عاشراً: الجرائم وإساءة الاستخدام وامن المعلومات على الإنترنت

Information Security and Internet Crime and Abuses

هنالك عدد من التجاوزات والجرائم، وإساءة الاستخدام على الإنترنت، وهي في تزايد مستمر، ويمكننا ذكر بعض منها، وكالآتي:

1- فيض الرسائل **Spamming** : حيث يرسل أصحاب الأسواق كميات غير مطلوبة من البريد الإلكتروني إلى جمهور المستلمين، الذين هم أساساً لم يقوموا بطلب مثل هذه المعلومات، مما قد يسبب المضايقة والإزعاج للعديد من هؤلاء المستلمين

Marketers send out unsolicited mass e. mail to recipients who have not requested this information

2- القرصنة**Hacking** : حيث يستغل القراصنة نقاط الضعف في الجوانب الأمنية لمواقع الشبكة العنكبوتي/الويب، فيحصلوا على فرص للدخول إلى البيانات الخاصة بهم، مثل المعلومات الخاصة عن الزبائن، وكلمات المرور. وقد يستخدم هؤلاء القراصنة أنواع من الفيروسات، مثل حصان طروادة، ليتظاهروا بأنهم برامجيات مشروعة اعتيادية لغرض الحصول على معلومات من الحاسوب المضيف.

Hackers exploit weakness in Web site to obtain access to proprietary data, such as customer information and passwords. They may use "Trojan horse" posing as legitimate software to obtain information from the host computer.

3- الشغب **Jamming** : يستخدم المشاغبون برمجيات روتينية لكي يربطوا موقع الويب للحاسوب المضيف بغرض أن لا يسمحوا للزائرين الشرعيين بالوصول إلى ذلك الموقع، والتواصل معه

Jammers use software routines to tie up the computer hosting a Web site so that legitimate visitors can't access the site

4- البرنـامج الخبيـث **Malicious Software** : يسـتخدم مخربـون لمواقـع المسـتخدمين علـى الإنـترنت بيانـات لنقـل فيروسـات، يمكـن أن تعطـل عمـل الحاسوب الذي قاموا بإصابته

Cyber vandals use data flowing through the Internet to transmit computer viruses, which can disable computers that they "infect"

5- التلصص **Sniffing**: وهو نوع من استراق أو اختـلاس السـمع، والدخول غير المشروع إلى مواقع وحواسيب المستخدمين وعرقلة الاتصال. حيث يقوم هؤلاء بوضع قطعة من البرامجيات التي تعترض المعلومات التي تمر من المستخدم إلى الحاسوب المضيف على موقع الويب. وقد تشتمل مثل تلك المعلومات على أرقام بطاقات الائتمان، وبيانات سرية أخرى.

A form of electronic eavesdropping involve placing a piece of software to intercept information passing from a user to the computer hasting s Web site. This information can include credit card numbers and other confidential data

6- الخداع **Spoofing**: هذه الطريقة هي أن يقدم البعـض أ،فسـهم للآخرين بشكل مخادع وغير صحيح، على أنهم ممثلين لشركات، واضعين مواقع وهمية على الويـب، بحيـث يسـتطيعون أن يجمعـوا معلومـات سـرية، مـن زوار غير متوقعين للموقع.

Spoofers fraudulently misrepresent themselves as other organizations, setting up false Web sites where they can collect confidential information from unsuspecting visitors to the site.

أما فيما يتعلق بأمن المعلومات وحمايتها من الفيروسات فقد تطرق الكاتبان في موضوع حماية الأعمال الإلكترونية من الفيروسات (انظر الفقرة الثانية عشر من هذا الفصل).

