RIESGOS DEL COMERCIO ELECTRÓNICO. RESPUESTA DE LA GERENCIA DE RIESGOS.

AGERS 2.000

D. Manuel Carpio
Gerente de Seguridad Lógica de
TELEFÓNICA DE ESPAÑA

¿Es posible la gestión de e-Riesgos?

Resumen

Existen desde hace tiempo soluciones tecnológicas capaces de hacer viable un comercio electrónico seguro a través de una red abierta como Internet. Sin embargo las administraciones públicas y muchas empresas presentan aún inercias respectivamente en el desarrollo del marco legislativo y en la adopción de un claro compromiso inversor en seguridad. La seguridad total nunca será posible, de manera que el riesgo residual deberá ser transferido.

La seguridad en Internet... o de cómo convertir la amenaza en oportunidad

La red Internet ya se ha convertido en el sistema nervioso de laTierra, permitiendo comunicación casi instantánea entre todos sus usuarios, acceso a prácticamente todo conocimiento existente, y la implementación de aplicaciones que prometen revolucionar muchos de los quehaceres humanos, incluyendo la educación, los medios de comunicación, los servicios bancarios, la compra-venta de productos y servicios, las telecomunicaciones, la publicación de obras originales, la publicidad comercial, etc. Virtualmente en todas esas aplicaciones, la seguridad representa un parámetro central para su diseño y efectividad. Sin embargo, el crecimiento explosivo y desordenado de Internet, la oferta de múltiples soluciones y "estándares" para la seguridad, y el hecho de que la mayoría de los países avanzados en este campo prohiben la exportación de fuerte
encriptación, han generado un ambiente de confusión en el usuario final y en los gerentes que toman decisiones sobre cómo integrar Internet en su negocio u organización.

Afirmar que "Internet es una red insegura" tiene tanto sentido como decir que el idioma español es inseguro. Internet es un medio de comunicación, y como tal su grado de seguridad dependerá de la voluntad y la capacidad inversora de quien lo quiera utilizar para sus transacciones. Lo que puede ser seguro o inseguro es la manera de implementar comunicaciones en este medio. Por un lado, el aspecto global de Internet y el hecho de que los paquetes IP se transportan de una manera autónoma hace que datos enviados por Internet se pueden interceptar por personas no autorizadas. Es cierto entonces que los datos enviados por Internet no están seguros. Lo mismo, en mayor o menor grado, es cierto sobre toda comunicación a larga distancia, sea

por teléfono, correo postal, telegrama o radio. Por otro lado, el hecho de que Internet es una red de ordenadores donde todos los datos se representan como datos digitales permite lograr un grado muy alto de seguridad que no es posible o muy difícil lograr con otros medios.

La evolución de las nuevas tecnologías, en especial el tremendo auge de las tecnologías Internet/Intranet, ha provocado la aparición de nuevas necesidades y la posibilidad de adquirir ventajas competitivas. Además hay que aclarar que lo que inicialmente partió como una opción de negocio se está transformando en una elección obligada si se desea mantener la posición en el mercado frente a los competidores; así, hasta los más reacios han debido claudicar ante la evidencia aplastante.

Los beneficios atribuibles a las nuevas tecnologías son muchos, pero también los riesgos: La pérdida de imagen (a menudo más crítica que la propia perdida de datos), la perdida de información, la suplantación de usuarios, el espionaje de información sensible o incluso el cumplimiento de la normativa vigente..

A pesar de lo cambiante del entorno, los requisitos de seguridad siguen siendo los mismos: Autenticación, confidencialidad, control de acceso, integridad y no repudio; aunque los objetivos y la implementación de los mismos evoluciona a velocidad vertiginosa.

La problemática de la Seguridad

A lo largo de los últimos años los problemas de seguridad que se vienen observando en las empresas y organismos han sido una constante recurrente; se pueden diferenciar en tres grandes grupos:

Los problemas estructurales

Habitualmente la estructura de la organización no se hace pensando en la seguridad por lo que no hay una definición formal de las funciones ni responsabilidades relativas a seguridad.

No suelen existir canales de comunicación adecuados para tratar incidentes de seguridad, predominando los canales de tipo informal y el boca a boca.

Exceptuando determinados ambientes como la banca o la defensa, no suelen existir recursos específicos dedicados a seguridad, y cuando existen suelen dedicarse a la seguridad física (puertas,

alarmas, dispositivos antincendios, etc.) por ser más fácilmente justificable su adquisición.

Problemas en el planteamiento

Los planteamientos de seguridad suelen adolecer de falta de coherencia ya que no suelen ser ni suelen están adaptados a las necesidades de la empresa.

Habitualmente las directrices no son homogéneas en toda la organización.

Como consecuencia de la falta de definición de funciones, nadie quiere responsabilizarse de los riesgos asumidos en la organización y nadie quiere adoptar medidas que puedan dificultar el proceso de negocio. El confusionismo operativo causa más estragos que legiones de hackers.

No se definen normas ni procedimientos salvo cuando su ausencia puede afectar al propio negocio (por ejemplo la existencia de copias de seguridad) o tras un incidente grave de seguridad. Buena parte de las medidas de seguridad actualmente implantadas, lo han sido como consecuencia de inconfesables incidentes: seguridad "a posteriori".

Al no existir beneficios inmediatos, resulta difícil justificar gastos y recursos.

El problema tecnológico

Quizá la tragedia a la que asistimos pueda compararse a la angustia de encontrarse en mitad de un incendio y no poder sofocarlo porque no sabemos usar el extintor que tenemos a nuestro alcance.

