SEGURIDAD Y PROTECCIÓN DE LA INFORMACIÓN

Introducción a la problemática de la Seguridad Informática

By Heineken Team

ÍNDICE

BIBLIOGRAFÍA

• "Site Security Handbook". Request For Comments 1244. P. Holbrook y J. Reynolds.
• "Definición de una política de seguridad". José R. Valverde. www.rediris.es/cert.
• "Computer Security Basics". D. Russell y G.T. Gangemi. O'Reilly & Associates.
• "Building Internet Firewalls". D.B. Chapman y E.D. Zwicky. O'Reilly & Associates. Cap. 3 y 11.
• "Security in Computing". C. P. Pfleeger. Prentice Hall. Second Ed. Cap.10.

1.1. Introducción

Las sociedades avanzadas de fin de este siglo son denominadas frecuentemente sociedades de la información, pues el volumen de datos que es procesado, almacenado y transmitido es inconmensurablemente mayor que es cualquier época pretérita.

Además, no sólo el volumen, sino la importancia de esta información para el desarrollo económico y social, no tiene ningún parangón con la que tuvo en el pasado. De hecho, en la actualidad, las organizaciones consideran que la información es un bien más de su activo y, en muchos casos, prioritario sobre los restantes.

Pero gran parte de esos datos que nosotros, o las entidades de nuestra sociedad, manejamos, han sido tratados, sea durante su proceso, o almacenamiento, o transmisión, mediante las llamadas tecnologías de la información, entre las que ocupa un lugar focal la informática. Consiguientemente, la seguridad de las tecnologías de información, y por ende las informática, se convierte en un tema de crucial importancia para el continuo y espectacular progreso de nuestra sociedad, e incluso para su propia supervivencia.

Por otro lado, la eclosión en los últimos años de las redes informáticas y fundamentalmente de Internet, ha sido el factor fundamental que ha hecho que la Seguridad Informática cobrase una importancia vital en el uso de sistemas informáticos conectados. Desde el momento en que nuestro ordenador se conecta a Internet, se abren ante nosotros toda una nueva serie de posibilidades, sin embargo éstas traen consigo toda una serie de nuevos y en ocasiones complejos tipos de ataque. Más aun, mientras en un ordenador aislado el posible origen de los ataques es bastante restringido, al conectarnos a Internet, cualquier usuario de cualquier parte del mundo puede considerar nuestro sistema un objetivo apetecible.

Existe un acuerdo y conciencia general sobre la importancia de la Seguridad de los Sistemas de Información (SSI). La SSI está relacionada con la disponibilidad, confidencialidad e integridad de la información tratada por los ordenadores y las redes de comunicación. Se usan comúnmente otros términos que en esencia tienen el mismo significado, tales como seguridad de la información, seguridad de los ordenadores, seguridad de datos o protección de la información, pero en aras de la consistencia, usaremos el término Seguridad de los Sistemas de Información en las páginas siguientes.

Los objetivos fundamentales del presente tema son los siguientes:

- Introducir el concepto de Sistema de Información, sus principales componentes y tipos de información manejados.
- Definir los conceptos básicos involucrados en la seguridad informática como son la confidencialidad, integridad y disponibilidad.
- Definir cuales son las principales amenazas y vulnerabilidades de un sistema informático, así como los distintos tipos de medidas que podemos utilizar para prevenirlas.
- Definir que se entiende por política de seguridad, cómo se fija y cuales son sus principales contenidos.
- Introducir algunos principios básicos que subyacen en la aplicación de cualquier política de seguridad informática.

1.2. Conceptos básicos

1.2.1. Información y Sistema Informático

Entendemos por información el conjunto de datos que sirven para tomar una decisión. En consecuencia, su necesidad es evidente tanto en la planificación estratégica a largo plazo como en la fijación de estándares para la

planificación a corto. La información también es necesaria para el estudio de las desviaciones y de los efectos de las acciones correctoras; es un componente vital para el Control.
En cuanto a su implantación, se puede hablar de:

- Subsistema formalizado: Normas, procedimientos e información de negocio.
- Subsistema no formalizado: Flujos de información que no pasan por el sistema de información formalizado (rumores, charlas informales, llamadas telefónicas, etc.).

El sistema informático es un subconjunto del subsistema formalizado, con distinto grado de cobertura. Por otra parte, se puede ver el sistema informático como el conjunto de los recursos técnicos (máquinas y utensilios), financieros (ingresos, gastos y patrimonio) y humanos (plantilla de informáticos y personal auxiliar), cuyo objetivo consiste en el almacenamiento, procesamiento y transmisión de la información de la empresa.

1.2.2. Aspectos clave en la SSI

Debido a la difusión de las tecnologías de la información, la mayoría de las organizaciones actuales están expuestas a una serie de riesgos derivados de una protección inadecuada o inapropiada de la información o de sus sistemas de tratamiento. Apuntaremos sólo dos ejemplos de esta vulnerabilidad creciente. Primero, con la gran expansión del uso de ordenadores personales se ha magnificado el problema de la SSI, debido sobre todo a la carencia de controles de seguridad básicos en este tipo de sistemas. En segundo lugar, la evolución hacia entornos con acceso global y múltiple, con un aumento de la conectividad entre organizaciones distintas, plantea retos importantes a la gestión de la seguridad.
Los riesgos fundamentales asociados con la incorrecta protección de la información son:

- Revelación a personas no autorizadas
- Inexactitud de los datos
- Inaccesibilidad de la información cuando se necesita

Estos aspectos se relacionan con las tres características que debe cubrir un SI seguro: confidencialidad, integridad y disponibilidad. Así pues, preservar estas tres características de la información constituye el objetivo de la seguridad.
Los problemas técnicos, las amenazas ambientales, las condiciones de instalación desfavorables, los usuarios, la situación política y social, son otros tantos factores susceptibles de poner en peligro el buen funcionamiento de los SI. Las amenazas a los SI van desde desastres naturales tales como inundaciones, accidentes o incendios, hasta abusos deliberados como fraudes, robos, virus, con un origen tanto interno como externo.
Aunque se pueda pensar que el problema de la seguridad de los SI está sobredimensionado, muchos intereses no son nunca detectados, o se ocultan por los gestores porque muestran fallos o debilidades de los procedimientos de seguridad, existiendo una natural resistencia en informar de los mismos a personas ajenas.

