الفصل الثاني عشر

حماية أمن المعلومات

مقدمة :

شهدت الأعوام الماضية دخول آلاف الشركات إلى شبكة الإنترنت وقامت هذه الشركات بتزويد موظفيها بالبريد الإلكتروني ومتصفحات إنترنت وأصبح من السهل على المستخدم الخارجي المسلح ببعض المعرفة وبعض الأهداف الخبيثة من التسلل إلى الأنظمة الداخلية وأصبحت التبادلات المصرفية السرية قريبة من متناول الكثيرين لذا بدأت أسواق امن الشبكات تستجيب بسرعة لتحديات أمن شبكة الإنترنت وذلك عن طريق تبني تقنيات التحقق Authentication والتشفير Encryption لتطبيقها على روابط شبكة الإنترنت.

مفاهيم ومحددات أولية لأمن المعلومات :

١. ما هي إستراتيجية أمن المعلومات (Security Policy)؟

هي مجموعة القواعد التي يطبقها الأشخاص لدى التعامل مع التقنية ومع المعلومات داخل المنشاة وتتصل بشؤون الدخول إلى المعلومات والعمل على نظمها وإدارتها.

٢. ما هي أهداف إستراتيجية أمن المعلومات؟

أهداف إستراتيجية أمن المعلومات تهدف إلى :

١. تعريف المستخدمين والإداريين بالتزاماتهم وواجباتهم المطلوبة لحماية نظم الكمبيوتر والشبكات وكذلك حماية المعلومات بكافة إشكالها.

٢. تهدف أيضا إلى تحديد الإلكترونية التي يتم من خلالها تحقيق وتنفيذ الواجبات المحددة على كل من له علاقة بالمعلومات ونظمها وتحديد المسؤوليات عند حصول الخطر.

٣. بيان الإجراءات المتبعة لتجاوز التهديدات والمخاطر والتعامل معها والجهات المناط بها القيام بذلك.

٣. من الذي يعد إستراتيجية أمن المعلومات؟

لتكون هذه الإستراتيجية مفعله وهادفة لا بد وان يساهم في إعدادها مختلف المستويات الوظيفية في المنشأة الواحدة إضافة إلى التعاون والدعم الكامل من الكل وتشمل :

١. مسؤولي أمن الموقع.
٢. مديري الشبكات.
٣. موظفي وحدة الكمبيوتر.
٤. مديري الوحدات المختلفة في المنشأة كوحدة الأعمال والتسويق والبحث وغيرها..
٥. فرق الاستجابة للحوادث والأعطال.
٦. ممثلي مجموعات المستخدمين ومستويات الإدارة العليا إلى جانب الإدارة القانونية.

٤. متى توصف إستراتيجية أمن المعلومات بأنها ناجحة؟

١. من حيث فعالية الإستخدام: فيجب أن تعمم بشكل شامل على كافة قطاعات الإدارة وأن تكون مقبولة وواقعية وأيضاً لا بد من توفير جميع الأدلة التوجيهية والإرشادية لضمان إدامة التنفيذ أي الإستخدام الفعلي لأدوات الحماية التقنية من جهة والتطبيق الفعلي لقواعد العمل من جهة أخرى.
٢. من حيث المحتوى: لا بد وأن تشمل الإستراتيجية سياسة واضحة بشأن اقتناء وشراء الأجهزة التقنية وأدواتها والبرمجيات والحلول المتصلة بالعمل والحلول المتعلقة بإدارة النظام وأيضاً يجب أن تشمل إستراتيجية الخصوصية المعلوماتية وهي التي تحدد مستوى المعلومات إذا كانت سرية أو غير سرية وأيضا إستراتيجية الاشتراكات التي تحدد سياسة المنشأة بشأن اشتراكات الغير في شبكتها أو نظمها وأيضاً إستراتيجية التعامل مع المخاطر بحيث تحدد ماهي المخاطر وإجراءات الإبلاغ عن المخاطر والتعامل معها والجهات المسؤولة عن التعامل معها.

تعريف أمن المعلومات:

أمن المعلومات من الزاوية الأكاديمية:

العلم الذي يبحث في نظريات واستراتيجيات توفير الحماية للمعلومات من المخاطر التي تهددها ومن أنشطة الإعتداء عليها.

أمن المعلومات من الزاوية التقنية:

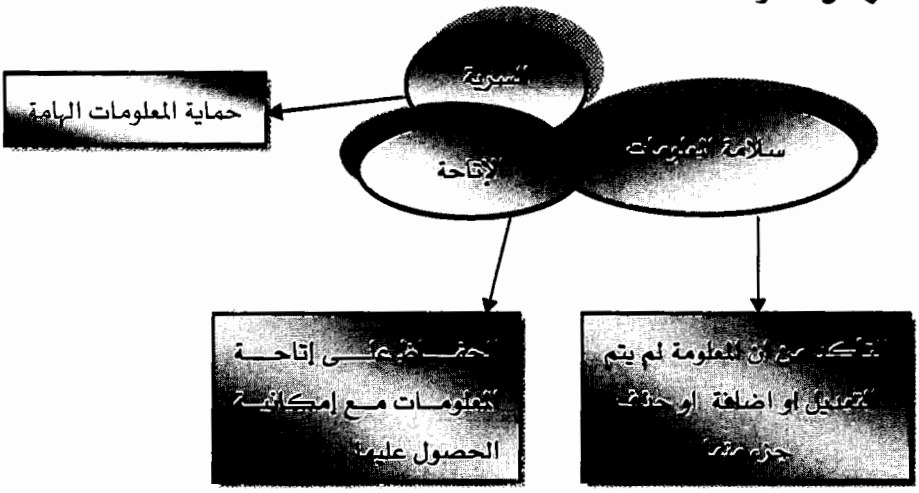
الوسائل والأدوات والإجراءات اللازم توفيرها لضمان حماية المعلومات من الأخطار الداخلية والخارجية.

أمن المعلومات من الزاوية القانونية:

دراسة وتدابير حماية سرية وسلامة محتوى وتوفر المعلومات ومكافحة أنشطة الاعتداء عليها أو استغلال نظمها في ارتكاب الجريمة.

ما هي سرية المعلومات[1]؟

عناصر أمن المعلومات[2]:



١. السرية أو الموثوقية وتعني التأكد من إن المعلومات لا تكشف أو يطلع عليها الأشخاص غير المخولين بالاطلاع على المعلومات

٢. التكاملية وسلامة المحتوى وتعني التأكد من أن محتوى المعلومات صحيح ولم يتم تعديله أو العبث به أو تدميره في أي مرحلة من مراحل المعالجة أو تبادل

1 - عبدالله يحي المبارك، أهمية أمن المعلومات في مجتمعنا، مركز التميز لأمن المعلومات، جامعة الملك سعود، ٢٠٠٦.

2 - أمن المعلومات ماهيتها وعناصرها واستراتيجياتها، ٢٠٠٦ www.elhandasa.net .

المعلومات سواء في مرحلة التعامل الداخلي مع المعلومات أو عن طريق تدخل غير مشروع.

٣. استمرارية توفر المعلومات أو الخدمة وتعني التأكد من استمرار عمل النظام واستمرار القدرة على التفاعل مع المعلومات وتقديم الخدمة وان المستخدم لن يتعرض إلى منع إستخدامه لها.

٤. عدم إنكار التصرف المرتبط بالمعلومات ممن قام بها وتعني ضمان عدم إنكار الشخص الذي قام بتصرف ما من إنكار انه هو الذي قام بهذا التصرف.

منطلقات خطة حماية المعلومات:

إن ضمان عناصر أمن المعلومات يعتمد على المعلومات فبعض المعلومات لا تتطلب السرية وليست كل المعلومات بنفس درجة الأهمية لذا قبل البدء بحماية المعلومات يجب الإجابة على الاستفسارات التالية:

١. ما الذي نريد أن نحميه؟

٢. ما هي المخاطر التي تتطلب هذه الحماية؟

٣. كيف يتم توفير الحماية؟

٤. ما العمل إن تحقق أي من المخاطر رغم وسائل الحماية؟

السؤال الأول ما الذي نريد أن نحميه؟

يتم تصنيف البيانات والمعلومات من حيث الأهمية

ا) معلومات تتطلب حماية قصوى

ب) معلومات لا تتطلب حماية قصوى

السؤال الثاني ما هي المخاطر التي تتطلب الحماية؟

١. قطع التيار الكهربائي

٢. اختراق النظام من الخارج

٣. اختراق النظام من الداخل من الموظفين

السؤال الثالث كيف يتم توفير الحماية؟

١. وضع كلمة سر على كل جهاز ولا يسمح للدخول على الجهاز إلا للشخص المخول.

٢. وضع برامج لمقاومة الفيروسات الإلكترونية والتأكد من مصدر البريد الإلكتروني.

٣. وضع جدران نارية تحد من دخول أشخاص من الخارج ومنع اعتداءات قد يتعرض لها النظام.

٤. في حال تبادل الرسائل الإلكترونية يجب أن يكون هناك تقنيات التشفير.

السؤال الرابع ما العمل إن تحقق أي من المخاطر بالرغم من وجود وسائل الحماية؟

لا بد من وضع وإعداد خطط مواجهة الأخطار عند حصولها وهذه الخطة تتضمن مراحل تبدأ من:

١. مرحلة الإجراءات التقنية والإدارية والإعلامية والقانونية.

٢. مرحلة إجراءات التحليل لطبيعة المخاطر التي قد تحصل وكيفية منعها.

٣. وضع خطة العودة إلى الوضع الطبيعي.

أنماط ومستويات أمن المعلومات:

١. الحماية المادية وتشمل كافة الوسائل التي تمنع الوصول إلى نظم المعلومات وقواعدها كالأقفال والحواجز والغرف المحصنة وغيرها من وسائل الحماية المادية التي تمنع الوصول إلى الأجهزة الحساسة.

٢. الحماية الشخصية وهي تتعلق بالموظفين العاملين على النظام التقني المعني من حيث توفير وسائل التعريف الخاصة بكل منهم وتحقيق التدريب والتأهيل للمتعاملين بوسائل الأمن إلى جانب الوعي بمسائل الاعتداء على المعلومات.

٣. الحماية الإدارية وهي سيطرة الإدارة على إدارة نظم المعلومات وقواعدها مثل التحكم بالبرمجيات الخارجية ومسائل التحقيق باخلالات الأمن ومسائل الإشراف والمتابعة لأنشطة الرقابة إضافة إلى القيام بأنشطة الرقابة ضمن المستويات العليا ومن ضمنها مسائل التحكم بالاشتراكات الخارجية.

٤. الحماية الإعلامية كالسيطرة على إعادة إنتاج المعلومات وعلى عملية إتلاف مصادر المعلومات الحساسة عند اتخاذ القرار بعدم إستخدامها.

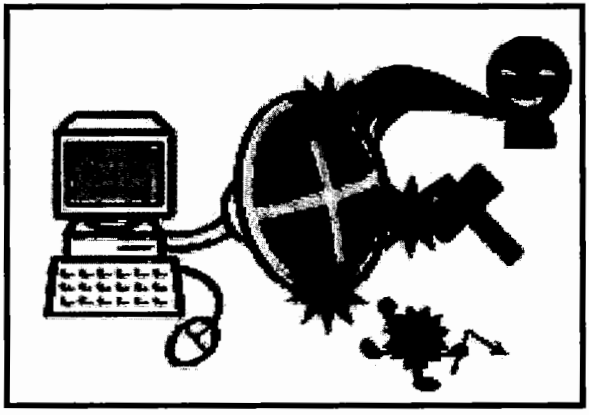
ماهي مواطن المخاطر:

١. **الأجهزة وهي:** كافة المعدات والأدوات المادية (النظم، الشاشات، الطابعات ومكوناتها، ووسائط التخزين..).

٢. **البرامج وهي:** جميع البرامج المخزنة على الجهاز أو خارجة أي أوامر العمل.

٣. **المعطيات وهي:** كافة البيانات المدخلة والمعلومات المستخرجة عقب معالجتها والمخزنة داخل النظم.

٤. **الاتصالات وهي:** شبكات الاتصال التي تربط الأجهزة التقنية والتي تتصل بالنظام.



عمليات المعلومات الرئيسية المتصلة بأمن المعلومات:

١. تصنيف المعلومات.

٢. التوثيق.

٣. المهام والواجبات الإدارية والشخصية.

٤. وسائل التعريف والتوثيق من المستخدمين وحدود الصلاحيات.

٥. سجل الأداء.

٦. عمليات الحفظ.

٧. وسائل الأمن الفنية ونظام منع الاختراق.

٨. نظام التعامل مع الحوادث.

١. تصنيف المعلومات:

هي عملية أساسية لدى بناء أي نظام أو أي نشاط يتعلق بالمعلومات وتصنف المعلومات إلى:

١. معلومات متاحة.

٢. معلومات موثقة.

٣. معلومات سرية.

٤. معلومات سرية للغاية.

٢. التوثيق:

هو إتباع نظام توثيق خطي لتوثيق بناء النظام وكافة وسائل المعالجة والتبادل ومكوناتها وهو ضروري لنظام التعريف والتخويل وتصنيف المعلومات والأنظمة التطبيقية، أما بما يتعلق في إطار الأمن فان التوثيق يتطلب أن تكون إستراتيجية أو سياسة الأمن موثقه ومكتوبة وان تكون إجراءاتها ومكوناتها كاملة محل توثيق، وأيضا لابد إلى توثيق خطط التعامل مع المخاطر والحوادث ومن هي الجهات المسؤوله وما هي مسؤولياتها وخطط التعافي وإدارة الأزمات وخطط الطوارئ المرتبطة بالنظام عند حدوث الخطر.

٣. المهام والواجبات الإدارية والشخصية:

لا بد من حسن اختيار الأفراد المؤهلين وعمق معارفهم النظرية والعملية، إن المهام الإدارية والتنظيمية تتكون من خمس عناصر رئيسية هي:

١. تحليل المخاطر.

٢. وضع السياسة أو الاستراتيجيات.

٣. وضع خطة الأمن.

٤. وضع البناء التقني الأمني.

٥. توظيف الأجهزة والمعدات والوسائل وتنفيذ الخطط.

- لابد من إدراك حقيقة أن نجاح هذه الواجبات يتطلب إدراك جميع العاملين بالمؤسسة بهذه النقاط ووعي العاملين بأهمية مسالة الأمن وحماية المعلومات وكيفية التعامل معها.

٤. وسائل التعريف والتوثيق وحدود الصلاحيات:

إن الدخول إلى الكمبيوتر وقواعد البيانات يمكن تقييده بالعديد من الوسائل ويتم ذلك بطريقتين:

١. أما أن تكون وسيلة التعريف هي اسم المستخدم.

٢. أو قبول وسيلة التوثق من صحة الهوية المقدمة.

إن وسائل التعريف تختلف حسب التقنية المستخدمة وتقسم إلى ثلاثة أنواع:

١. شيء يملكه الشخص (مثل البطاقات البلاستيكية).

٢. شيء يعرف الشخص (مثل كلمة السر أو الرمز أو الرقم الشخصي).

٣ شيء يرتبط بالشخص (مثل بصمة الأصبع أو العين أو الصوت).

- تعتبر كلمة السر من أكثر الطرق انتشارا لذا لا بد من وضع كلمات سر يسهل تذكرها والابتعاد عن الكلمات التي يسهل تخمينها.
- عندما يتم التأكد من كلمة الدخول فالمرحلة التي تليها هي مرحلة تحديد النطاق (تحديد نطاق الاستخدام) وهو ما يعرف بالتصريح وهي المسالة التي تتصل بالتحكم بالدخول إلى المعلومات أو النظام.

٥. سجل الأداء:

وهي السجلات التي تبين إستخدامات الجهاز وبرمجياته والية النفاذ وهي مهمة في حال تعدد المستخدمين وفي حال شبكات الكمبيوتر التي يستخدم مكوناتها أكثر من شخص[1].

أنواع سجلات الأداء:

١. سجلات الأداء إلتاريخية والسجلات المؤقتة.

---

1 - أمن المعلومات ماهيتها وعناصرها، ٢٠٠٦، www.elhandasa.net .

٢. سجلات التبادل والنظام والأمن .

٣. سجلات قواعد البيانات والتطبيقات.

٤. سجلات الصيانة أو السجلات التقنية.

- جميع هذه السجلات يجب أن يكون محدد بها المستخدم ووقت الإستخدام ومكانه وطبيعة الإستخدام وأي معلومات إضافية.

٦. عمليات الحفظ:

وهي عمل نسخ إضافية من المواد المخزنة على إحدى وسائط التخزين سواء داخل النظام أو خارجة، وتخضع عمليات الحفظ لقواعد يجب أن تكون محدده سلفا مثل (وقت الحفظ، حماية النسخة الاحتياطية، نظام الترقيم والتبويب، آلية الاسترجاع والإستخدام، مكان الحفظ، تشفير النسخ التي تحتوي معلومات خاصة وسرية).

٧. وسائل الأمن الفنية ونظام منع الاختراق:

تعتبر الجدران النارية من أهم الأنظمة لمنع الاختراق هذا بالإضافة إلى كلمة السر والتشفير ومسائل التعريف والصلاحيات ومقاومة الفيروسات

٨. نظام التعامل مع الحوادث:

لا بد من توفر نظام متكامل للتعامل مع المخاطر والحوادث والاعتداءات وهو متطلب أساسي جدا وتختلف مكونات النظام من مؤسسة إلى أخرى حسب طبيعة الخطر وما أظهرته عملية تحليل المخاطر .

يتكون نظام التعامل مع المخاطر من عدة مراحل وهي:

١. الإعداد المسبق والتحري.

٢. الملاحظة .

٣. الاحتواء والاستئصال.

٤. التعافي والعودة للوضع الطبيعي.

٥. المتابع.

المخاطر والتهديدات ونقاط الضعف وأنواع الهجمات والاعتداءات :

- التهديد: هو الخطر المحتمل الذي يمكن أن يتعرض له نظام المعلومات وقد يكون شخصا كالمتجسس أو الهاكرز(المخترق) أو أي شئ يهدد الاجهزه أو البرامج أو المعطيات أو انقطاع التيار الكهربائي والكوارث الطبيعية.
- نقاط الضعف أو الثغرات: هي أي عنصر أو نقطة في النظام يحتمل أن ينفذ من خلاله المعتدي أو يتحقق بسببه الاختراق ومثال على ذلك قد يكون الاتصال بالإنترنت نقطة ضعف إذا لم يكن مشفراً وإذا لم يكن الجهاز مجهز بأجهزة الحماية اللازمة قد يكون نقطة ضعف أيضا.
- المخاطر: تستخدم بشكل مترادف مع التهديد وهي تتصل بأثر التهديدات عند حصولها وتقوم إستراتيجية امن المعلومات الناجحة على تحليل المخاطر وهي عملية وليست مجرد خطة.
- الحوادث: تشمل المخاطر والأخطاء أي الأفعال المقصودة أو غير مقصودة
- الهجمات: وهي وصف لمختلف أنماط الإعتداءات التقنية وهي مرادفة للإعتداءات
- المخاطر: هناك أنواع مختلفة من المخاطر التي ممكن أن يواجهها أي نظام، فمن الممكن أن تكون مخاطر طبيعية أو مخاطر عامة وأيضا من الممكن أن تكون مخاطر إلكترونية. وهذه المخاطر مقسمة كما يلي:

١. مخاطر طبيعية مثل:

- الكوارث الطبيعة.
- الحريق .

٢. مخاطر عامة مثل:

- انقطاع التيار الكهربائي.
- انقطاع خدمة الإنترنت.
- سرقة البيانات.

٣. مخاطر الإلكترونية مثل:

- الفيروسات.
- أحصنة طروادة وديدان الإنترنت.
- جافا سكريبت وجافا ابليتس والاكتف اكس.
- الإختراق الأمني للنظام (من الداخل أو الخارج).
- جواسيس البريد الإلكتروني.

التخطيط لمواجهة المخاطر:

لماذا نحتاج للتخطيط لمواجهة المخاطر؟

- الإعتماد الكلى في العمل على تقنيات المعلومات وترك العمل اليدوي.
- الوصول بالخسارة المادية إلى أقل ما يمكن.
- للمحافظة على ثقة المؤسسات الأخرى التي تتعامل مع المؤسسة.
- للمحافظة على الصورة الجيدة للمؤسسة أمام العملاء.
- إستعادة النشاط إلى ما كان عليه في أسرع وقت .
- مواجهة الإلتزامات القانونية.
- حصر كافة البيانات المتراكمة خلال توقف الحاسب وكذلك جمع البيانات التي فقدت نتيجة الكارثة من أجل إدخالها لاحقا.
- لتقليل الخسائر المباشرة أو غير المباشرة الناتجة عن تأخر أو توقف معالجة البيانات.
- للتعامل بشكل مقبول مع الظروف التى تنشا عن توقف العمل وتغيير الحاسبات والمواقع.
- لتقليل الفوضى التي قد تنجم من الكارثة والسماح بإستعادة النشاط بشكل سريع.

الإصطلاحات القانونية:

١. إصطلاح الجرائم الإلكترونية.

٢. إصطلاح إرهاب السايبر أو إرهاب العالم الإلكتروني.

٣. إصطلاح حرب المعلومات.

- إصطلاح الجرائم الإلكترونية وهي: جميع جرائم الكمبيوتر والإنترنت.
- إصطلاح إرهاب السايبر وهي: هجمات تستهدف نظم الكمبيوتر والمعطيات لإغراض دينية أو سياسية أو فكرية أو عرقية وتعتبر جرائم إتلاف للنظم والمعطيات أو جرائم تعطيل للمواقع وعمل الأنظمة.
- إصطلاح حرب المعلومات وهو: إصطلاح ظهر في بيئة الإنترنت للتعبير عن إعتداءات تعطيل المواقع وإنكار الخدمة والاستيلاء على المعطيات وفي الغالب تكون هجمات بين جهات تتناقض في قطاع الأعمال أو بين جهات تتعارض مصالحها ومواقفها ومثال على ذلك حملات الهاكرز اليوغسلافيين على مواقع الناتو أبان ضربات الناتو حيث وصفت بأنها حرب معلومات.

