفير محركات الأقراص القابلة للإزالة مثل فلاش ميموري ، لا يستخدم (BitLocker To Go) التشفير بتقنية الـ (TPM) ، ولكنه لا يزال يوفر تشفيرًا للبيانات ويتطلب كلمة مرور.

7.1.3.3
System and Data Backups
النظام والبيانات النسخ الاحتياطي

النظام والبيانات النسخ الاحتياطي (System and Data Backups)

يمكن أن تفقد المؤسسة البيانات إذا قام مجرمو الإنترنت بسرقتها أو تخريبها أو حدوث كارثة ؛ لهذا السبب من المهم إجراء نسخ احتياطي للبيانات بانتظام.

النسخ الاحتياطي للبيانات تخزن كنسخة من المعلومات من كمبيوتر إلى وسائط إحتياطية القابلة للإزالة ، يخزن المستخدم النسخة الاحتياطية في مكان آمن ، تعد النسخ الإحتياطية للبيانات إحدى الطرق الأكثر فاعلية للحماية من فقد البيانات أو إذا فشل جهاز الكمبيوتر ، فيمكن للمستخدم استعادة البيانات من النسخة الاحتياطية بمجرد أن يعمل النظام.

يجب أن تتضمن سياسة أمان المؤسسة النسخ الاحتياطي للبيانات ، فيجب على المستخدمين إجراء نسخ احتياطي للبيانات بشكل منتظم ، عادة ما يتم تخزين النسخ الاحتياطية للبيانات خارج الموقع لحماية وسائط النسخ الاحتياطي إذا حدث أي شيء للمنشأة الرئيسية.

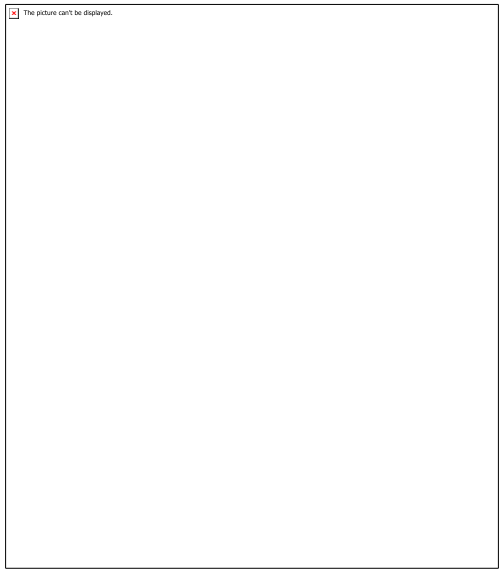
7.1.3.3
System and Data Backups
النظام والبيانات النسخ الاحتياطي

النظام والبيانات النسخ الاحتياطي

هذه بعض الاعتبارات للنسخ الاحتياطي للبيانات:

- منتظم ومتكرر (Frequency) : يمكن أن تستغرق النسخ الاحتياطية وقتًا طويلاً ، ففي بعض الأحيان يكون من الأسهل إجراء نسخ احتياطي كامل شهريًا أو أسبوعيًا ثم إجراء نسخ احتياطية جزئية متكررة لأي بيانات تم تغييرها منذ آخر عملية نسخ احتياطي كاملة ،ومع ذلك فإن وجود العديد من النسخ الاحتياطية الجزئية يزيد من مقدار الوقت اللازم لاستعادة البيانات.
- التخزين (Storage) : للحصول على مزيد من الأمان ، قم بالنسخ الاحتياطي للنقل إلى موقع تخزين خارج موقع معتمد على أساس متناوب إما يومي أو أسبوعي أو شهري وفقًا لما تتطلبه سياسة الأمان.
- الأمان (Security): حماية النسخ الاحتياطية بكلمات المرور ، يدخل المستخدم كلمة المرور قبل استعادة البيانات من النسخة الاحتياطية.
- التحقق من الصحة (Validation) : تحقق دائمًا من النسخ الاحتياطية لضمان سلامة البيانات.

نشاط نوع النشاط : فردي مدته : ٥ دقائق



ابحث عن إجراءات النسخ الاحتياطي؟

7.1.4.1
Content Screening and Blocking
فحص المحتوى والحظر

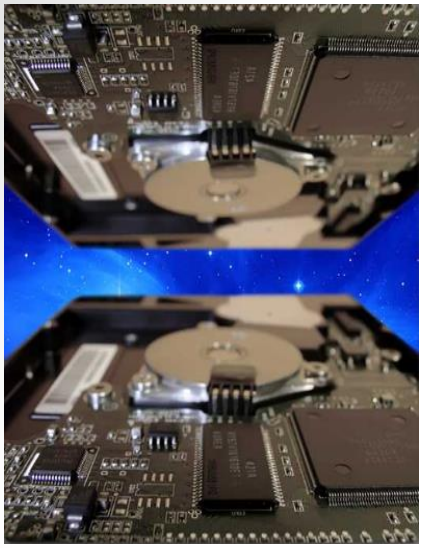
فحص المحتوى والحظر

برنامج التحكم في المحتوى يقيد المحتوى الذي يمكن للمستخدم الوصول إليه باستخدام متصفح ويب عبر الإنترنت ، يمكن أن تحظر برامج التحكم في المحتوى تلك المواقع التي تحتوي على أنواع معينة من المواد مثل المواد الإباحية أو المحتوى الديني أو السياسي المثير للجدل ، قد يقوم أحد الوالدين بتطبيق برنامج التحكم في المحتوى على الكمبيوتر الذي يستخدمه الطفل ، تقوم المكتبات والمدارس أيضًا بتنفيذ برنامج التحكم لمنع الوصول إلى محتوى يعتبر غير مرغوب فيه.