1.2.3. Definición de Seguridad Informática

No existe una definición estricta de lo que se entiende por seguridad informática, puesto que ésta abarca múltiples y muy diversas áreas relacionadas con los SI. Áreas que van desde la protección física del ordenador como componentes hardware, de su entorno, hasta la protección de la información que contiene o de las redes que lo comunican con el exterior.
Tampoco es único el objetivo de la seguridad. Son muy diversos tipos de amenazas contra los que debemos protegernos. Desde amenazas físicas, como los cortes eléctricos, hasta errores no intencionados de los usuarios, pasando por los virus informáticos o el robo, destrucción o modificación de la información.
No obstante sí hay tres aspectos fundamentales que definen la seguridad informática: la confidencialidad, la integridad y la disponibilidad. Dependiendo del tipo de sistema informático con el que tratemos (militar, comercial, bancario, ...), el orden de importancia de estos tres factores es diferente, e incluso entran en juego otros elementos como la autenticidad o el no repudio. El enfoque de la política de seguridad y de los mecanismos utilizados para su implementación está influido por el más importante de los tres aspectos. Estos aspectos también pueden entenderse como metas u objetivos.
Definición operacional: Un ordenador es seguro si podemos contar con que su hardware y su software se comporten como se espera de ellos.

1.2.4. Confidencialidad

Se entiende por confidencialidad el servicio de seguridad, o condición, que asegura que la información no pueda estar disponible o ser descubierta por o para personas, entidades o procesos no autorizados.
La confidencialidad, a veces denominada secreto o privacidad, se refiere a la capacidad del sistema para evitar que personas no autorizadas puedan acceder a la información almacenada en él.
En áreas de seguridad gubernamentales el secreto asegura que los usuarios pueden acceder a la información que les está permitida en base a su grado o nivel de autoridad, normalmente impuestas por disposiciones legales o administrativas.
En entornos de negocios, la confidencialidad asegura la protección en base a disposiciones legales o criterios estratégicos de información privada, tal como datos de las nóminas de los empleados, documentos internos sobre estrategias, nuevos productos o campañas, etc.
Este aspecto de la seguridad es particularmente importante cuando hablamos de organismos públicos, y más concretamente aquellos relacionados con la defensa. En estos entornos los otros dos aspectos de la seguridad son menos críticos.
Algunos de los mecanismos utilizados para salvaguardar la confidencialidad de los datos son, por ejemplo:

- El uso de técnicas de control de acceso a los sistemas.
- El cifrado de la información confidencial o de las comunicaciones.

1.2.5. Integridad

Se entiende por integridad el servicio de seguridad que garantiza que la información es modificada, incluyendo su creación y borrado, sólo por el personal autorizado.
Suelen integrarse varios conceptos análogas en este segundo aspecto de la seguridad:

- precisión accuracy,
- integridad integrity,
- autenticidad auntenticity.

El concepto de integridad significa que el sistema no debe modificar o corromper la información que almacene, o permitir que alguien no autorizado lo haga.
Esta propiedad permite asegurar que no se ha falseado la información. Por ejemplo, que los datos recibidos o recuperados son exactamente los que fueron enviados o almacenados, sin que se haya producido ninguna modificación, adición o borrado.
De hecho el problema de la integridad no sólo se refiere a modificaciones intencionadas, sino también a cambios accidentales o no intencionados.
En el ámbito de las redes y las comunicaciones, un aspecto o variante de la integridad es la autenticidad. Se trata de proporcionar los medios para verificar que el origen de los datos es el correcto, quién los envió y cuándo fueron enviados y recibidos.
En el entorno financiero o bancario, este aspecto de la seguridad es el más importante. En los bancos, cuando se realizan transferencias de fondos u otros tipos de transacciones, normalmente es más importante mantener la integridad y precisión de los datos que evitar que sean interceptados o conocidos (mantener la confidencialidad).
En el campo de la criptografía hay diversos métodos para mantener/asegurar la autenticidad de los mensajes y la precisión de los datos recibidos. Se usan para ello códigos/firmas añadidos a los mensajes en origen y recalculadas/comprobadas en el destino. Este método puede asegurar no sólo la integridad de los datos (lo enviado es igual a lo recibido), sino la autenticidad de la misma (quién lo envía es quien dice que es).

1.2.6. Disponibilidad

Se entiende por disponibilidad

- El grado en que un dato está en el lugar, momento y forma en que es requerido por el usuario autorizado.
- La situación que se produce cuando se puede acceder a un SI en un periodo de tiempo considerado aceptable.

Un sistema seguro debe mantener la información disponible para los usuarios. Disponibilidad significa que el sistema, tanto hardware como software, se mantienen funcionando eficientemente y que es capaz de recuperarse rápidamente en caso de fallo.
Lo opuesto a disponibilidad, y uno de los posibles métodos de ataque a un sistema informático, se denomina "denegación de servicio" (denial of service). Una denegación de servicio significa que los usuarios no pueden obtener del sistema los recursos deseados:

- El ordenador puede estar estropeado o haber una caída del SO.
- No hay suficiente memoria para ejecutar los programas.
- Los discos, cintas o impresoras no están disponibles o están llenos.
- No se puede acceder a la información.

