العنوان:	لمحات حول أمن المعلومات
المصدر:	مجلة المعلوماتية
الناشر:	وزارة التربية والتعليم - وكالة التطوير والتخطيط
المؤلف الرئيسي:	أبو عباة، أيمن بن عبدالعزيز
المجلد/العدد:	ع 3
محكمة:	لا
التاريخ الميلادي:	2004
الصفحات:	11 - 15
رقم MD:	27614
نوع المحتوى:	بحوث ومقالات
قواعد المعلومات:	HumanIndex
مواضيع:	أمن المعلومات ، علم المعلومات، اختزان واسترجاع المعلومات ، حفظ المعلومات ، مصادر المعلومات ، مراكز المعلومات، برامج المكتبات، وسائل الاتصال، الحاسبات الإلكترونية، الفيروسات
رابط:	http://search.mandumah.com/Record/27614

فـد يكون من العبـث الحديث عن أهمية أمن المعلومات، بـل ومن فضلة القول التأكيد على أن هذا المجال من الأهمية بمكان أن تتولى الإشـراف على بحـوثه المتقـدمة في الشـركات الكبـرى دوائر المخابـرات أو الجهات الأمنية خصوصاً في الدول المتقدمة تقـنياً كأمريكا وألمانيا وغيرها. ومن المعلوم أن الخبرات التقنية المتقـدمة في مجال أمن المعلومات تظل سـراً لا يكشـف حتى تتوصل تلك الجهات البحثية إلى خبرات أكثر تقـدماً فبـالتالي تكون تلك التقنية القديمة متاحة للمستهلكين غير المبـتكرين ممن يرونها قـمة التقدم العلمي ونهاية المطاف أحياناً في هذا المجال.

ويمكن أن يتمحور أمن المعلومات في عدة مجالات وأهمها:

- أمن حفظ البيانات و المعلومات.
- أمن نقل البيانات و المعلومات.
- البحث عن مصادر الخطر المتوقعة على المعلومة لمكافحتها.

أولاً: أمن حفظ البيانات و المعلومات

ويهتم هذا المجال بالعديد من الآليات العلمية والعملية حول:

١. مكان حفظ البيانات والبيئة المحيطة بها:

من خلال وجود ها في مواقـــع آمنة مثل مراكز المعلومات والتي يجب أن تخضع لرقابة دقيقـة من حيث الوصول الفيزيائي لهذه المواقع بحيث لا يصل إليه إلا من هو مصرح له من خلال البوابة الآمنة والتي تعتمد أحياناً على التقنيات المتقدمة مثل قراءة بـصمة اليد (Printfinger)أوقزحـية العين (Printeye) أو تردد الصوت أو من خلال الأرقـام المتسلسـلة أو البطاقات الممغنطة ، وغيرها .

٢. طريقة حفظ البيانات:

وذلك من خلال التقـنيات المتقـدمة في أنظمة تشـفير المعلومات المحفوظة (Encryption) بمختلف أنواع التشـفير المتماثل أو غير المتماثل سواء المعتمد دولياً أو التشفير المبتكر محلياً وتفاوتت قوة التشـفير حتى وصل طول مفتاح التشفير إلى ٣٠٠٠ بت ولكن هذه الدرجة بـالغة القـوة والتعقيد بحيث لا يمكن فك رموزها باسـتخدام التقـنية الحالية، لذلك لم تسـمح الحكومة الأمريكية بـتصدير أي تقـنية تشـفير يتجاوز طولها ١٢٨ بت والتي تعد كافية جداً لحماية التجارة الإلكترونية، إذ تحتاج إلى أرقام فلكية من المحاولات لفك الشفرة تقـاس بالأندبسـليون (١٠ مرفوع للقـوة ٣٦) كما أن هناك برامج خاصة أنتجت للمساعدة على التشـفير، لعل من أشهرها وأقواها على الإطلاق بـرنامج Pretty Good Privacy ويرمز له

أيمن بن عبدالعزيز أبوعباة
مشرف تقنية المعلومات والاتصال
وزارة التربية والتعليم
aaboabah@moe.gov.sa

بـالإختصار PGP الذي صممه فيليب زيمرمان ويمكن إختيار الأنسـب من البيانات.

٣. المواد التي تحفظ عليها البيانات:

من خلال الحفظ على الأنسب من الأقراص الصلبة (HDD) أو كروت الذاكرة (CASH) أو الأقراص المدمجة (CD) وغيرها من بيئات الحفظ المناسبة.

