المحاضرة المباشرة الاخيرة

الجزء الأول : أمن وحماية المعلومات

الجزء الثاني : الفايروسات

الجزء الثالث : برامج التجسس

الاستاذ محمد فهد طيفور

أمن شبكات الحاسب الآلي

مقدمة

في عصرنا الحاضر، أصبحت شبكات الحاسب الآلي من التجهيزات الأساسية لأي منشأة. وما يؤرق مالكي ومستخدمي شبكات الحاسب الآلي، هو موضوع أمن هذه الشبكات، خاصة في ظل تزايد استخدام شبكة الإنترنت (الغير آمنة) كناقل رئيسي للبيانات الموزعة. وفي هذا الجزء سنتطرق للمتطلبات الاساسية لأمن الشبكات وذلك على النحو التالي :

- التدابير الأمنية العامة لأمن شبكات الحاسب الآلي
- أمن وسائط نقل المعلومات
- استخدام جدران النار

التدابير الأمنية العامة لأمن شبكات الحاسب الآلي (1)

هناك بعض الإجراءات التي تساعد على المحافظة على أمن شبكات الحاسب الآلي، ويجب تطبيقها بشكل عام وهي :

- تطبيق وتفعيل ومراجعة سياسة أمن معلومات المنشأة. ومن ذلك على سبيل المثال، سياسة كلمات المرور .
- التدريب المتقن للمستخدمين على التعامل مع إجراءات وبرامج أمن المعلومات.
- التأكد من أمن المعدات وصعوبة الوصول إليها من قبل غير المخولين.
- تشفير البيانات عند الحاجة .
- تزويد المستخدمين بأجهزة لا تحتوي على محركات أقراص مرنة أو مضغوطة أو حتى أقراص صلبة قدر الإمكان. وكخيار آخر إبطال عمل هذه المحركات وقفل جميع منافذ الإتصال الغير ضرورية.

التدابير الأمنية العامة لأمن شبكات الحاسب الآلي (2)

- تفعيل خدمات تسجيل جميع العمليات التي يتم إجراؤها على الأجهزة الرئيسية وقواعد البيانات (Log Files) للرجوع لها عند الضرورة.
- إعطاء تصاريح (Permissions) للمستخدمين للوصول للبيانات و المعدات كل حسب طبيعة عمله.
- تزويد المستخدمين بحقوق (Rights) تحدد الأنشطة والعمليات المسموح لهم إجراءها على النظام .
- التنقيح (الفلتره) باستخدام العنوان الفيزيائي لبطاقة الشبكة (MAC Address) كآلية لتحديد أو توفير الوصول إلى الشبكة .
- حماية وسائط نقل المعلومات من كيابل وأجهزة ربط .
- استخدام جدران النار (أو جدران الحماية).
- استخدام الشبكات الخاصة الافتراضية.

أمن وسائط نقل المعلومات

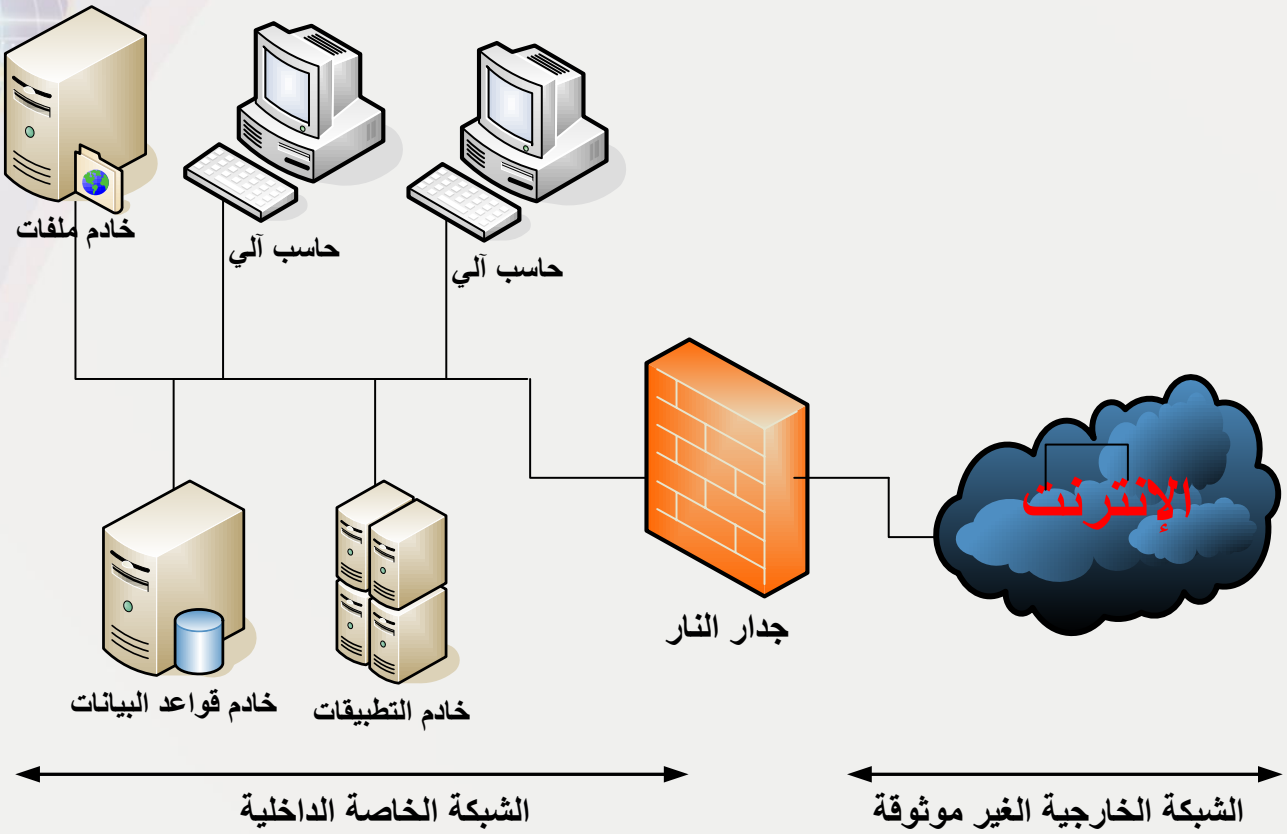
من أهم ما يوفر الحماية لهذه المكونات ما يلي :