كلمات المرور Pass Word:

ما هي كلمات المرور؟

كلمات المرور هي:

- سلسلة من الرموز والحروف والأرقام يتم إدخالها إلى النظام من اجل إثبات هوية المستخدم.
- يفضل أن تكون صعبة التخمين، سهلة التذكر.
- يجب حمايتها من الإفصاح عنها لئلا يؤدي ذلك إلى إستخدامها من قبل الأشخاص غير المخولين.

- استخدم كلمة المرور عندما تريد الدخول إلى حافظات الشاشة بتفعيل ما يسمى Screen Lock.

لها شروط مختلفة لتكون قوية:

١. لا يقل عدد مكوناتها عن ثمانية مثلا.
٢. ألا تكون من الكلمات التي يمكن تواجدها في القواميس.
٣. تكون خليطاً من الحروف والأرقام والرموز الخاصة.
٤. لا يكون جزء منها اختصاراً أو أسما لشيء معروف مثل اسم العائلة.
٥. لا تشبه أسم المستخدم .

- لكلمات المرور سياسة توضح أهدافها ومجالها وتفاصيلها تسمى سياسة كلمات المرور.
- هذه السياسة موجودة ضمن السياسات الوطنية لأمن وحماية المعلومات، والعمل بهذه السياسة يحمي الموظفين ويحمي الدائرة من الآثار السلبية لعدم تطبيقها.

المخاطر الإلكترونية:

١- الفيروسات:

تاريخ الفيروسات:

عندما تحدثت التقارير في عام ١٩٨٩ عن أول فيروسات الكمبيوتر، خيل للكثيرين (ومن بينهم خبراء في هذا المجال) إن ذلك مجرد خرافة ابتدعها احد كتاب قصص الخيال العلمي، وان وسائل الأعلام تحاول أن ترسخها في أذهان الناس كحقيقة رغم أنها لا تمت إلى الواقع بصلة . لقد امتدت تلك الظاهرة واتسعت حتى باتت تشكل خطرا حقيقيا يهدد الثورة

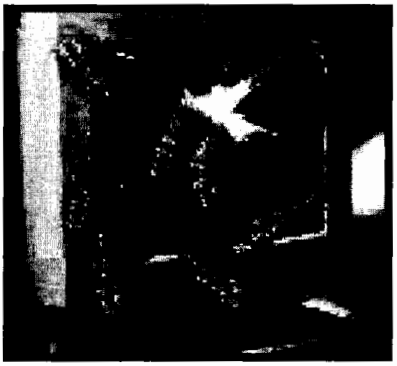
المعلوماتية التي فجرتها التقنيات المتطورة والمتصارعة في علوم الكمبيوتر. فمن بضعة فيروسات لا تزيد عن عدد أصابع اليد في السنة الأولى إلى ما يزيد عن (١٥٠٠٠) فيروس في يومنا هذا، وفي كل يوم تكتشف أنواع جديدة من الفيروسات المختلفة التأثير مما يقلق مستخدم الكمبيوتر ويسلبهم راحة البال . ومن فيروسات بسيطة الضرر والتأثير يسهل اكتشافها والتخلص منها مرورا، بفيروسات خبيثة بالغة الأذى تجيد التخفي ويطول زمن اكتشافها إلى فيروسات ماكرة ذكية تبرع في التغير والتحول من شكل لأخر مما يجعل تقفي أثرها وإلغاء ضررها أمراً صعباً.

أما الأسباب التي تدفع بعض الناس لكتابة البرامج الفيروسية فمنها :

- الحد من نسخ البرامج كما في فيروس brain أو Pakistani وهو أول فيروسات الكمبيوتر ظهوراً وأكثرها انتشاراً وكتبت من قبل أخوين من الباكستان كحماية للملكية الفكرية للبرامج التي قاما بكتابتها.
- البحث العلمي كما في فيروس STONEDالشهير والذي كتبه طالب دراسات عليا في نيوزلندا وسرق من قبل أخيه الذي أراد أن يداعب أصدقاءه بنقل الفيروس إليهم.
- الرغبة في التحدي وإبراز المقدرة الفكرية من بعض الأشخاص الذين يسخرون ذكاءهم وقدراتهم بشكل سيئ، مثل فيروسات V2P التي كتبها Mark Washburn كإثبات إن البرامج المضادة للفيروسات من نوع Scanners غير فعالة.
- الرغبة في الانتقام من قبل بعض المبرمجين المطرودين من أعمالهم والناقمين على شركاتهم وتصمم الفيروسات في هذه الحالة بحيث تنشط بعد تركهم العمل بفترة كافية أي تتضمن قنبلة منطقية موقوتة.
- التشجيع على شراء البرامج المضادة للفيروسات إذ تقوم بعض شركات البرمجة بنشر فيروسات جديدة ثم تعلن عن منتج جديد لكشفهما.

ماهي الفيروسات ؟

فيروس الكمبيوتر هو برنامج صغير يتم إدخاله على الحاسب الآلي من غير علم المستخدم بغرض تدمير بعض أو جميع البرامج والأجهزة المكونة للحاسب الآلي.



يعرف الفيروس في علم البيولوجيا على انه جزيئه صغيرة من مادة حية غير قادرة على التكاثر ذاتيا" ولكنها تمتلك مادة وراثية كافية لتمكنها من الدخول إلى خلية حية وتغيير العمليات الفعالة في الخلية بحيث تقوم تلك الخلية بإنتاج جزيئات جديدة من ذلك الفيروس و التي تستطيع بدورها مهاجمة خلايا جديدة.

و بشكل مشابه، يعرف الفيروس في علم الكمبيوتر على أنه برنامج صغير أو جزء من برنامج يربط نفسه ببرنامج آخر ولكنه يغير عمل ذلك البرنامج لكي يتمكن الفيروس من التكاثر عن طريقه، وله أهداف تدميريه تهدف إلى إحداث أضرار جسيمه بنظام الحاسوب سواء بالبرامج أو المكونات.

ويتصف فيروس الكمبيوتر بأنه: برنامج قادر على التناسخ(Replication) أي النسخ المتماثل والانتشار أي خلق نسخ (قد تكون معدلة) من نفسه. وهذا ما يميز الفيروس عن البرامج الضارة الأخرى التي لا تكرر نفسها مثل أحصنة طروادة (Trojans) والقنابل المنطقية (Bombs).

عملية التناسخ ذاتها هي عملية مقصودة وليست تأثيرا جانبيا وتسبب خللا أو تخريبا في نظام الكمبيوتر المصاب أما بشكل عفوي أو متعمد ويجب على الفيروس إن يربط نفسه ببرنامج آخر يسمى البرنامج الحاضن HOST بحيث أن أي تنفيذ لذلك البرنامج سيضمن تنفيذ الفيروس، هذا ما يميز الفيروس عن الديدان worms التي لا تحتاج إلى ذلك.

من أين تأتى:

- من خلال الرسائل الإلكترونية .

- صفحات الإنترنت "HTTP".
- نسخ البرامج المقلدة.
- الأقراص المرنة والأقراص الضوئية.

ما هو التأثير:

١. زيادة عدد العمليات التي تتم إلى ملايين العمليات فيتوقف الحاسب عن العمل.
٢. إلغاء بعض ملفات النظام.
٣. زيادة حجم الملف بإعادة كتابته على نفسه آلاف المرات .
٤. إغلاق الحاسب من تلقاء نفسه عند الدخول على الإنترنت مثلا.
٥. إلغاء البرنامج المكتوب على الـ BIOS.

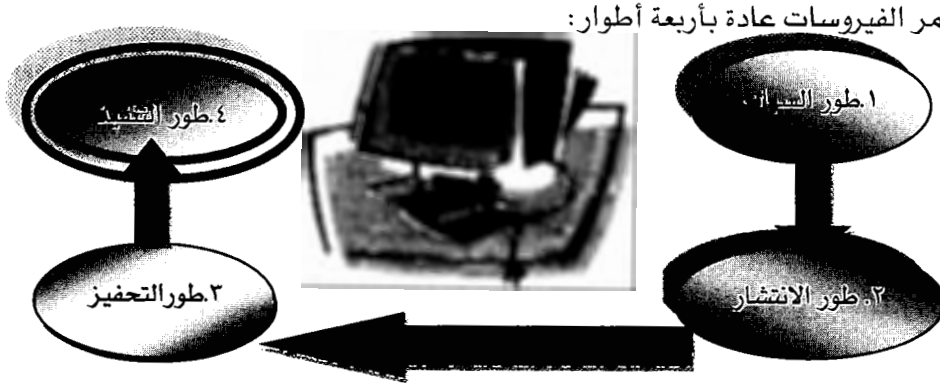
أسباب التسمية:

سمي الفيروس (Virus) بهذا الاسم لأنها تشبه تلك الكائنات المتطفلة في صفتين رئيسيتين:

أولا: فالفيروسات دائما تتستر خلف ملف آخر، ولكنها تأخذ زمام السيطرة على البرنامج المصاب. بحيث أنه حين يتم تشغيل البرنامج المصاب، يتم تشغيل الفيروس أيضا.

ثانيا: تتواجد الفيروسات في مكان أساسي في الحاسب كالذاكرة (Ram) مثلاً وتصيب أي ملف يشغل في أثناء وجودها بالذاكرة مما يزيد عدد الملفات المصابة كلما طال وقت اكتشاف الفيروس تستخدم عادة لغة التجميع (Assembly) لكتابة كود تنفيذ الفيروس.

تمر الفيروسات عادة بأربعة أطوار:



- طور السبات هو: الجزء الذي يخفي الفيروس عن الاكتشاف.
- طور الإنتشار هو: الجزء الذي يسمح للفيروس أن ينسخ نفسه.
- طور التحفيز هو: وهو الجزء الذي يسمح للفيروس بالانتشار قبل أن يعرف بوجوده كإستخدام توقيت الساعة في الحاسوب كما في فيروس (Michelangelo) الذي ينشط في السادس من آذار من كل عام.
- طور التنفيذ هو: وهو الجزء الذي ينفذ الفيروس عندما يتم تنشيطه.

طرق انتقال الفيروسات (العدوى):

يمكن أن نميز فئتين من فيروسات الحاسوب تبعاً لآلية العدوى وانتشار الفيروس:-

١. فيروس العدوى المباشر Direct Infection :

وذلك عندما يتم تنفيذ برنامج مصاب بفيروس من هذا النوع، فإن ذلك الفيروس يبحث بنشاط عن ملف أو أكثر لينقل العدوى إليه، وعندما يصاب أحد الملفات بالعدوى فإنه يقوم بتحميله إلى الذاكرة وتشغيله، وهذا النوع قليل الانتشار.

٢. فيروس العدوى غير المباشرة Indirect Infection:

عندما يتم تنفيذ برنامج مصاب بفيروس من هذا النوع، فإن ذلك الفيروس سينتقل إلى ذاكرة الحاسوب ويستقر فيها، ويتم تنفيذ البرنامج الأصلي ثم يصيب الفيروس بالعدوى كل برنامج يتم تحميله إلى الذاكرة بعد ذلك، إلى أن يتم قطع التغذية الكهربائية عن الحاسوب أو إعادة تشغيله.

تقسيم الفيروسات:

١- فيروسات تعمل عند بدء التشغيل

يحتاج الكمبيوتر عند تشغيله إلى تعليمات خاصة داخلية لمعرفة مكونات الجهاز، وهي توجد عادة في ملفات تدعى ملفات النظام (System Files)، التي تحتوي على البرامج الخاصة ببدء التشغيل ويقوم هذا النوع من الفيروسات بالتسلل إلى القطاع الخاص ببرنامج الإقلاع على القرص (Boot Sector)، وإتلاف محتوياته والعبث بها، مما يؤدي إلى تعطل عملية الإقلاع.

٢- فيروسات الملفات

يهاجم هذا النوع نظام التشغيل، وأي برامج أخرى موجودة على الكمبيوتر، كالتطبيقات المكتبية والألعاب وغيرها، ويعمل على العبث بمحتويات الملفات التي تنتهي بامتداد (Exe/Bin/Sys/Com) وتدميرها.

٣- فيروسات الماكرو

تصيب هذه الفيروسات برامج التطبيقات المكتبية مثل مايكروسوفت وورد أو اكسل. وهي من أكثر أنواع الفيروسات انتشاراً واستخداماً في عمليات التسلل إلى كمبيوترك عبر التطبيقات.

٤- الفيروسات متعددة الملفات

تنسخ هذه الفيروسات نفسها في صيغة أولية ثم تتحول إلى صيغ أخرى لتصيب ملفات أخرى.

٥- الفيروسات الخفية الأشباح

وهذه فيروسات مخادعة.. إذ أنها تختبئ في الذاكرة ثم تتصدى لطلب تشخيص وفحص قطاع التشغيل، ثم ترسل تقرير مزيف إلى السجل بأن القطاع غير مصاب.

٦- الفيروسات متعددة القدرة التحوليّة

وهذه الفيروسات لها القدرة الديناميكية على التحول وتغيير الشفرات عند الانتقال من ملف إلى آخر، لكي يصعب اكتشافها. توجد عدة تقسيمات للفيروسات، فمثلا من حيث سرعة الانتشار، هناك فيروسات سريعة الانتشار وفيروسات بطيئة الانتشار ومن حيث توقيت النشاط فهناك فيروسات تنشط في أوقات محددة وفيروسات دائمة النشاط ومن حيث مكان الإصابة تعتبر فيروسات مقطع التشغيل boot sector على الأقراص هي الأكثر شيوعا، أما من حيث حجم الضرر فهناك الفيروسات المدمرة للأجهزة بالطبع لا توجد فيروسات خارقه بحيث أنها تدمر الأجهزة كما نسمع أحياناً (احترق المعالج بسبب الفيروس، تعطلت وحدة التغذية بسبب الفيروس، أو تلفت الشاشة بسبب الفيروس ،... الخ) ولكن يمكن للفيروس أن يؤذي الذاكرة روم في الحاسب كما في فيروس تشرنوبيل أو أن يمحي المعلومات الرئيسية على مقطع التشغيل (Main Boot Sector – MBR) على القرص الصلب فتعود الأقراص الصلبة كما أتت من المصنع وفي الحالتين السابقتين لا يتم إقلاع الجهاز مما يوحي للبعض أن الفيروس (حرق) الحاسب، طبعا هذه الفيروسات تعتبر خطيرة جدا لأنها تتسبب في إتلاف البيانات المخزنة والتي قد تكون (البيانات) نتاج عشرات السنين مما تؤدي إلى خسائر جسيمة أو إلى توقف الحاسبات عن العمل كما في تشرنوبيل مما تؤدي إلى توقف الخدمات المقدمة، وهنالك أيضا الفيروسات المدمرة للبرامج وتأثيرها محدود طالما أن البيانات لم تتأثر حيث يمكن تخزين البيانات وإعادة تهيئة الحاسب وإعادة البرامج المتضررة من أقراصها الاصليه، والفيروسات عديمة الضرر وهي التي لا تقوم بأي عمل مؤذي وإنما تمت برمجتها لإثبات الذات والقدرة على البرمجة من بعض المراهقين فمنها ما يرسم كرة أو أي شكل على الشاشة طوال فترة عمل الكمبيوتر ومنها ما يغير بعض الأحرف (كتغيير حرف بحرف أينما وجد) أو تغيير مؤشر الماوس.. الخ.

٧- فيروس Brontok

الفيروس الذي يخفي خيارات المجلد أو يفقدك التحكم في الرجستري (Registry) فتصبح غير قادر على التحكم في الحاسوب، هذا الفيروس من ابرز مهامه انه يقوم بإخفاء خيارات المجلد من قائمة الأدوات الموجودة في نظام الويندوز وأيضاً يقوم بتكرار جميع المجلدات التي يصيبها حتى انك لاتعرف الأصل من النسخة وقد تحذف الأصل ظناً منك انه الفيروس، وهو أيضاً يقوم بفتح شاشة الإنترنت إكسبلورر ويقوم بفتح شاشة خضراء اللون بشكل مستمر مما يسبب بطء في النظام ومما يؤدي إلى زيادة انتشار هذا الفيروس في الكمبيوتر.

٨- فيروس xcopy :

الذي يصيب الـ Portion القسم للقرص الصلب ويجعله لايفتح مباشرة وذلك بزرع ملف auotorun وحينما تحاول فتح القسم يعطيك قائمة فتح بإستخدام ولا تستطيع الدخول إلى القسم الذي تريده إلا بطرق ملتوية مثل (استكشاف وتشغيل) للمحترفين فقط ويقوم أيضا بجعل الفلوبي دسك القرص المرن يطالب باستمرار بإدخال القرص المرن للكمبيوتر.

٩- فيروس Israeli :

ينتقل هذا الفيروس عن طريق أبواب العمليات المركزية (Processor Parts) إلى الاسطوانات الأخرى وتعتبر هذه الطريقة الأكثر صعوبة في الإخفاء والمقاومة، وقد هاجم هذا الفيروس في ١٩٨٨/٥/٣١، واحدة من أكبر شبكات الكمبيوتر في إسرائيل والتي تحتوي على أكثر من ١٠٠٠ جهاز كمبيوتر مرتبطة معا Network مسببه بطئاً وعدم كفاءة شديدين في عمل النظام، كما يقوم هذا الفيروس بإظهار عناوين المشتركين ويرسل رسائل على هذه العناوين الموجودة في كل رسالة يبعث نسخه منه أي رسالة حاملة للعدوى.

١٠- فيروس مايكل أنجلو Michelangelo :

هذا الفيروس ظهر في الفترة الأخيرة وسمى على اسم الفنان العالمي الكبير مايكل أنجلو وذلك لأنه يبدأ أماله التدميرية في يوم ٣/٦ المصادف ليوم ميلاد هذا

الفنان ويعتبر من البرامج الساكنة في الذاكرة تشمل تحطيم جدول تجزئة القرص (Partition Table) وقطاع بدء التشغيل (Boot Sector) ويمكن التغلب عليه عن طريق برنامج (Virus-scan) بشرط إستخدام نسخه حديثه منه .

١١- فيروس بلاستر Blaster :

ظهر هذا الفيروس في حزيران ٢٠٠٣ الذي اخترق مئات الآلاف من الحاسبات التي تتعامل مع برمجيات مايكروسوفت أوفيس ويعتبر من أخطر الفيروسات التي ظهرت لحد الآن ووقف عملها بشكل نهائي.

١٢- فيروس سوبيج أف:

ظهر هذا الفيروس في آب ٢٠٠٣ واقتحم مئات الآلاف من الحواسيب ويقوم بحقن برنامج في أجهزة الحواسيب المصابة ويعمل على فتح نظام النوافذ لإستخدامه في وقت لاحق لتوزيع كميات ضخمه من رسائل البريد الإلكتروني غير المطلوبة والإعلانات التجارية

١٣- فيروس Melissa:

انشأ الفيروس على شكل مستند Word ووضع في موقع للأخبار عندما يقوم أي شخص بتحميل الملف وفتحه فان الفيروس يتفاعل ويقوم بإرسال المستند إلى أول ٥٠ شخص في الAddress book والمستند يحتوي على ملاحظة لطيفة واسم الشخص المرسل إليه، وعندما يقوم المرسل إليه بفتح المستند يتم إرساله إلى ٥٠ شخص آخر وبهذه الطريقة أصبح فيروس Melissa أسرع فيروس في الانتشار.

١٤- فيروس I love you:

استخدم هذا الفيروس الطريق نفسها كما Melissa لكن عوضاً عن نسخ نفسه تلقائيا فانه يقوم بربط كوده برابط معين ضمن الرسالة وعند النقر عليه يقوم بإرسال نفسه إلى جميع العناوين الموجودة في الAddress book، واستخدم الفيروس ميزة الـ (Visual Basic Application- VBA) وهي لغة برمجة كاملة وتستطيع من خلالها أن تبرمج أي شيء مثل تعديل ملف أو إرسال الرسائل

الإلكترونية أي يمكنك كتابة أي برنامج وعند فتح المستند يتم تنفيذه طبعا وهي ميزة مفيدة ولكنها في نفس الوقت ميزة تنفيذ تلقائية خطيرة.

تصنيف الفيروسات حسب منطقة الإصابة:

يمكن تقسيم الفيروسات في فئتين وفقاً للمنطقة التي يصيبها الفيروس وهما:-

١. فيروسات قطاع بدء التشغيل Boot Sector Viruses

يمكن لهذا النوع أن يسبب العدوى إذا تم بدء التشغيل انطلاقاً من القرص المصاب، ولايتحتم أن يكون ذلك القرص هو قرص نظام System Disk . ولأن المساحة التي يحتلها برنامج بدء التشغيل Boot Program صغيرة جداً فإن برنامج الفيروس يتعمد إلى نقلة إلى مكان آخر على القرص ويحل محله ليضمن لنفسه أولوية التنفيذ . كمثال فإن فيروس STONED يضع برنامج بدء التشغيل القديم في نهاية فهرس الملفات وبالتالي لا تمكن ملاحظته حتى يصل عدد الملفات على القرص العدد الأعظم المسموح، بينما يحتل فيروس YALE القطاعات الأخيرة من المسار الأخير على القرص ولا تستطيع ملاحظته إلا عندما يمتلئ القرص بالكامل أما فيروس DEN ZUCK فإنه يهيئ مساراً إضافياً يختبئ فيه خارج المنطقة المعتادة على القرص وبالتالي تتعذر ملاحظته بالطرق العادية، بينما تبحث بعض الفيروسات عن مكان فارغ على القرص وتحشر نفسها فيه ثم تحدده بعلامة عدم الصلاحية للتخزين BAD SECTORS

٢. فيروسات البرامج Program Viruses

يقوم هذا النوع من الفيروسات بلصق نفسه بالملفات التنفيذية من نوع COM أو EXE أو BAT أو SYS وغيرها، وتكون العدوى بهذا النوع فعالة وسريعة وفيروسات هذا النوع أكثر تنوعاً من فيروسات قطاع بدء التشغيل إلا أنها أقل انتشاراً. ويمكن تصنيف فيروسات البرامج في أربع مجموعات هي:-

- الفيروسات المتطفلة Parasitic Viruses

وهي الفيروسات التي تلصق نفسها بالملفات لكي تتكاثر ويبقى الملف

نفسه بحالة سليمة في الغالب لأنها تضيف نفسها إما في بداية الملف Prepending Virus أو في نهايته Appending Virus والملفات من نوع COM يتم تحميلها للذاكرة ويبدأ تنفيذها عند أول أمر في البرامج لذا فإن الفيروسات التي تستهدفها تقوم بوضع نفسها قبل بداية البرنامج وعندما يتم تشغيل البرنامج فإن الفيروس ينفذ أولا.