De hecho, muchos ataques, como el caso del gusano de 1988, no buscaban borrar, robar, o modificar la información, sino bloquear el sistema creando nuevos procesos que saturaban recursos.

1.2.7. Otros aspectos relacionados

Existen otros aspectos o características de la seguridad que pueden en su mayor parte incluirse o asimilarse a uno de los tres aspectos fundamentales, pero que es importante concretar en sí mismos.

Autenticidad.

Esta propiedad permite asegurar el origen de la información. La identidad del emisor puede ser validada, de modo que se puede demostrar que es quien dice ser. De este modo se evita que un usuario envíe una información haciéndose pasar por otro.

Imposibilidad de rechazo (no-repudio)

Esta propiedad permite asegurar que cualquier entidad que envía o recibe información, no puede alegar ante terceros que no la envió o la recibió.
Esta propiedad y la anterior son especialmente importantes en el entorno bancario y en el uso del comercio digital.

Consistencia

Asegurar que el sistema se comporta como se supone que debe hacerlo con los usuarios autorizados. Si el software o el hardware de repente comienza a comportarse de un modo radicalmente diferente al esperado, puede ser un desastre. Por ejemplo si la orden "ls" comenzara a borrar los ficheros listados.
Esta propiedad es amenazada por ejemplo por el uso de los Caballos de Troya. Programas que no hacen lo que se supone que deben hacer, o que además se dedican a otras tareas.

Aislamiento

Regula el acceso al sistema, impidiendo que personas no autorizadas entren en él. Este aspecto está relacionado directamente con la confidencialidad, aunque se centra más en el acceso al sistema que a la información que contiene.

Auditoría

Capacidad de determinar qué acciones o procesos se han llevado a cabo en el sistema, y quién y cuándo las han llevado a cabo.

La única forma de lograr este objetivo es mantener un registro de las actividades del sistema, y que este registro esté altamente protegido contra modificación.
Supone el uso de los denominados ficheros de log en UNIX y en otros sistemas y del uso de sistemas de accounting. Este aspecto se relaciona por un lado con la
Prevención: al conocer los usuarios que se guarda registro de sus actividades, se abstienen de intentar dañar la información. Ello es debido al riesgo que corren de que sus acciones sean detectadas.
Información: Al conocer lo que ocurre en el sistema pueden detectarse comportamientos sospechosos.
Definición a posteriori del problema y su origen: Se puede realizar un análisis post-mortem de la información almacenada para conocer lo que ha ocurrido. Los datos dañados y, en ocasiones, quién y cuándo lo ha hecho. Además, habiendo guardado un registro de las modificaciones ocurridas en el sistema se facilita enormemente la recuperación de este en caso de fallo.

1.3. Política de Seguridad

La política de seguridad es una declaración de intenciones de alto nivel que cubre la seguridad de los SI y que proporciona las bases para definir y delimitar responsabilidades para las diversas actuaciones técnicas y organizativas que se requerirán.
La política se refleja en una serie de normas, reglamentos y protocolos a seguir, donde se definen las distintas medidas a tomar para proteger la seguridad del sistema, las funciones y responsabilidades de los distintos componentes de la organización y los mecanismos para controlar su correcto funcionamiento.
Son los directivos, junto con los expertos en tecnologías de la información, quienes deben definir los requisitos de seguridad, identificando y priorizando la importancia de los distintos elementos de la actividad realizada, con lo que los procesos más importantes recibirán más protección. La seguridad debe considerarse como parte de la operativa habitual, no como un extra añadido.
El compromiso de la Dirección con la SSI debe tomar la forma de una política de seguridad de los SI formalmente acordada y documentada. Dicha política tiene que ser consistente con las prácticas de seguridad de otros departamentos, puesto que muchas amenazas (incendio, inundación) son comunes a otras actividades de la organización.
Algunas reglas básicas a la hora de establecer una política de seguridad.

- Toda política de seguridad debe ser holística, es decir, debe cubrir todos los aspectos relacionados con el sistema.

  Debe proteger el sistema en todos los niveles: físico, humano, lógico y logístico.

  Debe tener en cuenta no sólo los distintos componentes del sistema, tales como el hardware, software, entorno físico y usuarios, sino también la interacción entre los mismos.

  Debe tener en cuenta el entorno del sistema, esto es, el tipo de compañía o entidad con que tratamos (comercial, bancaria, educativa, ...). De esta consideración surge la segunda regla básica
- La política de seguridad debe adecuarse a nuestras necesidades y recursos, el valor que se le da a los recursos y a la información, el uso que se hace del sistema en todos los departamentos.

  Deben evaluarse los riesgos, el valor del sistema protegido y el coste de atacarlo. Las medidas de seguridad tomadas deben ser proporcionales a estos valores.
- Toda política de seguridad debe basarse fundamentalmente en el sentido común. Es necesario:

  Un conocimiento del sistema a proteger y de su entorno.

  Un conocimiento y experiencia en la evaluación de riesgos y el establecimiento de medidas de seguridad.

  Un conocimiento de la naturaleza humana, de los usuarios y de sus posibles motivaciones.

A la hora de establecer una política de seguridad debemos responder a las siguientes tres preguntas:

- ¿ Qué necesitamos proteger?
- ¿ De qué necesitamos protegerlo?
- ¿ Cómo vamos a protegerlo?

lo que nos lleva a los siguientes pasos básicos:

1. Determinar los recursos a proteger y su valor.
2. Analizar las vulnerabilidades y amenazas de nuestro sistema, su probabilidad y su coste.
3. Definir las medidas a establecer para proteger el sistema.

   Estas medidas deben ser proporcionales a lo definido en los pasos 1 y 2.