- وضع جميع الكيبلات داخل مجارى خاصة بها (أو دكتات) مغلقة تحميها من الوصول إليها ومن وصل أي أدوات بها قد يتم سرقة المعلومات من خلالها.
- استخدام كبائن محكمة الغلق لتجميع الكيابل بها.
- استخدام كيابل الألياف البصرية للربط بين المباني وفي المناطق المهمة والحساسة لما تتميز به من عدم إمكانية تداخل الإشارات وعدم القدرة على التقاط البيانات المارة بها.
- عدم التمديد في الأماكن العامة في المنشأة أو خارج المباني إلا عند الضرورة القصوى.

جدار النـار (Firewall)

- عندما تكون شبكة الحاسب الآلي الخاصة (أو الحاسب الآلي الخاص) متصلة بشبكة الإنترنت أو أي شبكة خارجية، فإنه يتكون هناك طريقين للإتصال، أحدهما يصل من الخارج إلى الشبكة الخاصة والآخر من الشبكة الخاصة إلى الخارج.
- لمنع أي وصول غير مصرح به للشبكة الخاصة فيجب استخدام أداة منع خاصة تسمى "جدار النار".
- جدار النار إما أن يكون جهاز مستقل خاص يتم تصنيعه لهذا الغرض وبه برامجه الخاصة به، أو يكون برنامج يركب على أجهزة الحاسب الآلي العادية.

أساسيات عمل جدار النار (1)



شكل (8-1): أساسيات عمل جدار النار

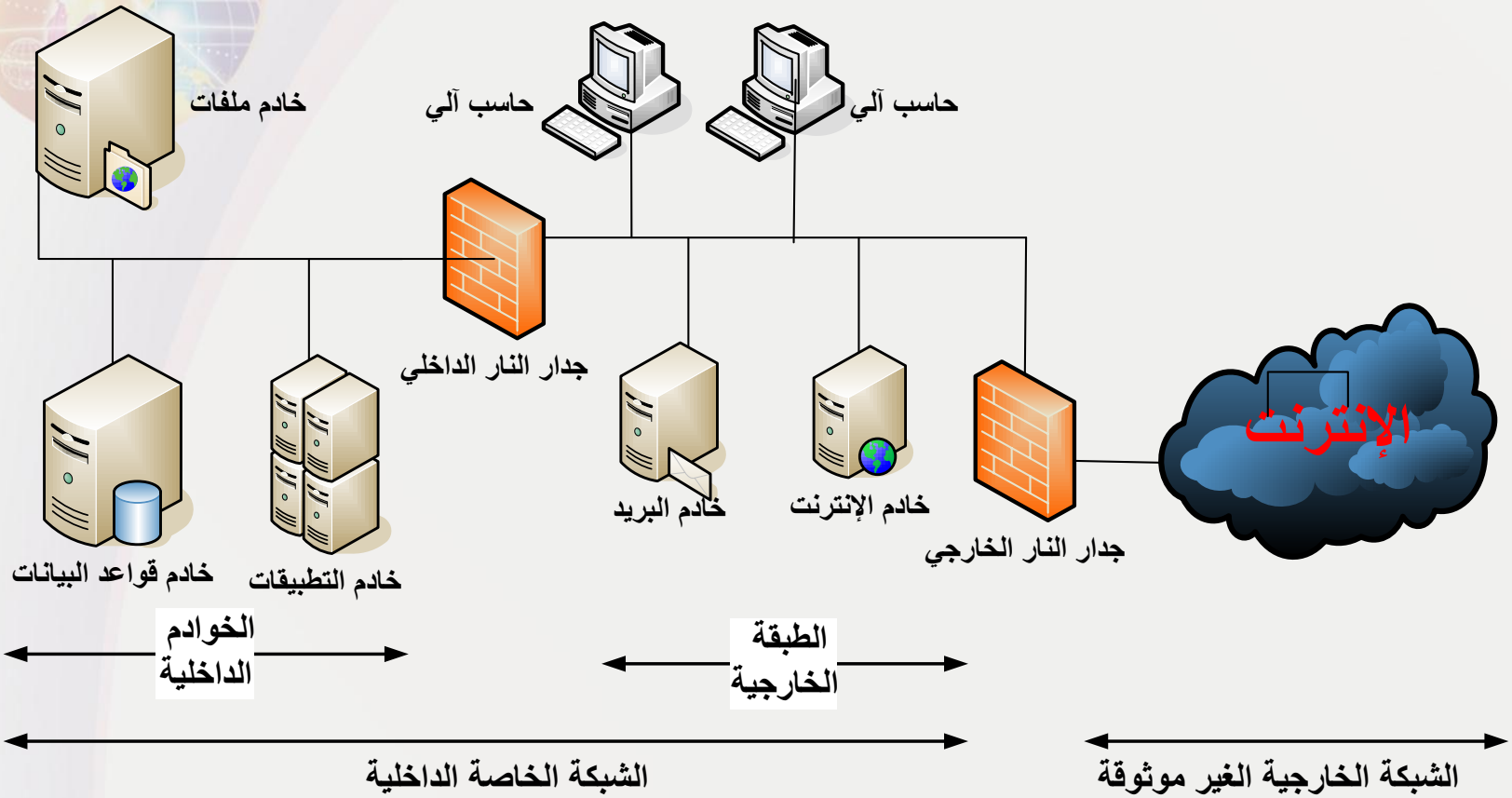
أساسيات عمل جدار النار (2)