حادي عشر: الفيروسات: أخطارها وأنواعها

Viruses: Its dangers and types

نستطيع أن نعرف الفيروس من خلال حقيقة أنه برنامج يتصف بثلاثة أنواع من الوظائف، نوضحها بالآتي:

1- **التكاثر والمضاعفة (Replication)** حيث يقوم الفيروس الواحد بمضاعفة نفسه في ملف ما، وبذلك يقوم بالانتشار وتأمين العدوى (Infection) المطلوبة، فإنه سيجد طريقه إلى الانتشار. ويحصل التكاثر عادة عندما يصل الفيروس إلى وحدة المعالجة المركزية CPU والقرص الثابتHD للحاسوب.

2- **الاختفاء أو التخفي (Concealment)** وعدم الظهور لغرض تسهيل مهمة التكاثر. ويساعده في التخفي عادة صغر حجمه، حيث أنه لا يشغل حيزاً كبيراً (إن أكبر فيروس لا يتجاوز حجمه عن (2KB).

3- **الانفجار (Bomb)** فحالما ينجح الفيروس في تخفيه وتكاثره، في ملف أو مجموعة ملفات، فإنه تظهر أعراض الإصابة به، ويبدأ بالتدمير. وقد يصل التدمير إلى كل ما هو موجود في القرص الثابت.

وعلى أساس ما تقدم فإننا نستطيع القول بأن كلمة فيروس قد أطلقت مجازاً على برنامج حاسوبي يقوم بإعمال تخريبية وتدميرية في برامج الحاسوب، والمعلومات المخزنة فيه. وهنالك أنواع عديدة من تلك الفيروسات التي تقوم بالعديد من الأعمال التخريبية، مثل:

1- تخريب محتويات القرص الصلب (Hard Disk) ومحوها.

2- تغيير نظام تقسيم القرص الصلب، وفقدان المعلومات فيه كنتيجة لذلك.

3- تغيير بغض بيانات نظام التشغيل (Operating System) مما يدعو المستخدم إلى إلغاء النظام ومحوه، ومن ثم إعادة نسخه وتثبيته.

4- التسبب في تخريب رقائقChips بدء التشغيل واللوحة الأساسي (Mother Board) مما يدعو إلى تغييرها.

5- تغيير وتخريب التطبيقات المخزونة في الحاسوب، مما يؤدي إلى حصول المستخدم على نتائج خاطئة، مما يقود إلى مشاكل وظيفية.

وعلى ضوء دراسة في هذا المجال قامت بها الجمعية الوطنية (الأمريكية) لأمن المعلومات (National Computer Security Association/NCSA) فإن الإصابة بالفيروس لا يزال في تزايد، ففي عام (1996) كان (10) من كل (1000) حاسوب مصاباً بفيروس، كل شهر. ثم تضاعف هذا العدد في السنوات التالية. ويعزى سبب تزايد الإصابة بفيروس الحاسوب إلى انتشار استخدام الإنترنت. وبضوء الإحصاءات فإن أكبر وسائط انتشار الفيروس هو القرص المرن. ووفق هذه الدراسة والإحصائية فإن ثلث المؤسسات المشمولة أوضحت بأن دماراً كبيراً قد أصاب (25) أو أكثر من حواسيبها، وذلك في عام (1997)

من جانب آخر فإنه يقدر عدد الفيروسات المعروفة في العالم بأكثر من (60000) فيروس. ولا يزال العمل مستمراً في إنتاج المزيد منها، وفي مختلف دول العالم . ويعتقد البعض أن بعض شركات الحواسيب والبرمجيات هي التي تنتج بعض من هذه الفيروسات، ثم تعود لانتاج فيروسات مضادة لها وتسوقها.

يمكن أن تكون المصادر التي تنقل الفيروس واحدة أو أكثر مما يأتي:

1- القرص المرن (Floppy Disk) حيث يتم ذلك عن طريق استخدام قرص مرن يحمل معلومات من حاسوب غير حاسوبك، كأن تقوم بطباعة معلومات مخزونة على قرص زميل لك لا يمتلك جهاز طباعة. أو أن تقوم بنقل

معلومات إلى حاسوبك من قرص مرن، تم خزن المعلومات عليه من حاسوب آخر.

