Seguridad y privacidad en los sistemas informáticos

Enrique Hernández Orallo (ehernandez@disca.upv.es)

La informatización de la sociedad ha proporcionado claras mejoras pero también nuevos problemas. Muchas entidades (Bancos, Compañías de Seguros, Administración Pública, etc.) contienen en sus ficheros de datos información personal cuyo acceso o difusión a personas no autorizadas podría perjudicar gravemente a la persona involucrada. Por ejemplo, cuando nosotros rellenamos un cuestionario de salud para contratar un seguro de vida ¿qué garantías tengo de que esa información esté protegida y no sea divulgada?

Tal como refleja el título de este artículo se pueden diferenciar dos aspectos muy importantes: *seguridad*, que la información depositada no se pierda o sea alterada de forma incorrecta y *privacidad*, que esta información sólo sea accesible cuando sea necesaria o con los autorizaciones pertinentes.

También hay otro tipo de información, que no siendo de carácter personal, si que es claramente vital para una empresa. Por ejemplo, toda empresa tiene almacenadas en sus sistemas informáticos las patentes de sus productos, nuevas campañas de marketing, planes estratégicos, etc. que si son accedidos por la empresa de la competencia podrían causar un grave perjuicio económico o incluso su ruina. Y no hablemos ya de los sistemas informáticos que controlan servicios vitales de un país: sistemas de control del tráfico aéreo, generación y distribución de electricidad, sistemas electrónicos de defensa, etc. Todos podemos imaginar las consecuencias catastróficas que puede suponer que un grupo terrorista pueda acceder y controlar estos sistemas (lo cual ya ha sido objeto de varias películas)

Por lo tanto, la información contenida dentro de los sistemas informáticos es claramente vital y por lo tanto tiene que ser protegida. Lo primero que hay que decir, aunque sea evidente, es que este acceso a la información privada es considerado un delito y por lo tanto perseguido por la justicia.

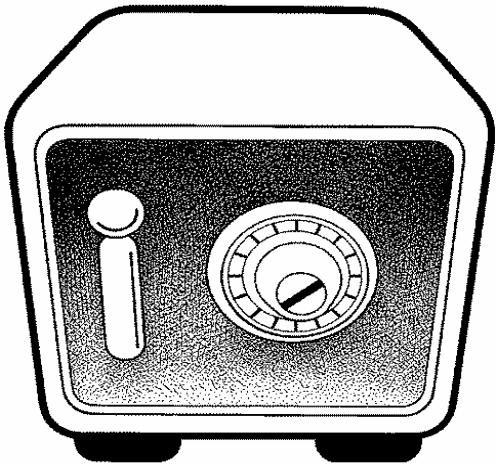

Figura 1: La seguridad de los datos informáticos

Como reflejo de la importancia de la seguridad voy a extraer unas pequeñas conclusiones de un informe realizado por la FBI de Mayo 1999 en la que se estu-

diaron 521 compañías de distinto tamaño y actividad:

- El 61% ha tenido perdidas de información debido al uso no autorizado de sus sistemas informáticos.
- El 50% de las compañías ha informado del abuso del uso de la red.
- La media de pérdida por robo o sabotaje es de 1.1 Millones de dólares.

El número de incidentes que afectan a la seguridad de un sistema informático esta creciendo exponencialmente (ver figura 2) y su coste es cada vez mayor. Por ejemplo, la revista *Computer Economics* cifró en 1300 millones de dólares el daño provocado por el virus *SirCam* [6].

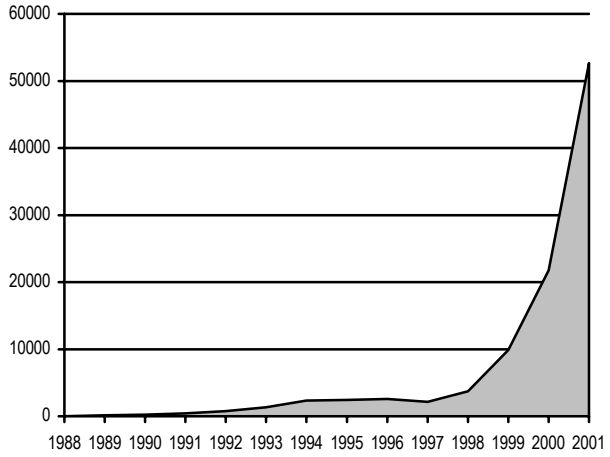

Figura 2: Incidentes de seguridad en los últimos años

MARCO LEGAL

El término privacidad es muy usado en informática ya que deriva de una mala traducción del término inglés *privacy*. En castellano, el término legal que refleja este aspecto es la intimidad o derecho a la intimidad. El derecho a la intimidad es el derecho que tienen las personas de poder excluir a las demás personas del conocimiento de su vida personal y la facultad para determinar en qué medida esa información sobre su vida personal puede ser comunicada o tratada por otras personas. Aunque el derecho a la intimidad abarca muchos aspectos legales de la vida personal, este artículo se centra en los aspectos que afectan a esta intimidad debido al tratamiento informático de la información personal.