- يعمل جدار النار كمصفي أو منقح لرزم (Packet) البيانات الداخلة والخارجة من وإلى الشبكة الخاصة.
- يكوّن جدار النار طبقة عازلة بين الشبكة الخاصة والعالم الخارجي (أنظر الشكل (8-1).
- تمر جميع رزم البيانات الداخلة والخارجة من وإلى الشبكة الخاصة عبر جدار النار ليقوم بتصفيتها والسماح فقط للرزم أو الأنشطة المصرح لها بالمرور.

أساسيات عمل جدار النار (3)

- التصفية تكون على عدة أشكال. فإما أن تكون على أساس نوع البيانات, فمثلاً قد يمنع أي رزمة من النوع الناقل للملفات (FTP) من المرور, أو تكون على أساس التاريخ والوقت, فمثلاً قد يمنع أي رزمة من نوع (HTTP) أثناء أوقات الدوام الرسمي للمنشأة, أو على أساس أي تصفية أخرى حسب الحاجة.
- إن جدار النار الموضح في الشكل أعلاه يكون مناسباً للشبكات التي تكون فيها الأخطار المتوقعة على المعلومات خارجية (الإنترنت مثلاً).

أساسيات عمل جدار النار (4)



شكل (8-2): استخدام طبقتين من جدران النار لمزيد من الحماية

أساسيات عمل جدار النار (5)

- في التصاميم الحديثة لشبكات الحاسب يجب أن يوضع جدار نار آخر كطبقة عازلة بين أجهزة الخوادم الرئيسية والشبكة الداخلية لمنع الأخطار الداخلية أيضاً، (أنظر الشكل 8-2) .
- توضح الدراسات الحديثة أن ما نسبته 70 – 80 % من المخاطر التي تتعرض لها الأجهزة الرئيسية تكون من المستخدمين الداخليين الذين عادة ما يكون لهم الصلاحية بالدخول عليها.
- تظهر أهمية عمل التهيئة والتعريفات اللازمة لجدار النار بالشكل الصحيح ومن المعروف أن عمل تهيئة خاطئة لجدار النار قد يكون له أثر سلبي أكثر مما لو لم يكن هناك جدار نار بالكلية.

أساسيات عمل جدار النار (6)

وتعتمد جدران النار في عملها على جداول التنقيح (الفلتره) التي يتم تخزينها داخل جدار النار. وهناك نوعان من عملية التنقيح :

- التنقيح الإيجابي : يسمح لرزم البيانات المطابقة للشروط المدونة في جدول التنقيح بالمرور ويمنع جميع الرزم الأخرى.
- التنقيح السلبي : يمنع رزم البيانات المطابقة للشروط المدونة في جدول التنقيح من المرور ويسمح لجميع الرزم الأخرى.

أساسيات عمل جدار النار (7)

من أشهر طرق التنقيح :

1. التنقيح باستخدام العناوين (Address Filtering) :

- يتم السماح لرزم البيانات من عدمه باستخدام جداول تنقيح العناوين بحيث تحتوي هذه الجداول على العناوين المسموح الإرسال إليها أو المسموح الاستقبال منها.
- هذه الطريقة لوحدها لا توفر حماية جيدة بسبب كثرة العناوين والتي تتطلب تخزين جداول كبيرة الحجم وكذلك تتطلب تحديث مستمر لهذه الجداول.

أساسيات عمل جدار النار (8)

2. التنقيح باستخدام المنافذ (Port Filtering) :

- هذه الطريقة من أشهر طرق التنقيح وأكثرها انتشاراً وفيها يتم السماح لرزم البيانات من عدمه بناءً على رقم المنفذ المستخدم.
- على سبيل المثال يستخدم بروتوكول نقل الملفات (FTP) المنفذين رقم (20, 21)، ويمكن السيطرة على هذه النوعية من الرزم بقفل هذه المنافذ وينتج عن ذلك عدم القدرة على نقل الملفات.

أساسيات عمل جدار النار (9)

3. التنقيح باستخدام النطاق (Domain Filtering) :

وتستخدم هذه الطريقة لقفل النطاقات الغير مرغوب فيها ومنع تلك النطاقات من الوصول إلى الشبكة الداخلية.