يمكن للمسؤول تنفيذ أنواع الفلاتر التالية:

- فلتر المتصفح من خلال ملحقات المتصفح (browser extension) تابع لجهة خارجية.
- فلتر البريد الإلكتروني من خلال فلتر يستند إلى العميل أو الخادم.
- فلتر من جانب العميل مثبتة على كمبيوتر معين.
- فلتر من جانب الراوتر : تمنع حركة معلومات من دخول الشبكة.
- فلتر من جانب البرامج تشبه طريقة الراوتر.
- فلتر من جانب الكلاود.

توفر محركات البحث مثل (Google) خيار تشغيل فلتر أمان لاستبعاد الروابط غير الملائمة من نتائج البحث.



7.1.4.2
Disk Cloning and Deep Freeze
استنساخ القرص والتجميد العميق

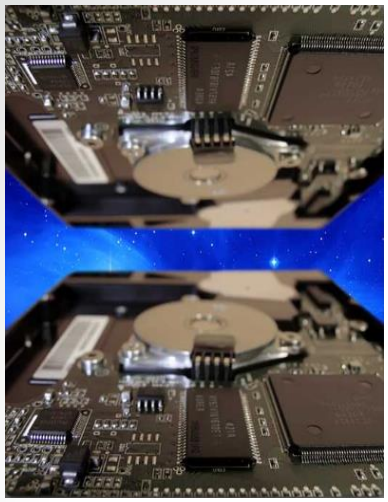
استنساخ القرص والتجميد العميق (Disk Cloning and Deep Freeze)

تتوفر العديد من تطبيقات الجهات الخارجية لاستعادة النظام مرة أخرى إلى الحالة الإفتراضية ، يسمح ذلك للمسؤول بحماية نظام التشغيل وملفات التهيئة لنظام.

ينسخ قرص الاستنساخ (Disk cloning) محتويات القرص الثابت للكمبيوتر إلى ملف رقمي(image file) ، على سبيل المثال يقوم المسؤول بإنشاء الأقسام المطلوبة على القرص الصلب لنظام ما وتنسيق القسم ثم يقوم بتثبيت نظام التشغيل ، تقوم بتثبيت جميع برامج التطبيقات المطلوبة وتكوين جميع الأجهزة ، ثم يستخدم المسؤول برنامج نسخ الأقراص لإنشاء ملف رقمي.

يمكن للمسؤول استخدام نسخة الملف الرقمي كما يلي:

- **لمسح نظام واستعادة صورة رئيسية نظيفة تلقائيًا**
- **لنشر أجهزة كمبيوتر جديدة داخل المنظمة**
- **لتوفير نسخة احتياطية كاملة للنظام**



7.1.4.2
Disk Cloning and Deep Freeze
استنساخ القرص والتجميد العميق

استنساخ القرص والتجميد العميق

(Deep Freeze) يقوم بتجميد قسم في القرص الصلب وعندما يقوم المستخدم بإعادة تشغيل النظام يعود النظام إلى تكوينه المجمّد ، لا يقوم النظام بحفظ أي تغييرات يقوم بها المستخدم ، لذلك يتم فقد أي تطبيقات مثبتة أو ملفات محفوظة عند إعادة تشغيل النظام.

إذا احتاج المسؤول إلى تغيير إعدادات النظام ، فعليه أولاً أن يقوم بما تسمى"ذوبان" (thaw) للقسم المحمي عن طريق تعطيل التجميد العميق (Deep Freeze) ، ثم بعد إجراء التغييرات ، يجب عليها إعادة تمكين البرنامج.

يمكن للمسؤول أن يجعل (Deep Freeze) يقوم بإعادة التشغيل بعد تسجيل خروج المستخدم أو إيقاف التشغيل بعد فترة من عدم النشاط أو إيقاف التشغيل في وقت مجدول.

هذه المنتجات لا توفر الحماية في الوقت الحقيقي (real-time) ، يظل النظام ضعيفًا حتى يقوم المستخدم أو الأمر المجدول بإعادة تشغيل النظام، بعد ذلك ، يحصل النظام المصاب على بداية جديدة ويزيل البرامج الضارة بمجرد إعادة تشغيل النظام.

7.1.5.1
Security Cables and Locks
كابلات الحماية والأقفال

كابلات الحماية والأقفال (Security Cables and Locks)

هناك عدة طرق لحماية أجهزة الكمبيوتر ماديًا:

- ✓ **استخدم أقفال الكيبل مع المعدات كما هو موضح في الشكل ١.**
- ✓ **الحفاظ على قفل غرف الاتصالات.**
- ✓ **استخدام أقفاص الأمان حول المعدات.**

تحتوي العديد من الأجهزة المحمولة وشاشات الكمبيوتر ذات التكلفة العالية على فتحة أمان خاصة من الفولاذ مضمنة لاستخدامها مع أقفال الكابلات.

النوع الأكثر شيوعًا لقفل الباب هو القفل العادي الذي يفتح من الداخل فقط ومن الخارج بمفتاح ، لا يقفل تلقائيا عند إغلاق الباب ولهذا يعد خطرًا ؛ لأنه يمكن للفرد مع الاسف إدخال بطاقة بلاستيكية رفيعة مثل بطاقة ائتمان بين القفل والباب لإجبار الباب على الفتح ، تختلف أقفال الأبواب في المباني التجارية عن أقفال الأبواب السكنية.