أما الملفات من نوع EXE ففيها جزء يسمى المقدمة Header في بداية الملف الذي يحدد حجم البرنامج وعدد الأقسام المستخدمة وطريقة ربطها معاً والمكان الذي سيبدأ التنفيذ عنده، لذا فإن الفيروسات التي تستهدفها تقوم بحفظ المحتوى الأصلي لهذه المقدمة وتنسخ نفسها في نهاية الملف وتعدل المقدمة لتضمن تحميل الفيروس كقسم من الملف وتنفيذه أولاً .

وتوجد حالة نادرة هي للفيروس COMMAND BOMBER الذي يبحث عن مساحات فارغة ضمن الملف المستهدف ويخزن نفسه في عدة مناطق متفرقة من الملف.

- الفيروسات المرافقة Companion Viruses

تعتمد هذه الفيروسات على قاعدة الأسبقية في التنفيذ، فعند وجود ملفين تنفيذيين من نوع COM و EXE لهما نفس الاسم فإن الملف COM هو الذي سينفذ أولاً إذا لم يذكر امتداد الملف عند طلب تنفيذه، وتتمكن من نقل العدوى بدون تغير طول الملف عند خلق ملف جديد له نفس الاسم ولكن بامتداد COM وعند تنفيذ الملف المصاب يقوم الفيروس بالبحث عن ملف EXE جديد وإصابته ثم يحمل الملف المطلوب كما في فيروس AIDS II، وكذلك يمكنها إصابة الملفات الدفعية BAT بخلق ملفات مرافقة من نوع (COM OR EXE).

- الفيروسات الرابطة Linking Viruses

تصيب هذه الفيروسات البرامج بتغير المعلومات في جدول مواقع الملفات بحيث تبدأ كل البرامج المصابة من نفس الموقع وهو عادة وحدة التخزين الأخيرة Cluster في القرص والتي تتضمن نص الفيروس مما يضمن للفيروس انتشاراً سريعاً كما في فيروس DIRII .

- الفيروسات المستبدلة Replacement Viruses

تقوم بالكتابة فوق جزء من البرنامج بدون تغير حجم الملف، مما يؤدي إلى فشل البرنامج عند تنفيذه . كما في فيروس BURGER 405 .

- فيروسات الماكرو Macro Viruses

تصيب هذه الفيروسات الملفات والوثائق المكتوبة تطبيقات الكمبيوتر التي تتضمن لغات ماكرو مثل مايكروسوفت وورد وإكسيل ففي معالج النصوص WORDينتقل الفيروس الماكرو من وثيقة مصابة عند فتحها ضمن البرنامج ويصيب القالب الرئيسيNORMAL DOT وبعدها ينتقل إلى جميع الوثائق التي يتم فتحها أو إنشاؤها . وأول فيروسات هذا النوع هو فيروس CONCEPTأما في برنامج Excel فينتقل الفيروس من جدول مصاب عند فتحه ويصيب القالب الرئيسي للبرنامج PERSONAL. XLSوبعدها ينتقل ليصيب الملفات بنفس الطريقة، وأول فيروسات هذا النوع هو فيروس LAROUX.

تصنيف الفيروسات حسب خطورته[1]:

١. العادي Trivial : لا يفعل الفيروس العادي شيئا سوى التكاثرreplication ولا يسبب أي ضرر أو تخريب للمعلومات مثل فيروس stupid
٢. الثانوي Minor: يصيب الملفات التنفيذية فقط executable files ولا يؤثر على البيانات.
٣. المعتدل Moderate : يقوم بتدمير جميع الملفات الموجودة على القرص بطريقتين إما باستبدال المعلومات بمعلومات لا معنى لها، أو عن طريق إعادة التهيئة Reformatting مثل فيروس Disk killer الذي يقوم بإعادة تهيئة القرص. ويمكن حل مشكلة هذه الفيروسات عن طريق إستخدام النسخ الاحتياطي.
٤. الرئيسي Major : يؤدي الفيروس ذو الضرر الرئيسي إلى تخريب المعلومات بشكل تدريجي وبطيء عبر فترة من الزمن كنسخ رسالة معينة أو تشكيل رمز

1 - عبد الحميد بسيوني، الكتاب الأسود عن فيروسات الحاسوب، دار الكتب العلمية، ٢٠٠٧، القاهرة.

من الرموز في الملفات وبشكل عشوائي، وبالرغم من أن هذا التخريب قد يجد طريقة للنسخ الاحتياطية إلا أنه مرئياً بسهولة بعد تشخيص و معرفة الإصابة مما يمكن من تحديد الملفات المتضررة ويسهل إصلاحها كما في فيروس RIPPER الذي يتسبب في واحدة من كل ألف عملية كتابة على القرص تسجيل المعلومات بشكل خاطئ مما يؤدي إلى تخريب تدريجي للنظام.

٥. الشديد SEVERE: يتمكن الفيروس ذو الخطر الشديد من إحداث تغيرات ذكية وبارعة للبيانات دون أن يترك أثراً يشير إلى التغير الحاصل، كأن يقوم بشكل عشوائي بمبادلة كتل من المعلومات المتماثلة في الطول بين بعض الملفات وإذا تأخر اكتشاف الإصابة به أكثر من بعضة أيام فإن هذا النوع من الضرر يستحيل إزالته لأن المعلومات الأصلية لن تكون موجودة في ذلك الوقت ولأن الضرر قد أستمر لفترة زمنية قبل تشخيص الفيروس فإن النسخ الاحتياطية ستكون مخربة على الغالب ولا يمكن الوثوق بها.

٦. اللا محدود Unlimited : تستهدف هذه الفيروسات الشبكات والملفات المشتركة وقد تمضي هذه الفيروسات وقتاً طويلاً لمعرفة كلمات السر للمستخدمين الأكثر فاعلية ثم تقوم بتمريرها إلى أكثر عدد ممكن من مستخدمين الشبكة أملاً منها بأن يتم استخدام هذه الكلمات لإغراض سيئة.

أنواع الملفات التي يمكن أن يصيبها الفيروس:

١. الملفات ذاتية التنفيذ مثل ملفات ذات امتداد (EXE , COM) ضمن أنظمة التشغيل دوس وميكروسوفت ويندوز .

٢. أو (ELF) في أنظمة لينكس .

٣. سجلات الملفات والبيانات (VOLUME BOOT RECORD) في الأقراص المرنة والصلبة والسجل رقم (٠) في القرص الصلب MASTER BOOT .

٤. ملفات الأغراض العامة مثل ملفات الباتش والسكريبت في ويندوز وملفات الشل في يونيكس .

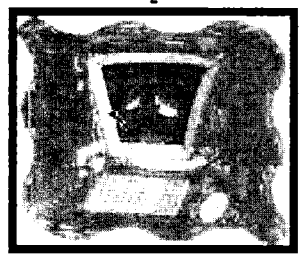
٥. ملفات الإستخدام المكتبي في النوافذ (WINDOWS) التي تحتوي ماكرو مثل الوورد والأكسل وأكسس.

٦. قواعد البيانات وملفات out look لها دور كبير في الإصابة ونشر الإصابة لغيرها ما تحويه من عناوين البريد الإلكتروني .

٧. ملفات الأكروبات (PDF) وبعض النصوص المهجنة (HTML) احتمال احتوائها على كود خبيث.

أعراض الإصابة:

كيف تعرف بأن جهازك مصاب بفيروس ما ؟ بما أن بعض الفيروسات يصعب اكتشافها فهناك بعض الأعراض التي قد تصيب الجهاز قد تنبهك إلى أن هناك فيروس ما في احد الملفات المذكورة أعلاه وهذه الأعراض هي:



- تكرار رسائل ا لخطأ في أكثر من برنامج.
- ظهور رسالة تعذر الحفظ لعدم كفاية المساحة.
- تكرار اختفاء بعض الملفات التنفيذية.
- حدوث بطء شديد في إقلاع نظام التشغيل أو تنفيذ بعض التطبيقات ورفض بعض التطبيقات للتنفيذ. فعند تشغيل البرنامج المصاب فانه قد يصيب باقي الملفات الموجودة معه في القرص الصلب أو المرن، لذا يحتاج الفيروس إلى تدخل من جانب المستخدم كي ينتشر، بطبيعة الحال التدخل عبارة عن تشغيله بعد أن تم جلبه من الايميل أو الإنترنت أو تبادل الأقراص المرنة.
- تعمل الفيروسات بطبيعتها على تعطيل عمل الحاسوب أو تدمير ملفاته وبرامجه وهناك فيروسات تعمل على خلق رسائل مزعجة وأنواع تعمل على تشغيل برامج غير مطلوبة وأنواع تعمل على إشغال المعالج بحيث تبطئ سرعة الحاسوب أو سرقة بيانات من حاسوب المستخدم مثل أرقام حسابات وكلمات السر أو أرقام

بطاقات الائتمان وبيانات مهمة أخرى وهذه أهم أهداف الفيروسات الحديثة وبرامج التجسس التي يتم تطويرها يوما بعد يوم.

كيفية الوقاية من الفيروسات:

الوقاية من الفيروسات تشمل عددا من الإجراءات التي يجب إتباعها وهذه الإجراءات كما وضحها الدكتور علاء السالمي بكتابة شبكات الإدارة الإلكترونية، ٢٠٠٥ هي كما يلي[1]:

١. يجب شراء البرامج الأصلية مغلفة بغلاف الشركة المنتجة تغليفا محكما والتأكد من أن البائع لدية سمعة جيده حيث أن ليست جميع البرامج المغلفة هي جيده ومضمونة.
٢. عند الحصول على أي برنامج جديد يجب تثبيت شريط الحماية بالنسبة للأقراص (٥,٢٥) بوصة أو فتح بوابة الحماية (write protect Door) للأقراص (٣,٥) بوصة لحماية القرص الاحتياطي أيضا.
٣. عند تحميل البرنامج على القرص الصلب يجب أن يتم التحميل من القرص الأصلي للبرنامج.
٤. يجب مقارنة الملفات المخزنة على القرص الأصلي بنفس الملفات المخزنة على القرص الاحتياطي (Backup) وعند ملاحظة أي اختلاف يصبح هناك شك في وجود فيروس (تتم المقارنة بإستخدام الأمر Disk comp أو الأمر Comp في نظام التشغيل.
٥. يجب اختبار كل برنامج موجود على القرص والتأكد من أنه يؤدي وظائفه بصورة طبيعية وملاحظة أي أشياء غريبة قد تحدث من أي برنامج.
٦. يمكن اختيار البرامج للبحث عن سلاسل حرفية معينه Strings ترتبط بوجود أنواع معينة من الفيروسات مثل الحروف.

---

1 - د. علاء السالمي، شبكات الإدارة الإلكترونية، دار وائل للنشر، عمان، الأردن، ٢٠٠٥.

ديدان الإنترنت (worm):

ما هي ديدان الإنترنت :-

هي مثلها مثل الفيروس وهي عبارة عن برنامج صغير مكتوب بأحد لغات الحاسب مصمم على أن يقوم بإعادة كتابة نفسه على الملفات الموجودة على الحاسب أو أي حاسب آخر ولكنها متميزة بكونها ترسل نفسها منفردة إلى قائمة البريد الإلكتروني أو إلى كل جهاز بالشبكة وهى تنتشر بسرعة هائلة.

فعند إصابة الجهاز يبحث البرنامج الخبيث عن عناوين الأشخاص المسجلين في دفتر العناوين على سبيل المثال ويرسل نفسه إلى كل شخص وهكذا... مما يؤدي إلى انتشاره بسرعة عبر الشبكة وقد اختلف الخبراء فمنهم اعتبره فيروس ومنهم من اعتبره برنامج خبيث وذلك كون الدودة لا تنفذ أي عمل مؤذي إنما تنتشر فقط مما يؤدي إلى أشغال موارد الشبكة بشكل كبير ومع التطور الحاصل في ميدان الحوسبة أصبح بإمكان المبرمجين الخبيثين إضافة سطر برمجي لملف الدودة بحيث تؤدي عمل معين بعد انتشارها (مثلا بعد الانتشار إلى عدد ٥٠٠٠٠ جهاز يتم تخريب الأنظمة في هذه الأجهزة) أو أي شيء آخر (مثلا في يوم معين أو ساعة أو تاريخ...الخ) وأصبحت الديدان من أشهر الفيروسات على الشبكة العالمية وأشهر عملياتها التخريبية وأخطرها تلك التي يكون هدفها حجب الخدمة تسمى (هجمات حجب الخدمة) حيث تنتشر الدودة على عدد كبير من الأجهزة ثم توجه طلبات وهميه لجهاز خادم معين (يكون المبرمج قد حدد الخادم المستهدف من خلال برمجته للدودة) فيغرق الخادم بكثرة الطلبات الوهمية ولا يستطيع معالجتها جميعا مما

يسبب توقفه عن العمل وهذه الديدان استهدفت مواقع لكثير من الشركات العالمية أشهرها مايكروسوفت وغيرها الكثير.

برنامج دودي (اسم) فئة فرعية من الفيروس. ينتشر البرنامج الدودي عادة بدون تدخل من المستخدم ويقوم بتوزيع نسخ كاملة (وربما معدّلة) عن نفسه عبر الشبكات. قد يستهلك البرنامج الدودي الذاكرة أو النطاق الترددي للشبكة، مما قد يؤدي إلى تعطيل الكمبيوتر.

ولأن البرامج الدودية لا تحتاج إلى التنقل بواسطة برنامج أو ملف "مضيف"، فبإمكانها أيضا الوصول عبر أسلوب النفق إلى النظام والسماح لشخص آخر بالتحكم بالكمبيوتر عن بُعد. تتضمن الأمثلة الحديثة على البرامج الدودية كل من البرنامج الدودي Sasser والبرنامج الدودي Blaster.

من أين تأتى:-

- من خلال الرسائل الإلكترونية .
- صفحات الإنترنت "HTTP".
- نسخ البرامج المقلدة.
- الأقراص المرنة والأقراص الضوئية.

ما هو التأثير:-

- زيادة عدد العمليات التي تتم إلى ملاين العمليات فيتوقف الحاسب عن العمل.
- التحميل الزائد على الشبكة مما قد يبطئ العمل عليها تماما.
- إحداث البطء الشديد في الإنترنت داخل المنشاة أو على الحاسب الشخصي.

آلية عملها :

تصيب الدودة الكمبيوترات الموصلة بالشبكة بشكل أوتوماتيكي، ومن غير تدخل الإنسان وهذا الأمر يجعلها تنتشر بشكل أوسع وأسرع عن الفيروسات. الفرق بينهم هو أن الديدان لا تقوم بحذف أو تغيير الملفات بل تقوم بتهليك موارد الجهاز وإستخدام الذاكرة بشكل فظيع مما يؤدي إلى بطء ملحوظ جدًا للجهاز.

تختلف الديدان في عملها من نوع لآخر، فبعضها يقوم بالتناسخ داخل الجهاز إلى أعداد هائلة، بينما نجد بعضها يتخصص في البريد الإلكتروني بحيث تقوم بإرسال نفسها برسائل إلى جميع الموجودين بدفتر العناوين، بل إن البعض منها يقوم بإرسال رسائل قذرة لعددٍ عشوائي من المقيدين بسجل العناوين باسم مالك البريد مما يوقعه بالكثير من الحرج.""

أنواعها:

- ديدان البريد

وتكون مرفقة في محتوى الرسالة وأغلب الأنواع من هذه الديدان تتطلب من المستخدم أن يقوم بفتح الملف المرفق لكي تصيب الجهاز وأنواع أخرى تكون تحتوي على رابط خارجي وبعد أن تصيب الجهاز تقوم بإرسال نسخ منها إلى جميع المضافين في القائمة البريدية باستعمال برتوكول SMTP.

- ديدان المراسلة الفورية

وهذا النوع من الديدان يقوم بإستخدام أحد برامج المراسلة الفورية للانتشار وذلك عن طريق إرسال الرسائل إلى جميع المتواجدين.

- ديدان أي أر سي (IRC)

وتقوم بالانتشار عن طريق نسخ نفسها في القنوات في حالة الدردشة باستعمال بروتوكول أي أر سي وإرسال روابط إلى العنوان المصاب بالدودة.

- ديدان برامج مشاركة الملفات

وتنتشر عن طريق وضع نفسها قي مجلدات المشاركة حتى تنتشر بين المستخدمين الآخرين في حالة تحميل الملفات عن طريق برنامج بيتلورد.

- ديدان الإنترنت

وتقوم بالانتقال عن طريق بروتوكول tcp/ip مباشرة دون الحاجة إلى مستوى أعلى مثل البريد الإلكتروني أو برامج تشارك ملفات، ومن الامثلة عليها هو دودة بلاستر التي تقوم عشوائيا بالانتشار عن طريق البحث عن عناوين يكون المنفذ رقم ١٣٥ مفتوحا لتقوم باستغلاله وإصابة جهاز الضحية

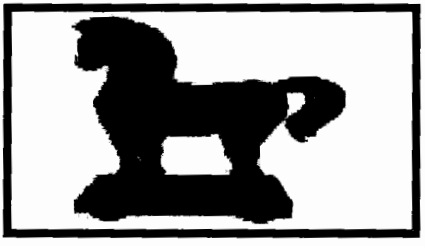
- ديدان My Doom

قدر الخبراء الحواسيب المتضررة من هذه الدودة بحوالي ربع مليون حاسوب خلال يوم واحد والذي كان في كانون الثاني ٢٠٠٤.

سبل الوقاية منها :

من المعلوم أن أشهر وسائل انتشار الديدان هو عن طريق الرسائل الإلكترونية المفخخة، والتي عادة ما تكون عناوين هذه الرسائل جذابا كدعوة لمشاهدة صور احد النجوم أو المشاهير، لذلك يجب الحذر حتى وان كانت الرسائل من مصدر معروف لأن بعض الديدان تقوم بإرسال نفسها من أي بريد لجميع الايميلات المضافة بدفتر العناوين فلذا فلتكن حذراً ولا تفتح أي رسالة إلا بعد التأكد تماما من أنها خاليه من أي ضرر. وأيضاً، فإنه من المهم تحديث نسخ النظام المستخدم في الجهاز كي يتم تجنب الديدان.

أحصنة طروادة (Trojan horse):



ماهى أحصنة طروادة:

سمي هذا الفيروس بحصان طروادة لأنه يذكر بالقصة الشهيرة لحصان طروادة حيث اختبأ الجنود اليونان داخله واستطاعوا اقتحام مدينة طروادة والتغلب على

جيشها وهكذا تكون آلية عمل هذا الفيروس حيث يكون مرفقا مع أحد البرامج أي يكون جزء من برنامج دون أن يعلم المستخدم وعندما يبدأ البرنامج بتنفيذ عمله ويصل إلى مرحلة ما ومثال على ذلك عندما تم توزيع قرص مجاني على المشافي به برنامج حول مرض الايدز (أسبابه - طرق انتشاره طرق العلاج.. الخ) وبعد مدة شهر من تشغيل البرنامج تم تشفير المعلومات على الحواسيب الحاضنة للفيروس وظهرت رسالة مفادها إن الحاسب مصاب بالايدز (المقصود هنا أنه تم تشفير ملفات الحاسب وإيقافها عن العمل بطريقه نظاميه) وعليك أن ترسل مبلغ كذا إلى الحساب كذا ليتم إرسال رقم فك الشيفره مما أجبر المختصين بالرضوخ للطلب كونهم لم يستطيعوا فك التشفير.

من أين تأتي:

١. تأتى غالبا مع الرسائل الإلكترونية المرفق معها ملفات قابلة للتشغيل لذا لا تفتح اى ملف مرفق مع الرسائل الإلكترونية إذا كانت ملفات قابلة للتشغيل.
٢. تأتى أيضا عند تحميلك للبرامج المجانية الموجودة على الإنترنت لذا لا تحمل اى برنامج مجاني من الإنترنت إذا كنت لا تعرف وتثق في الموقع الموجود عليه هذا البرنامج.

ما هو التأثير:

- يقوم بإلغاء الملفات.
- يرسل رسائل مزيفة منك إلى الموجودين في قائمة البريد الإلكتروني.
- يفتح الحماية الخاصة بك لمخترقي الحاسوب.

الجافا والجافا سكربت:

ماهي الجافا سكربت؟

الجافا عبارة عن لغة برمجة كينونية مشتقة من لغة سي بلس بلس، ولكنها تمتاز عن اللغات الأخرى بأنها تمكنك من كتابة برنامج مرة واحدة فقط ومن ثم تستطيع أن تشغل البرنامج على أي جهاز كمبيوتر آخر، حتى إذا كان من نوع آخر أو يعمل على نظام تشغيل مختلف، بدون الحاجة لإعادة تركيب البرنامج.