La Constitución Española garantiza explícitamente el derecho a la intimidad en la informática y el secreto en las comunicaciones, tal como viene redactado en el artículo 18, apartado 3 "*Se garantiza el secreto de la comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial*" y apartado 4 "*La Ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos.*".

La Ley a la que hace mención el apartado 4, es la Ley Orgánica 15/1999, del 13 de diciembre de 1999, conocida como LOPD: Ley Orgánica de Protección de Datos. Esta Ley sustituye a una anterior: la Ley Orgánica 5/1992, la LORTAD: Ley Orgánica de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal. La LOPD establece los límites en el tratamiento y almacenamiento de datos personales que toda entidad informatizada está obligada a cumplir. El concepto de datos personales se define en la LOPD como "*cualquier información concerniente a personas físicas identificadas o identificables*". La LOPD clasifica los datos personales en función de su importancia y su seguridad. Así hay datos personales especialmente protegidos que son los referidos a la ideología, religión, creencias, afiliación sindical, salud, vida sexual, origen racial y comisión de infracciones penales o administrativas. Aunque el objetivo de la LOPD es la protección de cualquier tipo de dato personal es en los datos especialmente protegidos en los que hace un mayor hincapié en temas de seguridad e intimidad, estando gravemente penado el incumplimiento de esta ley.

La LOPD también impone la obligación de velar por la seguridad de los datos que una entidad almacena. Para ello impone la creación de un reglamento de seguridad y de auditorías de seguridad para verificar el cumplimiento de estos reglamentos.

No voy a profundizar más en el tema de LOPD, sino simplemente mostrar la importancia (el que impone el estricto cumplimiento de Ley) en el diseño de la seguridad y privacidad en los sistemas informáticos de cualquier empresa que trabaje con datos personales.

SEGURIDAD EN LOS SISTEMAS INFORMATICOS

Pero, ¿qué es un sistema informático seguro? Se puede utilizar la siguiente simple definición: "Un sistema es seguro si se puede confiar en él y se comporta

de acuerdo a lo esperado" [2]. La seguridad se basa por tanto en conceptos como la confianza y el acuerdo. Esto no se diferencia del concepto común de seguridad: ¿por qué guardamos el dinero en un banco? Primero, porque confiamos en el Banco y segundo, sabemos que podemos obtener ese dinero de acuerdo a lo esperado.

La seguridad es un conjunto de soluciones técnicas, métodos, planes, etc. con el objetivo de que la información que trata nuestro sistema informático sea protegida. Lo más importante es establecer un plan de seguridad en el cual se definan las necesidades y objetivos en cuestiones de seguridad. Es importante remarcar que la seguridad supone un coste y que la seguridad absoluta es imposible. Por lo tanto, hay que definir cuales son nuestros objetivos y a que nivel de seguridad se quiere llegar.

Esto no es diferente a los planteamientos de seguridad en lo que se refiere a la protección física de una empresa o vivienda. Por ejemplo, en nuestra casa podemos tener una puerta blindada y sentirnos seguros. O bien, poner una alarma y contratar los servicios de seguridad de una empresa, o incluso tener guardias jurados las 24 horas. Por ello, la seguridad se tiene que planificar haciendo un análisis del coste y su beneficio (teniendo siempre en cuenta los requisitos de seguridad legalmente establecidos, que evidentemente hay que cumplir).

El término seguridad es muy amplio y comprende distintos aspectos:

- **Confidencialidad**: la información sólo puede ser accedida por aquel que esté autorizado.
- **Integridad**: La información no puede ser eliminada o modificada sin permiso.
- **Disponibilidad**: La información tiene que estar disponible siempre que sea necesario, evitando por tanto, ataques externos que puedan reducir esta disponibilidad o incluso una caída del servicio.
- **Consistencia**: Hay que asegurar que las operaciones que se realizan sobre la información se comporten de acuerdo a lo esperado. Esto implica que los programas realicen correctamente las tareas encomendadas.
- **Control**: Es importante regular y controlar el acceso a la información de la empresa.