   Las medidas deben establecerse a todos los niveles: físico, lógico, humano y logístico.

   Además debe definirse una estrategia a seguir en caso de fallo.
4. Monitorizar el cumplimiento de la política y revisarla y mejorarla cada vez que se detecte un problema.

Los pasos 1 y 2 se denominan Análisis de riesgos, mientras los pasos 3 y 4 se denominan Gestión de riesgos. La política de seguridad es el conjunto de medidas establecidas en el paso 3.

1.4. Análisis y Gestión de Riesgos

El objetivo de la SSI es mantener la confidencialidad, integridad y disponibilidad de la información. Una violación de la seguridad es cualquier suceso que compromete estos objetivos. El Análisis y gestión de riesgos es un método formal para investigar los riesgos de un SI y recomendar las medidas apropiadas que deberían adoptarse para controlar estos riesgos.
En toda evaluación de riesgos deben tenerse en cuenta tres costes o valores fundamentales:

Cr: Valor de nuestro sistema informático, esto es, de los recursos y la información a proteger.

Ca: Coste de los medios necesarios para romper las medidas de seguridad establecidas en nuestro sistema.

Cs. Coste de las medidas de seguridad.

Para que la política de seguridad de nuestro sistema sea lógica debe cumplirse la siguiente relación:
Ca > Cr > Cs
El que Ca sea mayor que Cr significa que el ataque a nuestro sistema debe ser más costoso que su valor. Así, los beneficios obtenidos de romper nuestras medidas de seguridad no deben compensar el coste de desarrollar el ataque.
El que Cr sea mayor que Cs significa que no debe costar más proteger la información que la información protegida. Si esto ocurriese, nos resultaría más conveniente no proteger nuestro sistema y volver a obtener la información en caso de perdida.

1.4.1. Evaluación del valor del sistema informático (Cr).

Al evaluar nuestro sistema informático, su valor puede desglosarse en dos partes fundamentales:

- El valor intrínseco del producto a proteger.
- Los costes derivados de su perdida.

Valor intrínseco

Es la parte más sencilla de valorar, puesto que en la mayoría de los casos podemos establecer unos valores objetivos y medibles de nuestros recursos e información. Se trata de enumerar los recursos incluidos en el sistema informático y de establecer su valor.
Por ejemplo, un servidor de un departamento donde trabajan varios grupos de investigación podría valorarse del siguiente modo:

- Valor del hardware. El ordenador y de sus periféricos.
- Valor del software. Programas y aplicaciones.
- Valor de los resultados de investigación, patentes, etc, almacenados.
- Coste del esfuerzo y material invertido para obtener los datos.
- Valor de la información personal que contiene.

Costes derivados

Son bastante más difíciles de enumerar y cuantificar que los anteriores. Dependiendo del tipo de sistema con que tratemos pueden ser muy distintos, o su valor e importancia relativa pueden variar enormemente. En términos generales podemos incluir los siguientes conceptos:

- Valor de sustituir el hardware.
- Valor de sustituir el software.
- Valor de los resultados.
- Coste de reproducir los experimentos significativos.
- Coste de regenerar la información personal.

Para comprender la variabilidad de este tipo de costes consideremos un par de casos.
Si la información perdida incluye los datos de planificación y el desarrollo de una campaña publicitaria en un entorno muy competitivo, p.e. el de las bebidas refrescantes, el valor de los datos perdidos y las consecuencias para la compañía pueden superar con mucho el coste de las horas invertidas o de los recursos utilizados. Existe un valor intangible muy superior al valor material en este tipo de información. Además en este caso puede entrar en juego el prestigio de la compañía. Este factor tiene un valor incalculable de cara a su imagen y a su capacidad de ventas. Si se conoce que los datos han sido robados puede suponer un golpe muy dura para las ventas de la compañía. De hecho esta es la razón por la que muchas compañías comerciales no comunican los ataques a sus sistemas.
El factor prestigio también tiene una importancia capital en las entidades bancarias o en las entidades publicas y sobretodo las de defensa. Imaginemos como reaccionaríamos ante un banco en el que tenemos una cuenta y del que conocemos que han sido robados los datos personales y financieros de todos sus clientes.
Otro ejemplo de la dificultad de valorar ciertas perdidas puede ser el relativo a los datos personales. ¿Qué valor le otorgamos a nuestros datos personales, expedientes académicos, datos sanitarios, información sobre nuestras cuentas o los datos de nuestros seguros, nuestra siniestralidad, morosidad, etc.? Aparte de afectar a nuestro prestigio personal, impedir que abramos una cuenta bancaria o que concertemos un seguro, pueden servir a otros para suplantarnos, y otorgarles impunidad para cometer crímenes o realizar gastos imputándonoslos a nosotros.
En resumen, aunque en principio pueda parecer fácil la valoración de los bienes protegidos, pueden existir numerosos costes ocultos inherentes a su pérdida o compromiso que sólo un análisis detallado puede revelar y que a menudo requieren una valoración por alguien con experiencia en seguridad en conjunción con expertos especializados en el tratamiento de los bienes protegidos.

1.4.2. Vulnerabilidad, amenazas y contramedidas

Hay tres conceptos que entran en discusión cuando hablamos de la seguridad de un sistema informático: vulnerabilidad o inseguridad (vulnerability), amenazas (threat) y contramedidas (countermesures).

Vulnerabilidad.

Punto o aspecto del sistema que es susceptible de ser atacado o de dañar la seguridad del mismo. Representan las debilidades o aspectos falibles o atacables en el sistema informático.

Amenaza.

Posible peligro del sistema. Puede ser una persona (cracker), un programa (virus, caballo de Troya, ...), o un suceso natural o de otra índole (fuego, inundación, etc.). Representan los posibles atacantes o factores que aprovechan las debilidades del sistema.

