Deontologia Informatica

La deontologia según el diccionario del a real academia de la lengua, es, un sentido mas amplio, la ciencia o tratado de los deberes y normas morales. En un sentido mas concreto, tiene que ver con el comportamiento moral o ético, es decir con los principios y normas morales que regulan las actividades humanas. La deontologia informatica, por extensión, trata, por tanto, de la moral o estica profesional en el manejo del activo mas importante que tienen las empresas, un bien cada vez mas apreciado, que es la información.

Historicamente, los profesionales de la informatica, como grupo, no han sido involucrados en cuestiones de etica. A menudo, sse ve, a las computadoras simplemente como maquinas y algoritmos y no se perciben las serias cuestiones de eticas inherentes a su utilización.

De cualquier modo, cuando se considera que esas maquinas influyen, directa e indirectamente, en la calidad de vida de millones de individuos se comprende que es un tema de gran importancia. Las computadoras se utilizan para diseñar, analizar, sportar y controlar las aplicaciones que protegen y guian las vidas de las personas. El uso de los sistemas informaticos puede tener efectos mas alla de lo que alcanza la imaginación.

Esa actitud estara dirigida en el futuro acia problemas de seguridad. En particular, se debe considerar, publicar ampliamente el codigo fuente de virus y otras amenazas para la seguridad.

Un tipo de conducta poco etica es la instrucción por medios informaticos, auque de esta no resulte ningun daño obvio. La actividad por si misma es inmoral e incluso si el resultado es una mejora de seguridad, aunque existen multidud de posibles razones para justificarla.

Seguridad Informatica

La seguridad informática, técnicas desarrolladas para proteger los equipos informáticos individuales y conectados en una red frente a daños accidentales o intencionados. Estos daños incluyen el mal funcionamiento del *hardware*, la pérdida física de datos y el acceso a bases de datos por personas no autorizadas. Diversas técnicas sencillas pueden dificultar la delincuencia informática. Por ejemplo, el acceso a información confidencial puede evitarse destruyendo la información impresa, impidiendo que otras personas puedan observar la pantalla del ordenador, manteniendo la información y los ordenadores bajo llave o retirando de las mesas los documentos sensibles. Sin embargo, impedir los delitos informáticos exige también métodos más complejos.

En un sistema de los denominados 'tolerante a fallos' dos o más ordenadores funcionan a la vez de manera redundante, por lo que si una parte del sistema falla el resto asume el control.

Los virus informáticos son programas, generalmente destructivos, que se introducen en el ordenador (al leer un disco o acceder a una red informática) y pueden provocar pérdida de la información (programas y datos) almacenada en el disco duro. Existen programas antivirus que los reconocen y son capaces de 'inmunizar' o eliminar el virus del ordenador. Para evitar problemas en caso de apagón eléctrico existen las denominadas UPS (acrónimo de *Uninterrupted Power Supply*), baterías que permiten mantener el sistema informático en funcionamiento, por lo menos el tiempo necesario para apagarlo sin pérdida de datos. Sin embargo, la única forma de garantizar la integridad física de los datos es mediante copias de seguridad.

El mayor problema que tienen que resolver las técnicas de seguridad informática es el acceso no autorizado a datos. En un sistema seguro el usuario, antes de realizar cualquier operación, se tiene que identificar mediante una clave de acceso. Las claves de acceso son secuencias confidenciales de caracteres que permiten que los usuarios autorizados puedan acceder a un ordenador. Para ser eficaces, las claves de acceso deben resultar

difíciles de adivinar. Las claves eficaces suelen contener una mezcla de caracteres y símbolos que no corresponden a una palabra real. Para ponérselo difícil a los impostores, los sistemas informáticos suelen limitar el número de intentos de introducir la clave.

Las tarjetas de contraseña son tarjetas de plástico que no pueden ser manipuladas, dotadas de un microprocesador que almacena una clave de acceso que cambia frecuentemente de forma automática. Cuando se entra en un ordenador mediante una tarjeta de acceso, el ordenador lee la clave de la tarjeta y otra clave introducida por el usuario, y las compara respectivamente con una clave idéntica a la de la tarjeta (que el ordenador genera automáticamente) y con la clave de acceso del usuario, que está almacenada en una lista confidencial. En el futuro, es posible que las claves y las tarjetas de acceso se vean reforzadas por mecanismos biométricos basados en características personales únicas como las huellas dactilares, los capilares de la retina, las secreciones de la piel, el ácido desoxirribonucleico (ADN), las variaciones de la voz o los ritmos de tecleado. Sistemas operativos como UNIX y WINDOWS−NT permiten restringir el acceso a recursos del sistema (ficheros, periféricos..) de acuerdo con esa identificación.

Algunos de los problemas hoy en dia son los siguientes:

Vulnerabilidad de obtención de credenciales NTLM

Microsoft ha publicado su primer boletín de seguridad del año, en el se informa de una vulnerabilidad que afecta a todos los sistemas con Office 2000, Windows 2000 o Windows Me, por el cual se pueden ver comprometidas las credenciales NTLM.

El Cliente Extensor Web (Web Extender Client, WEC) es un componente que se distribuye como parte de Office 2000, Windows 2000 y Windows Me. WEC permite a Internet Explorer visualizar y publicar archivos a través de carpetas web, de forma similar a como se visualizan y añaden archivos mediante el Explorador de Windows. Debido a un error en la implementación, WEC no respeta la configuración de seguridad de IE en relación con la autentificación NTLM, en su lugar WEC realizará la autentificación NTLM con cualquier servidor que lo solicite.

Este problema puede permitir a un webmaster malicioso obtener una copia de las credenciales de autentificación NTLM pertenecientes a un usuario que visite la página web. De esta forma, el usuario malicioso podrá emplear posteriormente una herramienta para realizar un ataque por fuerza bruta para obtener la password o mediante utilidades especializadas podrá enviar una variante de las credenciales en un intento de acceder a recursos protegidos.

La vulnerabilidad sólo proporcionará al usuario malicioso las credenciales de autentificación NTLM de otro usuario. Esto, por si mismo, no permitirá que el usuario malicioso pueda conseguir el acceso a los recursos para los que el usuario tiene acceso autorizado.

Para forzar las credenciales NTLM o posteriormente crackear la password, el usuario malicioso deberá tener acceso a un logon remoto en el sistema objetivo. Sin embargo las prácticas habituales de seguridad recomiendan que los servicios de acceso remoto sean inhabilitados en los dispositivos perimetrales, lo cual impedirá a cualquier atacante el uso de las credenciales obtenidas para acceder al sistema.

Para solucionar este problema Microsoft publica un parche que se encuentra disponible en las siguientes direcciones:

Para Microsoft Office 2000 (todas las plataformas):

http://officeupdate.microsoft.com/2000/downloaddetails/wecsec.htm

Para Microsoft Windows 2000 (sin Office 2000):

http://www.microsoft.com/Downloads/Release.asp?ReleaseID=26889

Para Microsoft Windows Me (sin Office 2000):

http://www.microsoft.com/Downloads/Release.asp?ReleaseID=26705

Grave vulnerabilidad en servidores Oracle

Guninski en un nuevo aviso alerta de una vulnerabilidad en las instalaciones por defecto de Oracle 8.1.7 para Windows 2000. A través del servlet Oracle XSQL y hojas de estilo xml es posible ejecutar java en el servidor.

En esta ocasión el problema afecta a las instalaciones de Oracle 8.1.7 bajo Windows 2000 aunque como indica el propio Guninski es muy posible que otras versiones y plataformas también se vean afectadas ya que el servlet problemático está escrito en java.

El servlet XSQL permite especificar una hoja de estilo xslt externa que puede estar alojada en cualquier sitio. El problema reside en que es posible ejecutar código java en el servidor web si este se incluye en el xslt. La ejecución de java en el servidor, puede provocar sin ninguna duda el compromiso total del servidor.

Oracle permite extensiones a las funciones incluidas en xslt mediante el uso de xmlns. Mediante el uso de este namespace es posible instanciar objetos java y ejecutar sus métodos. Guninski proporciona los archivos xsl y sxlt necesarios para llegar a reproducir el fallo.