مميزات جدار النار

- طريقة حماية جيدة لشبكات الحاسب الآلي ومصادر المعلومات الهامة في حالة تهيئتها ومراقبتها بالشكل الصحيح.
- يمكن أن يقوم جدار ناري واحد بحماية عدد كبير من الأجهزة خلفه الأمر الذي معه يمكن تقليل تكلفة الحماية.
- يشكل جدار النار نقطة تحكم مركزية يمكن التحكم فيها بسهولة.

عيوب جدار النار

- لابد من تهيئتها وإدارتها ومراقبتها من قبل أشخاص مدربين جيداً.
- التهيئة الخاطئة لجدار النار تشكل ثغرة أمنية كبيرة.
- في بعض الحالات يؤدي استخدام جدار النار إلى تخفيض سرعه أداء الشبكة عند تهيئته بشكل معقد.

الجزء الثاني

الفايروسات: البرامج الضارة وطرق مكافحتها

البرامج الضارة وطرق مكافحتها

مقدمة

البرامج الضارة (Malware)، هو مصطلح جديد نسبياً في مجال الأمان. وقد تم استخدام هذا المصطلح للحاجة لمناقشة البرامج أو التطبيقات التي صممت خصيصاً بحيث تحتوي على مهام اختراق الأنظمة، كسر سياسات وخطط الأمان، أو القيام بأعمال ماكرة أو عمليات مدمرة. ومن خلال هذا الجزء، نقدم شرحاً لأغلب وأشهر البرامج الضارة وبعد ذلك، نقدم طرق مكافحة هذه البرامج بشكل موحد.

تعريف فيروسات الحاسب الآلي

- تعتبر الفيروسات هي أكبر فئات البرامج الضارة من ناحية عدد الأشكال المعروفة ومن ناحية أثرها على بيئة الحاسب الآلي.
- يعرف فريد كوهين الفيروس بأنه "برنامج يقوم بتعديل البرامج الأخرى لكي تحتوي على نسخة معدلة من نفسها".
- يمكن تعريف الفيروسات بصورة عامة بأنها "البرامج التي تقوم بإقحام نفسها بنفسها في مادة أخرى قد تكون برنامجاً أو قرصاً أو وثيقة أو رسالة بريد الكتروني أو نظام كمبيوتر أو أي صيغة معلوماتية".

خصائـص الفيروسات

1. التخفي.
2. التضاعف.
3. الانتشار.

1. التخفي

ويعني القدرة على الارتباط ببرامج أو ملفات أخرى تبدوا سليمة ومألوفة للمستخدم بحيث يقوم الفيروس بإلحاق نفسه بالملف المصاب خفية ليصبح جزء منه.

ومن أشهر طرق تخفي الفيروسات ما يلي:

- التخفي في مرفقات البريد الإلكتروني.
- التخفي في الملفات التي يتم تحميلها من مواقع الإنترنت خاصة تلك التي تقوم بتشغيل وتبادل ملفات الصوتيات والفيديو.
- التخفي وراء الروابط والأوامر الموجودة في صفحات الإنترنت والبريد الإلكتروني.
- التخفي وراء روابط وملفات الإعلانات والبريد الدعائي.
- التخفي مع البرامج المنسوخة بشكل غير قانوني.

2. التضاعف

- ويعني ذلك أن يقوم الفيروس بنسخ نفسه عدة نسخ تصل في بعض الأحيان إلى ملايين النسخ.
- أي بمعنى أنه يتكاثر ليصيب أكبر قدر ممكن من الملفات والبرامج داخل نفس جهاز الحاسب الآلي أو الأجهزة الأخرى المرتبطة به.
- وتبدأ عملية التضاعف عندما يتم تحميل برنامج الفيروس إلى ذاكرة الحاسب الآلي ويقوم المعالج بتنفيذه.

3. الانتشار

ويعني انتقال الفيروس من جهاز إلى آخر عبر شبكات الحاسب الآلي أو وسائط التخزين المختلفة.

ومن أشهر طرق انتشار الفيروسات ما يلي:

- تحميل ملفات مصابه من مواقع شبكة الإنترنت أو زيارة مواقع تقوم بنشر الفيروسات بشكل تلقائي.
- فتح مرفقات بريد الكتروني مصابه.
- أن يقوم المستخدم بنسخ ملفات مصابه دون علمه وتخزينها على وسائط تخزين خارجية تنتشر معها أو يقوم بإرسالها عبر الشبكة (كاستخدام المجلدات المشتركة) فتنتشر عبر الشبكة.
- أن يقوم الفيروس بنسخ نفسه ثم إرفاق نفسه مع أي ملف آخر عند استثارته.

أنواع الفيروسات

1- فيروسات قطاع بدء التشغيل (الإقلاع).

2- فيروسات الملفات.

3- الفيروسات الجزئية الكبيرة.

4- فيروسات البريد الإلكتروني.