Contramedida.

Técnicas de protección del sistema contra las amenazas.

La seguridad informática se encarga de la identificación de las vulnerabilidades del sistema y del establecimiento de contramedidas que eviten que las distintas amenazas posibles exploten dichas vulnerabilidades. Una máxima de la seguridad informática es que: "No existe ningún sistema completamente seguro". Existen sistemas más o menos seguros, y más o menos vulnerables, pero la seguridad nunca es absoluta.

1.4.3. Tipos de vulnerabilidad

Realmente la seguridad es la facultad de estar a cubierto de algún riesgo o amenaza. Desde este punto de vista la seguridad total es muy difícil de logra, puesto que implicaría describir todos los riesgos y amenazas a que puede verse sometido el sistema. Lo que se manifiesta en los sistemas no es la seguridad, sino más bien la inseguridad o vulnerabilidad. No se puede hablar de un sistema informático totalmente seguro, sino más bien de uno en el que no se conocen tipos de ataques que puedan vulnerarlo, debido a que se han establecido medidas contra ellos.

Algunos tipos de vulnerabilidad de un sistema son los siguientes:

Vulnerabilidad física.

Se encuentra en el nivel del edificio o entorno físico del sistema. Se relaciona con la posibilidad de entrar o acceder físicamente al sistema para robar, modificar o destruir el mismo.

Vulnerabilidad natural.

Se refiere al grado en que el sistema puede verse afectado por desastres naturales o ambientales que pueden dañar el sistema, tales como el fuego, inundaciones, rayos, terremotos, o quizás más comúnmente, fallos eléctricos o picos de potencia. También el polvo, la humedad o la temperatura excesiva son aspectos a tener en cuenta.

Vulnerabilidad del hardware y del software.

Desde el punto de vista del hardware, ciertos tipos de dispositivos pueden ser más vulnerables que otros. Así, ciertos sistemas requieren la posesión de algún tipo de herramienta o tarjeta para poder acceder a los mismos.

Ciertos fallos o debilidades del software del sistema hacen más fácil acceder al mismo y lo hacen menos fiable. En este apartado se incluyen todos los bugs en los sistemas operativos, u otros tipos de aplicaciones que permiten atacarlos.

Vulnerabilidad de los medios o dispositivos.

Se refiere a la posibilidad de robar o dañar los discos, cintas, listados de impresora, etc.

Vulnerabilidad por emanación.

Todos los dispositivos eléctricos y electrónicos emiten radiaciones electromagnéticas. Existen dispositivos y medios de interceptar estas emanaciones y descifrar o reconstruir la información almacenada o transmitida.

Vulnerabilidad de las comunicaciones.

La conexión de los ordenadores a redes supone sin duda un enorme incremento de la vulnerabilidad del sistema. Aumenta enormemente la escala del riesgo a que está sometido, al aumentar la cantidad de gente que puede tener acceso al mismo o intentar tenerlo. También se añade el riesgo de intercepción de las comunicaciones:

- Se puede penetrar al sistema a través de la red.
- Interceptar información que es transmitida desde o hacia el sistema.

Vulnerabilidad humana.

La gente que administra y utiliza el sistema representa la mayor vulnerabilidad del sistema. Toda la seguridad del sistema descansa sobre el administrador del mismo que tiene acceso al máximo nivel y sin restricciones al mismo.

Los usuarios del sistema también suponen un gran riesgo al mismo. Ellos son los que pueden acceder al mismo, tanto físicamente como mediante conexión. Existen estudios que demuestran que más del 50% de los problemas de seguridad detectados son debidos a los usuarios de los mismos.

Por todo ello hay una clara diferenciación en los niveles de los distintos tipos de vulnerabilidad y en las medidas a adoptar para protegerse de ellos.

1.4.4. Tipos de amenazas

Las amenazas al sistema informático pueden también clasificarse desde varios puntos de vista.

En una primera clasificación según el efecto causado en el sistema, las amenazas pueden englobarse en cuatro grandes tipos: intercepción, modificación, interrupción y generación. Vamos a verlas con más detalle.

Intercepción.

Cuando una persona, programa o proceso logra el acceso a una parte del sistema a la que no está autorizada. Ejemplos:

- Escucha de una línea de datos.
- Copias de programas o ficheros de datos no autorizados.

Son los más difíciles de detectar pues en la mayoría de los casos no alteran la información o el sistema.

Modificación.

Se trata no sólo de acceder a una parte del sistema a la que no se tiene autorización, sino, además, de cambiar en todo o en parte su contenido o modo de funcionamiento. Ejemplos:

- Cambiar el contenido de una base de datos.
- Cambiar líneas de código en un programa.
- Cambiar datos en una transferencia bancaria.

Interrupción.

Interrumpir mediante algún método el funcionamiento del sistema. Ejemplos:

- Saturar la memoria o el máximo de procesos en el sistema operativo.
- Destruir algún dispositivo hardware.

Puede ser intencionada o accidental.

Generación.

Se refiere a la posibilidad de añadir información o programas no autorizados en el sistema. Ejemplos:

- Añadir campos y registros en una base de datos.
- Añadir código en un programa (virus).
- Introducir mensajes no autorizados en una línea de datos.

Como puede observarse, la vulnerabilidad de los sistemas informáticos es muy grande, debido a la variedad de los medios de ataque o amenazas. Fundamentalmente hay tres aspectos que se ven amenazados: el hardware (el sistema), el software (programas de usuarios, aplicaciones, bases de datos, sistemas operativos, etc.), los datos.
Desde el punto de vista del origen de las amenazas, estas pueden clasificarse en: naturales, involuntarias e intencionadas.