El tipo de empresa determina la importancia relativa que se da a los anteriores aspectos. Por ejemplo, un banco da mayor importancia a los aspectos de integridad y control que al resto, mientras que un sistema de control de tráfico aéreo dará mayor importancia a la disponibilidad y consistencia del sistema (evidentemente, sin dejar el resto de los aspectos de lado).

ANALISIS DE RIESGOS Y MEDIDAS DE SEGURIDAD

La primera pregunta a la hora de diseñar y planificar la seguridad en un sistema informático es la de analizar los riesgos. Este análisis trata de responder preguntas como: ¿qué quiero proteger?, ¿quién podría entrar en mi sistema? ¿Y cómo? Sabiendo a que peligros nos enfrentamos y qué es lo que tenemos que proteger podremos mejorar la seguridad de nuestro sistema informático. Por lo tanto no sólo hay que identificar los elementos tangibles: ordenadores, ficheros de datos, documentos, etc., sino también los intangibles: aspectos legales, imagen y reputación de la empresa

También hay que identificar los posibles riesgos: virus informáticos, intrusos en la red (*hackers*), empleados malintencionados, pérdidas de *backups*, robos de equipos (por ejemplo portátiles), fallos en el software, una catástrofe natural (terremotos, inundaciones), etc. De este tipo de riesgos hay que analizar cual es la probabilidad de que ocurran. Por ejemplo, en determinadas zonas es probable que ocurran inundaciones, lo cual puede provocar que los ordenadores se inunden y no estén disponibles, e incluso se pierda información vital en la empresa.

TIPOS DE RIESGOS

¿Cuáles son los posibles ataques que puede sufrir un sistema informático? Si sabemos cuales son los ataques podremos poner medidas de seguridad para evitarlos. En este punto voy a enumerar los tipos de ataques más comunes que puede sufrir un sistema informático y para los cuales existen, como veremos en los puntos siguientes, medidas bastante efectivas.

- Virus: es quizá el más conocido de los riesgos, y el que más difusión mediática ha tenido. Un virus es un software que se propaga por la red y que cuando "infecta" a un equipo puede producirle daños catastróficos (borrando la información del disco duro infectado). El objetivo

de un virus suele ser la simple destrucción del equipo infectado. Con la difusión de Internet en los últimos años los virus se han convertido en una plaga. Los virus pueden entrar por medio del navegador, del correo electrónico, en fichero bajados de red, etc.

- *Hackers*: el objetivo de un *hacker* es entrar en la red informática de una entidad. Lo que haga dentro ya depende del tipo de *hacker*: hay *hackers* que simplemente lo hacen por diversión: entran y dejan un rastro para indicar que han conseguido entrar, los hay maliciosos cuyo objetivo es sacar provecho de haber entrado: como por ejemplo hacer transferencias, modificar notas de exámenes, obtener documentos privados, etc. Estos últimos, evidentemente, suponen un grave peligro para cualquier empresa.

- Ataques masivos: recientemente se ha producido una forma de ataque que puede provocar la caída de un sistema informático o que quede inutilizado. Una forma simple de bloquear un servidor web es que mucha gente se conecte continuamente a este servidor con lo que se produce una especie de atasco y el sistema aparece bloqueado (a esta situación se suele denominar denegación de servicio). Esto ha ocurrido recientemente en caso de protestas masivas contra entidades o personas (por ejemplo, en las páginas web de distintos ministerios y partidos políticos por protestas por el hundimiento del Prestige y la guerra de Iraq). Evidentemente, en estos casos, el problema no es muy grave ya que en cuanto acaba la protesta el servicio se restablece. Esto sería muy grave, en el caso de que este bloqueo se produjese en equipos que ofrecen servicios vitales para el desarrollo de la empresa, como servicios Bancarios, venta por Internet, etc.

Cuando ya se han analizado los riesgos es importante determinar las consecuencias que supondría cada uno de ellos. Por ejemplo, ¿qué consecuencia puede tener un intruso en la red? Esto dependerá de la información con la que trabajemos: en un hospital es crítico que un intruso se lleve los historiales médicos de todos los pacientes mientras que en un taller mecánico no sería muy grave que se llevase información sobre los coches reparados. O bien, ¿qué pasaría si se inundase el centro de cálculo de una Entidad Financiera? (hecho que ocurrió en una recientes inundaciones en el País Vasco). En este caso, ¿cuánto tiempo podría estar la entidad financiera sin dar servicio a los clientes?, ¿horas?, ¿días?, ¿semanas?