وهي تنتمي لفئة البرمجة الشيئية object-oriented language (OOD) و تعتبر من اللغات المميزة حيث ساهمت في نشر التطبيقات على الإنترنت ، وذلك لأنها آمنة وقوية.

ولا شك بأن من أخطر الأكواد التي يمكنها تنفيذ أوامر محددة بجهاز المستخدم من خلال صفحات الويب هي اكواد الجافا وقد وصل الأمر أن أحد أكواد الجافا الشهيرة كانت السبب الرئيسي في تطوير ميكروسوفت لإصدارها من الويندوز مسنجر من الإصدار ٤,٧ إلى الإصدار الخامس حيث يقوم كود الجافا بمجرد قيامك بفتحة صفحة الويب تتضمنه بإرسال كافة قائمة الأصدقاء الموجودين بمسنجرك لبريد الهاكرز خلال ثواني معدودة ولذلك ينصح دائما بأنه في حالة عدم احتياج صفحات الويب لدعم الجافا أن يتم عدم تفعيل تلك الخاصية من خيارات الإنترنت بالمتصفح.

تنقسم البرامج في لغة java إلى قسمين :

١. برامج التطبيقات: وهذا القسم من البرامج شبيه ببرامج لغة C ويمكن تنفيذها على نفس OS (نظام التشغيل)الذي يعمل عليه الشخص.
٢. البرمجيات: و هي عبارة عن برامج صغيرة تستطيع أن تنتقل عبر صفحات الإنترنت و يتم تنفيذها بواسطة الشخص الذي يستخدم تلك الصفحة بواسطة المستكشف أو المستعرض مثل:
   ١. Internet Explorer
   ٢. Mozilla Firefox
   ٣. Avant Browser

   لذلك فهي آمنة ،لأنها تنفذ عن طريق برنامج موجود في الصفحة.

هنالك ثلاثة مستويات من جافا :

١) Java 2 Standard Edition (J2SE): النسخة الرئيسة من جافا، و تستخدم عادة لكتابة برامج للكمبيوتر الشخصي.

٢) Java 2 Enterprise Edition (J2EE): النسخة الأكبر من جافا. تشمل النسخة الرئيسة. تستخدم عادة لكتابة برامج كبيرة للشركات أو لكتابة مواقع الإنترنت.

٣) Java 2 Micro Edition (J2ME): النسخة الأصغر من جافا، و تستخدم لكتابة برامج للأجهزة الصغيرة مثل الهواتف النقالة و المساعدات الشخصية الرقمية (PDA).

جميع هذه المستويات تتعامل مع نفس أسلوب البرمجة، و لكنها تختلف بشكل رئيسي من ناحية المكتبات الجاهزة (API) و بعض الأشياء الأخرى غير الأساسية.

نبذة عن تاريخ جافا:

في عام ١٩٩١ قامت شركة صن مايكروسيستمز (Sun Microsystems) بتمويل بحث لإنشاء لغة برمجة لتطوير الأدوات الإلكترونية الذكية، و كنتيجة لهذا البحث ظهرت لغة برمجة مبنية على لغة سي بلس بلس (C++) أطلق عليها مخترعها جيمس غوسلنغ (James Gosling) اسم أوك (Oak). و لكن بعد ذلك تم اكتشاف أن هنالك لغة برمجة تدعى أوك. لذا، و أثناء زيارة بعض موظفي شركة صن مايكروسيستمز مقهى محلي، تم اقتراح اسم جافا (Java) و تم اختياره.

في هذا الأثناء كان المشروع الذي بنيت هذه اللغة من اجله يواجه بعض الصعوبات، حيث أن سوق الإلكترونيات الذكية لم ينمو كما كان هو متوقع. ولكن شاءت الصدف أن الشبكة العنكبوتية (World Wide Web) بدأت بالانتشار في عام ١٩٩٣ و أدركت شركة صن فائدة جافا لإضافة المحتوى الحيوي (Dynamic Content) و الصور المتحركة (Animation) إلى صفحات الشبكة.

في شهر مايو عام ١٩٩٥ قامت شركة صن بالإعلان عن جافا رسمياً، و كان إقبال القطاع التكنولوجي و قطاع الأعمال عليها كبير بسبب الاهتمام الكبير بالشبكة العنكبوتية.

الآن، يمكنك أن تجد جافا في برامج للشركات، أو تجدها تحسن الصفحات على الإنترنت، أو في برامج للأجهزة الاستهلاكية مثل الهواتف النقالة وغيرها الكثير و تعتبر ال java من أقوى لغات البرمجة.

SPY Where & AD Where:

الوظيفة الأساسية لبرامج التجسس هي مراقبة وتسجيل جميع التحركات والأفعال التي تتم على جهاز الحاسوب،فبعد أن يتم تثبيت البرنامج على جهاز الكمبيوتر، يقوم البرنامج بإخفاء نفسه من النظام بحيث يصعب على المستخدم إكتشاف وجودة وعادة ما يتم ربط البرامج التجسسية بالبرامج التي تعرض الإعلانات، أو بالبرامج التي تتعقب المعلومات الشخصية أو الحساسة ولكن ذلك لا يعني أن كافة البرامج التي توفر الإعلانات أو تتعقب نشاطاتك عبر إنترنت هي سيئة، فمثلاً يشترك المستخدم بخدمة مجانية عن طريق الإنترنت، وللقيام بالاستفادة من هذه الخدمة يجب فهم الشروط والموافقة عليها والموافقة على تلقي إعلانات هادفة، فإذا وافق المستخدم على تلك الشروط ،تكون هناك عملية تبادل فتتعقب تلك الشركة التي تقدم الخدمة المجانية نشاط المستخدم عبر الإنترنت وذلك لتحديد الإعلانات التي ستعرضها على المستخدم.

وهناك أنواع أخرى من برامج التجسس، تُجري تغييرات على جهاز الكمبيوتر ونظام التشغيل فقد تتسبب بإبطاء الجهاز أو بتعطيله أو إيذاء نظام التشغيل، وتستطيع أيضا هذه البرامج تغيير الصفحة الرئيسية أو صفحة البحث لمستعرض ويب، أو إضافة مكونات إضافية إلى المستعرض لا تحتاج إليها أو لا ترغب فيها، كذلك،وقد تصعّب هذه البرامج عليك تغيير الإعدادات وإعادتها إلى ما كانت عليه في الأصل.

ومن الأمثلة على برامج التجسس هو برنامج متابعة تصرفات المستخدم Spyware.

برامج التجسس ليست مثل الفيروسات فهي تعرف على أنها أي برنامج يدخل على جهازك بدون إذن ويتخفى من غير علم المستخدم.

ثمة طرق عديدة تستطيع من خلالها برامج التجسس استغلال الجهاز، وتكمن إحدى الحيل الشائعة في تثبيت البرنامج بشكل سري، خلال تثبيت برنامج

آخر ترغب فيه وبإمكان برامج التجسس القيام بأمور عديدة عندما تتسلل إلى جهازك من سرقة معلومات إلى استنزاف طاقات الجهاز دون إذن واضح من المستخدم.
يجب على المستخدم التخطيط الجيد للحماية من برامج التجسس عن طريق :

١. تثبيت البرامج التي تستخدم لاكتشاف وإزالة البرامج التجسسية.
٢. قراءة اتفاقية الترخيص قبل تثبيت أي برنامج.
٣. تحديث نظام التشغيل والمتصفح.
٤. تثبيت برامج لمكافحة الفيروسات وجدار الحماية.

انتشرت العديد من البرامج التي تدعي أنها برامج مكافحة للتجسس، والتي هي في الأساس برامج مزيفة تعمل عل التجسس على جهاز المستخدم مثل Antivirus Gold.

أمثلة على برامج التجسس[1]:

١. برنامج متابعة تصرفات المستخدم أو التجسس البسيط Spyware

وهي برامج حاسوبية تثبت خلسة على أجهزة الحاسوب للتجسس على المستخدمين أو إتخاذ سيطرة جزئية على الكمبيوتر، وهذا من دون علم المستخدم.

وتلك البرامج يمكنها جمع مختلف المعلومات الشخصية، مثل تصفح الإنترنت، ورصد المواقع التي تمت زيارتها، ويمكن لها أن تسيطر على الحاسوب المصاب بها، وتتحكم به وتقوم بعدة مهام، مثل:تركيب برامج إضافية، إعادة توجيه مستعرض الويب لمواقع ويب ضارة والتي تتسبب في المزيد من الفيروسات، يمكن أيضا لبرامج التجسس أن تغير إعدادات الكمبيوتر، مما قد يؤدي إلى بطئه والتأثير على الاتصال بشبكة الإنترنت[2].

---

1 - نوف علي الشنيفي، البرامج التجسسية Spyware أنواعها وطرق الحماية منها، مركز التميز لأمن المعلومات- جامعة الملك سعود.

2 -www.wikipedia.org .

٢. برنامج راصد لوحة المفاتيح Key Loggers:

وهي برامج تقوم بتسجيل كل ما يكتب بلوحة المفاتيح عن طريق المستخدم، فتلك البرامج تقوم بتسجيل المواقع التي يكتبها المستخدم بواسطة المتصفح وملفات المستخدم والمحادثات المكتوبة وعناوين البريد الإلكتروني و كلمات السر وأرقام الهوية و أرقام البطاقات الائتمانية فكل ما يدخله المستخدم بواسطة لوحة المفاتيح يسجل عبره،وقد يتم نقل تلك المعلومات المسجلة عبر البرامج ليتم إرسالها لعنوان بريد إلكتروني محدد.

٣. برامج مراقبة الإنترنت Internet monitoring software:

تقوم تلك البرامج بمراقبة ما يفعله المستخدم عبر الإنترنت،فتسجل أسماء وعناوين المواقع التي يزورها المستخدم والوقت الذي يقضيه المستخدم متصفحاً هذا الموقع ،وأيضاً مراقبة البرامج التي يقوم المستخدم بتنزيلها ،وتسجيل رسائل البريد الإلكتروني ومع تطور وظهور أنواع جديدة وقوية لبرامج التجسس، بدأت برامج مراقبة الإنترنت بالاندثار وأصبحت ميزة من ميزات البرامج الإلكترونية الأخرى.

٤. برامج الإعلانات Adware:

تلك البرامج التي تهدف إلى جمع معلومات عن المستخدم لتقييم اهتماماته وتحديد نوع الإعلانات التي تعرضها على المستخدم،فهذه البرامج يتم تنزيلها عبر مواقع الإنترنت بدون انتباه من المستخدم فقد تُعرض على المستخدم رسالة تطلب منه الضغط على زر معين وعندما يضغط المستخدم الزر يتم تثبيت هذه البرامج،وعندما يتم تثبيت هذه البرامج تقوم بمراقبة المواقع التي يزورها المستخدم وتعرض على المستخدم الإعلانات التي تناسب اهتماماته بناءً على تلك المواقع التي يزورها، العديد من الخبراء يصنفون برامج الإعلانات ضمن برامج التجسس فهي برامج خارقة أمنياً(spyware) لأنها تقوم بجمع معلومات خصوصية عن المستخدم بدون علمه.

ومن الأمثلة على تلك البرامج:

١. تقديم إعلانات لمنتجات معيّنة بمجرد البحث عن مثيلاتها في محرك البحث.

٢. تعطيل محرك البحث وتقديم محرك بحث آخر مقلد ليخدم مهام الجهة الإعلامية لبرنامج الإعلانات.

٣. تحويل المستخدم إلى مواقع تجارية دون إذنه.

الفرق بين برامج التجسس والفيروسات:

الفيروسات :هي عبارة عن جزء من شيفرة أو رموز صممت لنسخ نفسها، من حاسوب مرتبط مع حاسوب آخر، وتتكاثر بالاعتماد على ملفات أخرى وعادة ما تنتقل بين الحواسيب بعدة طرق مسببة تدمير الملفات الشخصية أو حتى نظام التشغيل.

أما برامج التجسس من جهة أخرى فهي غير مصممة لتدمير الحاسوب فبرامج التجسس تعرف على أنها أي برنامج يدخل على جهازك بدون إذن، يتخفى و يتجسس على الجهاز وينقل معلومات عن الجهاز ونشاطات المستخدم التي تمت عبر هذا الجهاز، و قد تسبب برامج التجسس تغييرات غير مرغوب بها وليست متوقعة بالنسبة للمستخدم.

أهم الوسائل التي تقوم بها البرامج التجسسية للوصول إلى الحواسيب:

ثمة طرق عديدة تستطيع من خلالها برامج التجسس أو البرامج الأخرى غير المرغوب فيها للوصول إلى الكمبيوتر. تكمن إحدى الحيل الشائعة في تثبيت البرنامج بشكل سري، خلال تثبيت برنامج آخر يرغب المستخدم فيه، فيرتبط برنامج التجسس بذلك البرنامج الذي يرغب المستخدم بتنزيله مثل برنامج مشاركة ملفات الموسيقى أو الفيديو.

- الصفحات الانبثاقية (pop-up) وهي برامج انبثاقية تفاجئ المستخدم بالظهور كإعلانات أثناء تصفح الإنترنت، محاولة تحميل نفسها على الحواسيب ناقلة بذلك برامج تجسسية وتستهلك موارد النظام والاتصال، وتسبب مشاكل أمنية جرّاء الإخفاق في سد الثغرات الأمنية للحاسوب.

- برامج التجسس قد تعمل على خداع المستخدم ليقوم بتحميلها وذلك عن طريق إظهار تنبيهات زائفة تخص نظام التشغيل أو حتى عن طريق إجبار المستخدم الضغط على أزرار الإلغاء في حين أن هذه الأزرار هي بالفعل تقوم بعكس ذلك تماماً.

طرق معرفة الإصابة بها:

هناك عدة طرق للتعرف على الإصابة ببرامج التجسس والمراقبة، من أهمها:

١. كثرة الصفحات الانبثاقية والتي ليس لها صلة بالموقع المزار، مثل صفحات بصور إباحية.
٢. حاسوبك يحاول الاتصال بالهاتف دون أمرك. وهناك برامج تقوم بالاتصال عن طريق هاتفك ودون أمرك وعلمك بأرقام هواتف دولية باهظة التكلفة.
٣. يصبح حاسوبك بطيء الاستجابة لدرجة ملحوظة.
٤. عندما تقوم بالبحث فإن المتصفح يستخدم محركاً للبحث غير الذي حددته.
٥. قائمة المواقع المفضلة في برنامج متصفح الإنترنت يحتوي على مواقع لم تقم بإضافتها.
٦. صفحة البداية تشير إلى موقع لم تقم باختياره كصفحة بداية و يبقى كذلك حتى لو غيرت صفحة البداية.

طرق الوقاية:

هناك عدة طرق وقائية ضد برامج التجسس وغيرها من البرامج الضارة:

١. داوم على سد الثغرات الأمنية بمتابعة آخر التحديثات لبرامجك الحساسة مثل: نظام التشغيل، ومتصفح الإنترنت، وبرنامج البريد الإلكتروني.
٢. دعّم حاسوبك ببرنامج أو جهاز جدار الحماية لتقليل تعرّضه للاختراق من قبل الغير.
٣. دعّم حاسوبك ببرنامج مكافح الفيروسات.
٤. عند الحاجة لبرامج مجانية حمّلها من مواقع معروفة مثل www.download.com.
٥. اقرأ محتويات الاتفاقية الخاصة باستخدام البرامج، لأن بعضها تنص بوضوح بأن البرنامج سيقوم بمراقبة سلوكك وإرسال بيانات لجهة خارجية.

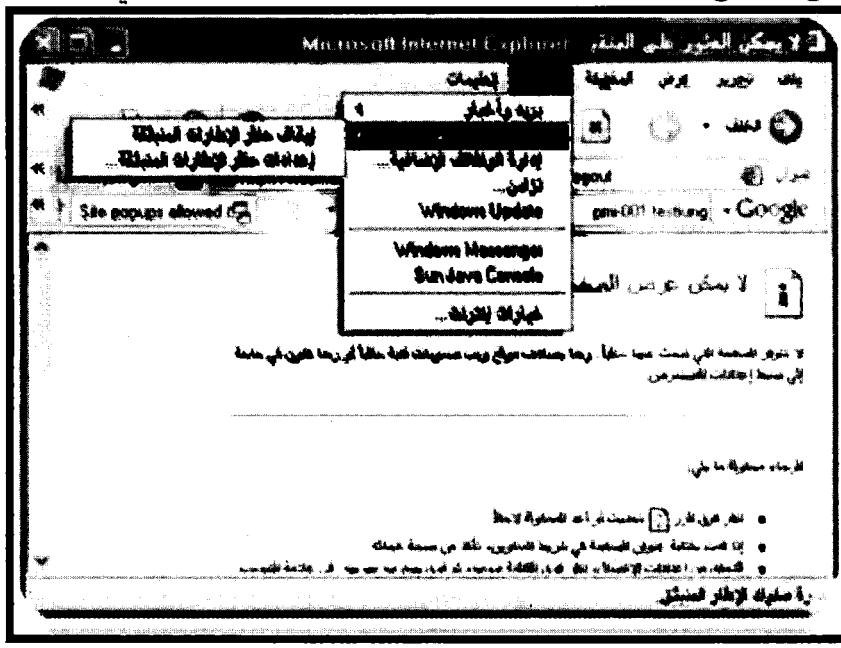
٦. تحاش زيارة المواقع المشبوهة مثل المواقع الإباحية، و مواقع القرصنة.

٧. تحاش برامج المشاركة P2P.

٨. تأكد من مرفقات رسائل البريد الإلكتروني، ولا تقم بفتحها حتى تتأكد من خلوها من الفيروسات، وأنها مرسلة من شخص موثوق به ومعروف ومتوقعة الوصول.

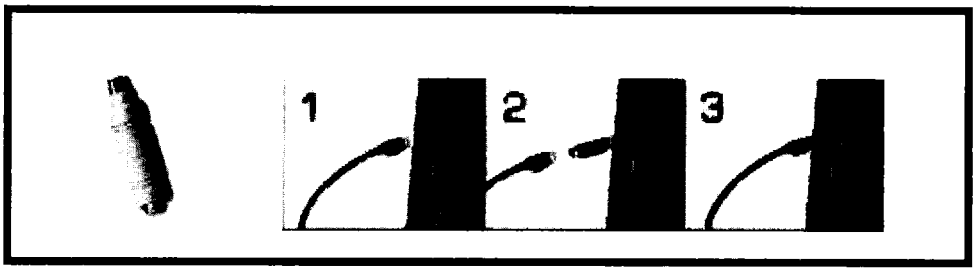
٩. تفحص حاسوبك بشكل دوري باستخدام برنامج مكافحة الفيروسات وبرنامج مكافحة برامج التجسس.

١٠. دعّم حاسوبك ببرنامج لمكافحة برامج التجسس والصفحات الفقاعية. وإذا كان حاسوبك مزوداً بالتحديث الجديد لنظام الويندوز اكس بي SP2 فيمكنك استخدام خاصية إيقاف الرسائل الفقاعية، ويمكن تفعيلها من برنامج متصفح الإنترنت تحت قائمة "أدوات" كما في الشكل التالي:

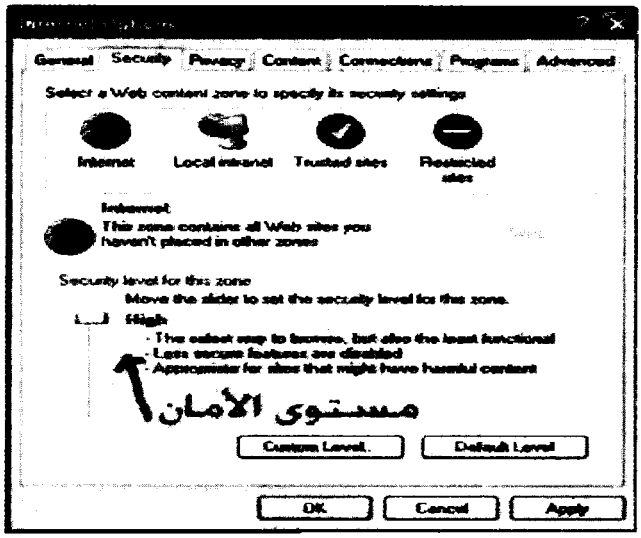


خاصية إيقاف الرسائل الفقاعية

١١. تأكد من أن نهاية سلك لوحة المفاتيح موصول بشكل مباشر للحاسوب ولا يوجد قطعة بينهما.



١٢. تأكد من أن مستوى الأمان في برنامج متصفح الإنترنت مرتفع كما في الشكل التالي.



مستوى الأمان في برنامج متصفح الإنترنت

Piggybacked

هي برامج مخاطبة الحاسوب بآخر أو برامج المشاركة التي يتم تحميلها والتي تقوم بتحميل برامج تجسسية، وإذا لم يتم قراءة تفاصيل التحميل بتمعن فإن المستخدم لن يلاحظ وجود مثل هذه الإضافات (التجسسية) على البرامج الأساسية والتي يرغب بتحميلها، وهذه توجد في البرامج المجانية كبديل للبرامج الأصلية الآمنة والتي تعود لمصادر موثوق بها والتي لها سعر فهي ليست مجانية.

- الإضافات التي تكون علي المتصفح تعطي هذه الإضافات التحسينات أو التعديلات المتصفح ومنها شريط أدوات إضافي، وصناديق البحث الإضافية. في

بعض الأحيان تقوم هذه البرامج بالتحسينات ولكن تتضمن على برامج تجسسية كجزء من عملها.

- البرامج التي تظهر بشكل برامج مضادة للتجسس تعتبر هذه البرامج من أخطر الحيل المستخدمة لتحميل البرامج التجسسية حيث تقوم هذه البرامج بالتخفي و إقناع المستخدم بأنها أداة تساعد على كشف وإزالة البرامج التجسسية.