٤. حماية المعلومة:

ويتم بعدة آليات من خلال:

- استخدام برامج الحماية الجدران النارية (Firewalls) للحماية من الاختراق للأجهزة المرتبطة فيزيائياً بشبكات. واستخدام المرشحات (filters) لضمان عدم نقل المعلومات غير المسموح بها. واستخدام برامج مكافحة الفيروسات (Anti-Virus) للحماية من الفيروسات المختلفة.

- النسخ الاحتياطي (BACK UP) وهذا يعالج مشكلة فقد البيانات الرقمية غير المكتوبة (Hard Copy)والتي تكون أكثر عرضة من غيرها للتلف أو العطب أو الفقد ويتم ذلك بعدد من الآليات:

- النسخ المتطابقة على نفس البيئة.

- النسخ الاحتياطي للكوارث (Disaster Recovery)وذلك بالخروج من النطاق الجغرافي والسياسي بالتخزين في بيئة بعيدة جغرافياً وذلك لضمان بقاء البيانات في حال - لا قدر الله - حدوث كارثة في موقع مركز المعلومات (كما حدث خلال الاجتياح العراقي للكويت عام ١٩٩٠ وإتلافه لجميع البيانات المدنية - وبعد لطف الله - وبسبب وجود نسخ خارج النطاق السياسي والجغرافي تمكنت حكومة الكويت من استعادة معظم البيانات الحساسة والتي فقدت في تلك الفترة).

ثانياً: أمن نقل المعلومات والبيانات:

قديماً كانت تستخدم آليات النقل الفيزيائي المباشر للبيانات وتحاط بسرية وحماية وتتم ببطء نسبي. والمتأمل حالياً يرى أن تلك الطريقة كانت أكثر أمناً من الطرق الحديثة من حيث التواصل الإلكتروني وبعد التقدم التقني أصبحت آليات النقل الحديثة بما تميزت به من سرعة في نقل المعلومة ودقة هي الأنسب عند أخذ الاحتياطات اللازمة في عمليات نقل البيانات ولذا نرى بأن هذا المجال يهتم بالبيئات الآمنة لنقل البيانات والمعلومات من خلال:

١. أمن نظم الاتصالات وبيئات النقل المستخدمة:

عندما يكون الاتصال مباشر (direct connection) بواسطة خطوط الهاتف (Dialup) أو بالاتصال المباشر بالأقمار الصناعية (Satellite). وذلك عندما يكون حجم البيانات متوسطاً نسبياً وتكمن الخطورة هنا عند وجود متلصصين يقومون بعمليات التلصص (Sniffing) على

خطوط الاتصال وتبرز هنا أهمية تشفير البيانات بقوة تشفير عالية والمحافظة على سلامة خط الاتصال من وجود المعترضين أو المتجسسين.

٢. التطبيقات المستخدمة والبروتوكولات المناسبة:

عندما يكون الاتصال غير مباشر وفي وسيط مثل الإنترنت أو يكون نقل البيانات لموقع خدماتي عالي الأهمية الأمنية مثل البنوك أو للشراء المباشر ببطاقات الائتمان الإلكترونية وهنا مكمن الخطر حيث يكون التجسس والاختراق من أبرز المشاكل الأمنية والتي لا يمكن القضاء عليها بشكل كامل بل يمكن الحد منها بشكل كبير عن طريق استخدام البروتوكولات الآمنة SSL (Secure Sockets Layer)أو ما يسمى بـ(HTTPS) . وتظهر أهمية التوقيعات الرقمية (PKI) والشهادات الإلكترونية للمواقع الآمنة وغيرها من وسائل الحماية.