Existe tecnología suficiente. La más importante, la criptografía, se conoce y se usa desde épocas tan antiguas como el imperio romano (cifrado César). El sector de productos y servicios de seguridad crece y se fortalece a golpe de portada de periódico. A veces resulta difícil decidir qué producto elegir, de entre una importante oferta, para una determinada funcionalidad de seguridad (la actual batalla de las PKIs adquiere tintes dramáticos).

Pero la tecnología por sí sola no es la panacea: Las herramientas son un soporte, pero si no hay una base con ideas sólidas no solucionan los problemas.

Además, las herramientas existentes, de por sí, no cubren todas las necesidades. Una máxima que circula por internet: "un tonto con una herramienta, sigue siendo un tonto...pero peligroso". Uno de los principales problemas a que nos enfrentamos, no sólo en el sector de la seguridad, es la falta de personal "realmente" cualificado.

La sensación de falsa seguridad provocada por la excesiva confianza en las soluciones tecnológicas induce a bajar la guardia.

Resumiendo, la situación real suele ser que en las empresas y organismos el negocio y la imagen se anteponen a la seguridad. La organización crece e implementa soluciones de seguridad de acuerdo a necesidades puntuales, no hay definida una estrategia, ni normas ni procedimientos, es decir, lo habitual es que no se contemple expresamente la seguridad.

El problema principal que se desprende de todo lo anterior es que normalmente no se conoce el riesgo que se está asumiendo, ni se sabe cómo medirlo.

Planificando la Seguridad

Una vez identificados los problemas generales llega la pregunta que supone el principal escollo para desarrollar un plan que corrija la situación: ¿cómo se debe abordar la seguridad en la organización?

El Plan de Seguridad debe ser un proyecto que desarrolle los objetivos de seguridad a largo plazo de la organización, siguiendo el ciclo de vida completo desde la definición hasta la implementación y revisión.

La forma adecuada para plantear la planificación de la seguridad en una organización debe partir siempre de la definición de una política de seguridad que defina el QUÉ se quiere hacer en materia de seguridad en la organización para a partir de ella decidir mediante un adecuado plan de implantación (fruto de un Análisis de Riesgos previo) el CÓMO se alcanzarán en la practica los objetivos fijados.

La Política de Seguridad englobará pues los objetivos, conductas, normas y métodos de actuación y distribución de responsabilidades y actuará como documento de requisitos para la implementación de los mecanismos de seguridad. La política debe contemplar al menos la definición de funciones de seguridad, la realización de análisis de riesgos por cada sistema que soporta los procesos fundamentales del negocio, la definición de normativa y procedimientos, la definición de

planes de contingencia ante desastres y la definición del plan de auditoría.

A partir del Análisis de Riesgos se podrá definir el Plan de Implementación, que es muy dependiente de las decisiones tomadas durante la fase de Gestión de Riesgos, en el que se contemplará: el estudio de soluciones, la selección de herramientas, la asignación de recursos y el estudio de viabilidad.

Hay dos cuestiones fundamentales que deberán tenerse en cuenta para implantar con éxito una política de seguridad: Es necesario que la política sea aprobada para que este respaldada por la autoridad necesaria que asegure su cumplimiento y la asignación de recursos; y es necesario que se realicen revisiones periódicas que la mantengan siempre actualizada y acorde con la situación real del entorno.

Política de Seguridad, Plan de Seguridad, Análisis y Gestión de Riesgos y la implantación propiamente dicha están íntimamente relacionados ya que la implementación debe ser un fiel reflejo de los procedimientos y normas establecidos en la Política y Plan de Seguridad.

El Plan de Seguridad, exigencia legal recogida en el RD 994/1999 de 11 de Junio, para todos aquellos ficheros que contengan datos de carácter personal, debe estar revisado para adaptarse a las nuevas necesidades del entorno, los servicios que vayan apareciendo y a las aportaciones que usuarios, administradores, etc. Vayan proponiendo en función de su experiencia. La revisión es esencial para evitar la obsolescencia de la política debido al propio crecimiento y evolución de la organización. Los plazos de revisión deben estar fijados y permitir además revisiones extraordinarias en función de determinados eventos (por ejemplo, incidentes).

La implementación debe ser auditado para asegurar la adecuación con las normas. Y debe realimentar a la Política de Seguridad. La experiencia, los problemas de implantación, las limitaciones y los avances tecnológicos, etc. permitirán que la política pueda adecuarse a la realidad, evitando la inoperancia por ser demasiado utópica y la mejora cuando el progreso lo permita.

Un enfoque como el propuesto asegurará la adecuación del nivel de seguridad implantado con las necesidades de la organización y el correcto seguimiento y control de los riesgos.

Criptografía, el brazo armado de la seguridad en internet.

La tecnología utilizada para mantener confidencialidad de datos y comunicaciones se llama criptología. Se trata aquí de operaciones matemáticas complejas, las cuales se aplican a los datos cuya confidencialidad se desea mantener. Criptología tiene dos componentes: Criptografía se refiere a las técnicas para convertir datos a una forma ilegible excepto por las personas autorizadas.

Criptanálisis se refiere a las técnicas que analizan los métodos de encriptación con el objetivo de encontrar una debilidad. Esos dos campos son íntimamente relacionados: un avance en las técnicas de criptanálisis motiva un avance en la criptografía y viceversa. Un método de criptanálisis efectivo se llama un ataque. Mucho del diseño de un sistema de seguridad se hace para defenderse contra uno u otro ataque conocido. Una problemática muy particular aquí se refiere a la posibilidad de que los sistemas de seguridad diseñados hoy tendrán que resistir ataques no conocidos todavía, puesto que se descubrirán en el futuro.

La criptografía contemporánea comienza con el ya mítico artículo publicado por Diffie y Hellmann en 1977, donde se establecen las bases de la criptografía de clave pública. Desde principios de la década de los '90, el IETF y otras organizaciones públicas y privadas han desarrollado una intensa labor de estandarización que ha dado como resultado la aparición, alrededor de 1995 de productos comerciales que implementan el concepto de Infraestructuras de Clave Pública (PKI).