2- القرص المكتنز (Copact Disc/CD) حيث يتم تسجيل المعلومات على مختلف أنواع المعومات على مثل هذه الأقراص، كأن تكون أقراص أقرأ ما في الذاكرة (CD-ROM) والأقراص أو الوسائط المتعددة (Multimedia) أو الأقراص الموسيقية والغنائية. وقد تحمل مثل هذه الأقراص فيروسات مؤذية إلى حاسوبك.

3- القرص الصلب (Hard Disk) حيث يقوم بعض مستخدمي الحاسوب، من المتقدمين في مجال الحوسبة والبرمجيات، بنقل معلومات من قرص صلب إلى آخر باستخدام الطريقة المغروفة باسم (Lab Link) ،أو عن بتركيب قرص صلب كتابع (Slave Hard Disk) ثم يتم نقل المعلومات من قرص إلى آخر. وهذه الطريقة وإن كانت ضرورية أحياناً وسريعة، إلا أنها قد تساعد على نقل الفيروسات من قرص صلب إلى آخر.

4- شبكة إنترنت، والبريد الإلكتروني، ومجموعة الأخبار. قد يقوم المستخدم بالإبحار داخل العديد من المواقع المنتشرة في شبكات ومواقع العالم الواسع المرتبط بإنترنت. وهنالك بعض المواقع تحتوي على برامج تنتقل إلى حاسوبك في هيئة فيروس، خاصة تلك البرامج المجانية والتجريبية، التي تقوم بتحميلها إلى حاسوبك، دون وجود أية ضمانة. كذلك فإن الرسائل المرسلة إلى حاسوبك عبر خدمة البريد الإلكتروني أو مجموعات الأخبار News Groupالتي تنقل معلوماتها إلى حاسوبك، بناء على طلب منك. فقد تحمل بعضاً من هذه الرسائل والمعلومات فيروسات، مقصودة من قبل بعض المحترفين في هذا المجال.

أما أنواع الفيروسات فإن الكتاب يجتهدون في تقسيماتها ومسمياتها. وقد ركز الكاتب على اتجاهين رئيسين في تصنيف أنواع المعلومات. فالاتجاه الأول

يحدد أنواع الفيروسات بالآتي:

1- فيروس رئيسي (Major virus)

2- فيروس شديد (Severe virus)

3- فيروس غير محدود (Unlimited)

4- فيروس مبتدئ أو عادي (Trivial Virus)

5- فيروس معتدل (Moderate Virus)

أما بالنسبة للتصنيف الثاني لأنواع الفيروسات فيمكننا تحديده بالآتي:

1- فيروس أجزاء التحميل (Boot-sector Virus)

2- فيروس الملفات (Virus File)

3- فيروس متعدد الأجزاء (Multipartite Virus)

4- فيروس واسع النطاق أو ضخم (Macro Virus)

5- فيروس القنبلة المنطقية (Logic Bomb)

6- الفيروس الطروادي أو المدمر (Trojan Horse)

فيروس قسم التحميل Boot-sector virus: قسم تحميل البيانات والبرامج في نظام الحاسوب يشتمل على معظم التعليمات الخاصة بالتحميل (instructions for booting) أو إعطاء الدفع ورفع القدرة (powering up) المطلوبة للنظام. وفيروس قسم التحميل يحل محل تعليمات التحميل هذه ويتغلغل فيها. وحالما يبدأ تشغيل النظام فإن الفيروسات تنتشر في الذاكرة الرئيسية ((main memory قبل نظام التشغيل (operating system) . ومن خلال هذا الموقع الذي يحتله الفيروس فإنه يستطيع التأثير في بقية الملفات. فكل قرص مرن يستخدم سواقة أو مشغل القرص (disk drive) في الحاسوب يصبح مصاباً بالفيروس. وعندما ينقل القرص المرن إلى حاسوب آخر فإنه ينقل الفيروس معه إلى ذلك