Para evitar este problema se recomienda añadir la línea

allow−client−style="no"

en el elemento document de cada página xsql. En los próximos días Oracle publicará un parche para remediar el problema.

Vulnerabilidades en Oracle Internet Application Server

Se han encontrado varios problemas que pueden ocasionar vulnerabilidades en el servidor de aplicaciones Internet de Oracle en todas sus plataformas.

La primera vulnerabilidad se puede encontrar en el componente WebDB/Portal Listener y modplsql, la segunda vulnerabilidad afecta a todas las versiones del gateway PL/SQL lo que incluye Oracle Application Server (OAS), WebDB/Portal listener e iAS (Internet Aplication Server).

El primero de los fallos hace referencia a un problema de configuración asociado a Portal Listener y modplsql. Cuando estos componentes se encuentran instalados la configuración por defecto permite a todos los usuarios el acceso a las páginas de administración de Listener y modplsql.

La segunda vulnerabilidad puede ocurrir si el administrador concede acceso público a los procedimientos PL/SQL. En particular a aquellos con acceso a la base de datos Oracle, como OWA, SYS y DBMS. Puesto que se puede acceder a los procedimientos públicos a través de una URL, esto puede permitir a un usuario invocar dichos procedimientos desde una URL y provocar la ejecución de expresiones SQL en la base de datos Oracle.

El primero de los fallos descritos puede ocurrir si no se cambian los permisos por defecto para las páginas de

administración tras la instalación de WebDB/Portal. El segundo depende del diseño de la aplicación que hace uso del gateway PL/SQL, pero puede ocurrir siempre que un procedimiento tenga acceso público.

Para evitar estos problemas será necesario especificar que el Listener y el administrador de modplsql deben ser uno o más usuarios conocidos. Esto se puede hacer fácilmente editando el archivo de configuración wdbsvr.app en WebDB/Portal. Al comienzo del archivo hay un campo titulado "administrators=", en el que se deberán especificar los nombres de los usuarios con privilegios administrativos.

Como medida de seguridad adicional, el administrador puede modificar la ruta de las páginas empleadas para la administración. La ruta por defecto es "admin_", pero puede modificarse en el archivo wdbsvr.app por cualquier otra cadena.

Para evitar los problemas producidos por los procedimientos PL/SQL con acceso público es recomendable cancelar el acceso público a procedimientos como OWA, SYS y DBMS que pueden permitir a un usuario la ejecución de comandos SQL especificados.

Permisos erróneos en el registro de Windows NT

Microsoft avisa de la existencia de permisos incorrectos en múltiples claves del registro de Windows NT 4.0. Los permisos por defecto pueden permitir a un usuario malicioso conseguir mayores privilegios en la máquina afectada.

Existen tres claves del registro con permisos por defecto inadecuados.La primera de las claves afectadas es la encargada de proporcionar determinados parámetros SNMP.

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SNMP\Parameters, proporciona el nombre de comunidad SNMP y los identificadores de administración SNMP, si existen. La lectura de esta información puede permitir a un usuario malicioso pasar como un administrador SNMP para cualquier comunidad a la que pertenezca el máquina afectada.

También resultan inadecuados los permisos de la clave de administración RAS, HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\RAS, que proporciona una forma para instalar productos RAS de terceras partes que trabajen con el servicio nativo RAS de Windows NT. Al modificar alguno de los valores de esta clave un atacante podrá especificar el código malicioso que desee como una herramienta de administración de otra compañía. Dicho código se ejecutará entonces dentro del contexto de la cuenta del sistema lo que permitirá al atacante tomar el control del sistema.

La última clave afectada, hace referencia a la administración de paquetes MTS,HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\TransactionServer\Packages. Esta clave incluye información sobre los usuarios con permisos para instalar y modificar paquetes MTS. Si en este punto, el atacante se añade a si mismo como administrador MTS podrá conseguir la facultad de añadir, borrar o modificar paquetes MTS.

Para realizar los cambios necesarios en estas claves Microsoft ha publicado una herramienta que se puede encontrar en:

http://www.microsoft.com/Downloads/Release.asp?ReleaseID=24501

Agujero en la máquina Java de Lotus Notes Client R5

Lotus Notes Client R5, la herramienta de mensajería y colaboración, cuenta con su propio navegador web y una máquina virtual Java para poder visualizar los applets. Existe una vulnerabilidad en la característica ECL

(Execution Control List), propietaria de la máquina virtual Java de Lotus, que permite chequear mediante un applet, de forma remota, la existencia o no de archivos en una ruta determinada.

La vulnerabilidad, descubierta por Hiromitsu Takagi, fue reportada por él mismo a Lotus el 3 de Mayo del presente año. Cuando ya transcurren más de 6 meses, y después de continuos contactos por correo electrónico y teléfono, Lotus no ha facilitado solución alguna al respecto. Takagi, ante la falta de una respuesta satisfactoria, ha optado por hacer pública la vulnerabilidad en busca de una reacción acorde con el problema.

La vulnerabilidad

El modelo de seguridad del estándar Java hasta JDK 1.1 prohíbe cualquier tipo de acceso a los archivos locales del sistema. La característica ECL introducida por Lotus en su máquina virtual es más flexible al respecto, ofreciendo la posibilidad al usuario final de aceptar o cancelar una acción cuando intenta acceder a un archivo local, mediante la aparición de un cuadro de diálogo donde se puede elegir "Execute" o "Cancel".

Cuando se invoca al método getSystemResource(String) de la clase java.lang.ClassLoader, el cuadro de diálogo aparece *sólo* si existe el archivo que se pasa como argumento. Si bien el método siempre devuelve el valor "null" se haya elegido cualquier opción del cuadro de diálogo o si este ni siquiera se ha visualizado, la diferencia de tiempo que transcurre es distinta. Es decir, cuando el archivo no existe el cuadro de diálogo no aparece, el valor "null" es devuelto de forma instantánea y la aplicación sigue su curso. Sin embargo, cuando el archivo existe aparece el cuadro de diálogo y el tiempo de proceso es mayor, por lo que midiendo el tiempo que transcurre antes y después de invocar al método se puede establecer si el archivo existe o no.

Código:

```
long start = System.currentTimeMillis();

URL resource = ClassLoader.getSystemResource(filePathname);

long diff = System.currentTimeMillis() − start;

if (diff > 400) { [existe]

...
```

Implicaciones

A continuación algunos ejemplos de las posibilidades que ofrece la explotación de esta vulnerabilidad:

−Conocer si el usuario ha visitado sitios web específicos, chequeando la existencia de sus respectivas cookies.

−Saber si una dirección web se encuentra en la clasificación de "favoritos" de Internet Explorer, chequeando la existencia del correspondiente archivo en \WINDOWS\Favorites\.

−Descubrir si un archivo determinado ha sido utilizado recientemente, chequeando la existencia de un acceso directo con el mismo nombre en la carpeta \WINDOWS\Recent\.

−Conocer si hay determinadas aplicaciones instaladas o configuraciones específicas del sistema, cuyo conocimiento puede ser aprovechado para llevar a cabo otros ataques.

Demostración

Takagi ha creado un applet que demuestra, y permite a los usuarios verificar, la existencia del agujero. El ejemplo, que funcionará de forma correcta en Lotus Notes Client R5, comprueba si tenemos instaladas determinadas aplicaciones chequeando la existencia de sus trayectorias y ejecutables por defecto, así como informa si hemos visitado el sitio web de PlayBoy tras examinar algunas cookies.

Más información:

Lotus Notes R5 Client:

http://www.lotus.com/home.nsf/welcome/notes

Lotus Notes Client R5 File Existence Verification Vulnerability:

http://www.securityfocus.com/bid/1994

Security Hole in ECL Feature of Java VM Embedded in Lotus Notes Client R5:

http://java−house.etl.go.jp/ml/archive/j−h−b/038904.html

Demostración:

http://java−house.etl.go.jp/~takagi/java/security/lotus−notes−existence−attack/Test.html

El futuro de la Seguridad en Internet

Washington, (NTX).− En los próximos años, la gente aumentará su confianza en Internet para compartir información delicada con interlocutores confiables acerca de sus finanzas, historias médicas, hábitos personales o preferencias como compradores. Al mismo tiempo, muchos pueden querer mantener en reserva esta información y usar Internet en forma anónima.