Una Infraestructura de Clave Pública es el conjunto de elementos Hardware y Software cuya misión es garantizar la implantación y la gestión de un entorno seguro para la identificación y autenticación de usuarios, basándose en el uso de Certificados Digitales y la generación para cada usuario de una pareja de claves, Publica y Secreta/Privada. La misión principal de una PKI es gestionar el ciclo de vida de los certificados digitales y de las claves asociadas.

Cada usuario dispone de un Certificado Digital, que contiene sus datos identificativos, y una pareja de claves relacionadas biunívocamente a través de un algoritmo matemático (RSA). La clave privada debe guardarla el usuario en algún soporte que puede ser, por ejemplo un PC o una tarjeta inteligente, según las necesidades propias de cada proyecto. La clave publica debe ser "publicada" para que sea conocida por el resto de los usuarios o aplicaciones con los que el usuario puede mantener una relación en la cuál es necesario garantizar la identidad.

Una PKI consta, básicamente de los siguientes elementos: Autoridad de Registro (RA), Autoridad de Certificación (CA), y un Servicio de Directorio para publicar los certificados y las claves públicas, aunque

este último elemento suele ser independiente de la RA y CA, al menos comercialmente. También debe considerarse un elemento de esta infraestructura un Help Desk que atienda las incidencias.

Las principales funciones de una Autoridad de Registro (RA) son típicamente:

- Gestión de altas
- Generación de Claves, Publica y Secreta
- Almacenamiento en soporte personalizado de la Clave secreta
- Emisión de Certificados Digitales
- Almacenamiento en el Directorio del Certificado con su clave publica.
- Entrega personalizada del certificado al usuario.

El sistema de la RA debe estar aislado, sin comunicaciones exteriores y con vigilancia física. En buena medida la seguridad global del sistema depende de la seguridad de la RA.

Las principales funciones de una Autoridad de Certificación (CA) son típicamente:

- Firmar, con la clave secreta de la CA los Certificados emitidos por la RA.
- Gestión de los Certificados durante su vigencia.
- Comprobación de la lista de Certificados Revocados.
- Revocación de Certificados por caducidad, robo, pérdida, deterioro.

Estas infraestructuras son estratégicas, hoy en día, para cualquier negocio o proyecto basado en Internet, Intranet y Redes Privadas Virtuales, en definitiva para cualquier entorno de e-business. Por lo tanto, todas las grandes corporaciones, hoy en día están en proceso de evaluación e implantación de estas infraestructuras, con la complejidad que ello implica, no sólo desde el punto de vista técnico, sino sobretodo desde un punto de vista estratégico y de negocio, al afectar a todas las áreas de una compañía, incluso siendo válidas para dar servicio a un grupo de empresas.

La aplicación más popular hoy en día es la posibilidad de realizar la declaración del IRPF vía Internet. La Agencia Tributaria utiliza una PKI implantada por la Fabrica Nacional de Moneda y Timbre.

Retos de seguridad en el comercio electrónico.

El dinero electrónico

Durante los últimos años, la informatización de los bancos ha permitido que la mayor parte del dinero que circula por el mundo lo haga en forma de silenciosos bits, ristras de unos y ceros que viajan a través de líneas telefónicas o enlaces de satélite en lugar de hacerlo físicamente en forma de monedas y billetes.

Con el advenimiento de las tarjetas de plástico con banda magnética, fue posible que los usuarios accedieran a través de los cajeros automáticos a su dinero almacenado electrónicamente en el banco. Más aún, los cheques, las tarjetas de crédito y las de débito, permiten hoy en día realizar prácticamente cualquier tipo de pago en casi cualquier comercio y lugar del mundo. A medida que su uso se extendió y se venció la reluctancia inicial de los ciudadanos, fueron adoptados como medio de pago común en Internet y en situaciones en que las partes no se encontraban físicamente en contacto. Se utilizaron protocolos de comunicaciones ya existentes para salir del paso, como SSL, o se desarrollaron otros con el comercio electrónico en mente, como SET o CyberCash. Sin embargo, a pesar de su gran versatilidad y utilidad, el pago mediante tarjeta presenta el problema del elevado coste de una transacción, volviéndolas por tanto inadecuadas para compras de escaso valor.

Recientemente, están apareciendo en este escenario el dinero electrónico y las tarjetas monedero, con la posibilidad de abaratar los costes por transacción, haciendo posible el comercio de mercancías de escaso valor, tanto a través de Internet como en comercios en la calle. Tecnologías de dinero digital como eCash o MilliCent, permiten mover monedas electrónicas de un ordenador a otro, mientras que con el uso de tarjetas monedero o servicios como Virtu@lCash, se transfiere dinero de una cuenta a otra, incluso por importes muy pequeños.

A medida que las tarjetas monedero se popularicen, más y más bienes y servicios podrán ser pagados con ellas. Con el tiempo, y en la medida en que se acerquen a las prestaciones del dinero común en cuanto a facilidad de uso, rapidez, aceptación en comercios, anonimato y conveniencia, monedas y billetes tenderán a desaparecer en el futuro. El dinero digital debe poseer toda una serie de características presentes en las tradicionales monedas y billetes para que se convierta en medio de pago universal desplazando a estos últimos: seguridad, fiabilidad, escalabilidad, anonimato, aceptación, base de clientes, flexibilidad, eficacia, facilidad de integración con otras aplicaciones software y facilidad de uso.