MEDIDAS DE SEGURIDAD

Como se ha comentado antes, los riesgos no pueden ser totalmente eliminados, sino que pueden ser reducidos. Por ello, la seguridad en un sistema informático tiene que basarse en objetivos realistas y plantearse como un clásico estudio de coste/beneficio. Por tanto, las medidas de seguridad a implementar tendrán que ser consecuentes con los análisis realizados. Las posibles medidas a establecer se pueden clasificar en

- **Protección física**: Guardias de seguridad, recintos vigilados, sistemas anti-incendios (de nada vale poner medidas de seguridad informática si cualquier persona puede entrar en un recinto y robar un ordenador vital de la empresa).

- **Medidas informáticas**: son los sistemas y soluciones informáticas que aumenta la seguridad de los sistemas informáticos. Estos incluyen el cifrado de la información, cortafuegos, antivirus, detectores de intrusos, etc.

- **Medidas organizativas**: cursos de formación sobre seguridad, auditorías informáticas, etc. El personal de una empresa tiene que ser consciente de que la seguridad empieza en los empleados.

CRIPTOGRAFIA Y AUTENTIFICACION

Como elementos indispensables para implementar un sistema seguro está la criptografía y los mecanismos de autentificación. La criptografía es una disciplina muy antigua cuyo objeto es la de ocultar la información a personas no deseadas. La base de la criptografía ha sido el cifrado de textos, aunque se ha desarrollado ampliamente desde la aparición de los primeros ordenadores (Ver [3] para una pequeña historia de la criptografía).

CRIPTOGRAFÍA

El cifrado es el proceso por el que un texto es transformado en otro texto cifrado usando una función matemática (también denominado algoritmo de encriptación) y una clave. El descifrado es el proceso inverso. El objetivo de la criptografía se puede resu-

mir en asegurar la [5]:

- **Confidencialidad**: el mensaje no puede ser leído por personas no autorizadas.
- **Integridad**: el mensaje no puede ser alterado sin autorización.
- **Autentificación**: se puede verificar que el mensaje ha sido enviado por una persona, y recibido por otra.
- **No repudio**: significa que después de haber enviado un mensaje, no se puede negar que el mensaje no es tuyo.

El cifrado es necesario entre otras funciones para:

- Proteger la información almacenada en un ordenador
- Proteger la información transmitida desde un ordenador a otro.
- Asegurar la integridad de un fichero.

El cifrado también tiene sus límites ya que no puede prevenir el borrado de información, el acceso al documento antes de su cifrado, por lo que un plan de seguridad no se puede basar simplemente en el cifrado de la información.

No todas las formas de cifrado tienen la misma seguridad. Hay cifrados muy simples que son fáciles de romper (se denomina romper un cifrado a la obtención del mensaje cifrado o la clave) y otros muchos más complejos que requieren de técnicas muy complejas para su descifrado. Hay que comentar que no existen mecanismos de cifrado totalmente seguros, ya que con un ordenador lo suficientemente potente (o muchos a la vez) y el tiempo necesario (años o siglos) siempre será posible romper el cifrado. Por lo tanto, el objetivo de la criptografía es obtener mecanismos de cifrado que sean lo suficientemente complejos para evitar su descifrado usando la tecnología actual.

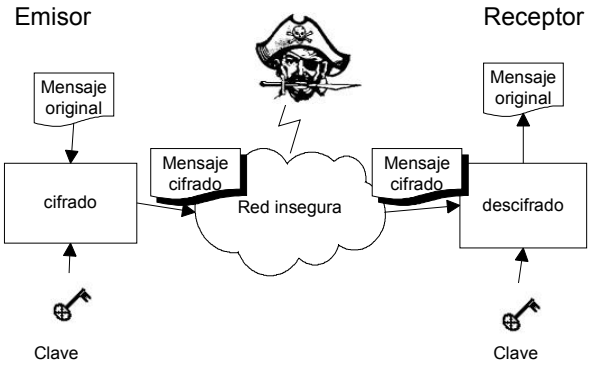

Figura 3: Cifrado y descifrado de un mensaje

En la figura 3 se puede ver un ejemplo de uso del cifrado para transmitir un mensaje en una red no segura (por ejemplo Internet). El emisor cifra su mensaje utilizando una clave y un algoritmo de cifrado. Este mensaje cifrado es transmitido por la red al receptor. Este, utilizando la clave y un algoritmo de descifrado puede obtener el mensaje original. De esta forma, aunque un intruso intercepte el mensaje no lo podrá descifrar si no sabe el algoritmo de descifrado y la clave.