Aunque la tecnología ha puesto en riesgo durante décadas la privacidad individual −la mayoría de los consumidores usa tarjetas de crédito e intercambia por teléfono información delicada con vendedores− la privacidad se convertirá en un asunto más de presión, en la medida en que Internet se convierte en el medio preferido por la gente para manejar sus finanzas o ponerse en contacto con su médico.

El uso de información personal por minoristas que ofrecen servicios personalizados, y por publicistas que desean capturar la atención de audiencias específicas, ha originado que algunos de ellos compartan información de sus consumidores sin notificarles, lo que ha generado una preocupación creciente en el público acerca de la seguridad de la información personal. Esto ha dejado a mucha gente renuente a proporcionar datos reales a sitios Web.

La industria privada y muchas herramientas de autorregulación del gobierno, así como determinadas tecnologías, son la mejor forma de proteger la privacidad. Ahora muchas organizaciones independientes aceptan por lo común "prácticas limpias de información", que garantizan la honestidad y la confiabilidad entre empresas que proporcionan y usan datos personales.

Pero como lo explican las contribuciones de Ellen Alderman y Caroline Kennedy a este proyecto, es aún poco claro cuán efectivas son estas herramientas. Proteger la privacidad individual es la mayor barrera que debe ser removida lo antes posible para mantener a Internet en movimiento hacia adelante.

Mantener una Internet Segura

La seguridad es siempre el mayor asunto para los empresarios y gobiernos, se sustenta en la confianza en las TI y siempre será así. Esto es también verdad para la seguridad de los individuos. Mucho antes de Internet, la gente ha entregado sus tarjetas de crédito en los restaurantes a meseros a quienes nunca antes había visto, y es difícil que eso cambie.

Pero mientras aumenta la dependencia de nuestra economía hacia Internet, la seguridad se convierte en una mayor preocupación. Los conocidos incidentes de intrusiones indeseadas, los fraudes con tarjetas de crédito y el anonimato de la Web, han dado a Internet una injustificada reputación de "Salvaje Oeste".

Para mantener a Internet como un lugar seguro para hacer negocios, las empresas fabricantes de programas tienen la responsabilidad de trabajar juntas para garantizar que sus productos siempre ofrezcan los máximos niveles de seguridad. Y el sistema judicial y la comunidad policial deben ir de la mano de los avances tecnológicos y aplicar la legislación penal completa y efectivamente.

Internet puede revolucionar la educación, dando a los niños la oportunidad de ver recompensada su curiosidad intelectual y explorar su mundo. Pero así como esta herramienta les ayuda a aprender sobre los dinosaurios o la historia del mundo, también los puede exponer a obscenidades, violencia o contenidos inapropiados. Como Internet es un medio global sin regular, es difícil censurarlo en la forma tradicional.

El sector privado ha hecho grandes esfuerzos para dar a los padres y maestros más control sobre lo que los pequeños pueden ver y hacer en Internet, a través de programas que actúan como filtros, bloqueando el acceso a sitios dudosos.

Las normas de la industria, como la Plataforma para la Selección de Contenidos en Internet y los proveedores de servicios de Internet, que en forma voluntaria regulan las actividades de sus consumidores, han sido instrumentos eficaces.

Los gobiernos juegan también su parte, apoyando el crecimiento del mercado de herramientas para proteger a los niños e incrementando la aplicación de la ley y el papel de la policía en la persecución de delincuentes informáticos.

El tema de la protección de los niños en Internet es un excelente ejemplo de cómo pueden trabajar juntos el sector privado y los gobiernos para afrontar problemas relativos a Internet.

Tendiendo puentes a la brecha digital

Internet puede impulsar y enriquecer las vidas de personas marginadas en el mundo, pero sólo si esa gente tiene acceso a la red. Las contribuciones de Robert Knoeling y Ernest Wilson a este proyecto muestran claramente que la brecha digital es un problema global. En Estados Unidos, donde un gran porcentaje de la población tiene acceso a Internet, es fácil olvidar que la mayoría de la gente que habita el planeta nunca ha hecho una llamada telefónica, mucho menos navegado en Internet.

En la década de 1930, el gobierno de Estados Unidos ayudó a romper la "brecha eléctrica", creando la Administración de Electrificación Rural, que llevó energía a las áreas rurales del país y los beneficios de la electrificación. En forma similar, programas de "servicio universal" ayudaron a algunas áreas remotas y a comunidades marginadas a tener acceso a servicios telefónicos baratos.

Estos esfuerzos han sido ampliamente exitosos en Estados Unidos, pero en una escala mundial hay un enorme trabajo que debe realizarse antes de que Internet puede marcar una verdadera diferencia. Es importante recordar que una gran parte del mundo permanece aún sin energía eléctrica adecuada ni servicio telefónico y carece de niveles aceptables de servicios de salud y educación.

Tender puentes para evitar la brecha digital es sólo una de las muchas formas en las que podemos mejorar la calidad de vida del mundo. Los beneficios de expandir el acceso a Internet y a la tecnología de las comunicaciones son lo suficientemente claros como para que los gobiernos ahora decidan si deberían aplicar un principio similar para garantizar que nadie se quede atrás en la Era de Internet.

¿Cuál debe ser el papel de los gobiernos? Internet es un cambio constante en la cadena global que no conoce fronteras, y presenta un problema único para los gobiernos que necesitan enfrentar los numerosos retos que les plantea. En los próximos años, los gobiernos deben tener la oportunidad de desarrollar políticas creíbles e innovadoras, que protejan a sus ciudadanos mientras alimentan la apertura, la flexibilidad y las oportunidades económicas, que hacen de Internet una tecnología indispensable.

La suavidad de las regulaciones gubernamentales ha creado un ambiente que ha permitido florecer a Internet, facilitando a las empresas la difusión de sus innovaciones entre los consumidores a una velocidad impresionante. Durante los próximos años los gobiernos del mundo se verán recompensados por seguir políticas que aceleren la construcción de la infraestructura que hará posible llevar los beneficios de Internet a más gente.

Esto incluye encontrar la forma de agilizar la aplicación de tecnologías de banda ancha, desregular lo que sea necesario para estimular la competencia, resistir la tentación de decretar nuevas regulaciones y redoblar esfuerzos para proteger los contenidos que viajan a través de Internet, haciendo más fuertes las leyes que protegen los derechos intelectuales.

Internet da a la gente la oportunidad de poner a trabajar sus conocimientos y de aprovechar grandes oportunidades para hacer sus vidas más productivas y plenas. Es la puerta de entrada al gran conocimiento, al arte y la cultura. Proporciona acceso igualitario a la información y las comunicaciones, permitiendo la formación de comunidades vigorosas y de conexiones reales entre la gente.

Rompe las barreras entre (y dentro) de las naciones, abre las economías y democratiza sociedades. Mientras las computadoras se hacen más baratas, Internet puede brindar todos estos beneficios a más y más gente en el mundo.

Asegurarnos de que Internet puede tener el mayor y más positivo impacto en el mayor número posible de personas será un tremendo reto para nuestros líderes políticos y empresariales. Hay algunos asuntos clave que necesitan ser superados para darnos cuenta del pleno potencial de Internet, pero estos retos no son totalmente nuevos y definitivamente no son insuperables.

Es claro que estos son retos como los que enfrentó la prensa escrita, el teléfono, la electricidad o el automóvil. Internet es una tecnología revolucionaria que está transformando nuestro mundo.

Otras noticias de seguridad

Kevin Mitnick se convierte en asesor de seguridad

Kevin Mitnick, el reconocido hacker capturado, quien recibió casi 5 años de cárcel y salió a principios de éste año, se convirtió en consultor de seguridad informática y dictó una charla en la conferencia de E−Business para profesionales en tecnologías de la información el mes pasado, donde comentó algunas de sus experiencias y consejos de seguridad.