Asumiendo la máxima de que "la economía es el motor del mundo", no es de extrañar que exista una gran variedad de protocolos ya en

funcionamiento, otros en pruebas y aún más en fase de diseño. En estos momentos nos encontramos en la excitante era del descubrimiento. Dentro de algunos años habrán sobrevivido los sistemas mejor adaptados a las necesidades del mundo real.

Cyberpunks

Inmediatamente conviene hacer la distinción entre el auténtico hacker, en su sentido original, que sabe programar en ensamblador y C, conoce los entresijos de Linux y Windows y sabe todo lo que se puede saber sobre protocolos TCP/IP, UDP e ICMP; y el conocido como "lamer", que tiene algunos conocimientos muy limitados de programación y mucho tiempo libre y aprovecha las vulnerabilidades descubiertas por los primeros en sistemas informáticos y los programas escritos por los primeros para explotar estos agujeros. Ser un auténtico hacker constituye un largo y arduo proceso de autoaprendizaje, mientras que para convertirse en "lamer" basta con frecuentar los conocidos sitios underground donde pueden obtenerse gratuitamente poderosas herramientas creadas por los verdaderos hackers.

En estas páginas de hackers, rara vez escritas por uno genuino, se ofrecen herramientas gratuitas de inusitada versatilidad y potencia, como las sofisticadas Nmap (www.nmap.org), Nessus (www.nessus.org) o Cheops (www.marko.net/cheops) para escaneo de puertos y detección de vulnerabilidades. El siguiente paso, una vez detectado con estos programas un buen agujero, consiste en intentar correr algún código que lo explote, códigos que normalmente se pueden encontrar en las mismas páginas de hacking (como por ejemplo www.anticode.com); o descargar un programa de ataque que ejecute un DoS (Denegación de Servicio) sobre la máquina objetivo para tirarla abajo; o probar con las instrucciones que se han encontrado en alguna buena página sobre cómo hacerse con privilegios de root explotando algún oscuro fallo de configuración en un servicio. Estos programas poseen un interfaz de usuario a veces sorprendentemente amigable y se encuentran a menudo incluso precompilados, por lo que el "lamer" ni siquiera necesita saber cómo compilarlos, no tiene más que ejecutarlos. Habida cuenta de la facilidad con que se obtienen, instalan y ejecutan estas herramientas, y dada la cantidad de información detallada acerca de agujeros, vulnerabilidades y caminos para explotarlas, resulta que prácticamente cualquiera con un ordenador y una conexión a Internet puede atacar con éxito una extraordinaria cantidad de sistemas en línea.

Estos ataques tienen éxito debido a que muchas redes funcionan ejecutando versiones antiguas de programas con vulnerabilidades conocidas y fácilmente explotables; configuraciones por defecto que

dejan abiertas enormes puertas de entrada; contraseñas de fábrica que nadie se molesta en cambiar y que son de todos conocidas; servicios innecesarios que descubren multitud de puertos; y otras triquiñuelas que se describen con profusión de detalles en sitios underground. A la vista de la facilidad con que un niño puede convertirse en un hacker peligroso en unas pocas horas, no estaría de más que los administradores de sistemas y personal encargado de la seguridad informática se diesen una vuelta por las citadas páginas y utilicen las mismas armas que los "lamers" para escanear sus redes, aprender acerca de los últimos exploits y tomar las medidas oportunas. Puede tratarse de una interesante y aleccionadora experiencia para más de uno, que siempre surtirá resultados positivos. Hoy en día, ser hacker resulta más sencillo que nunca. Dejar de ser una víctima fácil, también.

En algunos IRCs pueden leerse cosas como ésta:

"Yo no he pillado root ni he creado una cuenta, lo que pasa que desde esa shell de América, encontré el bouncer y para que no pillaran el host de la shell, porque era gratuito dos semanas y daban unos servicios que te cagas, que después iban a ser de pago, utilicé el bouncer ese que encontré".

Y en e-zines como la de los autobautizados "saqueadores", tras la descripción pormenorizada del ataque a los sistemas informáticos de una universidad y un e-banco, explotando vulnerabilidades de servidores Domino:

"CONCLUSIONES

¿Qué sería un estudio sin conclusiones?. La conclusión obvia es: 2 de 2.

Es disculpable que una universidad se deja la cartera encima de la mesa, no deberia ser la norma pero tampoco importa mucho. En cuanto al banco claramente se han preocupado algo mas por la seguridad pero como hemos visto no lo suficiente.

*No hagáis evaluaciones apresuradas, el problema no es que se pueda obtener esta información, el problema es **como** se obtiene. Con un navegador. Se podría disculpar si fuese necesario ser un 'gurú' de Domino para llegar a esto, lamentablemente a mi me basto dos días de leer guias para comenzar a encontrar huecos y sin ni siquiera usar o instalar Domino/Notes.*

No hace falta decir que algo falla, quizá todos estos programas son demasiados complejos para asegurarlos o puede que nadie este interesado en hacerlo.

Al final fueron necesarios cinco días de aprendizaje y un navegador, los administradores internos, la empresa de seguridad que (supongo) auditó el site y todos aquellos cuyo trabajo era prever este tipo de incidentes no debían disponer de tanto tiempo. O quizá no tienen ningún navegador.

Da que pensar.

Y recordad, hagáis lo que hágais.
Tened cuidado ahí fuera.

Paseante"

La mayoría de los ataques con éxito a ordenadores mediante Internet se pueden agrupar como la utilización de un reducido número de vulnerabilidades. La mayor parte de los ordenadores comprometidos durante el incidente conocido como "Solar Sunrise Pentagon" fueron atacados mediante una vulnerabilidad concreta. Una vulnerabilidad similar a esa fue la que se utilizó para controlar la mayor parte de los ordenadores que posteriormente se utilizaron masivamente en los ataques distribuidos de negación de servicio. De la misma forma, los recientes accesos ilegales a servidores web basados en Windows NT están asociados a la utilización de una vulnerabilidad sobradamente conocida. Otra vulnerabilidad, todavía, suficientemente estudiada para ser la causa de permitir el control ilegal de más de 30.000 sistemas Linux.