Hay dos tipos básicos de algoritmos de encriptación:

- **Clave secreta** (o clave simétrica): utiliza la misma clave para cifrar y descifrar un mensaje. Estos métodos de cifrado se usan principalmente para proteger información que se almacena en un disco duro o para transmisión de datos entre ordenadores. El algoritmo de encriptación más usado de este tipo es el DES (*Data Encryption Standard*) que usa una clave de 56-bits. Un mensaje cifrado con este algoritmo es bastante seguro aunque ya puede ser descifrado con máquinas muy potentes en menos de un día, por lo que su uso está restringido a ámbitos civiles. Otros algoritmos comúnmente usados son el RC2, RC4, RC5 e IDEA. La mayoría de estos algoritmos tienen patente, aunque su uso público está permitido.
- **Clave pública** (o clave asimétrica): que utiliza una clave pública para cifrar el mensaje y una clave privada para descifrarlo De esta forma cualquiera puede cifrar un mensaje pero solo quien tenga la clave privada puede descifrarlo. Esto sirve para poder enviar un mensaje a un determinado destino sin que otro pueda descifrarlo. El objeto de estos métodos es la de asegurar la integridad y la autentificación del ori-

gen de los datos (por ejemplo, usando firmas digitales). RSA es el algoritmo de encriptación más conocido de clave pública. RSA utiliza una clave pública que es usada para cifrar el mensaje y una clave privada que es usada para descifrar el mensaje.

Estos dos métodos de encriptación funcionan muchas veces conjuntamente. Por ejemplo, el protocolo SSL que se utiliza como conexión segura en Internet (el que usa el navegador cuando está en modo seguro y en la URL nos sale https), utiliza primero una clave pública para enviar de forma cifrada la clave secreta DES que posteriormente utilizarán en la comunicación. De esta forma la clave DES utilizada sólo la podrá descifrar el destino. Este método en general se denomina OTP (*One Time Password*) ya que para cada sesión se genera un nueva clave DES.

FIRMA DIGITAL

El objetivo de la firma digital es la de certificar los contenidos de un mensaje. En este caso el mensaje original no es necesario que vaya cifrado, sino que contiene (o va en un fichero aparte) un código que identifica el mensaje y que va cifrado con una clave privada. A este proceso de certificar el mensaje con una firma digital se denomina firmado. Esta firma digital nos sirve para asegura la integridad, autentificación y el no repudio. En este caso, el mensaje original no es necesario que vaya cifrado, aunque si lo va también garantizamos la confidencialidad del mensaje. El algoritmo de firma digital más usado actualmente es el MD5.

SEGURIDAD INTERNA

En la seguridad interna (o centralizada) se pueden engoblar todos los mecanismos que aseguran el sistema frente a riesgos procedentes del interior de una organización o empresa. Muchos de estos mecanismos sirven también para afrontar riesgos procedentes del exterior.

AUTENTIFICACION

Hay que asegurar que cualquier persona que entre en nuestro sistema informático esté autorizado y sólo pueda acceder a la información permitida en función de su cargo o función. La forma habitual de autorizar una persona es por medio de un identificador de usuario y una clave, y asociando a este usuario una serie de permisos. Por ello, es de vital importancia que estos usuarios y sus claves sean custodiados de forma adecuada. De nada vale implantar un sistema informático de alta seguridad si los usuarios y claves son fácilmente accesibles. Por ejemplo, es muy cómodo poner como clave dos letras o un único número, o incluso tenerla pegada en la pantalla del ordenador. Esto tipos de claves son muy fáciles de obtener por cualquier *hacker* con lo que podrían entrar en nuestro sistema. Para evitar estos problemas, algunos sistemas imponen claves complejas (con número y letras) o que tengan que variarse un cierto periodo de tiempo o incluso, en sistemas de alta seguridad, otros dispositivos de autentificación como tarjetas de acceso, reconocimiento de voz o huella, etc.

También es importante asegurar que cualquier empleado que entre en nuestro sistema informático esté autorizado y sólo pueda acceder a la información permitida en función de su cargo o función. Esto evitará que el acceso a determinada información crítica este restringida a determinadas personas de total confianza.

COPIAS DE SEGURIDAD (Backups)

Las copias de seguridad son una medida para recuperarse de un desastre (perdida voluntaria o involuntaria de información, ordenador estropeado, catástrofe natural, etc.), Por ello, es de vital importante que las copias de seguridad estén perfectamente planificadas y que se verifique el correcto funcionamiento de la copia.

También es importante que los soportes físicos de estas copias de seguridad se custodien de forma adecuada. No tiene sentido que una copia de seguridad de la base de datos de los clientes esté encima de la mesa del operador que la ha realizado (cualquier persona que pase por su mesa se podría llevar esta información tan importante).