الحاسوب، وهكذا تتكرر العدوى وتنتشر. وهنالك أمثلة ومسميات لهذا النوع من الفيروسات، مثل: (AntCMOS, AntiEXE, Form A, NYB/New York Boot, Ripper, Stoned, Empire Monkey)

فيروس الملف File virus: فيروسات الملف تربط نفسها عادة بالملفات القابلة للتنفيذ (executable files)، تلك الملفات التي تبدأ عادة كبرنامج. فعندما يبدأ البرنامج بالتشغيل، يبدأ عنها الفيروس بالعمل، محاولا الوصول إلى الذاكرة الرئيسية (main memory) للحاسوب، الانتقال بالعدوى إلى الملفات الأخرى التي ستتفاعل مع الجزء المصاب بالفيروس، وهكذا.

قنبلة منطقية Logic bomb: هو نوع من أنواع الفيروسات، يختلف عن بقية الفيروسات بكونه يبدأ عمله التخريبي في تاريخ محدد وتوقيت محدد. أو نستطيع أن نقول بأنه ينفجر في موعد محدد. فقد عمد أحد المبرمجين الساخطين على أحد المؤسسات المهمة المتعاقد معها، في الولايات المتحدة الأمريكية، بصنع مثل هذه القنبلة في البرنامج الذي أعده لها، محدد تاريخ ووقت انفجارها بعد شهرين، حيث يكون قد ترك عمله وانتهى عقده مع تلك المؤسسة. وكان قد صمم هذا النوع من الفيروس لحذف نظام متابعة الجرد (inventory tracking system). وقد تم اكتشاف فيروس القنبلة المؤقتة هذا بالصدفة، وأبطال مفعولها.

فيروس واسع Macro virus: وينتشر هذا النوع من الفيروس في الملفات التي تستحدث بواسطة البريد الإلكتروني وملاحقه attachments)، وكذلك صفحات النشر (spreadsheet) التي ترسل عبر شبكات الحواسيب. ولم يفكر المعنيون بمعالجة ومحاربة الفيروسات في هذا النوع من الفيروس إلا في السنوات الأخيرة. ويستغل هذا النوع من الفيروس عادة طبيعة عمل البرامج المصغرة (miniature programs) ليتغلغل داخل بيانات ملفاتها، ومن ثم ينتقل إلى الحواسيب الأخرى المرسلة إليها مثل تلك البيانات والملفات. ومن أمثلة هذا النوع

من الفيروسات (Concept) الذي يخترق ويلتصق بملاحق البريد الإلكتروني، و(Laroux) الذي يخترق ويلتصق بملفات صفحات النشر (Excel spreadsheet files). وقد احتاطت الجهات المعنية بهذا النوع من البرامج، فجاءت الطبعات الأخيرة للورد والأكسل (Word and Excel) ومعها مضادات وحمايات من هذا النوع من الفيروسات (built-in macro virus protection)

فيروس رئيسي Major virus: يؤدي الفيروس ذو الضرر الرئيسي إلى تخريب المعلومات بشكل تدريجي بطيء عبر فترة الزمن كنسخ رسالة معينة أو تشكيل من الرموز في الملفات وبشكل عشوائي ، وبالرغم من أن هذا التخريب قد يجد طريقه إلى النسخ الاحتياطية إلا أنه سيكون مرئياً بسهولة بعد تشخيص الإصابة يمكن من تحديد الملفات المتضررة ويسهل إصلاحها كما في فيروس RIPPER الذي يتسبب في واحد من كل ألف عملية كتابة على القرص تسجيل المعلومات بشكل خاطئ مما يؤدي إلى تخريب تدريجي للنظام .