1- فيروسات قطاع بدء التشغيل (الإقلاع)

- يوجد لكل نظام تشغيل قطاع في قرص التخزين الصلب مخصص لبدء عملية التشغيل (الإقلاع) وعادة يكون هذا القطاع هو القطاع الأول (Track 0).
- فيروسات قطاع بدء التشغيل (Boot Sector Viruses) هي الفيروسات التي تصيب قطاع بدء التشغيل في قرص التخزين الصلب.
- وتكمن خطورة هذا النوع من الفيروسات في إصابتها لمكان هام جداً يتم من خلاله توجيه الجهاز لتنفيذ البرامج التي يتم من خلالها استكمال تجهيز جهاز الحاسب الآلي للعمل وبدلاً من ذلك يقوم الفيروس بتوجيه الحاسب الآلي لتنفيذ الكود الخاص بالفيروس وبالتالي يفشل الجهاز في عملية الإقلاع ولا يمكنه العمل.

2- فيروسات الملفات

- فيروسات الملفات (File Infecting Viruses) هي الفيروسات التي تصيب الملفات على شتى أنواعها.
- يمكن أن تصيب ملفات نظام التشغيل كملف (Command.com) في نظام الويندوز أو أي ملف آخر.
- عادة ما ينتج عن هذه الفيروسات زيادة في أحجام الملفات.

3- الفيروسات الجزئية الكبيرة

- تستخدم الفيروسات الجزئية الكبيرة (Macro Viruses) البرمجة الجزئية الخاصة بتطبيق معين - مثل معالج الكلمات - للبدء بنشاطها.
- وتضرب هذه النوعية من الفيروسات ملفات البيانات (مثل ملفات برامج وورد واكسل من شركة مايكروسوفت) وتظل ساكنة في التطبيق نفسه عن طريق إصابة حقل التهيئة الخاص به.
- ورغم أن الفيروسات الجزئية الكبيرة تصيب ملفات البيانات، لكن بصورة عامة لا تعد من ضمن فيروسات الملفات. والسبب في ذلك أن فيروسات الملفات قد تصيب البرامج وملفات البيانات بينما فيروسات الجزئية الكبيرة لا تصيب إلا ملفات البيانات فقط.

4- فيروسات البريد الإلكتروني

- هي الفيروسات التي تنتقل بواسطة البريد الإلكتروني فبإضافة بعض الوظائف (عن طريق الفيروس) لبرنامج مقدم خدمة البريد الإلكتروني القياسي (مثل مايكروسوفت أوت لوك (Outlook)) أصبح للفيروسات إمكانية الانتشار عبر العالم خلال ساعات فقط بدلاً عن شهور.
- ومن أشهر فيروسات البريد الإلكتروني فيروس ماليسا (Melissa). وماليسا ليس أول فيروس بريد الكتروني، بل أول فيروس بريد الكتروني انتشر بنجاح بصورة شرسة هو فيروس (Christma Exec) في خريف 1987م .
- ويعتبر ماليسا من الفيروسات الجزئية الكبيرة، فبالإضافة إلى أنه يعمل كفيروس بريد الكتروني، إلا أنه يمكن أن يرسل نفسه ذاتياً في شكل وثيقة مصابة بالفيروس.

أعراض الإصابة بالفيروسات

- البطء الشديد.
- تعليق (أو تجمد) الحاسب الآلي.
- انهيار الحاسب الآلي.
- إضاءة لمبة القرص الصلب بشكل عشوائي ومتصل.
- زيادة أحجام الملفات وزيادة الزمن اللازم لفتحها أو تشغيل البرامج.
- وجود بيانات تالفة كانت صالحة من قبل.
- ظهور رسائل خطأ ومربعات حوار غير مألوفة وغير متوقعة.
- إعادة تشغيل الحاسب الآلي بشكل آلي مستمر دون تدخل المستخدم.

ديدان الحاسب الآلي (1)

- دودة الحاسب الآلي (Worm Computer) هي عبارة عن برنامج مستقل بحد ذاته وله ملف خاص به فالدودة تعتبر برنامج تطبيقي متكامل يمكن أن يعمل لوحده ولا يحتاج لأن يضيف نفسه لملف آخر كما هو الحال في الفيروسات.
- **الفوارق الأصلية بين الديديدان والفيروسات:**

1. الديدان تستخدم الشبكات وروابط الإتصالات لكي تنتشر، وهي خلافاً للفيروسات لا تلتحم مباشرة بالملفات القابلة للتنفيذ.

ديدان الحاسب الآلي (2)

2. تصيب الديدان أجهزة الحاسب الآلي المرتبطة بشبكات الحاسب الآلي المصابة دون تدخل المستخدم أو قيامة باستثارتها كفتح ملف معين أو تشغيل برنامج كما هو الحال في الفيروسات.
3. تنتقل إلى الجهاز بمجرد تصفح بعض مواقع الإنترنت أو بمجرد فتح بريد إلكتروني (إذا لم يكن الجهاز محمياً ببرنامج حماية محدث). وهذا الأمر يجعلها تنتشر بشكل أسرع وأوسع من الفيروسات.

طرق انتشار الديدان

من أهم الطرق التى تنتشر بها الديدان ما يلى:

1. مرفقات البريد الإلكتروني المصابة.
2. التسلل عبر الثغرات الأمنية في أنظمة التشغيل أو برامج الحماية.
3. التحميل التلقائي عند زيارة بعض مواقع الإنترنت التي من خلالها تنتشر الديدان أو عند استخدام احد الارتباطات داخل البريد الإلكتروني.