Amenazas naturales o físicas.

Son las que ponen en peligro los componentes físicos del sistema. En ellas podemos distinguir por un lado los desastres naturales, como las inundaciones, rayos o terremotos, y las condiciones medioambientales, tales como la temperatura, humedad, presencia de polvo.
Entre este tipo de amenazas, una de las más comunes es la presencia de un usuario sentado delante del ordenador con su lata de bebida refrescante y su bocadillo cerca del teclado o la unidad central .

Amenazas involuntarias.

Son aquellas relacionadas con el uso descuidado del equipo por falta de entrenamiento o de concienciación sobre la seguridad. Entre las más comunes podemos citar:

- Borrar sin querer parte de la información,
- Dejar sin protección determinados ficheros básicos del sistema
- Dejar pegado a la pantalla un post-it con nuestro password u olvidarnos de salir del sistema.

Amenazas intencionadas.

Son aquellas procedentes de personas que pretenden acceder al sistema para borrar, modificar o robar la información; para bloquearlo o por simple diversión.
Los causantes del daño pueden ser de dos tipos: internos y externos.
Los externos pueden penetrar al sistema de múltiples formas:

- Entrando al edificio o accediendo físicamente al ordenador.
- Entrando al sistema a través de la red explotando las vulnerabilidades software del mismo.
- Consiguiendo acceder a través de personas que lo tienen de modo autorizado.

Los internos pueden ser de tres tipos: empleados despedidos o descontentos, empleados coaccionados, y empleados que obtienen beneficios personales.

1.4.5. Tipos de medidas de seguridad o contramedidas

Los sistemas informáticos pueden diseñarse de acuerdo con criterios de economía, de eficiencia y de eficacia, etc., porque son claramente medibles y se asocian a parámetros que, maximizando unos y minimizando otros, se puede tender hacia diseños óptimos.
Diseñar sistemas mediante criterios de seguridad es más complejo, pues las amenazas son en muchos casos poco cuantificables y muy variadas. La aplicación de medidas para proteger el sistema supone un análisis y cuantificación previa de los riesgos o vulnerabilidades del sistema. La definición de una política de seguridad y su implementación o través de una serie de medidas.
En muchos casos las medidas de seguridad llevan un costo aparejado que obliga a subordinar algunas de las ventajas del sistema. Por ejemplo, la velocidad de las transacciones. En relación a esto, también se hace obvio que a mayores y más restrictivas medidas de seguridad, menos amigable es el sistema. Se hace menos cómodo para los usuarios ya que limita su actuación y establece unas reglas más estrictas que a veces dificultan el manejo del sistema. Por ejemplo, el uso de una política adecuada de passwords, con cambios de las mismas.
Las medidas de seguridad que pueden establecerse en un sistema informático son de cuatro tipos fundamentales: lógicas, físicas, administrativas y legales. Vamos a verlas con más detalle.

Figura 1.1: Medidas de Seguridad

Medidas físicas

Aplican mecanismos para impedir el acceso directo o físico no autorizado al sistema. También protegen al sistema de desastres naturales o condiciones medioambientales adversas. Se trata fundamentalmente de establecer un perímetro de seguridad en nuestro sistema.
Existen tres factores fundamentales a considerar:

- El acceso físico al sistema por parte de personas no autorizadas
- Los daños físicos por parte de agentes nocivos o contingencias
- Las medidas de recuperación en caso de fallo

Concretando algo más los tipos de controles que se pueden establecer, estos incluyen:

- Control de las condiciones medioambientales (temperatura, humedad, polvo, etc....)
- Prevención de catástrofes (incendios, tormentas, cortes de fluido eléctrico, sobrecargas, etc.)
- Vigilancia (cámaras, guardias jurados, etc.)
- Sistemas de contingencia (extintores, fuentes de alimentación ininterrumpida, estabilizadores de corriente, fuentes de ventilación alternativa, etc.)
- Sistemas de recuperación (copias de seguridad, redundancia, sistemas alternativos geográficamente separados y protegidos, etc.)
- Control de la entrada y salida de material (elementos desechables, consumibles, material anticuado, etc.)

Medidas lógicas

Incluye las medidas de acceso a los recursos y a la información y al uso correcto de los mismos, así como a la distribución de las responsabilidades entre los usuarios. Se refiere más a la protección de la información almacenada.

Entre los tipos de controles lógicos que es posible incluir en una política de seguridad podemos destacar los siguientes:

- Establecimiento de una política de control de accesos. Incluyendo un sistema de identificación y autentificación de usuarios autorizados y un sistema de control de acceso a la información.
- Definición de una política de instalación y copia de software.
- Uso de la criptografía para proteger los datos y las comunicaciones.
- Uso de cortafuegos para proteger una red local de Internet.
- Definición de una política de copias de seguridad.
- Definición de una política de monitorización (logging) y auditoria (auditing) del sistema.

Dentro de las medidas lógicas se incluyen también aquellas relativas a las personas y que podríamos denominar medidas humanas. Se trata de definir las funciones, relaciones y responsabilidades de distintos usuarios potenciales del sistema. Se trataría entonces de responder a preguntas tales como:

- ¿ A quién se le permite el acceso y uso de los recursos?
- ¿ Qué recursos puede acceder cada usuario y qué uso puede hacer de ellos?
- ¿ Cuáles son las funciones del administrador del sistema y del administrador de la seguridad?
- ¿ Cuáles son los derechos y responsabilidades de cada usuario?