ماذا يمكن أن تفعل برامج التجسس (spyware):

بإمكان برامج التجسس القيام بأمور عديدة عندما تتسلل إلى جهازك فبرنامج التجسس يعمل على انه برنامج مخفي يتم تشغيله عند تشغيل الجهاز بدون علم المستخدم.

فتقوم برامج التجسس بتشغيل برامج مختلقة كمتصفح الإنترنت أو عرض بعض الإعلانات بشكل مفاجئ وبغير تصرف من المستخدم، وقد تقوم بتغيير صفحة البداية لمتصفح الإنترنت أو تتحكم في محرك شبكة الإنترنت بحيث يجعل تحميل الصفحات بطيء أو تؤثر على عملية البحث في شبكة الإنترنت ونتيجة البحث، وأيضاً تقوم بالتسبب بإظهار مشاكل في الجهاز مثل عدم قدرة المستخدم الكتابة على القرص الصلب أو مشاكل في الذاكرة، وتستهلك موارد النظام و تستنزف طاقات الجهاز والاتصال دون إذن واضح من المستخدم، مما تجعل الجهاز بطيء نوعا ما.

ومن أهم وظائف برامج التجسس، التسلل والسرقة فتتسلل تلك البرامج إلى الحاسوب وتعمل مثل الجاسوس الحقيقي بحيث تتجسس على المستخدم وتعرف اسمه والرقم السري الخاص به و لها أدوات وطرق شبيهه بالفيروس أو لصوص الحاسوب فمثلا إن كان المستخدم من محبي التسوق واشتراك في مواقع البيع والشراء تقوم بعض المواقع بسرقة رقم بطاقة الإئتمان الخاصة بالمشتري و تسلب المستخدم كامل حقوقه وخصوصياته، وتتحكم في الجهاز من حيث السرعة والدقة والسعة.

طرق الحماية من البرامج التجسسية:

١. استخدام برامج خاصة للبحث عن البرامج التجسسية، هناك العديد من البرامج التي تستخدم لاكتشاف ولإزالة البرامج التجسسية ومن ضمنها Ad-aware Spybot, Microsoft Antispyware

٢. استخدم قفل مفاجئ، العديد من المتصفحات الحالية بما فيها Internet Explorer 6.0، Firefox 1.0 تتيح العديد من الخيارات لصد الانبثاقات من خلال خدمة Pop- Up Windows هذه الخدمة يمكن أن تبقى مفعلة طوال الوقت أو لتقوم بتنبيهك في كل مرة يرغب الموقع بإظهار منبثقة وبإمكانها كذلك إخبارك عن مصدرها وبالتالي يقوم المستخدم بقبول المنبثقات من مصادر موثوقة.

٣. استخدام (×) لإغلاق النوافذ التي تظهر بشكل مفاجئ.

٤. يجب على المستخدم البقاء بعيدا عن أزرار (No Thanks) (If you can help it) وبدلا من ذلك يجب عليه إغلاق النافذة باستخدام " × ".

٥. يجب على المستخدم أن يقرأ اتفاقية الترخيص بشكل كامل قبل تثبيت أي برنامج، لأن بعضها تنص بوضوح بأن البرنامج سيقوم بمراقبة سلوكك وإرسال بيانات لجهة خارجية.

٦. تحديث نظام التشغيل والبرامج المهمة بشكل دوري ومستمر.

٧. تثبيت برامج لمكافحة الفيروسات وجدار الحماية.

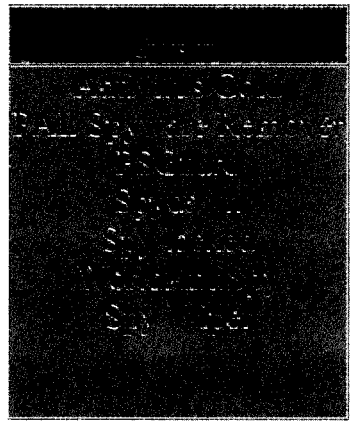
٨. تحديث المتصفح باستمرار والحرص على اقتناء وتثبيت الإصدار الأخير، الشركات المنتجة لهذه البرامج تقوم كل فترة بتطوير تعديلات تعالج بها الثغرات الأمنية التي تكتشف بهذه البرامج لكي تمنع وصول البرامج التجسسية إلى حاسبك من خلالها، فدائما ما تكون الإصدارات الأخيرة لبرامج تصفح الإنترنت أكثر أمنا.

٩. البعد عن المواقع المشبوهة علي شبكة الإنترنت، فهذه المواقع هي مزرعة للبرامج التجسسية ويمكنها في ثواني الانتقال إلى حاسبك بمجرد زيارة الصفحة الأولي لهذه المواقع.

١٠. يجب الحرص عند تثبيت البرامج المجانية، فعدد كبير منها يقوم بتثبيت بعض البرامج التجسسية أو الدعائية أثناء تثبيت هذا البرنامج المجاني وإذا أصبح الحاسوب أكثر بطأ بعد تثبيت أحد البرامج المجانية فيجب فورا إلغاء تثبيت هذا البرنامج ففي الغالب أن هذا البرنامج يحمل مع برنامج تجسسي.

برامج زائفة لمكافحة التجسس:

انتشرت العديد من البرامج التي تدعي أنها برامج مكافحة للتجسس، والتي ترسل للمستخدم تحذيرا مزيفا بوجود برامج تجسس على جهازه والتي تدفعه لشراء هذه البرامج حتى تزيلها، إلا أنها لا تفعل ذلك، بل الأسوأ من هذا ومن أمثلة هذه البرامج كما في الجدول أدناه:



طرق حماية نظام Domain Name System DNS [1]:

١. حماية الاتصال الشبكي لخادمات أسماء النطاقات(Network Security)

تطبق الحماية من خلال استخدام موجة أو جدار ناري و القيام بشروط معينة لفلترة الرسائل على الشبكة بحيث لا تفتح المنافذ إلا التي يحتاجها الخادم للقيام بعمله.

٢. حماية وتحديث نظام التشغيل (OS Security)

من اللازم حماية نظام التشغيل و ذلك من خلال التحديثات اللازمة بشكل.

---

1 - رائد بن إبراهيم الفايز، نظام أسماء النطاقات،ورقة عمل مقدمة للمركز السعودي لمعلومات الشبكة، جامعة الملك سعود، الرياض.

مستمر، و الحرص على دقة إعدادات نظام التشغيل و صحته و العمل على إزالة جميع البرامج و الخدمات الإضافية الغير لازمة أو التي لا حاجة لوجودها.

٣. التنوع في خادمات أسماء النطاقات (Diversity)

من الواجب وجود خادمين على الأقل لإعداد خادمات أسماء النطاقات بحيث يكون من الممكن إضافة أسماء النطاقات الرئيسي منها و الثانوي والأفضل أن توجد الخادمات على شبكات مختلفة و نظام تشغيل مختلف عن بعضهم البعض.

٤. إخفاء الخادم الرئيسي لأسماء النطاقات (Hiding the Primary Name server)

في نظام DNS يوجد على الأقل خادم رئيسي معلن لكل نطاق ولكن يفضل وضع خادم آخر رئيسي مخفي لا يعلم عنه أحد ولا يتم مخاطبته سوى من الخادم الرئيسي المعلن (الذي يأخذ منه ملفات النطاقات المستضافة) بعد ذلك يقوم بتوزيعها على الخادمات الثانوية، حتى يتأكد من الحصول على نسخة صحيحة من ملفات النطاقات المستضافة .

٥. تخصيص جهاز مستقل يعمل كخادم لأسماء النطاقات (Dedicated Machine for DNS servers)

يقوم بخدمة أسماء النطاقات و العمل على الحد من الخدمات الإضافية على الجهاز و التركيز على أمن نظام التشغيل للحد من إمكانية اختراق الجهاز.

٦. استخدام خدمة امتدادات نظام أسماء النطاقات الأمن (Domain Name Service Security Extension-DNSSEC)

وهي خدمة مهمة بحيث تقوم بأمرين مهمين هما: التأكد من مصدر المعلومة ومن حقيقة المعلومة نفسها.

٧. إخفاء نوع وإصدار الخادم(Hiding Server Version)

من الضروري إخفاء رقم إصدار خادم أسماء النطاقات و المقررات حتى يصعب على المهاجم تحديد نوع خادم أسماء النطاقات أو الإصدار الحالي لها، حتى في حال اكتشاف الثغرات الأمنية للخادم لا يمكن أن يستغلها.

٨. منع خدمة نقل ملفات النطاقات للجهات الغير مصرحة (Preventing Unauthorized Zone Transfers)

لاحتواء ملف النطاق على جميع أسماء وعناوين الأجهزة والخدمات المتوفرة يجب عدم السماح لأي شخص بالحصول على هذه المعلومات كاملة، لذلك يتم تحديد الخادمات التي تستطيع نقل ملف النطاق كذلك التحقق من طالب خدمة نقل الملفات.

الاختراق (Attacks):

المخترق من هو، وكيف يعمل؟

هكر.. اختراق.. قرصنة.. كلمات باتت تخيف كثيرا من الناس خصوصا مستخدمي الإنترنت الجميع يريد الحماية ويريدون من ينقذهم من هذا الكابوس القابع تحت مسمى القرصنة.

فالهاكرز هو عالم كبير وبداياته كانت قبل الإنترنت بل وقبل الكمبيوتر نفسه، وقد انتشر هذا المصطلح انتشاراً رهيباً في الآونة الأخيرة وأصبح يشير بصفة أساسية إلى الأفراد الذين يلجؤون بطريقة غير شرعية إلى اختراق أنظمة الحاسب بهدف سرقة أو تخريب أو إفساد البيانات الموجودة بها. وفي حالة قيام المخترق بتخريب أو حذف أي من البيانات الموجودة يسمى (كراكر)، لان الهاكر يقوم عادة بسرقة ما خف من البرامج والملفات ولا يقوم بالتخريب أو التدمير.

من هو الهاكر؟

١. هو الشخص الذي يستمتع بتعلم لغات البرمجة وأنظمة التشغيل الجديدة.
٢. هو الشخص الذي يستمتع بعمل البرامج أكثر من تشغيل هذه البرامج وأيضا يحب أن يتعلم المزيد عن هذه البرامج
٣. هو الشخص الذي يؤمن بوجود أشخاص آخرين يستطيعون القرصنة.
٤. هو الشخص الذي يستطيع أن يصمم ويحلل البرامج أو أنظمة التشغيل بسرعة.

٥. هو شخص خبير بلغة برمجة ما أو نظام تشغيل معين.. على سبيل المثال قراصنة اليونكس. يتضح مما سبق أن المخترق أو الهكر ذو تعريفات عدة، ومن الجدير بالذكر إن هذا الإنسان وكما يتضح في التعريفات السابقة هو إنسان طموح ومفكر يستخدم علمه للخير وتنمية القدرات، ترى لماذا كل هذا الشك والخوف اتجاه هذا الشخص!!

تاريخ الهاكرز:

قبل عام ١٩٦٩

في هذه السنوات لم يكن للكمبيوتر وجود ولكن كان هناك شركات الهاتف والتي كانت المكان الأول لظهور ما نسميهم بالهاكرز في وقتنا الحالي. ولكي نلقي بالضوء على طريقة عمل الهاكرز في تلك الفترة الزمنية نعود إلى عام ١٨٧٨م، في الولايات المتحدة الأمريكية، كان أغلب العاملين في شركات الهاتف المحلية من الشباب المتحمس لمعرفة المزيد عن هذه التقنية الجديدة والتي حولت وغيرت مجرى التاريخ. فقد كانوا يستمعون إلى المكالمات الشخصية ويغيرون الخطوط الهاتفية بغرض التسلية وتعلم المزيد حتى قامت الشركات بتغيير الكوادر العاملة بها من الرجال إلى كوادر نسائية للانتهاء من هذه المشكلة. وفي الستينات من هذا القرن ظهر الكمبيوتر الأول. لكن هؤلاء الهاكرز كانوا لا يستطيعون الوصول لهذه الكمبيوترات وذلك لأسباب منها كبر حجم هذه الآلات في ذلك الوقت ووجود حراسة على هذه الأجهزة نظرا لأهميتها ووجودها في غرف ذات درجات حرارة ثابتة. و لكن متى ظهرت تسمية هاكرز؟ الغريب في الأمر إن الهكر في الستينيات كان عبارة عن مبرمج بطل أو عبقري، فالهاكرز في تلك الفترة هو المبرمج الذي يقوم بتصميم أسرع برنامج من نوعه ويعتبر "دينيس ريتشي وكين تومسون" أشهر هاكرز على الإطلاق لأنهم صمموا برنامج اليونكس وكان يعتبر الأسرع وذلك في عام ١٩٦٩.

العصر الذهبي للهاكرز من عام ١٩٨٠- ١٩٨٩

في عام ١٩٨١ أنتجت شركة IBM المشهورة جهاز أسمته بالكمبيوتر الشخصي يتميز بصغر حجمه وسهولة إستخدامه وإستخدامه في أي مكان وآي وقت، ولهذا فقد بدا الهاكرز في تلك الفترة بالعمل الحقيقي لمعرفة طريقة عمل هذه الأجهزة وكيفية تخريبها والوصول إليها. وفي هذه الفترة ايضا ظهرت مجموعات من الهاكرز كانت تقوم بعمليات التخريب في أجهزة المؤسسات التجارية والرسمية. في عام ١٩٨٣ ظهر فيلم سينمائي اسمه (حرب الالعاب) تحدث هذا الفيلم عن عمل الهاكرز وكيف ان الهاكرز يشكلون خطورة على الدولة وعلى اقتصاد الدولة وحذر الفيلم من الهاكرز.

حرب الهاكرز العظمى من عام ١٩٩٠- ١٩٩٤

البدايات الأولى لحرب الهاكرز هذه في عام ١٩٨٤ حيث ظهر شخص اسمه "ليكس لوثر" وانشا مجموعة اسماها (LOD) وهي عبارة عن مجموعة من الهاكرز الهواة والذي يقومون بالقرصنة على أجهزة الآخرين. وكانوا يعتبرون من أذكى الهاكرز في تلك الفترة. إلى أن ظهرت مجموعة أخرى اسمها (MOD) وكانت بقيادة شخص يدعى (فيبر). وكانت هذه المجموعة منافسة لمجموعة (LOD). ومع بداية العام ١٩٩٠ بدأت المجموعتان بحرب كبيرة سميت بحرب الهاكرز العظمى وهذه الحرب كانت عبارة عن محاولات كل طرف اختراق أجهزة الطرف الآخر. واستمرت هذه الحرب ما يقارب الأربعة أعوام وانتهت بإلقاء القبض على (فيبر) رئيس مجموعة (MOD) ومع انتهاء هذه الحرب ظهر الكثير من المجموعات والكثير أيضا من عمالقة الهكرز.

كيفن ميتنيك يعتبر أشهر هاكر في الولايات المتحدة ويعتبر أشهرهم في التاريخ العالمي حيث انه قام بسرقات كبيرة دوخت آلاف بي اي (FPI) ولم يستطيعوا معرفته في أغلب سرقاته، وفي إحدى المرات استطاع أن يخترق شبكة الكمبيوترات الخاصة بشركة Digital Equipment Company وتم القبض علية في هذه المرة وتم سجنه لمدة عام. وبعد خروجه من السجن كان أكثر ذكاء. فكانوا لا يستطيعون ملاحقته فقد كان كثير التغيير في شخصيته وكثير المراوغة

في الشبكة، من أشهر جرائمه وأكثرها فتكا هي سرقته الأرقام الخاصة ب ٢٠٠٠٠ بطاقة ائتمان. والتي كانت آخر جريمة له. حيث تم القبض عليه بعدها وتم سجنه لمدة عام. ولكن إلى الآن لم يخرج من السجن لان آلاف بي اي يرون (FPI) بأن كيفن هذا خطير ولا توجد شبكة لا يستطيع اختراقها.

ظهرت أصوات تطالب الحكومة بالإفراج عن كيفن وظهرت جماعات تقوم بعمليات قرصنة باسم كيفن من بينها قرصنة موقع جريدة نيويورك تايمز والتي ظهرت شاشتها متغيرة كثيرا في مرة من المرات وظهرت كلمات غريبة تعلن للجميع بأن هذه الصفحة تم اختراقها من قبل كيفن ميتنيك. ولكن تبين بعد ذلك بأنه احد الهاكرز الهواة المناصرين لميتنيك.

هناك ثلاث أنواع من الاختراق وهم[1]:

١. Access Attacks .
٢. Reconnaissance Attacks.
٣. denial of service (DoS) attacks.

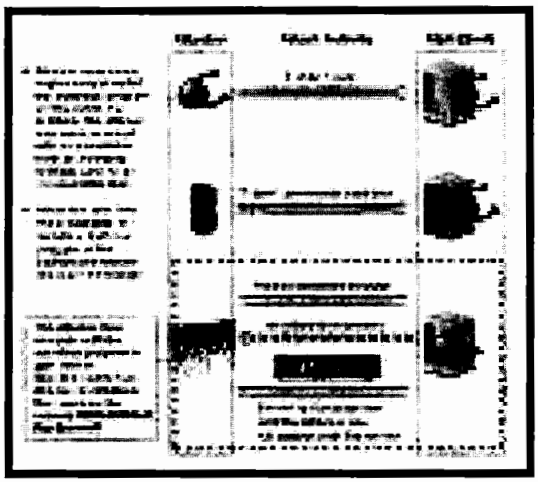
Access Attacks

محاولة الدخول بطرق غير شرعية من خلال تخمين أو إستخدام البرامج المتقدمة في عملية إنشاء الحساب والرقم السري (User name & Password) حتى يصل إلى كلمة مرور صحيحة ويتحكم بعد ذلك بالنظام.

Reconnaissance Attacks

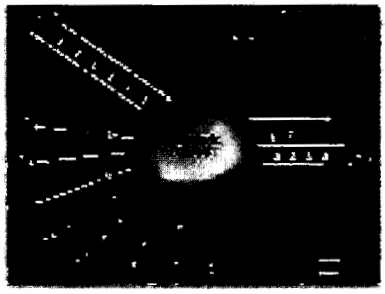
محاولة إستخدام نقاط الضعف الخاصة بالمنتج سواء كان Hard ware أو Soft ware للحصول على طريقة خلفية Back Door لاختراق النظام.

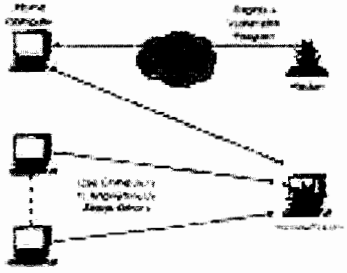
1- سلام تنوري، جرائم الحاسوب والإنترنت، ورقة عمل مقدمة في الجامعة اللبنانية، قسم الدراسات العليا.



Denial of service (DoS) attacks

في حالة صعوبة اختراق النظام الخاص بالسرية فان هناك إمكانية لعمل Shot Down للنظام ككل بإرسال ملايين الطلبات إلى الSecurity Server و Rooter & Switch بحيث لا يتحمل هذا العدد من المعلومات فيتم إغلاق النظام.





تصنيف الهجمات والمخاطر[1]:

١. خرق الحماية المادية:

- التفتيش في مخلفات التقنية وهي: قيام المهاجم بالبحث عن أي شئ يساعده على اختراق النظام مثل بعض الأوراق المدون عليها كلمات سر مثلا أو مخرجات الكمبيوتر التي تتضمن معلومات مفيدة أو الأقراص الصلبة المرمية بعد استبدالها.

---

[1] - د. محمود قطر، أمن المعلومات ماهيتها وعناصرها واستراتيجياتها، منتدى المكتبات والمعلومات، ٢٠٠٦، شبكة الإنترنت www.alyaseer.net.

- الالتقاط السلكي وهو: التوصل السلكي المادي مع الشبكة أو توصيلات النظام لجهة استراق السمع أو الاستيلاء على المعطيات المتبادلة عبر الأسلاك وهي أنشطة تتم بطرق سهلة أو معقدة تبعاً لنوع الشبكة وطرق التوصل المادي.
- استراق الأمواج: ويتم بإستخدام لواقط تقنية لتجميع الموجات المنبعثة من النظم باختلاف أنواعها كالتقاط موجات شاشات الكمبيوتر الضوئية أو التقاط الموجات الصوتية من أجهزة الاتصال.
- إنكار أو إلغاء الخدمة وهي: الإضرار المادي بالنظام لمنع تقديم الخدمة أو إرسال الرسائل البريدية الإلكترونية دفعة واحدة لتعطيل النظام.

٢. خرق الحماية المتعلقة بالأشخاص وشؤون الموظفين:

- التخفي بإنتحال صلاحيات شخص مفوض وهو: الدخول إلى النظام عبر إستخدام وسائل التعريف العائدة لمستخدم مخول.
- الهندسة الاجتماعية وهو: بأن يتصل شخص بأحد العاملين ويطلب منه الرقم السري بزعم أنه أحد العاملين بالصيانة أو التطوير وسميت بالهندسة الاجتماعية لطبيعة الأسلوب الشخصي في الحصول على معلومة الاختراق أو الاعتداء.
- الإزعاج والتحرش وهي: تهديدات يندرج تحتها أشكال عديدة من الاعتداءات والأساليب ويجمعها توجيه رسائل الإزعاج والتحرش وأحيانا التهديد والإبتزاز أو مزاح بشكل يسبب مضايقة وإزعاج وهي لا تكون فقط في بيئة العمل بل تكون أيضا عبر الشبكة وفي المنتديات وغيرها.
- قرصنة البرمجيات: وتتحقق عن طريق نسخ هذه البرمجيات دون تصريح أو استغلالها بدون تخويل بهذا الاستغلال وأيضا تقليدها أو الانتفاع المادي منها.