Con sólo algunas vulnerabilidades, en definitiva, se realizan la mayor parte de los ataques con éxito debido, en gran parte a que los atacantes son oportunistas – utilizan la vía más fácil y conveniente. Utilizan las brechas mejor conocidas mediante el uso de diversas herramientas de ataques muy efectivas y ampliamente difundidas. Se aprovechan de aquellas organizaciones que no aplican los parches para resolver los problemas, realizando habitualmente ataques de forma indiscriminada, rastreando en Internet por la existencia de sistemas vulnerables.

La mayor parte de los administradores de sistemas afirman que no han solucionado estas brechas de seguridad por la simple razón que desconocen cuales de los 500 problemas potenciales son los más peligrosos y carecen del tiempo necesario para poder corregirlos todos.

La comunidad de profesionales de la seguridad informática desea resolver este problema identificando las áreas de seguridad en Internet más críticas – el grupo de vulnerabilidades que los administradores de sistemas deben eliminar de forma inmediata. Esta lista consensuada, a

la que denominaremos Top Ten, es un ejemplo sin precedentes de cooperación activa entre la industria, los organismos públicos y las instituciones educativas. Los participantes provienen de las agencias federales con mayor conciencia en temas de seguridad, de los principales distribuidores de productos de seguridad, de consultoras especializadas; de diversas universidades con programas especializados en seguridad y del CERT/CC y el SANS Institute. Al final del articulo incluimos la relación completa de participantes.

Esta es la lista de los 10 problemas de seguridad en Internet más frecuentemente utilizados, con la relación de acciones que deben tomarse para proteger los sistemas de las mismas.

1. Debilidades de BIND: nxt, qinv e in.named permiten comprometer la cuenta de root inmediatamente.

2. Programas CGI y extensiones de aplicación (por ejemplo, ColdFusion) instalados en servidores web.

3. Debilidades en llamadas de procedimiento remoto (RPC) en rpc.ttdbserverd (ToolTalk), rpc.cmsd (Calendar Manager) y rpc.statd que permiten la obtención inmediata de privilegio de root.

4. Agujero de seguridad RDS en Microsoft Internet Information Server (IIS).

5. Debilidad por desbordamiento de buffer en sendmail; ataques mediante áreas de interconexión de memoria y MIMEbo; todas ellas permiten comprometer la cuenta de root inmediatamente.

6. sadmind y mountd.

7. Compartición de archivos global y compartición de información inapropiada mediante NetBIOS y los puertos 135 -> 139 en Windows NT (445 en Windows 2000), exports de NFS en Unix (puerto 2049), compartición vía web en Macintosh y Appleshare/IP en puertos 80, 427 y 548.

8. Cuentas de usuario, especialmente la de root o administrador, sin contraseña o con contraseña poco segura.

9. Vulnerabilidades de desbordamiento de buffer o configuración incorrecta en IMAP y POP3.

10. Nombres de comunidad SNMP por omisión ('public' y 'private').

Los medios de pago

El 23 de marzo, fueron arrestados por la policía británica dos personas, (la prensa británica los califica como "hackers", ambos de 18 años de edad, y ambos galeses) por la entrada ilegal en 9 webs de e-commerce, de cinco países diferentes, (Inglaterra,USA, Canadá, Tailandia, y Japón) apropiándose de la información de 26.000 tarjetas de crédito.

Se les acusa de violar la "Computer Misuse Act" de Reino Unido de 1990. Las webs afectadas han comunicado que los adolescentes habían usado un agujero en la seguridad de SQL Server de Microsoft, aunque en la web de feelgoodfalls.com, se entró a través del agujero del programa Microsoft Storefront. Según algunos de los afectados, también habría que achacar el resultado final a la mala organización de las propias empresas, la mayoría de ellas pequeñas empresas.

Según el FBI comenzaron a actuar en Enero, y usaban el nombre de "curador" en sus ataques, que no sólo quedaban en eso, sino que después publicaban los números de las tarjetas en las webs: e-crackerce.com y free-creditcard.com, así como en la página personal de xoom.com. Esta última fue cerrada en febrero, y actualmente lo están también las otras dos. En ellas había mensajes como "Gracias a mi amigo Bill Gates, alguien que vende productos como SQL Server, no puede ser tan malo".

Según el FBI el incremento de este tipo de incidentes empieza a ser alarmante, si bien es cierto que la suplantación de personalidad o el "robo de identidad" no es nada inventado en este siglo, si es cierto que la seguridad en las transacciones es una de las asignaturas pendientes de Internet.

Según las autoridades americanas, se han publicado las estadísticas correspondientes a 1999, y tan sólo en la "Social Security Administration" (es decir, el organismo que rige la Seguridad Social norteamericana) se han recibido mas de 30.000 quejas sobre mal uso de los números de las tarjetas de seguridad social, la mayoría sobre "robo de identidad", o suplantación de personalidad. Y ello frente a las 11.000 de 1998, o las 7.868 de 1997. Es decir, aumentó casi el triple el número de incidencias en un año.

El número de la Seguridad Social en Estados Unidos se usa como el número de carnet de identidad en otros países, así pues basta tener el número de la tarjeta de crédito y el número de la Seguridad Social de la persona para "poder hacer compras on-line" en la mayoría de los casos. Es más, hay empresas que por 49 dólares ofrecen ese número a quien lo solicite, o empresas, como Net Detective 2000, que se promociona con

anuncios como "la increíble herramienta que te permite saber TODO lo que querías sobre tus amigos, familia, vecinos, empleados o tu jefe". Y son legales.