فيروس ثانوي Minor virus: يسبب الفيروس ذو الضرر الثانوي تغييراً أو مسحاً لواحد أو أكثر من الملفات القابلة للتنفيذ Executable files والتي تصاب بالفيروس .وبما أن هذه الملفات قد أخذت أساساً من الأقراص الأصلية المقدمة من قبل منتجي البرامج فان إعادة تركيبها على الكمبيوتر بعد إزالة الفيروس هي عملية بسيطة نسبيا كما يمكن استرجاعها من النسخ الاحتياطية للبرامج كما في فيروس AIDS الذي يصيب الملفات من نوع COM ويكتب فوق الـ 13K الأولى منها.

فيروس معتدل Moderate virus: يمكن للفيروس ذو الضرر المعتدل تدمير جميع الملفات الموجودة على القرص الصلب غالباً عن طريق إعادة تهيئة reformatting أو استبدال المعلومات بكتابة معلومات أخرى تافهة فوقها. كما في فيروس DISK KILLER الذي يسبب إعادة تهيئة القرص الصلب عندما يبلغ عدد الأقراص المرنة التي تمت إصابتها عدداً محدداً أو فيروس COLUMBUS

الذي يفعل الشيء ذاته إذا تم تنفيذ ملف COM مصاب في تأريخ 12 أكتوبر. وبالرغم من إن الكثيرين قد يرون إن هذه المشكلة خطيرة إلا أن مسح جميع الملفات لا يشكل ضرراً حقيقيا طالما كانت عملية النسخ الاحتياطي BACKUP تتم بانتظام.

فيروس مبتدئ أو عادي Trivial virus: لا يفعل الفيروس ذو الضرر العادي شيئا سوى التكاثر (replication) ويمكن أن لا يشعرنا بوجوده و لا يسبب ضرراً أو تخريبا متعمداً للمعلومات في الأقراص. وحالما يتم تشخيصه واكتشافه فكل ما يتوجب هو حذف الفيروس فقط وبجهد قليل باستخدام أحد البرامج المضادة للفيروسات (Anti- virus programs) كما في فيروس (stupid) الذي لا يفعل شيئاً سوى البحث عن ملف نظيف وإصابته.

فيروس غير محدد الضرر Unlimited virus: يستهدف الفيروس ذو الضرر اللامحدود شبكات الكمبيوتر Networks ويمضي أكثر الوقت في محاولة معرفة كلمة السر password للمستخدمين الأكثر فاعلية ضمن الشبكة مثل supervisor وعندما يتمكن من الحصول عليها فانه يمررها إلى واحد أو أكثر من مستخدمي الشبكة على أمل أنهم سوف يستخدموها لأغراض سيئة . وعندما يفقد الشخص المؤهل سيطرته على كلمة السر ورقم الحساب إلى شخص آخر يصبح هو المتحكم بكامل الشبكة.

ثاني عشر: حماية الأعمال الإلكترونية من الفيروسات

Internet worked E-Business Defense

يواجه المهنيون وتواجه الأعمال تحديات كبيرة، هي أكبر من محاولات المديرين المعتمدين في أقسام تكنولوجيا المعلومات، بالنسبة إلى السياسات الأمنية المتعلقة باستثمار إمكانات وتطورات الإنترنت، في ضوء التغيرات الواسعة والسريعة للبنية التحتية للشبكات. وكيف يستطيع مثل هؤلاء المديرين من الموازنة

بين الحاجة إلى الجوانب الأمنية للإنترنت، من جانب، والوصول إليها واستثمار إمكاناتها الهائلة، من جانب آخر. وهل أن التخصيصات المرصودة للجوانب الأمنية كافية؟ وما هي تأثيرات الإنترانت، الاكسترانت، وتطور تطبيقات الشبكة العنكبوتية/ الويب على بنية وتركيبة الجانب الأمني؟ وكيف يتمكنون من تأمين أفضل الممارسات لتطوير سياسة أمنية للإنترنت؟