A la hora de responder a las preguntas anteriores hemos de diferenciar cuatro tipos fundamentales de usuarios. A cada tipo se le aplicará una política de control de accesos distinta y se le imputaran distinto grado de responsabilidades sobre el sistema:

- El administrador del sistema y en su caso el administrador de la seguridad.
- Los usuarios del sistema.
- Las personas relacionadas con el sistema pero sin necesidad de usarlo
- Las personas ajenas al sistema

Medidas administrativas

Las medidas administrativas son aquellas que deben ser tomada por las personas encargadas de definir la política de seguridad para ponerla en práctica, hacerla viable y vigilar su correcto funcionamiento. Algunas de las medidas administrativas fundamentales a tomar son las siguientes:

- Documentación y publicación de la política de seguridad y de las medidas tomadas para ponerla en práctica.
- Debe quedar claro quien fija la política de seguridad y quien la pone en práctica.
- Establecimiento de un plan de formación del personal.

  Los usuarios deben tener los conocimientos técnicos necesarios para usar la parte del sistema que les corresponda. Este tipo de conocimiento son fundamentales para evitar toda una serie de fallos involuntarios que pueden provocar graves problemas de seguridad.

  Los usuarios deben ser conscientes de los problemas de seguridad de la información a la que tienen acceso.

  Los usuarios deben conocer la política de seguridad de la empresa y las medidas de seguridad tomadas para ponerla en práctica. Además deben colaborar, a ser posible voluntariamente, en la aplicación de las medidas de seguridad.

  Los usuarios deben conocer sus responsabilidades respecto al uso del sistema informático, y deben ser conscientes de las consecuencias de un mal uso del mismo.

Medidas legales

Se refiere más a la aplicación de medidas legales para disuadir al posible atacante o para aplicarle algún tipo de castigo a posteriori.

Este tipo medidas trascienden el ámbito de la empresa y normalmente son fijadas por instituciones gubernamentales e incluso instituciones internacionales. Un ejemplo de este tipo de medidas es la LORTAD (Ley Orgánica de Regulación del Tratamiento Automatizado de Datos de Carácter Personal). Esta ley vincula a todas las entidades que trabajen con datos de carácter personal, define las medias de seguridad para su protección y las penas a imponer en caso de su incumplimiento.

1.4.6. Planes de contingencia

Al hablar de políticas de seguridad hay que contemplar tanto la prevención como la recuperación. La mayor parte de las medidas de las que hemos hablado hasta este momento se refieren a la prevención ante posibles amenazas. Sin embargo, y como ya hemos comentado anteriormente, ningún sistema es completamente seguro, y por tanto hay que definir una estrategia a seguir en caso de fallo o desastre. De hecho los expertos de seguridad afirman sutilmente que hay que definir un plan de contingencia para cuando falle el sistema, no por si falla el sistema.

La clave de una buena recuperación en caso de fallo es una preparación adecuada. Por recuperación entendemos tanto la capacidad de seguir trabajando en un plazo mínimo después de que se haya producido el problema, como la posibilidad de volver a la situación anterior al mismo habiendo reemplazado o recuperado el máximo de los recursos y de la información.

Adicionalmente existen otros aspectos relacionados con la recuperación como son la detección del fallo, la identificación del origen del ataque y de los daños causados al sistema y la toma de medidas a posteriori contra el

atacante. Todo ello se basa en buena medida en el uso de una adecuada política de monitorización y auditoria del sistema.
La recuperación de la información se basa en el uso de una política de copias de seguridad adecuada, mientras la recuperación del funcionamiento del sistema se basa en la preparación de unos recursos alternativos.
Una buena política de copias de seguridad debe contemplar los siguientes aspectos:

- Qué tipos de backups se realizan: completos o incrementales.
- Con qué frecuencia se realiza cada tipo de backup.
- Cuántas copias se realizan y dónde se guardan.
- Durante cuánto tiempo se guardan las copias.

Dependiendo del tipo de compañía puede ser necesario recuperar el funcionamiento en un plazo más o menos breve. A un banco por ejemplo le interesa volver a funcionar en unas pocas horas, mientras otros tipos de empresas pueden esperar un plazo mayor. Todo depende del uso que se haga del sistema y de las perdidas que suponga no tenerlo en funcionamiento.
Las compañías pueden mantener o contratar dos tipos de instalaciones alternativas: frías (cold site) o calientes (hot site).
Una instalación fría consiste en un lugar con las medidas de seguridad física disponibles, donde poder instalar el hardware y el software y funcionar en menos de una semana. Una instalación caliente incluye además ordenadores, periféricos, líneas de comunicaciones y otros medios e incluso personal para volver a funcionar en unas pocas horas.

1.5. Principios fundamentales de la Seguridad Informática

En el ámbito de la seguridad informática existen una serie de principios básicos que es necesario tener en cuenta al diseñar cualquier política de seguridad. Veamos algunos de los fundamentales:

* Principio de menor privilegio

Este es quizás el principio más fundamental de la seguridad, y no solamente de la informática. Básicamente, el principio de menor privilegio afirma que cualquier objeto (usuario, administrador, programa, sistema, etc.) debe tener tan solo los privilegios de uso necesarios para desarrollar su tarea y ninguno más. Esto quiere decir que cualquier usuario tan solo debe poder acceder a los recursos que necesite, para realizar las tareas que tenga encomendadas y sólo durante el tiempo necesario.
Al diseñar cualquier política de seguridad es necesario estudiar las funciones de cada usuario, programa, etc., definir los recursos a los que necesita acceder para llevarlas a cabo, identificar las acciones que necesita realizar con estos recursos, y establecer las medidas necesarias para que tan solo pueda llevar a cabo estas acciones.
Por ejemplo, en un sistema UNIX el usuario necesita acceder al fichero /etc/passwd, donde normalmente se guarda su password, para poder entrar al sistema. Sin embargo, durante el resto de su trabajo en el sistema no necesita acceder a los passwords. Siguiendo el principio de menor privilegio debería evitarse este acceso o bien situar los passwords cifrados en otro fichero. De hecho la mayoría de los sistema UNIX no aplican esta medida de seguridad y permiten que cualquier usuario pueda consultar todos los passwords cifrados en cualquier momento.