Inclusive si se compran los mejores productos de seguridad, alguien los vulnerará, dijo Mitnick. No hay una forma completamente segura de protegerse. Se debe manejar el riesgo, ya que no hay forma de eliminarlo.

Mitnick ofreció una introspección a al mente del hacker, y no fue muy reconfortante: Entre más seguros se

hacen los sistemas, más atraen a los hackers. Los hackers son movidos por la curiosidad de explorar la red y obtener conocimiento prohibido.

Hackear no requiere necesariamente habilidades técnicas. Alguien puede engañar a un empleado para obtener su contraseña y hacer algo en un computador, una técnica llamada ingeniería social.

Entre más grande es la compañía, más vulnerable es a la ingeniería social. Es más fácil para un atacante pretender ser alguien más en la compañía en un entorno donde los empleados no se conocen, dijo Mitnick.

Para reducir el riesgo, Mitnick sugiere que las compañías realicen los siguientes pasos:

−Utilizar software de manejo de contraseñas para ayudar a los empleados a elegir contraseñas complejas.

−Tener tiempo de expiración de contraseñas.

−Crear autenticación más fuerte combinando contraseñas con biometría.

También dijo que las compañías deben tener precaución contra otra técnica usada por los hackers para obtener información confidencial: Escudriñar los desechos. Recoger documentos, revisar qué hay en la papelera de reciclaje y borrar o destruir medios magnéticos son algunas formas de reducir éste riesgo.

En general, asegurar un e−Business significa educar a los empleados sobre la importancia de la seguridad de la información. Motivar a los empleados para hacer de la seguridad, su negocio, agregó Mitnick.

Virus (Informática)

Un virus informático es un programa, elaborado por una o más personas, en un leguaje de programación cualquiera, cuyo propósito es causar algún tipo de daño o problema al computador que lo aloja.

Hasta la actualidad se tiene catalogados más de 20,594 virus informáticos y cada día se descubren nuevos, desde los clásicos que pos programas ejecutables hasta los más modernos macros para Microsoft Word.

Es bien sabido que los virus son creados por estudiantes de informática, afanados en probar que son los mejores programadores carentes de moral, pero también son fruto de las mismas empresas que fabrican los antivirus que manipulan al mercado consumidor. ¿Antivirus? − Muy simple, programas dedicados a detectar y eliminar virus, por suerte, no existe virus sin su antivirus.

Si tu eres cuidadoso con los programas que utilizas, la información que introduces a tu computadora y con los lugares que visitas en el Internet, es muy posible que nunca tengas problemas con virus informáticos, lo que sí, es indispensable que tengas instalado un buen y actualizado antivirus.

Existen otros programas informáticos nocivos similares a los virus, pero que no cumplen ambos requisitos de reproducirse y eludir su detección. Estos programas se dividen en tres categorías: caballos de Troya, bombas lógicas y gusanos. Un caballo de Troya aparenta ser algo interesante e inocuo, por ejemplo un juego, pero cuando se ejecuta puede tener efectos dañinos. Una bomba lógica libera su carga activa cuando se cumple una condición determinada, como cuando se alcanza una fecha u hora determinada o cuando se teclea una combinación de letras. Un gusano se limita a reproducirse, pero puede ocupar memoria de la computadora y hacer que sus procesos vayan más lentos.

Cómo se producen las infecciones

Los virus informáticos se difuden cuando las instrucciones o código ejecutable que hacen funcionar los

programas pasan de un ordenador a otro. Una vez que un virus está activado, puede reproducirse copiándose en discos flexibles, en el disco duro, en programas informáticos legítimos o a través de redes informáticas. Estas infecciones son mucho más frecuentes en PC que en sistemas profesionales de grandes computadoras, porque los programas de los PC se intercambian fundamentalmente a través de discos flexibles o de redes informáticas no reguladas.

Los virus funcionan, se reproducen y liberan sus cargas activas sólo cuando se ejecutan. Por eso, si un ordenador está simplemente conectado a una red informática infectada o se limita a cargar un programa infectado, no se infectará necesariamente. Normalmente, un usuario no ejecuta conscientemente un código informático potencialmente nocivo; sin embargo, los virus engañan frecuentemente al sistema operativo de la computadora o al usuario informático para que ejecute el programa viral.

Algunos virus tienen la capacidad de adherirse a programas legítimos. Esta adhesión puede producirse cuando se crea, abre o modifica el programa legítimo. Cuando se ejecuta dicho programa, lo mismo ocurre con el virus. Los virus también pueden residir en las partes del disco duro o flexible que cargan y ejecutan el sistema operativo cuando se arranca el ordenador, por lo que dichos virus se ejecutan automáticamente. En las redes informáticas, algunos virus se ocultan en el *software* que permite al usuario conectarse al sistema.

Especies de virus

Existen seis categorías de virus: parásitos, del sector de arranque inicial, multipartitos, acompañantes, de vínculo y de fichero de datos. Los virus parásitos infectan ficheros ejecutables o programas de la computadora. No modifican el contenido del programa huésped, pero se adhieren al huésped de tal forma que el código del virus se ejecuta en primer lugar. Estos virus pueden ser de acción directa o residentes. Un virus de acción directa selecciona uno o más programas para infectar cada vez que se ejecuta. Un virus residente se oculta en la memoria del ordenador e infecta un programa determinado cuando se ejecuta dicho programa. Los virus del sector de arranque inicial residen en la primera parte del disco duro o flexible, conocida como sector de arranque inicial, y sustituyen los programas que almacenan información sobre el contenido del disco o los programas que arrancan el ordenador. Estos virus suelen difundirse mediante el intercambio físico de discos flexibles. Los virus multipartitos combinan las capacidades de los virus parásitos y de sector de arranque inicial, y pueden infectar tanto ficheros como sectores de arranque inicial.

Los virus acompañantes no modifican los ficheros, sino que crean un nuevo programa con el mismo nombre que un programa legítimo y engañan al sistema operativo para que lo ejecute. Los virus de vínculo modifican la forma en que el sistema operativo encuentra los programas, y lo engañan para que ejecute primero el virus y luego el programa deseado. Un virus de vínculo puede infectar todo un directorio (sección) de una computadora, y cualquier programa ejecutable al que se acceda en dicho directorio desencadena el virus. Otros virus infectan programas que contienen lenguajes de macros potentes (lenguajes de programación que permiten al usuario crear nuevas características y herramientas) que pueden abrir, manipular y cerrar ficheros de datos. Estos virus, llamados virus de ficheros de datos, están escritos en lenguajes de macros y se ejecutan automáticamente cuando se abre el programa legítimo. Son independientes de la máquina y del sistema operativo.

Tácticas antivíricas

Preparación y prevención

Los usuarios pueden prepararse frente a una infección viral creando regularmente copias de seguridad del *software* original legítimo y de los ficheros de datos, para poder recuperar el sistema informático en caso necesario. Puede copiarse en un disco flexible el *software* del sistema operativo y proteger el disco contra escritura, para que ningún virus pueda sobreescribir el disco. Las infecciones virales pueden prevenirse obteniendo los programas de fuentes legítimas, empleando una computadora en cuarentena para probar los

nuevos programas y protegiendo contra escritura los discos flexibles siempre que sea posible.

Detección de virus

Para detectar la presencia de un virus pueden emplearse varios tipos de programas antivíricos. Los programas de rastreo pueden reconocer las características del código informático de un virus y buscar estas características en los ficheros del ordenador. Como los nuevos virus tienen que ser analizados cuando aparecen, los programas de rastreo deben ser actualizados periódicamente para resultar eficaces. Algunos programas de rastreo buscan características habituales de los programas virales; suelen ser menos fiables.

Los únicos programas que detectan todos los virus son los de comprobación de suma, que emplean cálculos matemáticos para comparar el estado de los programas ejecutables antes y después de ejecutarse. Si la suma de comprobación no cambia, el sistema no está infectado. Los programas de comprobación de suma, sin embargo, sólo pueden detectar una infección después de que se produzca.