ثالثاً: البحث عن مصادر الخطر المتوقعة على المعلومة لمكافحتها:

تعتبر مصادر الخطر على أمن البيانات كثيرة جداً ولعل من أهمها خطورة الوصول إلى البيانات من قبل أشخاص غير مسموح لهم بالوصول إليها وبالتالي يتم تسريب المعلومات أو إتلافها أو تغييرها ويمكن أن يستعين أولئك بالعديد من الوسائل التي توصلهم للبيانات أو تمكنهم من إتلافها أو تغييرها بعدة طرق من أهمها:

١. الاختراق (Hacking)

وهذا علم مستقل بذاته فهو يجمع بين الهواة والمحترفين ففي عام (١٩٨٤م) ظهرت البدايات الحقيقية للهكرز حيث ظهر شخص اسمه (ليكس لوثر) أنشأ مجموعة أسماها (LOD) ووهي عبارة عن مجموعة من الهكرز الهواة والذين يقومون بالقرصنة على أجهزة الآخرين, وكانوا يعتبرون من أذكى الهكرز وكانت بقيادة شخص يدعى (فيبر) وكانت هذه المجموعة منافسة لمجموعة (LOD) ومع بداية عام (١٩٩٠م) بدأت المجموعتان بحرب كبيرة سميت بحرب الهكرز العظمى وهذه الحرب كانت عبارة عن محاولات لكل 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 مجموعات الهكرز بعد ذلك.

وعليه يمكن تقسيم الهاكرز إلى صنفين :

- الصنف الأول: وهم الهواة و عامة الهاكرز منهم ويعتبرون مخترقين من الدرجة الثانية وهم من يستخدمون برامج للاختراق سهلة الإستخدام وغالبية هذه البرامج تعمل تحت بيئات نظام التشغيل(Windows) . وهؤلاء عادة لا يتمكنون من الوصول إلى بيانات إي جهاز إلا إذا كان متصل بشبكة الإنترنت ومصاب ببانشات (Trojans) فيروسات من نوع "حصان طروادة " تدعم برامج المخترقين حيث يقوم حصان طروادة بفتح منفذ (Port) في الجهاز المصاب يمكن المخترق من التحكم في جهاز الضحية والوصول لبياناته. وعادة ما ينشر هؤلاء المخترقون " البانشات " التي تدعم برامجهم في المنتديات و ما يسمى فضاءات (Chat) والمواقع المشبوهة من خلال إرفاقها مع الصور أو ملفات

الفيديو أو عروض الفلاش وغيرها.

- الصنف الثاني: وهم القلة والأخطر وهم الهاكرز المحترفون (Professional) وعادة ما يكونوا مبرمجين أو متخصصين في مجال الشبكات وعادة ما يكونوا على شكل تحالفات في عالم الإنترنت الافتراضي وهؤلاء عادة لا يعتمدون فقط على برامج الاختراق بل يقومون باستغلال الثغرات الأمنية لأنظمة التشغيل أو الثغرات الأمنية الموجودة في شبكات معينة ويقومون باعتراض البيانات والحصول على نسخة منها في نقاط الاتصال سواء كانت أجهزة ربط شبكات مثل الموجهات (Routers) أو موزعات الشبكة (Manageable Switches) أو يقومون بالتواصل مع الموجهات (Routers) وبالتالي يقومون بتعطيل نطاقات (Domains) كاملة عن العمل أو قد يتمكنوا من ضرب أجهزة الربط والإضرار بقطاع كبير من مستخدمي الشبكة الإنترنت وتكمن خطورة هؤلاء في إمكانية عملهم دون حاجتهم للباتشات بشكل مباشر بل قد يتمكن الكثير منهم من صناعة أجزاء البيانات البكت (Packetes) وهي أصغر وحدة نقل بيانات عبر الشبكة. ومن خلال صناعة أجزاء البيانات البكت يمكن أن يتحاور مع أي جهاز ويكون أوامر بداخله وبالتالي يهدد أمن المعلومات.

٢. الفيروسات:

الفيروس هو برمج صغير تم تصميمه بهدف لا يخدم نظام الحاسب, و ويبرمج عادة بحيث لا يبدأ نشاطه إلا بعد فترة كافية من الوقت حتى يضمن حرية الانتشار دون أن يلفت الانتباه ليتمكن من إصابة أكبر عدد ممكن من الملفات في النظام, و تختلف الفيروسات من حيث آلية البدء فهنالك من يبدأ بتاريخ أو وقت محدد, وهنالك من يبدأ العمل بنشاط بعد تنفيذ أمر معين وهنالك من لا يبدأ إلا بعد تحقيق عدد محدد من النسخ. و يقوم الفيروس عادة بعدة أنشطة تخريبية حسب الغرض من إنشاء ذلك الفيروس فهناك ما يقوم بعرض رسالة تحذيرية عن امتلاء الذاكرة أو رسالة تستخف بالمستخدم وهناك أنواع أخرى تقوم بحذف أو تعديل بعض ملفات جهازك وهناك من يقوم بتكرار ونسخ نفسه حتى يشل تماما وهناك أنواع أشد فتكا فتقوم بمسح كل المعلومات من قرصك الصلب. وتختلف أنواع الفيروسات تباعاً لاختلاف أنظمة التشغيل.