* La seguridad no se obtiene a través de la oscuridad

Un sistema no es más seguro porque escondamos sus posibles defectos o vulnerabilidades, sino porque los conozcamos y corrijamos estableciendo las medidas de seguridad adecuadas. El hecho de mantener posibles errores o vulnerabilidades en secreto no evita que existan, y de hecho evita que se corrija.
No es una buena medida basar la seguridad en el hecho de que un posible atacante no conozca las vulnerabilidades de nuestro sistema. Los atacantes siempre disponen de los medios necesarios para descubrir las debilidades más insospechadas de nuestro sistema.
No se consigue proteger un sistema evitando el acceso de los usuarios a la información relacionada con la seguridad. Por ejemplo, evitando el acceso a determinados manuales donde se especifican las ordenes que pueden utilizarse para entrar en el sistema. Educar a los usuarios o diseñadores sobre el funcionamiento del sistema y las medidas de seguridad incluidas, suele ser mejor método para protegerlo.
No obstante tampoco se trata de hacer público en las noticias un nuevo fallo de nuestro sistema o un método para romperlo. En primer lugar hay que intentar resolverlo, obtener un medio para eliminar la vulnerabilidad y luego publicar el método de protección.

* Principio del eslabón más débil

En todo sistema de seguridad, el máximo grado de seguridad es aquel que tiene su eslabón más débil. Al igual que en la vida real la cadena siempre se rompe por el eslabón más débil, en un sistema de seguridad el atacante siempre acaba encontrando y aprovechando los puntos débiles o vulnerabilidades.
Cuando diseñemos una política de seguridad o establezcamos los mecanismos necesarios para ponerla en práctica, debemos contemplar todas las vulnerabilidades y amenazas. No basta con establecer unos mecanismos muy fuertes y complejos en algún punto en concreto, sino que hay que proteger todos los posibles puntos de ataque.
Por ejemplo, supongamos que establecemos una política de asignación de passwords muy segura, en la que estos se asignan automáticamente, son aleatorios y se cambian cada semana. Si en nuestro sistema utilizamos la red ethernet para conectar nuestras máquinas, y no protegemos la conexión, no nos servirá de nada la política de passwords establecidas. Por defecto, por ethernet los passwords circulan descifrados. Si cualquiera puede acceder a nuestra red y "escuchar" todos los paquetes que circulan por la misma, es trivial que pueda conocer nuestros passwords. En este sistema el punto débil es la red. Por mucho que hayamos reforzado la seguridad en otros puntos, el sistema sigue siendo altamente vulnerable.

* Defensa en profundidad

La seguridad de nuestro sistema no debe depender de un solo mecanismo por muy fuerte que este sea, sino que es necesario establecer varias mecanismos sucesivos. De este modo cualquier atacante tendrá que superar varias barreras para acceder a nuestro sistema.
Por ejemplo en nuestro sistema podemos establecer un mecanismo de passwords altamente seguro como primera barrera de seguridad. Adicionalmente podemos utilizar algún método criptográfico fuerte para cifrar la información almacenada. De este modo cualquier atacante que consiga averiguar nuestro password y atravesar la primera barrera, se encontrará con la información cifrada y podremos seguir manteniendo su confidencialidad.
* Punto de control centralizado
Se trata de establecer un único punto de acceso a nuestro sistema, de modo que cualquier atacante que intente acceder al mismo tenga que pasar por él. No se trata de utilizar un sólo mecanismo de seguridad, sino de "alinearlos" todos de modo que el usuario tenga que pasar por ellos para acceder al sistema.
Este único canal de entrada simplifica nuestro sistema de defensa, puesto que nos permite concentrarnos en un único punto. Además nos permite monitorizar todos los accesos o acciones sospechosas.
* Seguridad en caso de fallo
Este principio afirma que en caso de que cualquier mecanismo de seguridad falle, nuestro sistema debe quedar en un estado seguro. Por ejemplo, si nuestros mecanismos de control de acceso al sistema fallan, es mejor que como resultado no dejen pasar a ningún usuario que que dejen pasar a cualquiera aunque no esté autorizado.
Quizás algunos ejemplos de la vida real nos ayuden más a aclarar este concepto. Normalmente cuando hay un corte de fluido eléctrico los ascensores están preparados para bloquearse mediante algún sistema de agarre, mientras que las puertas automáticas están diseñadas para poder abrirse y no quedar bloqueadas.
* Participación universal
Para que cualquier sistema de seguridad funcione es necesaria la participación universal, o al menos no la oposición activa, de los usuarios del sistema. Prácticamente cualquier mecanismo de seguridad que establezcamos puede ser vulnerable si existe la participación voluntaria de algún usuario autorizado para romperlo.
La participación voluntaria de todos los usuarios en la seguridad de un sistema es el mecanismo más fuerte conocido para hacerlo seguro. Si todos los usuarios prestan su apoyo y colaboran en establecer las medidas de seguridad y en ponerlas en práctica el sistema siempre tenderá a mejorar.
* Simplicidad
La simplicidad es un principio de seguridad por dos razones. En primer lugar, mantener las cosas lo más simples posibles, las hace más fáciles de comprender. Si no se entiende algo, difícilmente puede saberse si es seguro. En segundo lugar, la complejidad permite esconder múltiples fallos. Los programas más largos y complejos son propensos a contener múltiples fallos y puntos débiles.
Documento creado en Agosto de 2001
Autor : Heinekn Team (www.heinekenteam.com.ar)
Bajado de : www.softdownload.com.ar