Los programas de vigilancia detectan actividades potencialmente nocivas, como la sobreescritura de ficheros informáticos o el formateo del disco duro de la computadora. Los programas caparazones de integridad establecen capas por las que debe pasar cualquier orden de ejecución de un programa. Dentro del caparazón de integridad se efectúa automáticamente una comprobación de suma, y si se detectan programas infectados no se permite que se ejecuten.

Contención y recuperación

Una vez detectada una infección viral, ésta puede contenerse aislando inmediatamente los ordenadores de la red, deteniendo el intercambio de ficheros y empleando sólo discos protegidos contra escritura. Para que un sistema informático se recupere de una infección viral, primero hay que eliminar el virus. Algunos programas antivirus intentan eliminar los virus detectados, pero a veces los resultados no son satisfactorios. Se obtienen resultados más fiables desconectando la computadora infectada, arrancándola de nuevo desde un disco flexible protegido contra escritura, borrando los ficheros infectados y sustituyéndolos por copias de seguridad de ficheros legítimos y borrando los virus que pueda haber en el sector de arranque inicial.

Estrategias virales

Los autores de un virus cuentan con varias estrategias para escapar de los programas antivirus y propagar sus creaciones con más eficacia. Los llamados virus polimórficos efectúan variaciones en las copias de sí mismos para evitar su detección por los programas de rastreo. Los virus sigilosos se ocultan del sistema operativo cuando éste comprueba el lugar en que reside el virus, simulando los resultados que proporcionaría un sistema no infectado. Los virus llamados infectores rápidos no sólo infectan los programas que se ejecutan sino también los que simplemente se abren. Esto hace que la ejecución de programas de rastreo antivírico en un ordenador infectado por este tipo de virus pueda llevar a la infección de todos los programas del ordenador. Los virus llamados infectores lentos infectan los archivos sólo cuando se modifican, por lo que los programas de comprobación de suma interpretan que el cambio de suma es legítimo. Los llamados infectores escasos sólo infectan en algunas ocasiones: por ejemplo, pueden infectar un programa de cada 10 que se ejecutan. Esta estrategia hace más difícil detectar el virus.

Historia

En 1949, el matemático estadounidense de origen húngaro John von Neumann, en el Instituto de Estudios Avanzados de Princeton (Nueva Jersey), planteó la posibilidad teórica de que un programa informático se reprodujera. Esta teoría se comprobó experimentalmente en la década de 1950 en los Laboratorios Bell, donde se desarrolló un juego llamado Core Wars en el que los jugadores creaban minúsculos programas informáticos que atacaban y borraban el sistema del oponente e intentaban propagarse a través de él. En 1983, el ingeniero

eléctrico estadounidense Fred Cohen, que entonces era estudiante universitario, acuñó el término de "virus" para describir un programa informático que se reproduce a sí mismo. En 1985 aparecieron los primeros caballos de Troya, disfrazados como un programa de mejora de gráficos llamado EGABTR y un juego llamado NUKE−LA. Pronto les siguió un sinnúmero de virus cada vez más complejos. El virus llamado Brain apareció en 1986, y en 1987 se había extendido por todo el mundo. En 1988 aparecieron dos nuevos virus: Stone, el primer virus de sector de arranque inicial, y el gusano de Internet, que cruzó Estados Unidos de un día para otro a través de una red informática. El virus Dark Avenger, el primer infector rápido, apareció en 1989, seguido por el primer virus polimórfico en 1990. En 1995 se creó el primer virus de lenguaje de macros, WinWord Concept.

Algunos tipos de virus son los siguientes:

Melissa

El más sonado virus de este año se llama Melissa. El único daño que causa es utilizar tu programa de correo electrónico para enviar decenas de mensajes con información pornográfica, no es poco si piensas en la saturación de los servidores y en los problemas posteriores a enviar esos mensajes a tu amigos o clientes.

Melissa llega como un e−mail con título "Trust No One" y con contenido de "Be careful what you open. It could be a virus.", acompañado de un archivo adjunto que aloja al virus.

Para colmo, ya existen variaciones de Melissa como:

Macro.Word97.Melissa.b
Macro.Excel97.Papa.a
Macro.Excel97.Papa.b

Afortunadamente ya tenemos la solución, el antivirus está disponible en:
www.pcmag.com/machrone
www.pcmag.com/pctech/download/daily/index.html

Virus en lenguaje Java

Ikarus, empresa australiana de antivirus alertó de su último descubrimiento, un virus elaborado en lenguaje Java, lenguaje de uso casi exclusivo para Internet.

Este virus, llamado "*BeanHive*" es muy similar a su antecesor el "*Strange Brew*". No muy dañinos, pero nadie los quiere en su computador.

Virus vía correo electronico

Es el año de los virus transmitidos por el correo electrónico (e−mail), es cierto hay muchos, entre ellos el famoso Melissa, pero también existen demasiados rumores, entonces a tomar en cuenta los siguientes aspectos:

- Todo virus enviado por e−mail, llega a tu casilla como *attach*, es decir, como archivo adjunto al mensaje, normalmente archivos con extensión EXE o DOC.
- Para que un virus enviado por e−mail cause algún daño a tu computador, primero, deberá ser ejecutado, un archivo enviado por e−mail no puede ejecutarse solo. Para ejecutarlo debes hacer un doble click sobre él o autorizar al tu computadora a abrirlo en un otro programa (MS Word).
- Aún si no ejecutas el archivo portador del virus, el virus estará como pasajero en tu disco duro mientras no borres el mensaje que lo trajo.

Es así que protegerse de virus llegados por e−mail es muy fácil si sigues los siguientes pasos:

- Nunca abras mensajes llegados a tu casilla si no sabes de donde provienen más si contienen archivos adjuntos tipo EXE, COM o DOC.
- En cuanto recibas mensajes con títulos como "sexo sin límites" u "oferta gratuita", bórralos de tu disco duro sin siquiera abrirlos.
- Cuando recibas archivos adjuntos de amigos o clientes, primero verifica la presencia de virus en ellos y luego ábrelos.
- Por último, no seas curioso con los mensajes anónimos llegados a tu casilla, sé precavido y bórralos!

MS Word 97 Macro Class Virus

Un nuevo virus esta por llegar a tu casilla de e−mail, oficialmente llamado "MS Word 97 Macro Class Virus", el virus se presenta como un mensaje con el título "is a big stupid jerk" y con un archivo DOC adjunto.

Su daño, muy simple, cada día 14 se activa y genera documentos de MS Word 6 o 97 con un menú que dice "is a big stupid jerk".

Verifica tu computador con tu antivirus preferido y asegúrate que en tu MS Word esta activada la opción "Enable Macro Virus Protection".

"Hybris", un nuevo giro en la historia de los virus

El año pasado, aproximadamente a estas alturas, el virus "Babylonia" rompió moldes en el mundo de la programación de este género de engendros informáticos, y aportó nuevas y peligrosas posibilidades, en simbiosis con Internet, hasta el momento desconocidas: era el primer espécimen capaz de actualizar su cód

igo por medio de la Red. Esta vez es el turno de "Hybris", un gusano programado por el mismo autor que se presenta como el patógeno más difícil de combatir, así como, probablemente, el más complejo aparecido hasta el momento.

El funcionamiento básico de este "i−worm" recuerda al de "Happy99", en cuanto a que, tras haber sido ejecutado por el usuario, procede a instalarse en el sistema modificando WSOCK32.DLL, la librería de comunicaciones por Internet empleada por Windows, con el fin de poder enganchar las funciones "connect", "recv" y "send", por medio de las cuales el gusano es capaz de monitorizar las acciones claves que están teniendo lugar en cada conexión a la Red. Por si esto fuera poco, "Hybris" además modifica la porción de código de carga inicial de esta librería con su propio código, tras lo cual cifra el fragmento original, para dificultar sobremanera −incluso convertir en una decisión arriesgada− su desinfección.