٣. خرق الحماية المتصلة بالاتصالات والمعطيات:

١- هجمات المعطيات:

- النسخ غير المصرح به للمعطيات وهي العملية الشائعة حيث يمكن الاستيلاء عن طريق النسخ على كافة أنواع المعطيات وتشمل البيانات والمعلومات والبرامج والأوامر.

- تحليل الاتصالات وهي مراقبة حركة النظام بغرض انتهاز الوقت المناسب للهجوم.
- القنوات المخفية وهي صورة من عمليات التخزين حيث يخفي المقتحم معطيات أو برمجيات معلومات مستولى عليها كأرقام بطاقات ائتمان في موضع معين من النظام.

ب- هجمات البرمجيات

- المصائد والأبواب الخلفية وتعتبر ثغره أو منفذ في برنامج يتيح للمخترق الوصول من خلاله للنظام.
- السرقة أو اختلاس المعلومة وهو أن يستغل الشخص إستخداما غير مشروعا من قبل غيره للنظام فيستخدم النظام عندما تتاح له الفرصة لانشغال المستخدم دون علمه.
- الهجمات عبر التلاعب بنقل المعطيات عبر أنفاق النقل وتعتبر طريقة غير مشروعة عند نقل بيانات غير مشروعة.
- الهجمات الوقتية وهي هجمات تتم بطرق تقنية معقدة للوصول غير المصرح به إلى البرامج أو المعطيات وتقوم على فكرة استغلال وقت تنفيذ الهجمة متزامنا مع فواصل الوقت التي تفصل العمليات المرتبة في النظام.
- البرمجيات الخبيثة مثل الفيروسات وحصان طروادة والدودة الإلكترونية والسلامي والقنابل المنطقية وهي جميعها برامج ضارة تستغل للتدمير سواء تدمير النظام أو تدمير البرمجيات والملفات أو المعطيات.

٤. الهجمات والمخاطر المتصلة بعمليات الحماية:

- العبث بالبيانات ويستهدف هذا الهجوم تغيير البيانات أو إنشاء بيانات وهمية في مراحل الإدخال أو الاستخراج.
- خداع بروتوكول الإنترنت حيث يقوم المهاجم بتزوير العنوان المرفق مع حزمة البيانات المرسلة بحيث يوعز للنظام على أنه عنوان صحيح مرسل من داخل الشبكة بحيث يسمح النظام لحزمة البيانات بالمرور باعتباره مشروع.

- كلمات السر(جمع والتقاط كلمات السر) وهو برنامج يقوم بجمع أول ١٢٨ بايت من كل اتصال بالشبكة التي تجري مراقبتها وتتبع حركة الاتصال عليها وعندما يطبع المستخدم كلمة السر أو اسم المستخدم فان البرنامج يجمع هذه المعلومات وينسخها إضافة إلى أن أنواع هذه البرامج تجمع المعلومات الجزئية وتعيد تحليلها وربطها.
- المسح والنسخ وهو أسلوب يستخدم فيه برنامج الماسح وهو يقوم على فكرة تغيير التركيب أو تبديل احتمالات المعلومة ويستخدم تحديداً بشأن احتمالات كلمة السر أو رقم الهاتف (هاتف المودم) بمسح قائمة أرقام كبيرة للوصول إلى إحدى الأرقام المستخدمة مودم الاتصال بالإنترنت.
- هجمات استغلال المزايا الإضافية والفكرة هنا تتصل بواحد من أهم استراتيجيات الحماية فالأصل أن مستخدم النظام من داخل المؤسسة محدد له نطاق الإستخدام ونطاق الصلاحيات بالنسبة للنظام ولكن ما يحدث في الواقع العملي أن مزايا الإستخدام يجري زيادتها دون تقدير للمخاطر ودون علم الشخص نفسه وهنا يتمكن المخترق التلاعب ببيانات المستخدم الذي دخل على النظام من خلال اشتراكه ويتمكن من تدمير مختلف ملفات النظام حتى غير المتصلة بالمدخل الذي دخل منه وذلك لأنه استخدم المزايا الإضافية التي يتمتع بها المستخدم.

طرق و أنواع الاختراق[1] :

هناك العديد من الطرق التي يتم بها اختراق أجهزة الكمبيوتر و الإيميل وسنقوم بشرح مبسط لكل طريقة من هذه الطرق حتى يكون الجميع بمأمن من الوقوع بها:

- الاختراق الكامل للجهاز

---

[1] - د. إبراهيم المحيسن، اختراق أجهزة الكمبيوتر والإميلات وطرق مهمة للرقابة منه شبكة الإنترنت، ٢٠٠٩، www.mohysoin.com

و هذا النوع من الاختراق هو أخطر شيء حيث أنه عند اختراق جهازك فإن المخترق يكون لديه تحكم كامل في الجهاز و من الأمور التي يستطيع أن يقوم بها المخترق:

١. سحب أي ملف أو صورة من جهاز الضحية.
٢. إرسال أي ملف أو صورة للضحية.
٣. حذف أي ملف من جهاز الضحية.
٤. إغلاق الجهاز .
٥. إعطاء أوامر للطابعة .
٦. عمل فورمات للجهاز .
٧. فتح السي دي روم و إغلاقه .
٨. تشغيل أي ملف صوتي أو فيديو في جهاز الضحية.
٩. فتح أي موقع في جهاز الضحية .
١٠. تغيير خلفية الشاشة.
١١. اخذ صور من الكاميرا حتى لو كانت الكاميرا غير مستعملة و يكفي أن تكون مشبوكة في الجهاز حتى يتم التقاط الصور منها.
١٢. اخذ أي باسورد يتم فتحه على الجهاز و الكثير من الأمور الأخرى.

- الاختراق عن طريق الكي لوجرKeyloger :

وهذا النوع من الاختراق يعتبر جزئي أي لا يتمكن المخترق من إرسال أو سحب ملفات و غيرها من الأمور السابقة الذكر و إنما يقتصر على التجسس على كل كلمة يكتبها الضحية و إرسالها إلى أيميل يحدده المخترق و يتم هذا النوع من الاختراق عن طريق إرسال ملف للضحية سواء عن طريق المسينجر أو الايميل أو وضعه على الإنترنت و من الممكن أن يكون هذا الملف مدمج بصورة أو ملف أخرى حتى لا يعرف الضحية انه مخترق .

- اختراق الايميل :

و من اسمه يدل على أنه مخصص لسرقة باسورد أيميل معين و هناك عدة طرق و برامج لهذا النوع من الاختراق نذكر منها ما يلي:

١. الاختراق عن طريق ملف معين يتم إرساله للضحية بطريقة ما سواء كانت عن طريق الايميل أو المسينجر أو بوضع هذا الملف على النت و عند فتح هذا الملف يتم إرسال الباسورد مع الاي بي (IP) مباشرة إلى المخترق و هناك نوع من هذه البرامج الخاصة بالياهو مسينجر حيث يتم فيها إرسال الباسورد مع رقم الآي بي إلى مسينجر المخترق في كل مرة يقوم بها الضحية بفتح المسينجر و أن تم تغيير الباسورد فيتم إرسال الباسورد الجديدة إلى المخترق طالما أن هذا الملف بقي على الجهاز.

٢. اختراق الايميل: عن طريق الكي لوجر و الذي سبق شرحه في الأعلى .

٣. اختراق الايميل عن طريق الصفحات المزيفة.

وهذه الطريقة تأخذ عدة أشكال و منها الطريقة التي يتم بها خداع الأعضاء عن طريق صفحة من البالتوك، وهناك طرق أخرى منها بأن تقوم بعمل صفحة مزيفة للبالتوك وتضع بها في الأعلى شعار البالتوك الموجود في موقع البالتوك وتكتب انه عن طريق هذه الصفحة يمكن الدخول للبالتوك بدون البرنامج عن طريق أيميل الياهو والهوتميل وتضع خانة للايميل و خانة للباسورد و تكتب بالصفحة التي تأتي بعد وضع الايميل و الباسورد تقول إن السيرفير مشغول الآن الرجاء المحاولة ثانية فيقوم البعض بفتح الصفحة والمحاولة أكثر من مره بحيث انه لا يعرف بأن هذه الصفحة مزيفة.

أما الطريقة الأخرى فهي عبارة عن بروفيل صفحة الياهو و تقوم بنسخ صفحة الياهو ووضعها في صفحة خاصة للمخترق على الإنترنت و تجعل خاصية الدخول للبروفيل لمن هم فوق ١٨ سنة حتى تطلب الصفحة الايميل و الباسورد و بعد أن يقع الضحية ويضع الايميل والباسورد كانت الصفحة تحولهم مباشرة على صفحة بروفيل حقيقية و هكذا لا احد يعرف أن الصفحة مزيفة و انه تم اختراق الايميل و لذلك انصح الجميع بعدم وضع باسورد أيميله في أي مكان غير صفحة الايميل نفسها و أن تقوم بفتحها بنفسك و ليس عن طريق رابط من أي مكان.

اختراق الإيميل عن طريق حيل أخرى و منها ما تجده على بعض المنتديات بمواضيع معنونة احصل على باسورد أي أيميل تريده كأن يطلب منك أن تكتب أمور معينة و من ضمنها أن تضع أيميلك و باسورد أيميلك و أيميل الشخص الذي تريد أن تحصل على باسورده و تبعثه هذه المعلومات ليسرفير الهوتميل و يكون الايميل على هذا الشكل مثلا server000tht@hotmail.com، طبعا هذا الايميل يكون عبارة عن أيميل المخترق و الذي سوف تصل أليه المعلومات التي تضعها أنت لذلك الحذر من هذه الحيل .

طرق الوقاية من الاختراق[1]:

١. وجود مكافح للفيروسات على جهاز الكمبيوتر
٢. عدم استقبال أي ملف من شخص لا تثق به و حتى إن كنت تثق بشخص معين يجب عليك التأكد من الملف حيث من الممكن أن هذا الشخص لا يعلم أن الملف يحتوي على فيروس أو من الممكن أن أيميل صديقك تم اختراقه و شخص آخر هو من يتحدث معك لذا يجب الحذر من أي ملف تستقبله.
٣. فحص أي ملف تقوم بتحميله من الإنترنت قبل فتحه و أن قمت بتحميل ملف من منتدى يجب عليك قراءة المشاركات في نفس الموضوع حيث أنه من الممكن أن يكون هذا الملف يحتوي على فيروس و قام أحد المشاركين بالتنويه لذلك.
٤. في حالة إرسال جهازك للتصليح يفضل أن تقوم بعمل فورمات له لأنه من الممكن أن هذا الشخص وضع عليه باتش أو أي برنامج للتجسس عليك .
٥. أنصح الجميع بإستخدام أيميل الجي ميل أو أيميل الياهو للمراسلات الخاصة و ترك أيميل الهوتميل للمسينجر فقط لأن أيميل الجي ميل و الياهو أكثر أمانا من أيميل الهوتميل.
٦. أنصح الجميع بعدم إبقاء أي صور خاصة في الإيميل و إن كان و لا بد أن تكون في مجلد مضغوط محمي بباسورد .

---

1 - عبد الحميد بسيوني، أمن الشبكات والمعلومات، دار الكتب العلمية، القاهره،٢٠٠٦.

٧. بعض الفيروسات تقوم بإرسال نفسها عن طريق الايميل أو المسينجر لذلك عند استقبالك رسالة على المسينجر أو الايميل بها رابط تطلب منك الدخول أليه عدم فتحه .

٨. عدم وضع باسوردات تكون معروفة مثل رقم تلفون جوالك أو رقم تلفون البيت أو تاريخ ميلادك أو أي حدث معروف للجميع.

٩. عدم وضع أرقام متسلسلة مثل ١٢٣٤٥٦ أو أصفار أو ما شابه و يفضل أن تكون حروف و أرقام.

حماية الملفات و الصور الخاصة في حالة الاختراق:

بالرغم من الإجراءات الوقائية التي نتخذها للحيلولة دون اختراق أجهزتنا إلا أننا في بعض الأحيان نتعرض للاختراق و قد يكون السبب ظهور فيروسات جديدة لم تتعرف عليها مكافحات الفيروسات بعد أو إن جهاز الكمبيوتر يتم إستخدامه بأكثر من شخص في البيت الواحد و قد يكون احد أفراد البيت ليس لديه الخبرة الكافية و يستقبل ملفات تحتوي على فيروسات و للتقليل من اثر الاختراق و حماية الملفات الضرورية و الصور العائلة الخاصة و التي لا تريد أن يطلع عليها احد في حالة الاختراق أن تقوم بوضع هذه الملفات و الصور في مجلدات و حمايتها عن طريق وضعها في ملف مضغوط بباسورد و أن يكون الباسورد طويل جدا و يحتوي على أرقام و حروف صغيرة و كبيرة لان بعض البرامج تقوم بفك الباسورد إذا كانت أرقام فقط أو كلمة قصيرة .

كما يفضل أن يتم وضع هذه المجلدات في ملف مخفي بين عدة ملفات في جهازك. ينطبق الأمر نفسه على الـ USB أو الفلاش ميموري.

طريقة حماية ملف مضغوط بباسورد:

نضغط بزر الماوس الأيمن على المجلد الذي نريد أن نقوم بحمايته و منه نختار add to Archive و نتبع التعليمات الموجودة في الصور.

حماية معلوماتك البنكية و بطاقات الائتمان من السرقة:

قبل أن تقوم بوضع رقم حسابك أو بطاقة الائتمان الخاصة بك في أي موقع تريد الشراء منه أو أثناء تسجيلك الدخول لحساب البي بال (PayPal) الخاص بك يجب عليك

أن تتأكد أن هذه الصفحة حقيقية و ليست صفحة مزيفة مصممة لسرقة بطاقات الائتمان وأرقام الحسابات البنكية و يمكن التأكد من ذلك من خلال شريط العنوان الخاص بالموقع حيث يجب أن يكون حرف S موجود بعد http أي يكون بالشكل التالي https و ليس http و حرف S اختصار لكلمة secure والتي تعني امن و نفس الشيء ينطبق على صفحة الدخول لإيميل الياهو و أيميل الجي ميل لكن هذه الخاصية غير متوفرة في صفحة الدخول للهوتميل.

أخطر برامج الاختراق المتداولة :

١. Net Bus.
٢. Deep Throat.
٣. Girl.
٤. Back Orifice.
٥. Sub Seven.
٦. Hack a Tack.
٧. Master Paradise.
٨. ICQ Trojan.
٩. Friend 8.
١٠. Net Sphere9.
١١. Win Crash01.
١٢. Big Cluck.
١٣. Executer.
١٤. Back Door.

البرنامج نت بص **Net Bus**:

تمكن مبرمج سويدي اسمه كارل نيكتر في عام ١٩٩٨ من إصدار نسخة تجريبية تعمل على الوندوز ٩٥ من برنامج لم يطلق عليه اسما في ذلك الوقت ٠

يستطيع مستخدم البرنامج تشغيله بواسطة كمبيوتر بعيد ٠ هذا البرنامج سماه Net Bus صدرت بعد ذلك نسخ عديدة منه، أذكر منها النسخة ١,٦ و ١,٧ Net Bus Pro وأخيرا Net Bus 0002 .

إمكانياته :

يسمح البرنامج لأي شخص بالسيطرة على جهاز الضحية عن بعد على الشكل التالي:

١. عرض صورة مفاجئة على شاشة الضحية، أو تغيير إعدادات الشاشة دون تدخل من المستخدم

٢. فتح و غلق باب سواقة السي دي تلقائيا ، دون تدخل من المستخدم.

٣. وضع مؤشر الماوس في مكان معين بحيث لا يمكن للمستخدم تحريكه عن هذه المنطقة

٤. ظهور حركة للماوس دون أي تدخل من صاحب الجهاز .

٥. عرض رسالة قصيرة على الشاشة تختفي وتظهر فجأة أو تبقى معلقة دائما بالشاشة فلا يستطيع المستخدم التخلص منها

٦. التجسس على المستخدم ورؤية كل ما يفعله .

٧. عـــرض محتويات القرص الصلب بالكامل عن بعد .

٨. إنزال أي ملف من جهاز الضحية إلى جهاز المخترق .

٩. تحميل أي ملف من جهاز المخترق إلى جهاز الضحية .

١٠. التحكم في علو وانخفاض الصوت.

١١. في حالة ارتباط مايكروفون بجهاز الضحية فيمكن للمخترق الاستماع لما يدور من حديث بالغرفة المتواجد بها جهاز الضحية.

١٢. حذف أي ملف من القرص الصلب وقت ما يشاء المخترق .

١٣. إقفال أي نافذة من النوافذ المفتوحة بشاشة الضحية

١٤. تغيير أو حذف كلمات السر الخاصة بالضحية واستبدالها بكلمات أخرى

١٥. تغيير إعدادات النظام بالجهاز الخاص بالضحية.

كل هذه الوظائف السابقة يمكن لأي مخترق لديه هذا البرنامج، كما هو الحال في معظم برامج الاختراق، أن ينفذها ، أو بمعنى أوضح السيطرة الكاملة على جهاز الضحية .

كيف تعرف إذا تم اختراق جهازك بهذا البرنامج ؟

إن المخترق لكي يتمكن من الاختراق عليه الدخول من أحد المنافذ Ports والبرامج المضادة للمخترقين كفيلة بإغلاق تلك المنافذ في وجه المخترق؛ ولكن، حتى نقطع الطريق على المخترق، إليكم طريقة ممتازة لاكتشاف المنافذ المفتوحة وإغلاقها بطريقة يدوية من خلال الوندوز ويجب تنفيذ هذا الإجراء أثناء الاتصال بالإنترنت online حتى نتمكن من رؤية جميع المنافذ المتصلة بطريقة غير شرعية أثناء الاتصال بالإنترنت.

١. من قائمة ابدأ اختر التشغيل Start/Run
٢. عند ظهور مربع الحوار الخاص بتنفيذ الأوامر أكتب Command
٣. سيظهر لك إطار نظام التشغيل دوس وفي داخل الإطار وأمام خانة المؤشر اكتب :netstat – a
٤. ثم اضغط على Enter
٥. والآن قارن بين أرقام المنافذ التي ظهرت لك مع أرقام المنافذ التالية، وهي المنافذ التي يفتحها في العادة ملف التجسس الباتش التابع لبرنامج Net Bus فإن وجدت رقم المنفذ ضمنها، فان جهازك قد اخترق، وعليك في هذه الحالة التخلص أولا من ملف التجسس.

وهذه منافذ دخول برنامج النت باص:

- ٤٣٠٠٢ - ٥٤٠١ - ٠٩٥٤ - ١١٧٦ - ٠٠٣٧ - ١٠٣٧ - ٦٠٣٧ - ٣٠٣٧ -
٨٠٣٧ - ٩٢٠٠٣ - ٠٠١٠٣ - ١٠١٠٣ - ٢٠١٠٣ - ٧٣٣١٣ - ٨٣٣١٣ - ٩٣٣١٣

التخلص من برنامج الباتش الخاص بالنت باص وإغلاق منافذه المفتوحة:

الرابط الرئيسي بين كمبيوتر المخترق وكمبيوتر الضحية هو ملف التجسس المزروع بجهاز الضحية وإذاً تم تحديده والتخلص منه، قطعت عليه طريق التجسس. أما المنافذ التي فتحت فهي جزء من الذاكرة يتعرف عليها الجهاز بأنها منطقة اتصال ومتى ما تم حذف ملف التجسس (الباتش) فإن الوندوز يعيد إغلاق

تلك المنافذ اتوماتيكيا عقب إعادة تشغيل الجهاز لان مصدرها (ملف الباتش) وملف الباتش قد قضي عليه تماما.

صب سيفن (**Sup Seven**) أخطر برامج الاختراق :

يعد البرنامج صب سيفن Sub Seven من أشهر البرامج المستخدمة من قبل المخترقين العرب، يسمونه القنبلة وهو مرغوب ومطلوب لبساطته وسهولة تعلمه وسهولة إستخدامه. يتميز بمخادعة الشخص الذي يحاول إزالته فهو يعيد تركيب نفسه تلقائيا بعد حذفه من ملف التسجيلRegistry بالوندوز بطرق ثلاث، ولكن هناك طريقة جديدة وخارقة لحذفه سأشرحها لاحقا قبل شرح أعراض الإصابة التي يخلفها هذا البرنامج في جهاز الضحية، تأكد أولا من عدم فتح منافذ الاتصال الخاصة به في جهازك بنفس الطريقة التي شرحتها من قبل في الإعداد السابقة وقارنها بالمنافذ التالية، فان وجدتها فان جهازك حتما مصاب، وعليك أن تتعامل مع هذا الملف الخبيث جدا وتوجد لهذا البرنامج جمعية على الإنترنت متخصصة في تطوير هذا البرنامج الشيطاني، بل وتعطى الحق في أن تنزل هذا البرنامج على جهازك كي تشجع عمليات القراصنة وتحمل هذه الجمعية على الإنترنت موقعا خاصا بها ظهر الإصدار الجديد من هذا البرنامج منذ شهر تقريبا يعمل هذا البرنامج في بيئة X/NT/w00029ويعد بمثابة كارثة حقيقية حيث يصل وزن ملف التجسس ٥٦ الى٦٠ إلى جانب إمكانيته الجديدة الخطيرة جداً وهذا البرنامج لا يعرف العبث، فاحذر أن تعبث ببرنامج مثل هذا لو وقع تحت يدك صدفة. منافذ دخول برنامج الـ Sub Seven 1999/ 1243/ 6776/ 6711 .