El Instituto para la Seguridad Informática (Computer Security Institute) ha publicado su encuesta "delito informático y seguridad 2000", basándose en la respuesta de 643 directivos de empresas, gobierno, instituciones financieras, hospitales y Universidades. El FBI ayudó en la encuesta, y muestra que 273 encuestados declaran perdidas económicas, robo de información y fraude financiero. El 90 por ciento declaran haber tenido problemas de seguridad, el 71 por ciento en relación con accesos no autorizados

En ocasiones, el hacker no necesita desarrollar especiales dotes y maestría para perpetrar sus ataques, sino que se limita a explotar el descuido, el desconocimiento o las prisas de un presionado administrador del sistema.

Cuando se decide emplear un software comercial para montar un comercio electrónico, una tienda en Internet, hay que leer muy bien todas las instrucciones de instalación y proceder a una instalación cuidadosa, y prestar atención a las partes más importantes del programa. Incluso en ocasiones hay que llegar más allá de la propia documentación y comprobar personalmente todos los elementos que conforman el comercio, como si de una tienda real se tratara y pusiéramos lejos del alcance de los clientes la caja registradora. La base de datos de productos, de usuarios y de pedidos son datos fundamentales que deben estar
cuidadosamente protegidos

Por otro lado la "industria" de las tarjetas de crédito rechaza esta visión pesimista y afirma que si bien el fraude existe, no es más que un pequeño porcentaje de los cientos de billones de dólares que las compras con tarjeta de crédito mueven cada año. Sin embargo, el pasado 3 de Noviembre, Visa Internacional ha reconocido estar preparando un plan de choque contra las tiendas virtuales clientes que no garanticen unas mínimas medidas de seguridad para las transacciones electrónicas.

Dispuesta a disipar los miedos del usuario hacia el comercio on-line, VISA ha anunciado un plan mediante el que se cumplimentará por la razón y por la fuerza lo que los cyberpunks no han logrado mediante sus continuas incursiones en webs comerciales: proteger los números de tarjeta y datos de sus clientes.

Bajo este plan, el gigante de medios de pago californiano comenzará a monitorizar los miles de negocios on-line que aceptan transacciones con

tarjeta Visa para garantizar el cumplimiento de la normativa de seguridad de la compañía. Esta normativa recomienda el uso de cortafuegos, criptografía y la actualización contínua del software de base añadiendo los necesarios parches de seguridad. Habrá sanciones económicas para aquellos negocios que no cumplan los estándares.

Supongamos que un supuesto cracker ha conseguido un número blanco de tarjeta de crédito, en alguno de los webs mencionados arriba. Veamos con un ejemplo cómo podría explotarlo, según un reciente artículo en un popular informativo on-line:

1. Un usuario (la víctima) entra en un sitio de mercadillo o subastas "online", donde puede observar una auténtica ganga por un precio muy inferior al del mercado, con manuales, embalajes originales, etc.

2. El usuario se muestra interesado por semejante oferta y se pone en contacto con el propietario.

3. El propietario (nuestro supuesto cracker) le dé todas las facilidades del mundo. Incluso se ofrece a enviar la mercancía al domicilio del incauto cliente, sin una señal monetaria previa. Sí lo exige un compromiso de devolución del producto, si no se está satisfecho, o la transferencia de la cantidad acordada si la mercancía le satisface.

4. Dado semejante "chollo", el cliente no duda en proporcionar su dirección postal, nombre, etc.

5. Con esa información, el "pretendido" propietario de la mercancía realiza una compra on-line del producto en cuestión, naturalmente a precios de mercado. Para ello emplea una tarjeta de crédito robada. Como dirección de envío, pone los datos del usuario inicial.

6. Tras unos días, el usuario recibe la mercancía en su casa y, con casi total seguridad, realizará la transferencia bancaria.

La historia termina con que al propietario de la tarjeta de crédito se le efectúa al cargo, el usuario final tendrá en su propiedad mercancía robada y el verdadero criminal recibirá un jugoso ingreso en una cuenta de difícil seguimiento, típicamente en el extranjero.

La seguridad total no existe. Es un mito. Siempre existirá un riesgo residual que necesita ser transferido. La verdad es que es muy difícil, incluso para las páginas con las defensas más fuertes, asegurar que sus páginas Web no serán hackeadas, aunque siempre pueden asegurar una parte de sus pérdidas causadas por estas intrusiones. Tampoco debemos olvidarnos del "factor humano", o como diría Donn B. Parker, padre de

los ciberpolicías norteamericanos del Standford Research Institute: "Insiders take billions".

Con todo esto, no es de extrañar que algunas compañías de seguros, que muchas veces se han considerado con poco atractivo para internet, están siendo más usadas como consecuencia de los últimos ataques malintencionados sufridos por algunas páginas famosas. omo el portal Yahoo!, donde ya están asegurados por si se quedan sin servicio a causa de un fallo eléctrico o un terremoto. Pero las compañías de seguros aún balbucean y dudan ante un eventual desembarco en este nuevo negocio.

Problemas de procedimientos

La entrega de pedidos es el punto débil del e-commerce en Europa Según un estudio realizado por Andersen Consulting mediante 445 compras efectuadas en 162 webs de Alemania, España, Francia, Italia, Reino Unido y Suecia, existen serios problemas en la entrega de los pedidos, ya que, en muchos casos, es necesario esperar varias semanas antes de recibir lo comprado, o incluso no recibirlo nunca.

El 39% de las compras on-line no pudieron concluirse por cuestiones técnicas o de procedimiento. El 57% de los pedidos realizados se entregaron en un plazo de siete días, y el 60% de los pedidos internacionales han tardado más de una semana.