Como suele suceder, en caso de que el archivo WSOCK32.DLL esté en memoria, activo, el "malware" no será capaz de modificarlo, por lo que procederá a efectuar una copia del mismo, empleando un nombre generado de manera aleatoria, e incluirá una instrucción para poder renombrarlo en el archivo WININIT.INI, que llevará a cabo esta tarea en el siguiente inicio de sesión del sistema operativo afectado. A este respecto es importante comentar que, asimismo, "Hybris" crea una entrada en el registro de configuraciones del usuario por medio de la cual ejecuta la copia del código maligno tras el siguiente arranque, una operación aparentemente redundante cuya única causa sería, aparentemente, la necesidad que tiene el gusano de asegurarse de que la sustitución de WSOCK32.DLL se hace efectiva.

A partir del momento en que la librería infectada es cargada en la memoria del computador, el patógeno pasa a controlar absolutamente todas las comunicaciones que tienen lugar por medio de Internet, a partir de las cuales es capaz de interceptar nuevas direcciones de correo electrónico a las que enviar copias de sí mismo. Hasta el momento se han detectado numerosas posibilidades en torno al aspecto de los e−mails portadores; las

más populares son las enviadas por el remitente "Hahaha<hahaha@sexyfun.net>", que contienen un breve fragmento en alusión al cuento de Blanca nieves, traducido a portugués, español, inglés o francés, emparejado con un asunto fijo y cuatro posibles nombres de archivo adjunto para cada una, y con referencias de tipo pornográfico:

Asunto: Branca de Neve pornô!

Posibles adjuntos: branca de neve.scr

atchim.exe

dunga.scr

anão pornô.scr

Texto:

Faltava apenas um dia para o seu aniversario de 18 anos. Branca de Neve estava muito feliz e ansiosa, porque os 7 anões prometeram uma *grande* surpresa. As cinco horas, os anõezinhos voltaram do trabalho. Mas algo nao estava bem... Os sete anõezinhos tinham um estranho

brilho no olhar...

Asunto: Enanito si, pero con que pedazo!

Posibles adjuntos: enano.exe

enano porno.exe

blanca de nieve.scr

enanito fisgon.exe

Texto:

Faltaba apenas un día para su aniversario de 18 años. Blanca de Nieve fuera siempre muy bien cuidada por los enanitos. Ellos le prometieron una *grande* sorpresa para su fiesta de cumpleaños. Al entardecer, llegaron. Tenían un brillo incomun en los ojos...

Asunto: Snowhite and the Seven Dwarfs − The REAL story!

Posibles adjuntos: sexy virgin.scr

joke.exe

midgets.scr

dwarf4you.exe

Texto:

Today, Snowhite was turning 18. The 7 Dwarfs always where very educated and polite with Snowhite. When

they go out work at mornign, they promissed a *huge* surprise. Snowhite was anxious. Suddlently, the door open, and the Seven Dwarfs enter...

Asunto: Les 7 coquir nains

Posibles adjuntos: blancheneige.exe

sexynain.scr

blanche.scr

nains.exe

Texto:

C´etait un jour avant son dix huitieme anniversaire. Les 7 nains, qui avaient aidé `blanche neige´ toutes ces années après qu´elle se soit enfuit de chez sa belle mère, lui avaient promis une *grosse* surprise. A 5 heures comme toujours, ils sont rentrés du travail. Mais cette

fois ils avaient un air coquin...

Asimismo, se han detectado versiones más recientes de "Hybris", con mensajes de apariencia distinta, cuyo asunto está compuesto a partir de combinaciones de las siguientes opciones, emparejando una palabra de la primera columna con otra de la segunda:

Anna sex

Raquel Darian sexy

Xena hot

Xuxa hottest

Suzete cum

famous cumshot

celebrity rape horny

Y acompañados por un archivo anexado, bajo alguno de los nombres de la siguiente lista:

Anna.exe

Raquel Darian.exe

Xena.exe

Xuxa.exe

Suzete.exe

famous.exe

celebrity rape.exe

leather.exe

sex.exe

sexy.exe

hot.exe

hottest.exe

cum.exe

cumshot.exe

horny.exe

anal.exe

gay.exe

oral.exe

pleasure.exe

asian.exe

lesbians.exe

teens.exe

virgins.exe

boys.exe

girls.exe

SM.exe

sado.exe

cheerleader.exe

orgy.exe

black.exe

blonde.exe

sodomized.exe

hardcore.exe

slut.exe

doggy.exe

suck.exe

messy.exe

kinky.exe

fist−fucking.exe

amateurs.exe

Y es que, precisamente, la capacidad que tiene "Hybris" de cambiar su código por medio de actualizaciones enviadas con "plug−ins" es una de sus principales características, que, si bien aparentemente idéntico al concepto aportado por "Babylonia", presenta un par de novedades fundamentales que convierten a este espécimen en todo un quebradero de cabeza para las compañías antivirus interesadas en programar antídotos para combatirlo: el patógeno recibe "plug−ins" por medio de los grupos de noticias de Internet, y éstos aparecen cifrados con algoritmo RSA y una llave de 128 bits, de tal modo que resulta prácticamente imposible impedir que este gusano se siga actualizando por medio de Internet, sin posibilidad de bloquear direcciones o de cerrar cuentas en las que las actualizaciones se encuentren.

Así, por medio del grupo de noticias "alt.comp.virus", "Hybris" va recibiendo nuevos "plug−ins" enviados por su autor, que, tras haber sido procesados, son automáticamente instalados y asimilados por cada una de las copias del espécimen. Esta característica es la que ha llevado al conocido foro de debate orientado hacia la lucha antivírica a verse colapsado en las últimas semanas por un verdadero aluvión de mensajes de origen anónimo y de contenido ininteligible, que en un principio hicieron pensar a los contertulios que no se trataba más que de la broma pesada de un "spammer".

Este tipo de "plug−ins" que el patógeno recibe por medio del grupo de noticias "alt.comp.virus" presenta un peculiar formato por medio del cual "Hybris" es capaz de distinguir el tipo de actualización y la versión de la misma, para así saber si es necesario descargar el mensaje e instalar el nuevo componente (almacenado en el disco duro con un nombre generado de forma aleatoria) en el sistema.

Hasta el momento se han podido encontrar varios "plug−ins" que, por suerte, todavía no resultan muy peligrosos, si bien es cierto que el "i−worm" en cualquier momento se encuentra en condiciones de modificar su cifrado y el aspecto de los mensajes que envía, con el fin de obligar a las compañías antivirus a también actualizar la información de sus vacunas y descripciones. Por ahora, Vecna, el autor de "Hybris", ha publicado componentes que:

1) Infectan archivos RAR y ZIP, insertando una copia de su código en los mismos, y suplantando a los archivos EXE presentes, en caso de existir.

2) Envían copias del espécimen a máquinas afectadas por el troyano "SubSeven", por medio de la puerta trasera que éste deja abierta.

3) Cifran los archivos adjuntos con un algoritmo polimórfico.

4) Infectan archivos EXE de formato MZ y PE (DOS y Win32).

Por el momento se desconocen datos oficiales por parte del organismo encargado de ofrecer una aproximación de la prevalencia de los virus "en libertad" (`in the wild´), la "WildList", pero el número de usuarios infectados con "Hybris" parece más que significativo, a tenor de la cantidad de e−mails recibidos por laboratorios y por el número de "plug−ins" que están siendo enviados desde hace semanas al grupo de noticias "alt.comp.virus". El mejor consejo ante una alerta como ésta es el de la prevención: cualquier archivo adjunto no solicitado, por fiable que sea el remitente, debería ser automáticamente enviado a la papelera de reciclaje, con lo que se puede evitar de raíz ser afectado por cualquier "i−worm".