REGISTROS Y AUDITORIA

Es necesario mantener un registro de las operaciones realizadas sobre los sistemas informáticos. De esta forma se puede realizar una auditoría sobre el acceso a los sistemas y posibles fallos de seguridad. Este registro suele ser un conjunto de ficheros donde se traza las operaciones realizadas sobre datos, equipos, etc. Por ejemplo, para una entidad financiera sería importante saber quien a consultado las cuentas reservadas, por ello, cuando se consulten estas cuentas se añadirá un registro indicando que empleado lo ha consultado y cuando.

SEGURIDAD PERIMETRAL

El objetivo de la seguridad perimetral es evitar el ataque externo a nuestros sistemas informáticos. Este ataque puede ocurrir de muchas formas y con diferentes objetivos. Hay intrusos cuyo único objetivo es conseguir entrar en una entidad por cualquier puerta falsa (los denominados *hackers*). También están los virus, que pueden entrar por correo electrónico. Si estuviéramos en la edad media lo más parecido a la seguridad perimetral sería un castillo con una buena fortaleza, foso, y puente levadizo que sería la única vía de entrada permitida (figura 4). De esta forma tendríamos más controlado el acceso a nuestro sistema informático. Otro tipo de ataque muy común es el de *bormbardeo*. Esto puede provocar que nuestro sistema se quede bloqueado y no pueda ofrecer servicio (sería muy parecido a un asedio a nuestra fortaleza).

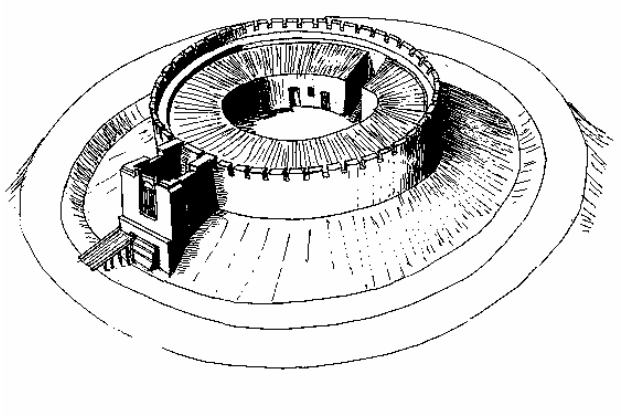

Figura 4: Fortaleza con un sólo punto de entrada

La forma más simple de asegurar nuestro sistema es no tener ninguna conexión con el exterior. Esto significa, que nuestro sistema está aislado y no puede entrar nadie externo. Pero esta solución no es posible en la mayoría de los sistemas informáticos, ya que se requiere la consulta de datos de sistemas externos o/y la provisión de información a clientes externos (por ejemplo, vía un navegador). Para aumentar la seguridad y permitir esta comunicación con sistemas externos la solución más segura es mantener un único (o bien algunos pocos) enlaces con el exterior. Usando el símil de un castillo medieval, el único punto de entrada y salida a la fortaleza sería el puente levadizo con lo que es más fácil controlar quién entra y quién sale. Este control se implementa en los sistemas informáticos por medio de un dispositivo denominado cortafuegos (o *firewall*).

CORTAFUEGOS (*firewalls*)

El término de cortafuegos viene prestado de su propia definición de puerta de seguridad antiincendios. Esta puerta puede aislar una determinada zona de un edificio del incendio en otra parte (durante un tiempo limitado, por supuesto). Con esta idea, la función de un cortafuegos en una red informática es la de aislar el sistema informático interno de problemas externos.

Tal como representa la figura 5 la función fundamental de un cortafuegos es la de limitar y controlar el tránsito de información entre una red externa (por ejemplo Internet) de una red interna (la Intranet). El cortafuegos permite añadir varias barreras para que un ordenador externo no pueda acceder a los ordenadores internos, haciendo más difícil el acceso a la red interna. Para configurar un cortafuegos hay que definir que información hay que dejar pasar y cual no, es decir, hay que definir una política de permisos. Las funciones de un cortafuegos son varias:

- Permite bloquear el acceso a determinadas páginas de Internet (por ejemplo, algunas de uso interno de una empresa).
- Monitorizar las comunicaciones entre la red interna y externa.
- Controlar el acceso a determinado servicios externos desde dentro de una empresa (por ejemplo, puede evitar que los empleados de una empresa usen Internet para descargarse ficheros).