En los casos en que no se ha proporcionado una fecha de entrega, el 59% de las veces no se entregó el pedido.

La democratización del e-business: PSAs

PSA representa la tendencia más novedosa en modelos de negocio basados en Internet. Se fundamenta en ofrecer una solución de red integrada y total, que incluya software, hardware, cableado, mantenimiento, soporte, conectividad a Internet con acceso fijo y/o móvil (WAP), actualización constante tanto de los programas como del hardware y otros servicios igualmente interesante. Básicamente, se trata de servir en alquiler software especialmente caro, personal cualificado, servidores y canales de acceso de gran capacidad, de manera que la empresa que contrata al PSA se evite esas inversiones iniciales, que de entrada pueden resultar prohibitivas. La idea consiste pues en alquilar en vez de comprar, externalizar en vez de afrontar grandes gastos.

Desplegar una sofisticada aplicación de comercio electrónico, con la consiguiente inversión en programas y servidores, mano de obra, mantenimiento, etc., pasaría a ser una posibilidad asequible con PSA, al alcance de pequeños empresarios de limitados recursos de Tecnologías de la Información. La PSA hace frente a las necesidades de adquirir servidores más potentes o canales de comunicación de mayor capacidad.

Pero no todo pueden ser ventajas. Su riesgo más evidente es para la seguridad de la empresa que contrata al Proveedor de Servicios de Aplicaciones. Cuanto mayor sea el atractivo de hacerse con la información mantenida por el PSA, mayor será el número de ataques. Resulta obvio que de forma natural los PSA se convertirán en blanco preferido de los hackers.

Los servicios de seguridad mínimos exigibles al PSA serán:

- Cifrado de las comunicaciones, utilizando canales seguros con SSL de 128 bits o acudiendo a tecnologías de VPN (cuidado aquí con soluciones cerradas como PPTP de Microsoft, con agujeros ya encontrados).

- Autenticación fuerte, basada en técnicas criptográficas robustas e infalsificables, que por supuesto deberán guardar proporción con el nivel de sensibilidad de la información a proteger.

- Detección de intrusos, escaneos de puertos y de otras operaciones sospechosas.

- Se deberá dotar al sistema de una capacidad de respuesta rápida y eficaz.

- Utilización de un sistema operativo seguro, o al menos, seguramente configurado, con definición de permisos de accesos muy restrictivos y especial cuidado en programas ejecutables accesibles a través de las redes. Resulta fundamental que los clientes de un PSA no puedan acceder a los datos de otros clientes (de la competencia) albergados en el mismo PSA.

- Mantenimiento realizado preferiblemente desde las propias consolas de los servidores, ya que se previenen problemas de agujeros en los accesos remotos. Es importante establecer quién accede a los datos de quién. ¿Puede un administrador del PSA acceder rutinariamente a la información confidencial y sensible de una empresa?

A pesar de todas las medidas de seguridad, los mayores peligros a los que se enfrenta un servicio de PSA ofrecido a través de redes públicas son:

- Denegación de servicio: si el PSA deja de prestar el servicio transitoriamente, bien por ataques de hackers, bien por causas técnicas, la empresa puede ver su negocio seriamente afectado, dependiendo su impacto de la mayor o menor necesidad de prestación continuada del servicio a sus clientes. Hoy por hoy, habida cuenta del ciclo de vida tradicional del software, donde son los clientes, y no sus creadores, los que prueban el software y descubren vulnerabilidades, resulta muy arriesgado confiar en que el PSA se mantendrá a prueba de ataques con todas las brechas de seguridad cerradas y que garantizará un servicio durante el 100% del tiempo, incluso bajo ataques con éxito. La redundancia física y lógica de servidores juega aquí un papel crítico.

- El personal interno: una vez más, el mayor riesgo no procede de fuera, sino de dentro del propio PSA. Si alberga en él información confidencial de gran valor, un empleado desleal del PSA o implantado allí por un rival podría sentirse tentado de robarla para su uso o venderla al mejor postor. Nadie como él conoce cómo funciona internamente el Proveedor, por lo que nadie mejor que él para atacar sin dejar rastro. Estos empleados también podrían ser vulnerables a ataques de ingeniería social, sobornos, extorsiones, etc.

En la actualidad, los PSA se encuentran en su infancia. A pesar de la publicidad, los riesgos superan con mucho a las ventajas como para apostar fuerte por un PSA de acceso a través de redes públicas. Por supuesto, esta situación cambiará en el futuro, especialmente en la medida en que la seguridad se afronte como un objetivo prioritario del ASP y no como una mera cláusula del contrato

La Firma Electrónica y su validez jurídica

La firma electrónica, como ya se sabe, se reguló en España con el Real Decreto Ley 14/99 de 17 de septiembre, se intentaba con ello aumentar la seguridad y confianza en las comunicaciones telemáticas, además de garantizar la autenticación y la identidad del comunicante. Intentando cumplir las siguientes funciones, así identificación y atribución del mensaje (indica el origen y voluntad del firmante), función de privacidad (cifrado de mensaje y firmante), función de seguridad e integridad (evidencia si ha habido apertura o alteración del mensaje).

Cuando salió la ley, hay que reconocerle que fue una de las primeras sobre dicho tema. Se conocían sólo la Ley Alemana, la de Singapur, y la del estado de California (USA), pero esa celeridad ha sido criticada por algunos ya que, según éstos, ha dejado algunas lagunas sin resolver, como luego veremos, que pueden hacer de la seguridad una simple ilusión.

La ley maneja diferentes conceptos, así la "firma electrónica" (conjunto de datos, mensaje e identifica al autor o autores), y "firma electrónica avanzada" o digital (permite la identificación de signatario, le vincula, y detecta modificaciones del mensaje, en su caso).