أضرار الديدان

من أهم أضرار الديدان ما يلى:

- تتيح للمهاجم أن يستخدم الحاسب الآلي المصاب لمهاجمة مواقع الإنترنت أو إرسال بريد إلكتروني أو تحميل برامج ضاره إليه.
- يمكن من خلالها فتح باب خلفي (Back Door) في الجهاز المصاب حيث يمكن التحكم به من خلال ذلك الباب.
- يمكن للديدان أن تقوم بنسخ نفسها وإرسال نسخة إلى كل بريد الكتروني في عناوين البريد المخزنة في جهاز الحاسب الآلي المصاب.

برامج أحصنة طروادة

- في مجال أمان الحاسب الآلي، يعرف حصان طروادة بأنه جزء من برنامج (كود) قابل للتنفيذ يقوم بأداء بعض لمهام لا يتوقعها المستخدم.
- سبب تسمية هذا البرنامج الضار بهذا الاسم هو تشابه عمله مع أسطورة الحصان الخشبي الذي اختبأ به عدد من الجنود وكانوا سبباً في فتح مدينة طروادة فبرنامج حصان طروادة هو برنامج ضار (الجنود) مختبئ داخل برنامج بريء (حصان خشبي).
- تختلف أحصنة طروادة عن فيروسات وديدان الحاسب الآلي بأنها لا تتكاثر أو تتضاعف .

مكافحة البرامج الضارة

يمكن مكافحة البرامج الضارة باستخدام حزمة برامج واحدة لمكافحة كل من الفيروسات والديدان وأحصنة طروادة في آن واحد ومن أشهرها:

1. حزمة برامج مكافي (McAfee).
2. حزمة برامج سيمانتك (Symantec).
3. حزمة برامج كاسبر سكاي (Kasper SKY).
4. حزمة برامج نورتون (NORTON).

وفي جميع الحالات لابد من أتباع الخطوات التالية للحصول على مكافحة جيدة :

- ✓ تحديث برنامج المكافحة بشكل آلي ودوري.
- ✓ تحديث نظام التشغيل بشكل دوري وآلي عن طريق تنشيط خاصية التحديث التلقائي.
- ✓ عدم فتح مرفقات البريد الإلكتروني التي لها الامتدادات التشغيلية.
- ✓ تحميل ملفات الإصلاح الأمنية الخاصة بأنظمة التشغيل وبعض البرامج التطبيقية الأخرى (كنظام الأوفيس) التي يتم إصدارها من قبل الشركات المصنعة (كشركة مايكروسوفت) بشكل مستقل لسد ثغرة أمنية خاصة لم يتم سدها من خلال التحديث التقائي. وكذلك تحميل حزم الخدمة (Service Pack) الجديدة حال ظهورها.

ويمكن أن تعمل برامج المكافحة على أحد أو جميع الطرق التالية ومن الأفضل تفعيل جميع هذه الطرق لتوفير حماية أفضل وأشمل :

- ✓ باستخدام جدول زمني معين يتم من خلاله تحديد عمل برنامج المكافحة ليبدأ بفحص جميع مكونات الجهاز عند أوقات محددة (عند منتصف الليل من كل يوم مثلاً).
- ✓ عند الطلب من قبل المستخدم ويمكن أن يكون ذلك في أي وقت.
- ✓ عند تشغيل البرامج أو فتح الملفات أياً كان نوعها. وفي هذه الحالة يقوم برنامج المكافحة بفحص الملف المراد فتحة قبل أن تتم عملية الفتح الفعلية للتأكد من خلوه من الفيروسات والديدان وأحصنة طروادة.

الجزء الثالث

برامج التجسس وطرق مكافحتها

أهداف هذا الجزء

- التعريف ببرامج التجسس وأنواعها.
- توضيح طريقة عمل برامج التجسس.
- معرفة أعراض وجود برامج التجسس وطرق مكافحتها.

ما ستتعلمه في هذا الفصل

- برنامج التجسس وخطورته وماذا يفعله في الجهاز الضحية.
- برنامج راصد المفاتيح كمثال على برامج الرصد والتسجيل.
- برنامج المتتبع كمثال على برامج التجسس التي تقوم بمراقبة عادات المستخدم وتسجيلها وبناء معلومات إحصائية عنه.
- كيف تعمل برامج التجسس.
- أعراض وجود برامج التجسس وطرق انتقالها.
- طرق مكافحة برامج التجسس.

برامج التجسس وطرق مكافحتها

مقدمة

خلال السنوات القليلة الماضية ظهرت فئة جديدة من البرامج الماكرة هي برامج التجسس. وبرنامج التجسس ليس بفيروس ولكن فعله أقوى وأخطر من الفيروسات والديدان وأحصنة طروادة. فبالرغم من عدم تسببه في تلف البيانات، إلا أنه يعمل عمله من وراء الكواليس بكل هدوء ودون علم المستخدم، ويقوم بنقل المعلومات لمالكه. وبرنامج التجسس هو عبارة عن خدعة ماكرة مثله في ذلك مثل الفيروس ولكنه بصورة عامة أقل شهرة.

تعريف برنامج التجسس

- يعتبر تعريف ويبوديا لبرنامج التجسس أفضل التعاريف الموجودة حيث عرّفه بأنه "أي برنامج يقوم سراً بالحصول على معلومات عن المستخدم عن طريق الربط بالانترنت وخاصة بدعاوى دعائية وإعلانية".
- عادةً يتم تضمين برامج التجسس في شكل مكونات مجانية خفية أو برامج مشاركة يمكن تنـزيلها من شبكة الإنترنت.