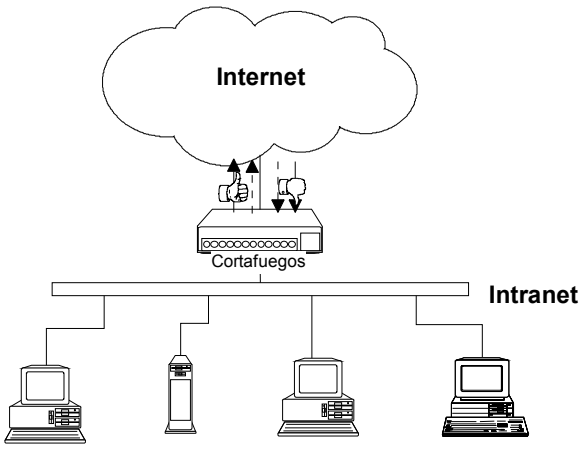

Figura 5: Cortafuegos

Este mecanismo de cortafuegos suele ser más

complejo en implementaciones reales. Normalmente se compone de varios ordenadores y una red perimetral que ofrece los servicios que una entidad quiere proporcional al exterior (por ejemplo, servidores de páginas web, correo electrónico. etc.) de tal forma que para entrar en la red interna tendrían que pasar dos barreras: el cortafuegos de la red perimetral y el cortafuegos de la red interna.

Los cortafuegos también se pueden usar para separar distintas sub-redes dentro de una gran empresa. Por ejemplo, se podrían aislar los ordenadores que gestionan las nóminas del resto de la red de la empresa (para evitar que un empleado de la empresa pueda entrar en el ordenador de nóminas y se modifique su nómina, o pueda consultar la nómina del director general). De esta forma también se aumenta la seguridad de estas sub-redes al ir añadiendo nuevas barreras.

Recientemente han aparecido los denominados cortafuegos domésticos, cuyo objetivo es el mismo que los cortafuegos en red. El motivo de la aparición de estos cortafuegos es el incremento del número de ordenadores domésticos conectados permanentemente a Internet (vía ADSL, cable-modem, etc.), lo que los hace muy vulnerables a ataques externos. Estos cortafuegos se instalan en el propio ordenador personal y lo protegen de posibles intrusos, alertando al usuario cuando alguien quiere entrar en el ordenador.

ANTIVIRUS PERIMETRALES

El objetivo de un antivirus perimetral es la de analizar todo el tráfico que entra y sale de la red y comprobar si tiene virus. Lo más habitual es analizar únicamente el tipo de tráfico que puede introducir virus: el correo electrónico y la navegación por Internet.

Estos antivirus están en permanente actualización: están conectados a la bases de datos de la empresa fabricante con lo que si aparece un nuevo virus y se descubre su antídoto, rápidamente el antivirus perimetral lo podrá interceptar evitando así su propagación.

DETECCION DE INTRUSOS

Incluso con los sistemas de protección más avanzados, la seguridad absoluta no existe, por lo que siempre es posible que alguien entre dentro de nuestro sistema. Por ello, es necesario, un sistema de detección de intrusos que nos alerte de cuando se produce un fallo en la seguridad de nuestro sistema. En esencia, un sistema de detección de intrusos es como una alarma en una casa. Los sistemas de detección de intrusos pueden actuar en tiempo real: avisan de forma inmediata cuando hay un intruso o a posteriori: analizando el sistema pueden averiguar que ha habido un intruso.

Hay varias formas de detectar un intruso: comprobar que un usuario no autorizado se ha conectado en una máquina, deducir que alguien ha entrado por que ha modificado ficheros en el sistema, un comportamiento anómalo en los ordenadores (sobrecarga, fallos continuos, etc.).

Los dos tipos más importantes de sistemas de detección de intrusos son los basados en red y los basados en host [7]:

- **Basados en red**: Estos detectores son aplicaciones que están conectadas a la red interna de la empresa y analizan todo el tráfico detectando anomalías que puedan indicar que hay intrusos. La ventaja de estos sistemas es que sirven para todos los equipos de una red, aunque si el tráfico de la red está cifrado no suele ser muy eficientes.

- **Basados en host**: Estos detectores están instalados en la misma máquina a proteger y analizan un comportamiento anómalo en el equipo. Estos sistemas suelen ser más eficientes aunque tienen el inconveniente de tener que instalarse en cada ordenador a proteger.

Pero cuando se detecta un intruso, ¿qué podemos hacer? Lo más drástico (y efectivo) es apagar el ordenador donde el intruso ha entrado con lo que no podrá hacer más daño. Otras opciones menos drásticas son eliminar los programas que haya arrancado el intruso o bien desconectarlos de la red externa. En muchas ocasiones el intruso sólo se detecta cuando el daño se ha cometido. En este caso hay que analizar el daño causado, como ha podido entrar y poner remedio a este fallo de seguridad. También es necesario denunciar esta intrusión a la policía, aunque si el daño no ha sido grave en muchos casos no se suele denunciar para evitar la mala publicidad que puede producir.