أعراض الإصابة :

تختلف أعراض الإصابة في هذا البرنامج عن البرنامجين السابقين، فمن أهم الأعراض ظهور رسالة شهيرة عند كل مرة يدخل فيها المخترق لجهاز الضحية وهي (قام هذا البرنامج بإنجاز عملية غير شرعية....) !! لحظه واحدة.. لا يعني من رأى منكم هذه الرسالة على شاشته أن جهازه قد اخترق.. قلنا: إن في هذا البرنامج الكثير من الخبث مما جعله مرغوباً خصوصاً في منطقة الوطن العربي، فهو حينما

يعطي رسالة كهذه إنما يوهم المخترق بأن هذه الرسالة شائعة ومعروفة، ومن تظهر له فقد تعود عليها فلن يشك مطلقا قبل قراءة هذه الأسطر في أن جهازه قد اخترق.

كيف نميز بين الرسالة الصادقة البريئة والرسالة الكاذبة الخبيثة؟؟

١. افتح ملف الـ win.ini الموجود في مجلد الويندوز وابحث في بداية السطور الأولى عن أي قيم شبيهة بالقيم التالية: run = xxxx.exe أو run = load = xxxx.exe أو xxxx.dl load = xxxx.dl .

لاحظ أنxxxx تعني اسم الخادم فإذا عثرت على أي قيمة منها فاحذفها فوراً وبمعنى آخر يجب أن لا يظهر أي سطر من السطور أعلاه في بداية السطور الأولى لملف الـwin.ini فإن ظهر فاحذفه على الفور.

٢. افتح الملف system.ini الموجود بمجلد الوندوز وستجد في السطر الخامس العبارة التالية : Shell = Explorer.exe إن كان جهازك مصابا فستجد شكل العبارة السابقة يكون هكذا: shell = Explorer.exe xxx.exe مع العلم بأن xxx هو اسم الخادم : rundlll6.exe و Task_Bar.exe إن وجدت جهازك مصابا فقم بمسح اسم الخادم فقط ليصبح السطر كما يلي: shell=Explorer.exe .

والآن، لقد قمت بقطع الطريق بين ملف التجسس واسم الخادم الخاص به فلا يبقى إلا التخلص من هذا الملف الخبيث وعليك القيام بحذف ملف التجسس الخاص بهذا البرنامج كما شرحته سابقا.

مبادئ حماية معلومات الحكومة[1]:

١. نشر الوعي الأمني المعلوماتي: من الضروري جدا أن تقوم الحكومة الإلكترونية بحملة توعية عامة حول امن البلاد الإلكتروني تبدأ من الرئيس وصولا إلى الموظفين والمواطنين وتشرح لهم المخاطر الأمنية الإلكترونية وكيفية تفاديها وما هي الإجراءات التي قامت بها الحكومة في هذا المجال ويفضل إصدار نشرة إعلامية شهرية خاصة.

1 - مركز دراسات الحكومة الإلكترونية، مبادئ حماية معلومات الحكومة، لبنان.

٢. الاستراتيجيات التنظيمية والهيكلية: لا بد أو من الضروري أن تقوم الحكومة بإجراءات وقائية تتناسب مع امن المعلومات الإلكتروني بحيث لا يتم إعطاء مسؤولية الأمن الإلكترونية لمجموعة من الأشخاص داخل الدولة كجزء إضافي من مهامهم ولا بد من إنشاء تشكيلات خاصة بالأمن الإلكتروني قد تكون تابعة لأجهزة الدولة الأمنية بحيث يكون تطوير الأمن الإلكتروني ورسم سياسات الدفاع والهجوم الإلكترونية في صلب مهامها.

٣. تطوير الاتفاقيات الأمنية الخارجية: من المهم جدا أن يتم تطوير الاتفاقيات الأمنية الثنائية أو الجماعية مع الدول الخارجية لكي تشمل قضايا ومواضيع الأمن الإلكترونية وأوجه التعاون المحتملة بين البلدين أو تبادل الخبرات الأمنية الإلكترونية مع تلك الحكومات.

٤. إستراتيجية الترغيب والترهيب: بحيث تشمل إستراتيجية الترغيب على تشجيع المواطنين على الإبلاغ عن محاولات الاعتداء الإلكتروني بدون أن يتم الكشف عن المخبرين ويمكن للدولة أن تعمد إلى تخصيص خط هاتف ساخن من أجل استقبال ملاحظات المواطنين في هذا المجال، هذا من جهة ومن جهة أخرى ينبغي على الحكومة أن تضع العقوبات الرادعة لمرتكبي الجرائم الإلكترونية بحيث تقوم بإرهابهم قبل أن يفكروا بمحاولة الاعتداء الإلكتروني.

٥. اعتماد مفاتيح التشفير: تعتمد تكنولوجيا التشفير الحديثة على أن تمتلك كل جهة أو فرد مفتاحين لتشفير وفك تشفير البيانات، المفتاح الأول وهو المفتاح الخاص ويكون فقط بحوزة الجهة المخولة، والمفتاح الثاني وهو المفتاح العام ويتم نشره على الإنترنت أو على شبكة الحكومة الإلكترونية من اجل إستخدامه من قبل الجهات الأخرى لتشفير الملفات والمعلومات المراد إيصالها إلى الطرف الآخر. وعلى سبيل المثال من أجل تشفير المعلومات المرسلة من قبل المواطن إلى دائرة ترخيص السيارات من أجل ترخيص سيارته، فإن المواطن يستخدم المفتاح العام الخاص بدائرة الترخيص لتشفير المعلومات قبل إرسالها وتستخدم الدائرة مفتاحها الخاص لفك تشفير المعلومات بعد استقبالها، وتدعم

هذه التقنية مستويات تشفير عالية تصل إلى ١٢٨ بت وهو ما اثبت فعاليته ضد محاولات الكسر.

٦. الهوية الإلكترونية الموحدة: إن موضوع الهوية الإلكترونية يعتبر من المواضيع الجديدة على ساحة النقاش الالكترو حكومي وهو لم يكتمل بعد، ولكن الهدف من هذه الهوية هل ستكون قادرة على التعريف عن الأشخاص وغير قابلة للنقل من شخص إلى آخر وستتمكن الحكومة من التعرف إلى مواطنيها من خلال الباس ورد أي كلمة السر.

٧. تقنية الترخيص الإلكتروني: إن الهوية الإلكترونية سوف تخدمنا للتعريف عن أنفسنا لدى الحكومة الإلكترونية ولكن هذا لا يعني انه باستطاعة جميع المواطنين الحصول على كافة المعلومات والخدمات الإلكترونية، فبعض الخدمات سوف تكون مقصورة على الرؤساء وغيرها خاص بالمؤسسات إن كانت تجاريه أو عسكريه فعلى سبيل المثال يمكن للحكومة أن تعطي تراخيص البحث عن معلومات تجارية لأصحاب المؤسسات المسجلين لدى الدولة والتي تدفع الضرائب بشكل منتظم، ويمكن إصدار الترخيص الإلكتروني الخاص بإستخدام أجهزة الأمن للإفراد المخولين بهذه المهام وهكذا.

٨. تشفير المعلومات المنقولة والمحفوظة: لا بد من اعتماد تقنيات تشفير عالية بحيث تظهر تلك المعلومات بصورة مبهمة تماما لكل من يحاول التصنت عليها عبر الشبكة السلكية واللاسلكية وأحد التقنيات المستخدمة في هذا المجال هي تقنية SSL المتوفرة عالميا وفي معظم البرامج والأنظمة الإلكترونية هذا على صعيد المعلومات المنقولة وينبغي اتخاذ نفس الإجراءات بالنسبة للمعلومات الحساسة المحفوظة في الأجهزة بحيث يتم حفظها وهي مشفرة.

٩. تسجيل الأثر الإلكتروني: من الضروري أن تعمد الحكومة الإلكترونية إلى إنشاء خدمات لتسجيل الأثر الإلكتروني لطالب الخدمة وعلى سبيل المثال يمكن تسجيل معلومات عن اسم المستخدم وتاريخ طلب الخدمة ووقتها وعنوانه على الشبكة والبلد الذي طلب منه الخدمة بالإضافة إلى عدد محاولاته

للدخول إلى الشبكة وستكون جميع هذه المعلومات بخدمة قسم الرقابة الإلكترونية.

١٠. كلمات مرور معقدة وديناميكية: يجب أن تكون كلمات السر تطابق الحد الادني لمواصفات الأمن والسرية بحيث تكون طويلة كفاية ولا تستخدم الكلمات المفتاحية أو أسماء العلم أو الحيوانات أو الكلمات التي يحتمل وجودها في معاجم اللغة، ويمكن زيادة تعقيد هذه الكلمات بجعلها تتغير أوتوماتيكيا مع مرور الوقت عليها.

١١. محاكاة أساليب الهجوم الإلكتروني: يسمى هذا الأسلوب في بعض الأحيان بالمناورات الأمنية الإلكترونية وتعمل خلالها أجهزة الأمن الإلكتروني على القيام بهجوم تجريبي غير ضار على أنظمة ادارات الدولة المختلفة للتحقق من صلابتها ومقاومتها وقد يتم هذا الهجوم بدون سابق إنذار للتأكد من فعالية أجهزة الحماية ومستوى تطبيق الإدارات الحكومية لمعايير الأمن الإلكتروني

١٢. الحماية المادية للأجهزة والأنظمة: حيث تخصص الدولة فرق حماية مكونة من عناصر الشرطة والأمن، تحتاج مواقع الحكومة الإلكترونية وأماكن تواجد أنظمتها إلى حماية أمنية للتأكد من عدم تجرؤ أطراف عدوة على العبث والتخريب وتدمير المكونات المادية للحكومة الإلكترونية، وقد ينفع من فترة إلى أخرى إجراء مسح راداري لاسلكي للتأكد من عدم وجود أجهزة تصنت إلكترونية في نطاق عمل الحكومة الإلكترونية.

وسائل الأمن الفاعلة[1]:

إن وسائل امن المعلومات هي مجموعة من الآليات والإجراءات والأدوات والمنتجات التي تستخدم للوقاية من أو تقليل المخاطر والتهديدات التي تتعرض لها الكمبيوترات والشبكات ونظم المعلومات وقواعدها ويمكن تصنيف هذه الوسائل إلى ما يلي:

١. مجموعة وسائل الأمن المتعلقة بالتعريف بشخص المستخدم وموثوقية الإستخدام ومشروعيته.

---

1 - سوسن المهتدي، مشروع تخرج مادة أمن المعلومات لدبلوم الحكومة الإلكترونية، الجامعة الأردنية، ٢٠٠٨.

٢. مجموعة الوسائل التي تهدف إلى منع إفشاء المعلومات لغير المخولين بذلك
٣. مجموعة الوسائل الهادفة لحماية التكاملية (سلامة المحتوى).
٤. مجموعة الوسائل المتعلقة بمنع الإنكار(إنكار التصرفات الصادرة عن الشخص).
٥. مجموعة الوسائل المتعلقة بمراقبة الإستخدام وتتبع سجلات النفاذ أو الأداء.

مجموعة وسائل الأمن المتعلقة بالتعريف الشخصي هي:

- الوسائل التي تهدف إلى ضمان إستخدام النظام أو الشبكة من قبل الشخص المخول وبهذا الإستخدام وتضم (كلمات السر بأنواعها، البطاقات الذكية المستخدمة للتعريف، وسائل التعريف البيولوجية.
- الوسائل المتعلقة بالتحكم بالدخول والنفاذ إلى الشبكة وهي التي تساعد في التأكد من أن الشبكة ومصادرها قد استخدمت بطريقة مشروعة وتشمل قوائم أشخاص المستخدمين أنفسهم.

مجموعة الوسائل التي تهدف إلى منع إفشاء المعلومات:

- تشمل تقنيات التشفير (تشفير المعطيات والملفات).
- إجراءات حماية نسخ الحفظ الاحتياطية ومكونات الشبكات.
- وتشمل أيضا إستخدام الفلترات والموجهات.

مجموعة الوسائل المتعلقة بسلامة المحتوى وهي:

الوسائل المناط بها ضمان عدم تعديل محتوى المعطيات من قبل جهة غير مخولة بذلك وتشمل تقنيات الترميز والتواقيع الإلكترونية وبرمجيات تحري الفيروسات.

مجموعة الوسائل المتعلقة بمنع الإنكار:

تهدف هذه الوسائل إلى ضمان عدم قدرة شخص المستخدم من إنكار أنه هو الذي قام بالتصرف وهي وسائل ذات أهمية بالغة في بيئة الأعمال الإلكترونية والتعاقدات على الخط وترتكز هذه الوسائل على تقنيات التوقيع الإلكتروني وشهادات التوثيق الصادرة عن طرف ثالث.

مجموعة وسائل مراقبة الإستخدام وتتبع سجلات الأداء وهي:

التقنيات التي تستخدم لمراقبة العاملين على النظام لتحديد الشخص الذي قام بالعمل المعين في وقت معين وتشمل كافة أنواع البرمجيات والسجلات الإلكترونية التي تحدد الإستخدام.

سبل الوقاية:

وللوقاية والحماية أثناء إستخدام البريد الإلكتروني يجب إتباع الآتي:

- إستخدام برامج مضادة للفيروسات وبرامج حماية وبرامج التشفير المتخصصة
- إستخدام كلمات عبور سهلة التذكر ولكن صعبة التخمين كأن تكون مكونة من حروف وأرقام أو خليط من الأحرف الكبيرة والصغيرة.
- غلق المتصفح حال ابتعادك عن الجهاز لتعطيل خاصية الرجوع للخلف في المتصفح.
- عدم إستخدام خاصية تذكر اسم المستخدم وكلمة العبور
- عدم إستخدام خاصية الإكمال الآلي والتلقائي للاسم وفراغات النماذج في المتصفح.
- عدم إستخدام خاصية تذكر الصفحات التي تقوم بزيارتها لفترات طويلة وتقليل هذه المدة على قدر المستطاع.
- عدم فتح الملفات المرفقة إذا كانت من أحد الأنواع التي تم ذكرها في البداية.
- عدم تحويل الرسائل المشبوهة الى أصدقائك ومعارفك.
- تعديل خاصية الأمن في المتصفح إلى المستوى المتوسط أو الأعلى مع تعطيل خاصية الجافا سكريبت. وتعديل مستوى الأمن في خاصية الآكتف اكس.

عند الانتهاء من قراءة الرسائل عليك الخروج بطريقة صحيحة من الموقع أو البرنامج ويكون ذلك بتسجيل الخروج أو ما يعرف ب Sign out، لان هناك بعض برامج البريد أو المواقع تتذكرك لمدة تصل إلى ٨ ساعات وترحب بك مباشرة حال دخول أي شخص آخر للموقع ذاته.

Backup Solution

لا شك أنه إذا كان هناك نسخة احتياطية من البيانات الهامة لديك سيكون ذلك عنصر من عناصر الأمان في استرجاع آخر نسخة موجودة قبل حدوث

أي تخريب في البيانات المخزنة لذا لا بد من اتخاذ الإجراءات التالية عند عمل أي ملف للعمل:

- نسخ احتياطية من قواعد البيانات.
- نسخ احتياطية من الملفات المتداولة يوميا لموظفي المؤسسة.
- نسخ احتياطية من النظم المملوكة للمؤسسة.
- نسخ احتياطية من البريد الإلكتروني.
- نسخ احتياطية من مواقع المؤسسة.
- صور من الأجهزة المطلوب تشغيلها فورا (Image)

Antivirus:

هناك العديد من أنظمة الحماية من الفيروسات ومنها ما يعمل بصورة فردية على الحاسبات الشخصية ومنها ما يعمل في بيئة الشبكات والأخير هام جدا في المؤسسات التي بها عدد كبير من الأجهزة لما لها من خاصية السيرفر والذي يتيح التحديث لكل الأجهزة مرة واحدة وكذلك التحذير المباشر لمسئول الشبكات عند دخول أي فيروس إلى أي حاسب بالشبكة كما يتيح لمسئول الشبكات من عمل إزالة للفيروس من أي جهاز مصاب دون الانتقال إلى الجهاز وبالتالي يسهل عملية التخلص من الفيروسات مباشرة.

ما هو برنامج مكافحة الفيروسات(Antivirus):

تساعد برامج مكافحة الفيروسات في حماية الكمبيوتر من معظم الفيروسات والبرامج الدودية وأحصنة طروادة ومخترقي الكمبيوتر الآخرين غير المرغوب فيهم الذين قد يقوموا بأفعال ضارة. قد يقوموا بحذف الملفات أو الوصول إلى البيانات الشخصية أو إستخدام الكمبيوتر الخاص بك في مهاجمة أجهزة الكمبيوتر الأخرى. يأتي برنامج مكافحة الفيروسات مثبتًا على الكمبيوتر الخاص بك أو يمكنك شرائه وتثبيته بنفسك.

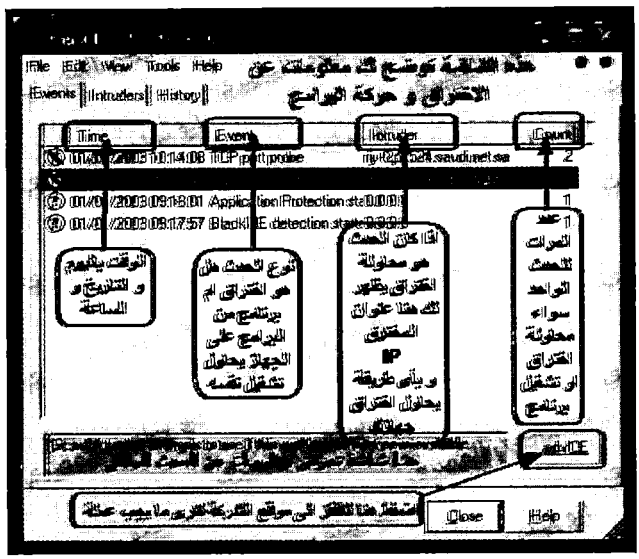
Firewall الجدران النارية:

الجدار الناري Firewall هو وسيط اعتيادي أو تطبيق برمجي يقوم بمراقبة

جميع البيانات والمعطيات التي تصل إلى المخدم عن طريق الإنترنت. إن الهدف الرئيسي من الجدار الناري هو حماية المعطيات المخزنة على مخدم الويب أو أي مخدم آخر متصل بالإنترنت من أي هجوم يقوم به العابثين والمخترقين من خارج الشركة. ويمكن إعداد الجدران النارية بحيث تتمكن من مراقبة أنماط معينة من البيانات، كالأوامر والتعليمات الغير مسموح بتنفيذها على المخدم. ومن الممكن القيام بحجب بيانات من مصادر معينة، كالمعلومات الآتية من دولة معينة، أو من مستخدم معين. تستخدم الشركات الجدران النارية عندما تقوم بتشغيل مواقع الويب على مخدماتها الخاصة، كالشركات الضخمة مثل IBM و Microsoft. تُستخدم الجدران النارية أيضا لاستضافة المواقع على مخدمات مزودي خدمات الإنترنت ISPs. إضافة، يتوجب إستخدام الجدران النارية إذا كانت حواسب الشركة متصلة بالإنترنت، سواء كانت الشركة كبيرة أم لا.

عندما يقوم المستخدم، ودود كان أم عابث، بالدخول الى مخدم الويب، يتم إرسال أوامر خاصة الى المخدم تطلب إتمام عملية الدخول. فإذا كان غرض المستخدم هو استعراض أحد صفحات الموقع، يقوم متصفح المستخدم بارسال أوامر خاصة ببروتوكول HTTP الى المخدم، وطلب ارسال معطيات الصفحة المطلوبة كي يقوم بمعاينتها على شاشة حاسبه. وتتم عملية إرسال الأوامر هذه بدون تدخل من المستخدم. لذا، فلا يكون للجدران النارية ضرورة عندما يكون المستخدمين شرفاء النية.

وتبرز الحاجة لإستخدام الجدران النارية عندما يبدأ المخترقين بالدخول بغرض العبث، أو التخريب، أو الاطلاع على ما ليسوا مخولين بالاطلاع عليه، ويتم منعهم من الدخول من خلال إيقاف الأوامر التي يرسلونها. ومع إن الجدار الناري يقوم بإيقاف محاولات قراصنة المعلومات غير الشرعية، إلا أنه يسمح بمرور الحركة الشرعية بدون عرقلة.



التصميم:

هناك نوعان من الجدران النارية المتوفرة. النوع الأول هو نظام فرز رزم المعطيات ويسمى Packet Filter، وهو الأقل تعقيدا. يقوم نظام فرز الرزم باختبار كل "بت" من البيانات القادمة من الإنترنت. وتتطلب عملية إعداد هذا النظام تعديل جدول يدعى جدول الفرز، والذي يتضمن العديد من القواعد التي تمنع أو تسمح للرزم بالدخول. فمثلا، يمكن إعداد الجدول بحيث يمنع خروج الرزم من عنوان محدد، أو تعريف قيود خاصة تمنع الدخول إلى مساحات محددة على المخدم.

إن ابسط طريقة لإعداد جدار ناري هي تركيب موجّه Router وتثبيته بين المخدم وخط اتصال الإنترنت، بحيث يقوم بمنع البيانات الغير مرغوب بها من الدخول إلى المخدم.

أما النوع الآخر من الجدران النارية فيدعى مضيف Bastion Host، وهو أكثر أنواع الجدران النارية تعقيدا.

Bastion Host هو عبارة عن حاسب مكرّس للأمن، يتم تركيبه بين خطوط اتصال الإنترنت من جهة، ومخدم الويب من جهة أخرى. تحتوي إعدادات هذا المضيف الأساسية على عدد محدود جدا من الملفات والمعطيات، أما مهمته فهي فحص البيانات الداخلة إلى النظام بالدرجة الأولى. فإذا طابقت البيانات القادمة من الإنترنت شروط هذا الجدار الناري، تم السماح لها بالمرور إلى مخدم الويب والاستجابة لطالبها.