La firma electrónica avanzada tiene en relación con el documento electrónico, el mismo valor jurídico que la firma manuscrita en relación con el documento en formato papel. La firma electrónica avanzada será admitida como prueba en juicio respecto a los datos signados, y será valorada conforme a los criterios de apreciación judicial establecidos en las normas procesales. El documento firmado electrónicamente no tiene valor de documento público: la firma electrónica no sustituye la función del fedatario público en relación con la formalización, validez y eficacia de las obligaciones y los contratos. Y esto es importante distinguirlo, la firma electrónica no hace de Notario nunca, tendrá valor de documento privado, (es decir, menor fuerza probatoria en un juicio que el documento público).

Y además para que esto sea así, es decir, si deseamos que la firma electrónica sea equivalente a la firma manuscrita en un juicio ("firma avanzada"), los certificados que se empleen en la comprobación de una firma electrónica deben haber sido expedidos por un proveedor de servicios de certificación (PSC) acreditado en España que cumpla con la normativa del RD-L 14/99 y con todos los requisitos legales necesarios para ser un PSC, obviamente.

La prueba de la compra es la clave para dotar al comercio electrónico de seguridad jurídica. Esta seguridad jurídica por el momento solo es alcanzable con la firma electrónica, bien sea a través de las Infraestructuras de Clave Pública y la firma digital o con la utilización de otra técnica de firma electrónica en donde necesariamente intervenga una tercera parte de confianza o Trusted Third Party, que certifique que los datos de firma consignados en el documento de compra pertenecen a una determinada persona.

El problema fundamental radica en la valoración que de esta prueba realicen los tribunales de justicia. A pesar de que el RDL 14/1999 de 17 de septiembre otorga a la Firma Electrónica el mismo valor jurídico que a la Firma Manuscrita, el valor probatorio en juicio es distinto. Generalmente en un proceso judicial la prueba pericial caligráfica suele

ser prueba plena, mientras que la prueba de una firma electrónica es una prueba de presunciones. Esta diferencia estriba en el rasgo o peculiaridad física que tiene la firma manuscrita, ya que la misma ha de ser realizada por la mano de la persona que firma, mientras que la firma electrónica es la introducción de una clave secreta o PIN para la ejecución de la misma en el documento electrónico, de ahí que se presuma que la ha realizado esta persona, pero puede ser probable que otra persona que se conozca el PIN o clave secreta haya ejecutado esa firma. En este sentido, se alcanzará igual valor probatorio entre ambos tipos de firma cuando en la ejecución de la firma electrónica intervengan rasgos biométricos de la persona, es decir, cuando sea el iris del ojo, la huella dactilar etc. el rasgo físico que ejecute la firma almacenada en el ordenador o en la tarjeta chip, solo entonces podrá existir igual efecto probatorio en juicio, y eso a pesar de que en nuestro ordenamiento jurídico existe la libre valoración de la prueba por parte de los jueces y tribunales, y por tanto al final la última palabra la tiene el juez. Habrá por tanto, que esperar a que se establezca este sistema biométrico para conseguir plena equiparación en juicio con la firma manuscrita.

Mientras tanto tendremos una prueba de presunciones que también será válida para probar que una determinada oferta fue aceptada.

Hasta el momento la técnica más segura sería la combinación de los certificados de firma X509 v3 almacenados en tarjeta chip, y el protocolo de comunicación seguro SSL.

A pesar de la seguridad en la comunicación, la utilización este protocolo de comunicación en el pago de los productos y servicios podría producir desconfianza en el Cliente, ya que potencialmente el Vendedor puede realizar cualquier tipo de fraude con total impunidad al poseer su número de tarjeta y no quedar garantizada la integridad del documento de pago. Sólo las empresas con muy buena reputación podrían, a priori, contar con la confianza del consumidor. Por otro lado, el consumidor en el caso de pago con tarjeta puede negar la compra del producto y el banco estará obligado a devolver el dinero si "no ha sido presentada directamente o identificada electrónicamente" (artículo 46 Pago mediante tarjeta de crédito, del capítulo II Venta a distancia, del título III Ventas especiales de la Ley del comercio minorista L7/96 de 15 de Enero). Aquí no habría muchos problemas si lo comprado es un bien físico y hay una dirección de entrega, pues podríamos saber de quién se trata, el problema surge cuando se utilizase para comprar bienes o servicios intangibles, es decir, bienes que no necesitan traslado físico, ya que sería más difícil de probar a donde ha ido a parar el producto o servicio y por tanto si se comete el fraude el perjudicado es sin duda alguna el comercio. Además, el más que posible fraude con números de tarjetas robados hace que las Entidades

de Crédito añadan una comisión en las compras bastante elevada (un 5% +/-) para compensar este tipo de fraude. Esto hace que el precio de la compra se incremente considerablemente, lo que anula el atractivo inicial de comprar por Internet: los precios bajos.

Si embargo, con la emisión de Certificados para firma se producirá una mayor confianza tanto en el consumidor como en el vendedor. Esto es debido a que al firmar el pago o formulario de pedido hay integridad del documento (es decir el vendedor no puede cambiar la fecha o cualquier otro dato), hay autenticidad en la compra (el comprador es quién dice ser pues su firma digital lo prueba, ya que está respaldada por una tercera parte de confianza o autoridad de certificación) y se produce el efecto del no repudio. De este modo con la combinación de estas dos técnicas de seguridad se podría establecer un comercio electrónico seguro para las tres partes intervinientes, Consumidor Vendedor y Banco. Con esta técnica habría todavía un problema a salvar, y no es otro que la intimidad de los datos de la tarjeta, los cuales no quedarían asegurados, siendo imprescindible utilizar otra técnica más segura SET (Secure Electronic Transaction) que por el momento no ha visto su despegue definitivo.