Más información:

I−Worm.Hybris

http://www.avp.ch/avpve/worms/email/hybris.stm

Hybris

http://www.f−secure.com/v−descs/hybris.htm

W32.Hybris.gen

http://www.sarc.com/avcenter/venc/data/w32.hybris.gen.html

W32/Hybris.gen@M

http://vil.nai.com/vil/dispVirus.asp?virus_k=98873

W32/Hybris

http://www.pandasoftware.es/enciclopedia/gusano/W32Hybris_1.htm

W32/Hybris−B

http://www.sophos.com/virusinfo/analyses/w32hybrisb.html

TROJ_HYBRIS.C

http://www.antivirus.com/vinfo/virusencyclo/default5.asp?VName=TROJ_HYBRIS.C

El gusano "Sonic", capaz de actualizar su código

Uno de los "i−worms" más destacados de las últimas semanas ha sido, sin lugar a dudas, "Sonic", de probable origen francés. El patógeno forma parte de un reducido pero cada vez más abundante grupo de especimenes de índole vírica capaces de auto actualizar su código por medio de Internet, siguiendo así el camino marcado ya el pasado año por el virus "Babylonia".

Sin embargo, el método empleado por "Sonic" presenta una serie de originales y peligrosas innovaciones con respecto a los virus de características similares conocidos hasta el momento: en lugar de instalar su código principal en el sistema y luego ir añadiendo al mismo pequeños componentes extra o "plug−ins", este gusano ofrece un punto de vista alternativo.

El espécimen, que se reproduce por medio de mensajes de correo electrónico vacíos, con la frase "Choose your poison" (elige tu veneno) como asunto y un archivo adjunto llamado "girls.exe", está compuesto por dos

módulos: un cargador, que es el que viaja en los e−mails que "Sonic" envía, y un portador del código principal, que es el que contiene las rutinas necesarias para la reproducción del patógeno por medio de Internet.

El cargador, de una longitud aproximada de 25 kilobytes, tras haber sido comprimido con UPX, tiene por misión instalarse en el sistema sin levantar las sospechas del usuario, y, posteriormente, descargar de una página Web el módulo portador. Así, una vez ejecutado, el programa procede a mostrar un mensaje de error:

u:\Ubicación\girls.exe n´est pas une application Win32 valide.

Donde "u:\Ubicación" es la especificación correcta del directorio desde el que está siendo ejecutado el cargador. Mientras tanto, el "i−worm" habrá ya procedido a colocar una copia de su código en la carpeta de sistema, bajo el nombre "GDI32.EXE" (que no debe ser en ningún caso confundido con "GDI.EXE" o "GDI32.DLL", archivos legítimos de Windows); tras este paso, "Sonic" pasa a incluir una nueva entrada en el registro de configuraciones, en:

HKLM\Software\Microsoft\Windows\CurrentVersion\Run

El propósito de esta operación consiste en la necesidad del gusano de asegurarse su residencia en memoria después de cada arranque del sistema, ya que su trabajo lo desempeña como un proceso oculto que nunca se llega a cerrar, hasta que la sesión actual de Windows llega a su fin. El motivo no es otro que la monitorización permanente de las conexiones a Internet: el cargador debe buscar en la Red a su media naranja, el portador del código principal de "Sonic".

Para esto, el programa se conecta con un servidor Web, por medio del puerto estándar para este tipo de comunicaciones, el 80, y obtiene un archivo llamado "LASTVERSION.TXT", que contiene un número formado por dos dígitos, empleado para representar la última versión del gusano que se encuentre disponible; en caso de ser más reciente que la ya existente en el sistema, el módulo cargador procederá entonces a descargar otros dos archivos del mismo servidor: "GATEWAY.ZIP", que contiene una versión actualizada del propio cargador, y "xx.ZIP", donde "xx" es el número especificado en "LASTVERSION.TXT", que se corresponde al último módulo portador disponible.

De esta ingeniosa forma, el autor del gusano se puede permitir el lujo de efectuar cualquier cambio en el código de su creación, algo que hasta el momento, a otros especimenes similares, les resultaba imposible, pues eran capaces tan sólo de añadir módulos de código adicionales al "malware" principal. Así, una vez instalado el módulo portador de "Sonic", de unos 40 kilobytes de longitud (también comprimidos con UPX), éste procede a efectuar una autocopia en el directorio de sistema, como "GDI32A.EXE", tras lo cual accede a la libreta de direcciones del usuario infectado y, por medio del cliente de correo electrónico Microsoft Outlook, envía e−mails a cada una de las entradas existentes, independientemente de cuántas sean, a las que adjunta la versión más reciente del módulo cargador.

Más información:

Sonic

http://www.f−secure.com/v−descs/sonic.htm

I−Worm.Sonic

http://www.avp.ch/avpve/worms/email/sonic.stm

W32.Sonic.Worm

http://www.symantec.com/avcenter/venc/data/w32.sonic.worm.html

W32/Sonic.worm

http://vil.nai.com/vil/dispVirus.asp?virus_k=98868

I−Worm/Sonic.B

http://www.pandasoftware.es/enciclopedia/gusano/IWormSonicB_1.htm

W32/Sonic−B

http://www.sophos.com/virusinfo/analyses/w32sonicb.html

TROJ_SONIC.B

http://www.antivirus.com/vinfo/virusencyclo/default5.asp?VName=TROJ_SONIC.B

Hackers y Crackers

Inmersos en una de las revoluciones más dinámicas de la historia, después de la agrícola y la industrial, el proceso de conversión analógico−digital nos está llevando rápidamente a la sistematización global de las organizaciones y la sociedad y a una auténtica era del conocimiento, basada en el uso intensivo de las denominadas infoherramientas.

Y es en este escenario tecno−cultural, donde las figuras del hacker, el craker y el ciberpunk, cobran forma como los nuevos adalides de la contracultura informática.

¿Pero qué es un hacker? ¿Qué lo diferencia de un cracker o de un ciberpunk?

¿Existe ya una cultura del hacker? Son héroes, genios programáticos, piratas informáticos o terroristas digitales o todo lo anterior.

Dónde surge el mito y en dónde comienza la realidad de su influencia, de esos creadores de virus informáticos, desafiadores de sistemas e iconoclastas del sistema imperante en las nuevas fronteras digitales.

Surgidos desde los orígenes de la explosión informática de las últimas dos décadas del fenecido siglo XX, junto con el nacimiento y el auge de los sistemas personales de computo: las ubicuas PCs; los hackers que pueden ser definidos como aquéllos individuos que han tomado como propio el reto de penetrar y alterar los sistemas de información establecidos, para imponer sus normas e intenciones más allá de cualquier restricción o legislación.

Son una expresión ejemplar del sentimiento ambiguo y de la fachada gótica que acompaña a los iconos hostiles a la ciencia cibernética. Estos genios de los números computables, de la electrónica avanzada, se han convertido en personas de moda por sus recientes ataques a las instituciones cibernéticas.

En una acepción muy simple podíamos considerar al hacker como un programador muy hábil, que se impone el reto de abrir programas, desproteger sistemas o entrar a una red restringida como un desafío para ver quién es más listo, el que programó la protección o él. Son profesionales y siguen un código de ética, llegan a la información pero no se dedican a corromperla o venderla, son el grupo más amigable dentro de ésta clasificación.

En el caso del cracker, aparte de imponerse un reto semejante, también se aboca al diseño de virus que pueden dañar un sistema, alterándolo; o bien entrar a un sistema y hacer cambios en él con fines propios como pueden ser la defraudación o simplemente la burla o el terrorismo, cosas totalmente intencionales. El cracker es la versión negativa del hacker.

Los crackers actuarán a través del diseño de virus destructivos, en el sabotaje de sistemas públicos y privados, en delitos informáticos y en actos que atentan contra la seguridad del Estado.

Dentro del grupo de los crackers, los piratas informáticos robarán información para su comercialización ilegal, replicarán software y desencriptarán información para su beneficio económico.

El ciberpunk es una figura más contestataria dentro del punto de vista intelectual o literario, contra la sistematización acelerada de nuestros organismos sociales. Y que se destaca por incorporar a sus argumentos el uso de las tecnología de las redes de computadoras. El caso del ciberpunk es particular, pues al igual que la hiperciencia que le da nombre, forma parte de una literatura híbrida, como sucedió al nuevo periodismo de la década de los 60´s, mitad crónica, mitad ficción. La novela que inaugura éste genero, es la ya clásica Neuromancer, escrita en 1984 por William Gibson.