بإمكان مضيف Bastion Host القيام بفحص حركة البيانات على مستوى التطبيقات والبرمجيات (الطبقة السابعة في نظام OSI)، بدلاً من فحصها على مستوى الشبكة والبرتوكلات IP (الطبقة الثالثة في نظام OSI)، كما هو الحال في معظم الجدران النارية الأقل تعقيدا. إضافة، بمقدور المضيف إنشاء سجلات دخول، وإعطاء تنبيه بالأفراد الذين يحاولون اختراق الشبكة أو العبث بالمعطيات، مقدما بذلك مستوى متطور من الحماية.

إن إستخدام هذا النوع من الجدران النارية يعني تركيب ثلاثة أجهزة على الأقل: مخدم شبكة، ومخدم ويب، ومضيف Bastion Host، وتكون كلها مكرسة لخدمة الشبكة.

أنواع الجدران النارية:

يتوفر حاليا ثلاثة أنواع من الجدران النارية :

١. جدران حماية لمستوى الشبكةNetwork layer التي توفر الحماية على أساس عناوين محددة في الشبكة يسمح لها بالتواصل دون الخوض في محتويات التواصل على الرغم من أن بعض الشركات حديثا توفر جدران حماية تقوم بتفحص محتويات الرسائل بين نقاط شبكة الاتصال. وتعتبر هذه الأنظمة سريعة ولكن يعاب عليها أن من السهل تخطيها والتلاعب عليها من قبل المستخدمين المحترفين.

٢. جدران حماية لمستوى التطبيقات Application layer عبارة عن حاسبات Hosts يتوفر بها حاسبات خادمة وكيل Proxy Servers وهو عبارة عن برامج تمنع الاتصال المباشر بين الشبكات وتسمح بالاتصال والدخول إلى الشبكات بعد التدقيق من توفر الصلاحية للجهة طالبة الاتصال. ويعتمد هذا النوع على البرامج التي تقوم بعميلة الترجمة للعناوين الشبكية التي ترغب في الاتصال. ولعل أهم نقطة ضعف في هذا النوع من أنظمة الجدران النارية هو البطء مقارنة بالنوع الأول.

٣. جدران حماية هجين Hybrids في الوقت الحاضر أصبحت الشركات المنتجة لأنظمة الجدران النارية تعتمد الطريقتين السابقتين بجعل الأنظمة تعتمد على طبقة الشبكات

وطبقة التطبيقات، حيث تطور الأمر لتصبح الأنظمة في الجزء المخصص لطبقة الشبكات قادر على تفحص عناوين الاتصال وطبقة التطبيقات قادرة على تفحص محتويات الاتصال عن طريق التأكد من توفر الصلاحيات، النتيجة توفر أنظمة توفر السرعة في الغربلة رزم الاتصال، كما إن الأنظمة الجديد توفر أنظمة تشفير يصعب اختراقها. مع ضرورة التأكيد أن الكثير من الأنظمة أصبحت توفر الحماية على كل المستويات، كما هو معلوم إن مقاييس الاتصالات التي تعتمد نظام ISO تتيح الاتصال عبر سبع طبقات تسمى نظام OSI الاتصال المفتوح Open Systems Interconnect الذي في مجمله يقسم الاتصال عبر الطبقات، وكل طبقة توفر خدمة للمستوى الأعلى عند النظر من الطبقات الدنيا للعليا.

تعتبر أنظمة الجدران النارية من النوع الأول جدران حماية لمستوى الشبكة Network layer أسرع ولكن من السهل اختراقها.

من هنا من الأفضل عند اختيار أنظمة الجدران النارية اختيار النوع الثالث الهجين الذي يوفر الحماية والتصفية على مستوى الشبكة والتطبيقات

أكثر وسائل الأمن شيوعا في بيئة نظم المعلومات:

١. الجدران النارية:

إن عمل الجدران النارية هو تصفية حركات البيانات وقد ظهرت أول الجدران النارية للشبكات في عام ١٩٨٠ وكانت عبارة عن موجهات تستخدم في تقسيم هذه الشبكات إلى شبكات محلية وقد تم إستخدام أول الجدران النارية لتحقيق الأمن في أوائل التسعينات وكانت عبارة عن موجهات لبرتوكول مع قوانين فلتره وكانت تسمح لبعض الأشخاص بالدخول إلى الملفات وكانت فعالة ولكنها محدودة وكان من الصعب إتقان وضع قوانين فلتره البيانات وكان يستدعي في بعض الأحيان إلى تغيير القوانين لذلك كان الجيل الجديد من الجدران النارية أكثر قدرة وأكثر مرونة للتعديل.

كانت توضع الجدران النارية على ما يعرف بالمستضيفات الحصينة وأول جدار ناري من هذا النوع والذي استخدم الفلاتر وبوابات التطبيقات كان من شركة ديجيتال الذي يستخدم البرمجيات الوسيطة (بروكسي) ثم تم طرح نظام خارجي يدعى بحارس البوابة وهو

النظام الوحيد الذي كان يمكنه مخاطبة الإنترنت وكان هناك أيضا بوابة للفلترة ومشبك داخلي للبريد.

❖ بدأ التنافس يزيد مما أدى إلى المزيد من الابتكارات في مجال الجدران النارية وتقديم خدمات متعددة مثل:

١. التحقق من هوية المستخدمين.

٢. الشبكات الافتراضية الخاصة وهي تشفير بيني للجدران النارية وكان أول منتج من هذا النوع هو Ans interlock وهي شبكات خاصة تستخدم التشفير.

٣. مراقبة المحتوى ومن بعض الإضافات التي وضعت في الجدران النارية هي البحث عن الفيروسات ومراقبة عناوين الإنترنت ومنع برمجيات جافا وبرمجيات فحص ومراقبة الكلمات السرية.

❖ الجدران النارية الخاصة Firewall appliances وهو جيل جديد من الجدران النارية وهو يحتوي على عدد من التقنيات بما في ذلك حلول جدران ناريه جاهزة Turnkey أي لا تحتاج إلى إعداد من قبل المستخدم ويمكن البدء بإستخدامها فور الحصول عليها دون الحاجة إلى إجراء أية تعديلات خاصة على نظام التشغيل أو البنية التحتية المستخدمة.

٢- تشفير البيانات:

نبذة تاريخية :

استخدم الإنسان التشفير منذ نحو ألفي عام قبل الميلاد لحماية رسائله السرية، وبلغ هذا الإستخدام ذروته في فترات الحروب؛ خوفا من وقوع الرسائل الحساسة في أيدي العدو. وقام يوليوس قيصر بتطوير خوارزميته المعيارية المعروفة باسم شيفرة قيصر (Caesar Cipher) التي كانت نصّا مشفّرا (Cipher text)؛ لتأمين اتصالاته ومراسلاته مع قادة جيوشه. وظهرت فيما بعد العديد من الآلات التي تقوم بعمليات التشفير، ومنها آلة التلغيز(Enigma machine).

وشكّل الكمبيوتر في بدايات ظهوره وسيلةً جديدة للاتصالات الآمنة، وفك تشفير رسائل العدو. واحتكرت الحكومات في فترة الستينيات حق التشفير وفك التشفير. وفي أواخر الستينيات، أسست شركة أي بي أم (IBM) مجموعة تختص بأبحاث التشفير، ونجحت هذه

المجموعة في تطوير نظام تشفير أطلقت عليه اسم لوسيفَر (Lucifer). وكان هذا النظام مثارا للجَدَل، ورغم تحفّظات الحكومة الأمريكية علية لإعتقادها بعدم حاجة الشركات والمؤسسات الخاصة إلى أنظمة التشفير، إلا أنه قد حقق انتشارا واسعاً في الأسواق. ومنذ ذلك الحين، أخذت العديدُ من الشركات تقوم بتطويرَ أنظمة تشفير جديدة، مما أبرز الحاجة إلى وجود معيار لعمليات التشفير.

ومن أبرز المؤسسات التي أسهمت في هذا المجال، المعهد الوطني للمعايير والتكنولوجيا (National Institute of Standards and Technology- NIST) المعروف سابقا باسم المكتب الوطني الأمريكي للمعايير (U.S. National Bureau of Standards)، إذ طوَّر هذا المعهد عام ١٩٧٣ معيارا أطلق عليه معيار تشفير البيانات (Data Encryption Standard- DES). ويستنِد هذا المعيار إلى خوارزمية لوسيفَر (Lucifer algorithm) التي تستخدِم مفتاح تشفير بطول ٥٦ بت (bit)، وتشترط أن يكون لكل من المرسِل والمستقبِل المفتاحَ السري ذاته. وقد استخدمت الحكومة هذا المعيار الرسمي عام ١٩٧٦، واعتمدته البنوك لتشغيل آلات الصراف الآلي (ATM).

وبعد عام واحد من تطبيق معيار تشفير البيانات (DES)، طوَّر ثلاثة أساتذة جامعيون نظامَ تشفير أخر أطلقوا عليه اسم (RSA)، ويستخدم هذا النظام زوجا من المفاتيح (مفتاح عام (public key)، ومفتاح خاص (private key)) عوضا عن إستخدام مفتاح واحد فقط. ورغم إن هذا النظام كان ملائما جدا لأجهزة الكمبيوتر المعقّدة، إلا انه قد تم اختراقه فيما بعد. وبقيت الحال على ذلك حتى قام فيل زيمرمان (Phil Zimmerman) عام ١٩٨٦ بتطوير برنامج تشفير يعتمد نظام (RSA)، ولكنه يتميز بإستخدام مفتاح بطول ١٢٨ بت، ويُدعى برنامج الخصوصية المتفوِّقة (Pretty Good Privacy- PGP). ويتوفر من هذا البرنامج نسخة تجارية و نُسخة مجانية، وهو من أكثر برامج التشفير انتشارا في وقتنا الحالي.

ما هو التشفير:

هو تغير شكل البيانات المنتقلة عبر الشبكة حتى لا يتمكن أحد من الاطلاع عليها وبالتالي لا يمكن التعديل أو الحذف بها. وبالتالي يكون تحقق الخصوصية السرية مع أتاحه البيانات.

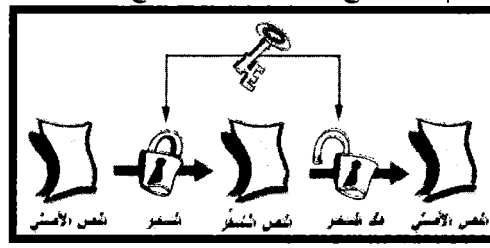
أنواع التشفير[1]:

١- التشفير المتماثل (المفتاح السري):

هو نوع من أنواع التشفير والذي يحتوى على مفتاح للشفرة ونفس المفتاح لفك الشفرة. في التشفير المتماثِل، يستخدم كل من المرسِل والمستقبل المفتاحَ السري ذاته في تشفير الرسالة وفك تشفيرها. ويتفق الطرفان في البداية على عبارة المرور (passphrase) (كلمات مرور طويلة) التي سيتم إستخدامها. ويمكن أن تحوي عبارة المرور حروفا كبيرة وصغيرة ورموزا أخرى. وبعد ذلك، تحوِّل برمجيات التشفير عبارة المرور إلى عدد ثنائي، ويتم إضافة رموز أخرى لزيادة طولها. ويشكِّل العدد الثنائي الناتج مفتاح تشفير الرسالة.

وبعد استقبال الرسالة المُشفَّرة، يستخدم المستقبل عبارةَ المرور نفسها من اجل فك شيفرة النص المُشفَّر (cipher text or encrypted text)، إذ تترجم البرمجيات مرة أخرى عبارةَ المرور لتشكيل المفتاح الثنائي (binary key) الذي يتولى إعادة تحويل النص المُشفَّر إلى شكله الأصلي المفهوم.

ويعتمد مفهوم التشفير المتماثِل على معيار Data Encryption Standard DES. أما الثغرة الكبيرة في هذا النوع من التشفير فكانت تكمن في تبادُل المفتاح السري دون أمان، مما أدى إلى تراجُع إستخدام هذا النوع من التشفير، ليصبح شيئا من الماضي.



٢- التشفير اللامتماثل (المفتاح العام)

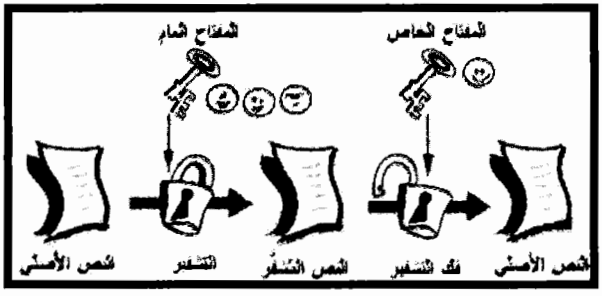
جاء التشفير اللامتماثل حلا لمشكلة التوزيع غير الأمن للمفاتيح في التشفير المتماثل، فعوضا عن إستخدام مفتاح واحد، يستخدِم التشفير اللامتماثِل مفتاحين اثنين تربط بينهما علاقة. ويُدعى هذان المفتاحان بالمفتاح العام (public key)، والمفتاح الخاص (private key).

---

1 - شبكة الإنترنت، شبكة مشروع سمو الشيخ محمد بن راشد آل مكتوم لتعليم تكنولوجيا المعلومات، التشفير، www-itep.ae.

ويكون المفتاح الخاص معروفا لدى جهة واحدة فقط أو شخص واحد فقط؛ وهو المرسِل، ويُستخدَم لتشفير الرسالة وفك شيفرتها. أما المفتاح العام فيكون معروفا لدى أكثر من شخص أو جهة، ويستطيع المفتاح العام فك شيفرة الرسالة التي شفَّرها المفتاح الخاص، ويمكن إستخدامه أيضا لتشفير رسائل مالك المفتاح الخاص، ولكن ليس بإمكان احد إستخدام المفتاح العام لفك شيفرة رسالة شفَّرها هذا المفتاح العام، إذ أن مالك المفتاح الخاص هو الوحيد الذي يستطيع فك شيفرة الرسائل التي شفرها المفتاح العام.

ويُدعى نظام التشفير الذي يستخدم المفاتيح العامة بنظام Rivest, Shamir, and Adelman RSA وهي أسماء مخترعين هذه التقنية، ورغم انه أفضل وأكثر أمنا من نظام DES إلا انه أبطا؛ إذ أن جلسة التشفير وجلسة فك التشفير يجب أن تكونا متزامنتين تقريبا. وعلى كل حال، فان نظام RSA ليس عصيا على الاختراق، إذ أن اختراقه أمر ممكن إذاً توفَّر ما يلزم لذلك من وقت ومال. ولذلك، تمّ تطوير نظام PGP الذي يُعَدُّ نموذجا محسَّنا ومطوَّرا من نظام RSA. ويستخدم PGP مفتاحا بطول ١٢٨ بت، إضافة إلى إستخدامه البصمة الإلكترونية للرسالة (message digest). ولا يزال هذا النظام منيعا على الاختراق حتى يومنا هذا.



التشفير اللامتماثل

وتستنِد هذه المفاتيح إلى صيَغ رياضية معقَّدة (خوارزميات)، وتعتمد قوة وفعالية التشفير على عاملين أساسيين:

١. الخوارزمية.
٢. وطول المفتاح (مقدَّرا بالبت (bits)). ومن ناحية أخرى، فان فك التشفير هو عملية إعادة تحويل البيانات إلى صيغتها الأصلية، وذلك بإستخدام المفتاح المناسب لفك الشيفرة.

لماذا نستخدم التشفير:

١. لمنع الاطلاع على المعلومات المنتقلة عبر الشبكة.
٢. إستخدام بياناتك الشخصية لإرسال رسائل مزيفة نيابة عنك.
٣. التغير في البيانات المنقولة عبر الشبكة.
٤. تغير كلمات السر الخاصة.

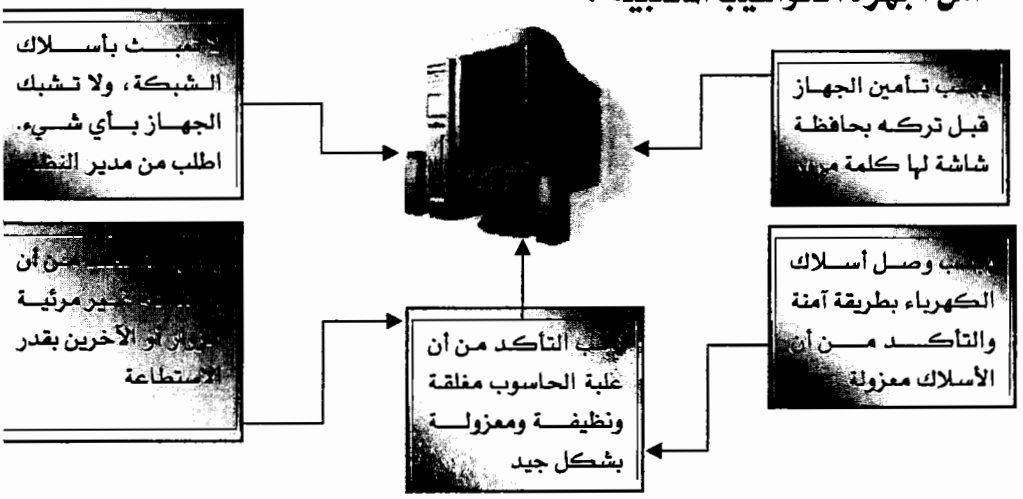
طرق التشفير المتاحة:

١. شفرة قيصر.
٢. شفرة (Data Encryption Standard- DES).
٣. التشفير بإستخدام المفتاح العلني.
٤. شفرة (Rivest ,Shamir & Adleman RSA).
٥. شفرة (Escrowed Encryption System EES).

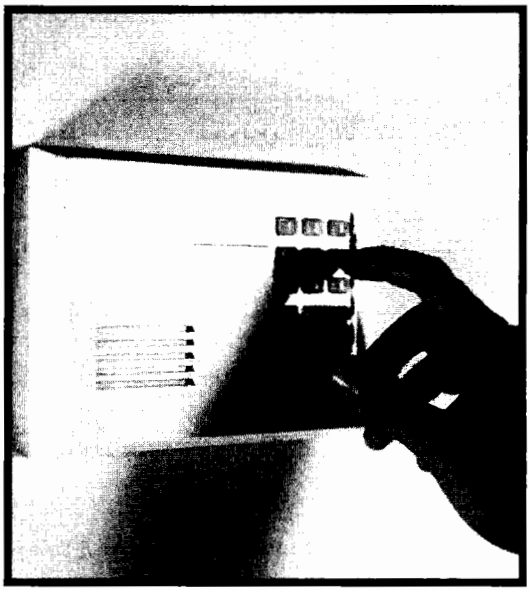
أمن أجهزة الحواسيب المكتبية:

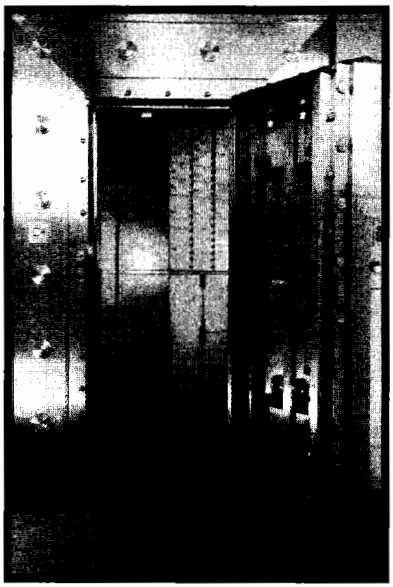
١. أجهزة الحاسوب المكتبية هي من أكثر موارد المعلومات إستخداما في الدوائر.
٢. أجهزة الحاسوب المكتبية هي المدخل والمخرج لأغلب المعلومات في الدائرة.
٣. كيف نحمي أجهزة الحاسوب المكتبية في الدائرة؟

أمن أجهزة الحواسيب المكتبية :



ضوابط الدخول:





- هل تظن أنه من المناسب أن تعطي الحرية لجميع المستخدمين والموظفين بعمل ما يشاؤون داخل الدائرة دون وضع ضوابط تتحكم في وصولهم إلى المعلومات ومواردها؟
- أي فوضى ومخاطر يمكن أن تحدث عند غياب مثل هذه الضوابط؟
- هل فكرت يوماً ماذا يمكن أن يحدث إذا لم تكن هناك كلمات مرور؟ أو مفاتيح أو بطاقات مرورو، أو كاميرات مراقبة وأسلاك شائكة سواءاً في المواقع المدنية أو العسكرية مثلا؟؟

لذا ،لا بد من ضوابط للدخول حيث أنها تبني العلاقة بين الجهة الطالبة (Subject) والشيء المطلوب (Object) على أنها الآليات التي يتم بها منح أو تقييد وصول الجهة الطالبة إلى الشيء المطلوب وطبيعة العلاقة بينهما.

لضوابط الدخول عدة أنواع مفصلة على النحو التالي:

الرادعة	تكون إستباقية قبل محاولة الوصول وتتبني عليها عادة عقوبات مثل القوانين
المانعة	تمنع دخول الأطراف غير المخولين إلى الأنظمة مثل كلمات المرور
الكاشفة	تتبع الأطراف الذين استطاعوا الدخول بشكل غير مخول مثل سجل الحركات
التصحيحية	تعدل الآثار الناتجة عن الدخول غير المخول مثل النسخ الإحتياطي

ومن أهم مبادئ ضوابط الدخول ما يلي:

١. الفصل بين المهام: أي إعطاء الموظفين صلاحيات محددة تعتمد على متطلبات الوظيفة الخاصة به، دون أن تتقاطع مع غيره من الموظفين.

٢. المعرفة على قدر الحاجة: أي عدم إعطاء صلاحيات موسعة تزيد على القدر المطلبو لإنجاز العمل المطلوب.

٣. مبدأ الإمتيازات الأقل: أي إعطاء أقل حد ممكن من الصلاحيات لإتمام العمل المطلوب، أو الدخول إلى نظام ما، أو الإستفادة من خدمات معينة.