لذا، ومن منطلق هذه التساؤلات وغيرها بخصوص الجوانب الأمنية في استثمار إمكانات الشبكات الداخلية والمتداخلة في الأعمال الإلكترونية للشركات والمنشآت، هي هاجس مهم وتحدي إداري مهم. وإن العديد من الشركات تتسارع نحو الارتباط بالويب والإنترنت لأغراض التجارة الإلكترونية، وإنهم يعيدون هندسة إجراءات أعمالهم مع الإنترانت، وبرامجيات المنشأة، وارتباطاتهم بالمستهلكين، والمجهزين، وشركاء الإعمال الآخرين، عن طريق الأكسترانت.

والروابط الشبكية الرئيسية وانسيابية الأعمال هي بحاجة لان تقدم لها الحماية من الاعتداءات الخارجية، عن طريق الجرائم المحترفة، وكذلك من بعض الجرائم والتصرفات غير المسؤولة من داخل المنظمة. وكل هذا يتطلب أدوات ووسائل أمنية، ومعايير دفاعية ووقائية. وكذلك برنامج إداري للتنسيق الأمني. ومن وسائل الحماية الأمنية المهمة التشفير Encryption ، وجدران النار Fire Walls، ورفض الخدمةDenial of Service Defenses

أولاً: التشفير Encryption: لقد أصبحت طريقة تشفير البياناتData encryption هامة وأساسية في حماية البيانات وموارد الشبكات الحاسوبية، وخاصة الإنترنت، والإنترانت، والأكسترانت. فكلمات المرور، والرسائل، والملفات، والبيانات الأخرى passwords, messages, files, and other data يمكن أن ترسل بشكل مجمع أو غير مجمع scrambled or unscrambled بواسطة نظام الحاسوب للمستخدمين المخولين authorized users فقط. والتشفير يشتمل على استخدام حسابات رياضية خاصة، أو مفاتيح، لتحويل

البيانات إلى رموز مجمعة أو ممزوجةscrambled code قبل إرسالها. ثم القيام بفك رموز decode البيانات عند استلامها. وإن الطريقة الأكثر استخداما في التشفير هي مفاتيح عامة أو خاصة مزدوجة. وفريدة لكل شخص a pair of public and private key unique to each individual. مثال ذلك، فان البريد الإلكتروني يمكن أن يجمع ويمزج، ويشفر باستخدام مفتاح عام يكون معروفا عند المستلم. وبعد إرسال البريد الإلكتروني يكون المرسل فقط هو المطلع على السر الشخصي private key الخاص بفتح الرسالة.

ووسيلة التشفير تسوق وتباع عادة كمنتج برمجي مستقل، بغرض بناءها في البرامجيات الأخرى المستخدمة. وهنالك عدد من البرمجيات التشفيرية المعيارية المعروفة، ولكن في مقدمتها اثنتان، RSA (by RSA Data Security) and PGP (pretty good privacy) والمستخدمة والمتاحة على الإنترنت. وإن المنتجات البرمجية التي تشتمل علىMicrosoft Windows NT, Novel Netware, Lotus Notes, and Netscape Communicator تقدم عروضاً باستخدام النوع الأول المذكورRSA software

ويوضح المخطط رقم (49) التالي طريقة التشفير باستخدام ما يطلق عليه المفتاح العام والمفتاح الخاص.

ثانياً: رفض أو إعاقة الخدمة Denial of Service Defenses: لقد أصبح الإنترنت، والشبكات الأخرى الداخلية والخارجية المرتبطة به، عرضةً للهجمات والاختراقات، بواسطة العديد من القراصنة والدخلاء، خصوصاً ماله علاقة بما يطلق عليه هجمات (فيروس) إنكار أو إعاقة الخدمةDenial of Service/DOS attacks . ويوضح المخطط رقم (47) الخطوات التي ينبغي على المنظمة إتباعها لغرض حماية نظم معلوماتها من هجمات إعاقة الخدمة.