أنواع برامج التجسس (1)

- يمكن تصنيف برامج التجسس إلى نوعين رئيسيين: برامج رصد وتسجيل، وبرامج تتبع.
- برامج الرصد والتسجيل
- النوع المعروف من برامج الرصد والتسجيل هو مسجل أو راصد المفاتيح (من لوحة المفاتيح) وحركات الفأرة وهي أكثر الأنواع شيوعاً وإزعاجاً في عملية سرقة كلمات السر وأرقام بطاقات الائتمان.
- يعمل في صمت في الخلف ويقوم بتسجيل ضغطات المفاتيح وحركات الفأرة لكي يعيد ترتيب وتكوين ما يقوم بفعله المستخدم.

أنواع برامج التجسس (2)

- هناك أيضاً راصدات ومسجلات للبريد الإلكتروني والدردشة.
- برامج التتبع (المتتبعات)
- تقوم بمراقبة عادات الاستخدام وأنماطه

وتخزينها كبيانات إحصائية بهدف عمل التقارير بناءً عليها.

طريقة عمل برنامج التجسس (1)

- فنياً لا يصنف برنامج التجسس كفيروس ولذلك لا يمكن مكافحته بشكل كامل من خلال البرامج المصممة لمكافحة الفيروسات.
- تقوم الفيروسات بإتلاف البيانات على جهاز الحاسب الآلي ونسخ نفسها ذاتياً، في حين تعمل برامج التجسس خلسة ولا تتلف البيانات بل تتجسس عليها.
- يمكن لبرامج التجسس أن تقوم بنسخ نفسها على الجهاز وتعمل كمهمة خلفية، وتنقل المعلومات السرية الخاصة بالمستخدم لمالكها دون علم المستخدم.

طريقة عمل برنامج التجسس (2)

- لدى برنامج التجسس مكونان أساسيان:
  - جزء في الواجهة الأمامية وهو برنامج عادي يعمل في العلن ويوفر وظائف مفيدة،
  - جزء في الخلف وهو برنامج تجسس يراقب وينقل المعلومات.
- يمكن لبرنامج التجسس البقاء في أي صورة أو شكل من أشكال البرامج القابلة للتنفيذ بما في ذلك التطبيقات مثل (ActiveX, Plug-in) أو أكواد (Applets).

طريقة عمل برنامج التجسس (3)

- عادة لا تقوم برامج التجسس بجمع المعلومات الشخصية فقط، ولكن بالإضافة إلى ذلك تجمع المعلومات الديموغرافية وعادات التصفح.
- المعلومات المتحصل عليها من المحتمل أن يتم بيعها وإضافتها لقواعد البيانات الأخرى لبناء سجلات عن المستخدم وعادات استخدامه.
- يقوم البرنامج (الذي في جهاز الضحية) في كل مرة بنسخ المعلومات من جهاز الضحية بغرض تحديث سجل الضحية لدى مالك برنامج التجسس.

أعراض وجود برامج التجسس وطرق انتقالها (1)

1. نشاط أعلى من الحد المعتاد.
2. القيام بطلب الإتصال بالإنترنت تلقائياً.
3. ظهور أشرطة أدوات غير مألوفة تتم إضافتها لمتصفح الإنترنت.
4. اختيار صفحة بداية لمتصفح الإنترنت خلاف الصفحة التي تم ضبط المتصفح عليها من قبل المستخدم.

أعراض وجود برامج التجسس وطرق انتقالها (2)

ومن أشهر الطرق التي تنتقل بها برامج التجسس طريقتين هما :

1. تظهر وكأنها برامج نافعة أو عادية حتى يتم تثبيتها على الحاسب الآلي من قبل المستخدم وبعلمه.
2. الاختفاء في برامج أخرى بحيث يتم تثبيتها مع تثبيت هذه البرنامج دون علم المستخدم.

مكافحة برامج التجسس

من أخطر ما تقوم به برامج التجسس هي أنها تقوم بإزالة برامج مكافحة التجسس. ويمكن القول بأنه ليس هناك برنامج يقوم بالحماية من برامج التجسس بدرجة كاملة، ولكن يمكن أخذ بعض التدابير الوقائية ومنها :

1. فلاتر خصائص استرجاع البيانات.
2. حاجبات الإعلانات والنوافذ المنبثقة.
3. استخدام مضادات برامج التجسس.
4. استخدام جدار النار الشخصي وبرامج كشف التطفل.
5. تأمين متصفح الإنترنت.
6. تأمين إدخال كلمات المرور.

1. فلاتر خصائص استرجاع البيانات (1)

- يمكن إعداد (تفعيل/تعطيل) وسائل استرجاع البيانات أو ما يسمى بملفات الكوكي (Cookie Screeners) الخاصة بالمواقع التي تتم زيارتها وذلك من خلال المتصفح.
- العديد من المستخدمين يقومون بتعطيل كافة وسائل استرجاع البيانات إلا أن هذا الإجراء قد لا ينصح به لأن الكثير من المواقع تتطلب تفعيل هذه الخدمة بالكامل.

