

La necesidad de proteger la información.

www.g2security.com Disponer de información cuyo conocimiento no está generalizado permite usarla y manipularla en beneficio propio. El conocimiento, en todos los sentidos, es poder

Para las personas que poseen y custodian ese conocimiento, que normalmente se traduce en datos y en estos tiempos, los datos se almacenan habitualmente en formato magnético, esto es, ficheros en discos duros. Para estas personas, digo, es necesario estudiar los procedimientos que hacen la información ininteligible a toda persona no autorizada que ellos designen como tal. Por supuesto, este estudio incluye una proporcionalidad entre los medios necesarios para su obtención y el beneficio previsto. Es decir, según la valía de la información para otras personas, así serán las medidas a tomar. La mejora de los medios para transmitir y utilizar la información, la ingente conectividad existente entre dispositivos informáticos (ahí tenemos la world wide web, que supone la mayor telaraña de dispositivos interconectados del mundo) ha aumentado la amenaza de inseguridad para esa información. Los sistemas informáticos cada vez más complejos, tienen cada vez más puntos débiles debido simplemente a su mayor dimensión, pues el número de posibles atacantes crece (también debido a la mayor conectividad) y los medios disponibles para vulnerar un sistema son más sofisticados.

La Ley de Moore (visionario que predijo que la capacidad de los procesadores se duplica cada año y medio) se lleva cumpliendo desde hace más de treinta años, y es difícil predecir su defunción. Esta misma ley se puede aplicar hoy en día a los anchos de banda, a la potencia, a la memoria....

Posibles amenazas a un sistema informático.

Un sistema informático, como todos sabemos, se compone de hardware, software, personal dedicado y de lo más importante, datos (el motivo de todo el sistema). Deben permitir tres operaciones principales. Almacenamiento, procesamiento y transmisión de esa información. En el almacenamiento y en la transmisión están sobretodo los puntos clave para que esa información pertenezca solamente a su dueño.

Los posibles tipos de ataques pueden englobarse en cuatro grandes tipos:

Intercepción: Una persona, programa o proceso accede a una parte del sistema a la que no está autorizado. Es difícil de detectar (sniffers, keyloggers...)

Modificación: Además de tener acceso, modifica, destruye, reemplaza o cambia los datos o el funcionamiento del sistema.

Interrupción: Consiste en impedir que la información llegue a su destino. Es bastante fácil de detectar pero igual de difícil que los anteriores de evitar.

Generación. Se refiere a la posibilidad de incluir campos y registros en una base de datos, añadir líneas de código a un programa, añadir programas completos en un sistema (virus), introducir mensajes no autorizados por una línea de datos...

Los elementos vulnerables a estos ataques son todos los que componen un sistema informático, esto

es, como ya hemos dicho, hardware de software, personal dedicado y datos.

Ataques al hardware: Se pueden producir de forma intencionada o no. Incendios fortuitos en los sistemas, fallos físicos, rotura física de cables....

Ataques al software: Se pueden centrar contra los programas del sistema operativo, a los programas de utilidad o a los programas de usuario. Necesita de mayores conocimientos técnicos (para los ataques hardware, por ejemplo, bastaría con unas tijeras, un mazo... cerillas...) Existe gran variedad de ataques software:

Bomba lógica: el programa incluye instrucciones que, al cumplirse una condición, provocan una distorsión del funcionamiento normal del programa, que normalmente, deriva en daños al ordenador que lo ejecuta. Esta técnica es usada por algunos programadores. Introducen en la aplicación un código que se activa en una fecha determinada para que, si no ha cobrado por su trabajo ese día, destruya la información del ordenador en el que ha sido instalado.

Virus. Todos sabemos lo que son, cómo se comportan e incluso habremos sufrido sus consecuencias. Hoy en día, la conectividad entre ordenadores hace que existan muchísimos más de los 30 o 40 mil conocidos a finales de los 80, y que su impacto, cuando logran trascender, sea mucho mayor.

Gusanos. Son programas que se replican, la línea que los separa de los virus es muy delgada.

Backdoors o puertas falsas: Son programas que permiten la entrada en el sistema de manera que el usuario habitual del mismo no tenga conocimiento de este ataque.

Caballos de Troya: El objetivo de estos programas no es el mismo para el que aparentemente están diseñados. Se utilizan normalmente para instalar puertas traseras.

Ataques al personal: Aunque lo parezca, no consiste en perseguir con un cuchillo a los administradores. Se suele conocer más como ingeniería social. Consiste realmente en mantener un trato social con las personas que custodian datos. Indagar en sus costumbres o conocerlas más profundamente para perpetrar posteriormente un ataque más elaborado. La ingeniería social incluye desde suplantación de identidades confiables hasta la búsqueda en papeleras y basuras de información relevante.

Criterios para establecer la seguridad de la información.

Son las características fundamentales al establecer la seguridad de la información. La información custodiada, almacenada, emitida o procesada, debería cumplir estos requisitos.

Confidencialidad: La información disponible sólo para los usuarios autorizados a manejarla. Puede ser accesible a atacantes, pero no sabrán interpretarlas o entenderlas. Este servicio proporciona protección contra la revelación deliberada o accidental de los datos en una comunicación.

Integridad: Este servicio garantiza que los datos recibidos por el receptor de una comunicación coinciden con los enviados por el emisor. Garantiza que la información no se falsea y que se ha mantenido intacta.

Autenticidad: Asegurar el origen y destino de la información.

No Repudio: Quién envía no puede alegar que no envió los datos.

Disponibilidad: Asegura que el sistema de computación esté disponible a las partes autorizadas siempre que sea requerido, y no existan problemas de caídas, cuelgues o funcionamiento dudoso de los máquina que prestan los servicios.

Control de acceso: Este servicio se utiliza para evitar el uso no autorizado de recursos. Incluiría la autenticación sobre la que ya he hablado en otros artículos.

Normalmente, los mecanismos que pueden proporcionar alguna de estas características proporcionan más de una al mismo tiempo, por ejemplo, control de acceso y autenticidad están muy relacionados.

Aún estableciendo estos servicios de seguridad, no se puede asegurar la invulnerabilidad de la información, pues existe el problema de los protocolos. Esto es, los pasos que hay que tomar entre dos interlocutores para establecer una comunicación segura. Aún si los datos están cifrados y las partes confían una en la otra, si el protocolo no está bien diseñado, la comunicación puede ser interceptada, modificada, interrumpida o generada. Pero los protocolos de comunicación segura, formarán parte de otro artículo.

Sergio de los Santos
s.delossantos@g2security.com

Fecha artículo: 2002-07-31 23:29:16 - url artículo: <http://www.internautas.org/html/42.html>

Logos y marcas propiedad de sus respectivos autores.

Los comentarios son propiedad y responsabilidad de cada autor.

© 1998-2009 Asociación de Internautas - <http://www.internautas.org>

Inscrita en el Registro Nacional de Asociaciones con el número 164343 - e-mail: asociacion@internautas.org