أنواع الفيروسات: يمكن تصنيف الفيروسات عدة تصنيفات مختلفة من حيث آلية عمل الفيروس أو من حيث أثره على المستخدم أو من حيث الفئة المستهدفة من الفيروس أو نوع الأنظمة التي يتمكن من إصابتها وعلى كل حال سيتركز الحديث عن طبيعة عمل الفيروس والغرض منه:

أ. حصان طراودة: (Trojans hours) هو جزء صغير من الكود يضاف الى البرمجيات ولا يخدم الوظائف العادية التي صممت من أجلها هذه البرمجيات ولكنه يؤدي عملا تخريبيا للنظام, وتكمن خطورته في أن النظام لا يشعر بوجوده حتى تحين اللحظة المحددة له ليؤدي دوره التخريبي ومنه: القنبلة المنطقية (Logic Bomb) و هي أحد أنواع حصان طراودة وتصمم بحيث تعمل عند حدوث ظروف معينة أو لدى تنفيذ أمر معين, فقد تصمم بحيث تعمل عند بلوغ عدد الموظفين في

الشركة عددا معينا من الموظفين مثلا أو إذا تم رفع إسم المخرب (واضع القنبلة) من كشوف الراتب, وتؤدي القنبلة في هذه الحالة الى تخريب بعض النظم او الى مسح بعض البيانات أو تعطيل النظام عن العمل. وكذلك القنابل الموقوتة(Time bomb) هي نوع خاص من القنابل المنطقية وهي تعمل في ساعة محددة أو في يوم معين.وأيضاً باب المصيدة(Trap door) هذا الكود يوضع عمدا بحيث يتم- لدى حدوث ظرف معين - تجاوز نظم الحماية والأمن في النظام. ويتم زرع هذا الكود عند تركيب النظام بحيث يعطي المخرب حرية تحديد الوقت الذي يشاء لتخريب النظام فهو يظل كامننا غير مؤذ حتى يقرر المخرب استخدامه, وكمثال على ذلك إقحام كود في في نظام الحماية والأمن يتعرف على شخصية المخرب ويفتح له الابواب دون إجراء الفحوص المعتادة.

ب. الديدان (Worms) الدودة هي عبارة عن كود يسبب أذى للنظام عند استدعائه, وتتميز الدودة بقدرتها على إعادة توليد نفسها, بمعنى أن أي ملف أو جهاز متصل بالشبكة تصل إليه الدودة يتلوث , وتنتقل هذه الدودة إلى ملف آخر أو جهاز آخر في الشبكة وهكذا تنتشر الدودة وتتوالد.

ج. الفيروسات المموهة : هي الفيروسات التي تقوم بتغير شكل شيفرتها مع كل إصابة جديدة تماما و قد تحوي على بلايين و بلايين التحولات و لا توجد بصمة واحدة و ثابته من عينة الى عينة أخرى لهذا النوع من الفيروسات يمكن من خلالها اكتشافها

د. وهناك العديد من الأنواع الأخرى مثل :

- الفيروسات المصاحبة: و تقوم باستبدال البرنامج المستهدف بعد أخذ نسخة إحتياطية منه
- الفيروسات الخفية "الشبح": تقوقع نفسها بعد تنفيذها, و تقوم بإخفاء زيادة حجم الملف المصاب أو التغير في التاريخ ... الخ
- فيروسات القطاعات: تقوم بتغير عناوين الملفات في جدول توزيع الملفات ليصبح العنوان المحول عنوان الفيروس
- فيروسات المناعة: تهاجم برامج الحماية ضد الفيروسات

مما سبق نلمس أن هذا الموضوع لا يمكن أن يستوفي حقه في مقالة علمية موجزة ولكن اكتفينا من السوارة ما أحاط بالعنق وهذا قليل من كثير ولعلنا مستقبلاً نأتي على كل جزء منها بالتفصيل.

المصادر

١. التشفير: "الرياض" العدد ١٢٥٢٥ - اقتباس بتصرف

٢. الفيروسات: مقالة الكترونية م. إبراهيم بدر محرز - اقتباس بتصرف