1. فلاتر خصائص استرجاع البيانات (2)

- البديل الآخر هو استخدام خاصية "التحذير قبل القبول" لكي يتم تنقيح المسترجعات يدوياً. ولكن هذا من شأنه أن يؤدي لامتلاء الجهاز بأوامر حث تشغيل ملفات الكوكي (Cookie) عند القيام بتصفح الإنترنت.
- في متصفحات الإنترنت الحديثة يمكن للمستخدمين نقل إعدادات الخصوصية للمواقع التي تتم زيارتها، وسيقوم المتصفح برفض الإسترجاعات تلقائياً بالنسبة للمواقع التي ليس بها سياسة خصوصية

2. حاجبات الإعلانات والنوافذ المنبثقة (1)

- حاجبات الإعلان والنوافذ المنبثقة (Pop-UP Blockers)هي عبارة عن برامج تقوم على إجهاض تنـزيل وعرض صور الإعلانات الدعائية والإغراق الإعلاني، وكذلك منع النوافذ المنبثقة من الظهور التلقائي.
- يمكن لحاجبات الإعلان أن تحسن من أداء المتصفح. ويمكن للمستخدمين أن يحافظوا على خلو الأقراص الصلبة الخاصة بهم من أي ملفات غير ضرورية باستخدام حاجبات الإعلانات.

2. حاجبات الإعلانات والنوافذ المنبثقة (2)

- يمكن لبعض حاجبات الإعلانات أن تحسن من عملية الخصوصية عن طريق تحديد المعلومات التي يتم إعطاؤها.
- لدى مانعات الإعلان بعض الأثر السلبي الخفيف حيث إنها تعمل على حجب بعض الإعلانات المفيدة من خلال بعض المواقع غير الموقع الأصلي للإعلان.
- ينصح بشدة بعدم السماح للنوافذ المنبثقة التي تظهر تلقائياً عند زيارة بعض المواقع وعدم استخدامها إلا بعد التأكد من مرجعيتها وصحة العنوان الذي تحمله.

3. استخدام مضادات برامج التجسس

- من أفضل وسيلة للدفاع ضد برامج التجسس وإزالتها في حال وجودها هي استخدام برامج مكافحة التجسس (Antispyware Scanners). وهي برامج شبيهة ببرامج مضادات الفيروسات من حيث طريقة تركيبها وتشغيلها وتحديثها.
- يعمل برنامج مكافحة برامج التجسس بنفس طريقة برنامج مكافحة الفيروسات، كما يقوم برنامج مكافحة التجسس بحذف ملفات الكوكي الغير آمنة.

4. استخدام جدار النار الشخصي وبرامج كشف التطفل (1)

- برامج التجسس يمكن أن تثبت نفسها أثناء تصفح الإنترنت، لذا فإن تثبيت برنامج الجدار الناري (Personal Firewall) قد يوفر بعض الحماية. وهذه الجدران النارية تقوم بحجب برامج التجسس إن وجدت ومنعها من الإتصال بالانترنت دون إذن المستخدم.
- يمكن للجدران النارية تنبيه المستخدمين حول أي محاولات للدخول لجهاز الحاسب أثناء تصفح الإنترنت. وكذلك إعلام المستخدمين إن كان هناك أي برنامج يحاول إرسال بيانات دون تفويض بذلك.

4. استخدام جدار النار الشخصي وبرامج كشف التطفل (2)

- تستخدم أنظمة كشف التطفل (Intrusion Detection Systems) (IDS) لرصد محاولات الدخول الغير المصرح به، وكذلك مراقبة حركة الشبكة أو حالة النظام.
- يعتمد نظام (IDS) على الخطة الموضوعة له. فهو يتطلب قاعدة بيانات تحدد ما هي السلوكيات السيئة أو غير المقبولة.
- عن طريق قاعدة البيانات يتعرّف نظام كشف التطفل على ماهية الأنشطة العادية، ومن ثم يمكنه مراقبة التغييرات التي جرت والتي تدل على عملية التطفل أو النشاط المشكوك فيه.

5. تأمين متصفح الإنترنت

- من الإجراءات المضادة لبرامج التجسس هي ضبط إعدادات أمان متصفح الإنترنت لدرجة مقبولة من الأمان.
- يجب وضع الأمان في المستوى المتوسط أو العالي، مع الخيارات التالية لكل من (ActiveX) و (Plug-ins) (في أنظمة تشغيل ويندوز) :

1. إبطال كود (ActiveX) الغير مؤشر عليها بأنها آمنة.
2. تنشيط التحكم بكل من (ActiveX) و (Plug-ins).
3. تنشيط التحكم بتنزيل (ActiveX)، وذلك من خلال السماح للمعروفة منها بأنها آمنة (Singed) ومنع غير الآمنة (Unsigned).

6. تأمين إدخال كلمات المرور

- من أحد طرق مكافحة برامج التجسس هي استخدام لوحة مفاتيح افتراضية مرسومة على الشاشة عوضاً عن لوحة المفاتيح العادية عند إدخال كلمات المرور والأرقام السرية.
- يمكن من خلال هذا الإجراء منع برامج الرصد والتسجيل من التقاط الأزرار التي يتم الضغط عليها من قبل المستخدم. وقد تم استخدام هذه الطريقة من قبل العديد من مواقع البنوك التجارية.

انتهت المحاضرة المباشرة

لتعزيز التواصل قبل الاختبارات النهائية

- لتعزيز التواصل والرد على الاستفسارات الاكاديمية على البريد الالكتروني الجامعي: mftayfour@uod.edu.sa

- وعلى تويتر : https://twitter.com/Tayfourjo