El termino hacker ha pasado a formar parte de nuestra vida cotidiana en el ciberespacio y existe una tendencia generalizada errónea de asociarlo con un vándalo oscuro que destruye deliberadamente todo aquello que toca y que carece de escrúpulos para utilizar información ajena en su propio provecho, confundiéndolo con el denostado cracker.

Sin embargo aquellos que se consideran auténticos hackers reivindican una causa altruista afirmando que su talento no es utilizado en su beneficio y se definen como románticos e idealistas, cuyo fin último es conseguir que la información circule libremente en la Red.

Según Bruce Sterling autor del libro: `The Hacker Crackdown', los hackers auténticos son entusiastas de las computadoras de mentalidad independiente, pero cumplidores de la ltaria sino sobre cosas complicadas como las computadoras y los sistemas. Se apasionan por lograr que esas máquinas sean instrumentos de lo interesante, siempre y cuando se trate de sus propias ideas y no de una orden de alguien. No les gustan las rutinarias tareas cotidianas que llevan a mantener una existencia normal, si bien son ordenados en sus vidas intelectuales, tienden a ser caóticos en el resto y prefieren un desafío tecnológico a una recompensa monetaria por su labor
Al contrario `el cracking` o `el crackear` se puede definir como las técnicas para desproteger programas, para su uso ilegal sin pagar licencias, el adueñarse de conocimientos, con fines de lucro o con daño intencional a través del uso de virus informáticos.

Así los hackers como verdaderos cerebros o `nerds` son también utilizados por la industria para combatir estos virus y sus creadores, los temibles crackers.

En el caso del hacker existe un código de principios, que busca mantener limpio su nombre y evitar que se tengan problemas con la justicia. A poco de andar los pioneros elaboraron sus reglas, que sin haber colegio de hackers o escuela profesional, y que son las que Steve Levy consigna en su libro `los hackers héroes de la revolución informática` que se ha convertido en un clásico del hacking, destacándose algunos como:

−El acceso a las computadoras o cualquier cosa que te enseñe cómo funciona el mundo debe ser total e ilimitado.

−Apelar siempre el imperativo de manos a la obra.

−Toda información debe ser libre y gratuita.

−Hay que desconfiar de la autoridad y promover la descentralización de la información.

−Los hackers deberán ser juzgados por sus hackeos y no por falsos criterios como títulos, raza o posición.

−En una computadora se puede crear arte y belleza.

−Las computadoras pueden cambiar la vida para mejorar.

El código ético de los hackers especifica cosas como:

−Nunca dañes algo intencionalmente; si no, sólo te buscarás problemas.

−Modificar sólo estrictamente para entrar y evitar ser identificado o para poder acceder otras veces.

−Procura que tus acciones se realizan en servidores lejanos, pues entre más cercanos será más fácil rastrearte.

Los hackers y los crackers y por ende cualquier grupo organizado, siguen una pauta social determinada y un patrón de comportamiento remarcado. Dentro de los subgrupos de hackers, existen determinadas clases virtuales, dependiendo de las experiencias y de los conocimientos adquiridos. Por ejemplo, todos los hackers iniciados tienen que comenzar sus andaduras por el mundo del hackmode modo y forma de vida de los hackers) de la mano de un mentor, que les enseña los primeros pasos, introduciéndolos en las técnicas básicas del hacking, insulflándoles una buena dosis de paranoia y, por supuesto, dejándoles bien claro que sus acciones están siempre en el limite último de la legalidad.

Muchos de los `lammers` o iniciados al hacking, suelen representar un papel, de acuerdo con circunstancias o presiones externas y reales, pero llegan a idealizar un papel referencial (aceptar un papel general con tal de pertenecer a un grupo con unas características determinadas y muy delimitadas).

La sociedad actual está sufriendo un proceso acelerado de cibertización en el cual lo más importante es la información. La tecnología ocupa un papel Central en el desarrollo de una sociedad equilibrada, y éste proceso de crecimiento del sistema hace que se creen nuevas víctimas, en este caso cibervíctimas.

Muchos son los estereotipos asignados al modo de vida de los hackers, incluso se les puede catalogar como una cibercultura desviada o una contracultura informática, pero la realidad va mucho más allá de ésta compleja visión. Desde un punto de vista sociológico, se puede considerar a los hackers dentro del subgrupo de conductas contestatarias, siendo el resultado de cambios sociales profundos, unidos al seguimiento de modas; aunque desde los años 70s han coexistido como un grupo organizado, selecto y unido, tienen su propio manifiesto, y sobre todo disfrutan de una gran consistencia intercambiando todo tipo de información relevante.

A pesar de eso, no se han hecho muchas investigaciones sociológicas acerca de los hackers y su cultura. La perspectiva de una sociedad de clase dual, en la que la población es separada en los ricos−informados y los mal−informados en las nuevas fronteras e infofeudos digitales es ya una realidad en la ` sociedad de la información ` de este milenio, lo que verdaderamente se califica ya como un serio problema social.

La comunidad de hackers, y el importante papel que esta subcultura juega en la nueva sociedad debe ser estudiado con igual atención. Buscan hacer así realidad una de las promesas más importantes para el mundo del futuro, que ya estamos viviendo intensamente hoy: que cualquier persona tenga acceso a la Red, desde cualquier lugar, con cualquier dispositivo, en cualquier momento, lema que han hecho suyo, corporativos como el de Sun Microsystems y los pugnadores por los sistemas abiertos, como Linus Torvald, creador de

Linux.

Como ocurre con cualquier subcultura revolucionaria, el movimiento hacker es estigmatizado, desacreditado y perseguido por los medios de comunicación y la cultura corporativa como juvenil, trastornadora y criminal, y todo el tiempo es generalmente malinterpretada.

Así los hackers son rebeldes con causa y se perfilan ya como los nuevos guerrilleros contra el establishment informático: el Gran Hermano Digital y sus ambiciones de control de la información en beneficio de una minoría privilegiada. Como una verdadera manifestación del sistema inmunológico del nuevo organismo social digital, los hackers son los anticuerpos que preservan su salud contra las amenazas totalitarias.

La guerra por la libertad informática ha comenzado y el brazo militar de los hackers está actuando, como una reacción a la persecución indiscriminada que ya se ha desatado contra ellos a nivel mundial.

Pero sin duda, el más famoso hacker conocido como el chacal de la Red es Kevin Mitnick. Este sencillo nombre, oculta la verdadera identidad de uno de los mayores hackers de la historia. Como un Mozart cibernético, a los 3 años podía reconocer los diferentes tonos de infinidad de números telefónicos. Conocido también por todos como ` El Cóndor ` fue una de las mayores pesadillas del Departamento de Justicia de EU.

Con sólo un ordenador portátil y un teléfono celular alterado, burló por más de dos años al FBI, creó números telefónicos imposibles, entró virtualmente a una base de misiles y llegó a falsificar 20,000 números de tarjetas de crédito. El final de este ` hacker−cracker−phone −breaker`, sobrevino cuando su `curiosidad` le llevó a la computadora del físico computista, Tsutomu Shimomura, experto en sistemas de seguridad, que se encargó de seguirlo virtualmente hasta entregarlo a las autoridades federales que lo condujeron a una fría celda, con numerosos juicios pendientes, éste personaje ha sido leyenda y élite para sus seguidores.

Cuando estábamos al cierre de este reportaje nos llegan noticias de intervenciones de los crackers a la Bolsa de Valores de Nueva York, ataques a E−Bay, Amazon, Yahoo y a la central de noticias CNN y la Casa Blanca anuncia una reunión de emergencia con el presidente Clinton, el Consejero de Seguridad Nacional, La Procuradora de Justicia y ejecutivos de las principales compañías de Internet, para tomar medidas de emergencia contra los ataques cibernéticos y la inversión de miles de millones de dólares para combatirlos... por lo que creo que ésta historia continuará.