DENEGACION DE SERVICIO

Como se ha comentado antes la denegación de servicio es un ataque a nuestro sistema en el que alguien abusa de nuestros sistemas informáticos de forma que otros usuarios no puedan utilizarlos. Existen varias formas de evitar este abuso de nuestro sistema: poniendo cotas o límites al uso del sistema a

cada usuario.

Más difícil de solucionar es cuando esta denegación del servicio se produce porque se satura la red que conecta nuestro sistema al exterior, debido a un ataque masivo de gente. Estos ataques suelen ser de tipo de protesta colectiva y el objetivo es que un grupo muy elevado de usuarios se conecten a un ordenador (por ejemplo una página web) de forma que la red quede saturada y el sistema sea inoperativo. En este caso, la solución la tiene que proporcionar nuestro proveedor de Internet (por ejemplo, rechazando las conexiones en el origen).

Recientemente han surgido otros tipos de ataques más elaborados y peligrosos. Se basan en utilizar un conjunto elevado de ordenadores que previamente han sido infectados con un virus, que en determinado momento realizan el ataque a un determinado servidor web, bloqueándolo.

REDES PRIVADAS VIRTUALES

La evolución de los sistemas de comunicaciones ha permitido nuevas formas de trabajo al permitir el acceso a los sistemas de información de una empresa desde cualquier punto del mundo. No es raro ver un comercial de una empresa en casa del cliente con su portátil conectado al ordenador de la empresa realizando un pedido. O bien, el teletrabajo, gente trabajando con un ordenador en su casa. Incluso, empleados con agendas electrónicas (o PDA) que consultan el correo electrónico de la empresa con conexión inalámbrica.

Esto nuevos medios de acceso a la información de la empresa es un arma de doble filo: permite una mayor flexibilidad al empleado pero aumenta los riesgos de acceso a la información. Dado que la información viaja desde el punto donde esta el empleado a la empresa por medio de redes de comunicaciones que la empresa no controla, esta información está más expuesta a posibles interceptaciones. Por ejemplo, si nos conectamos desde casa por medio de un modem, no es difícil que un intruso pinche la línea y espíe lo que se transmite por ello.

La solución a estos problemas se concreta en lo que se denomina Redes Privadas Virtuales: el objetivo es que el cualquier ordenador que se conecte remotamente tenga un canal de comunicaciones tan seguro como si estuviese dentro de la empresa. Para ello se suelen utilizar los estándares de seguridad IPSec y EAP).

CONCLUSIONES

La seguridad en los sistemas informáticos se ha convertido en algo imprescindible en toda empresa que gestione datos informáticos. La alta informatización de la sociedad actual ha conllevado el aumento de los denominados delitos informáticos.

Más importante es la gestión de los datos personales y su privacidad. La LOPD ha limitado el uso que una empresa puede hacer de los datos personales.

Definir un plan de seguridad es el primer paso para aumentar la seguridad. Este plan de seguridad puede incluir medidas tanto físicas, informáticas como de gestión. En el ámbito informático se han descritos varios mecanismos para aumentar la seguridad, frente a ataques internos como externos. Pero siempre es necesario recordar que la seguridad absoluta no existe.

REFERENCIAS

1. G.Gallo, I. Coello de Portugal, F. Parrondo y H.Sánchez, "La protección de datos personales: Soluciones en entornos Microsoft". Microsoft Ibéri-ca. 2003.
2. S. Garfinkel y G.Spafford, "Practical Unix and Internet Security". O'Reilly and Associates, Inc. Second Edition 1996.
3. J.A.Labodía, "Protección de la informática a través del cifrado", Manuales formativos ACTA. Número 16, Año 2000[
4. "Computer Crime Survey" del FBI, proporcionado por Secure Site E-News del 22 de mayo de 1999,
5. A. Menezes, P. van Oorschot and S. Vanstone, "Handbook of Applied Cryptography", CRC Press, 1996.
6. A. Householder, K. Houle and C.Dougherty, "Computer Attack Trends Challenge Internet Security", Security and Privacy. IEEE Press. 2002.
7. G.Álvarez, "Sistemas de detección de intrusos", PCWorld, Enero 2003.
8. R.A.Kemmerer and G.Vigna, "Intrusion Detection: A brief History and Overview." Security and Privacy. IEEE Press. 2002.
9. PCWord, "Seguridad: ¿cómo pueden preservarse las empresas?. Suplemento PCWorld Número 116. Marzo 2003.