Seminario – Seguridad en desarrollo del Software

Tema: Panorama general de la seguridad informática

Autor: Leudis Sanjuan

Seminario (seguridad en desarrollo del software)

¿Qué es la seguridad informática?

Existen muchas definiciones para este término, pero la más completa que podemos encontrar, para mi concepto, es: La seguridad informática es un conjunto de métodos y herramientas destinados a proteger la información y, por ende, los sistemas informáticos ante cualquier amenaza. En esta definición hay dos términos muy importantes que debemos destacar: amenaza e información.

Una amenaza es cualquier evento que puede desencadenar un incidente en la organización, produciendo daños materiales o pérdidas inmateriales. En el capítulo siguiente trataremos más a fondo este tema. Por otra parte, encontramos el término información; como bien sabemos, la información es el recurso más importante que tiene una organización. Se debe entender como información en una organización:

- Todo el historial de productos, procesos, procedimientos.
- Todos los mensajes intercambiados (correo, chat…).
- Todo el conjunto de datos y archivos de una empresa.
- Todo el historial de clientes y proveedores.
- En definitiva, el *know-how* de la organización.

Si esta información se pierde o deteriora, le será muy difícil a la empresa recuperarse y seguir en el mercado.

El éxito de una empresa dependerá, entonces, de la calidad de la información que genera y gestiona. Así, una empresa tendrá una información de calidad si ésta posee, entre otras características, la confidencialidad, la integridad, la disponibilidad y en algunos casos el no repudio.

- **Confidencialidad**

La confidencialidad busca prevenir el acceso no autorizado, ya sea en forma intencional o no intencional de la información. La pérdida de la confidencialidad puede ocurrir de muchas maneras, por ejemplo, con la publicación intencional de información confidencial de la organización.

- **Integridad**

El concepto de integridad busca asegurar:

- Que no se realicen modificaciones por personas no autorizadas a los datos, información o procesos.
- Que no se realicen modificaciones no autorizadas por personal autorizado a los datos, información o procesos.
- Que los datos o la información sea consistente tanto interna como externamente.
- **Disponibilidad**

La disponibilidad busca el acceso confiable y oportuno a los datos. Sólo los usuarios autorizados podrán tener acceso a la información.

- **No repudio**

El no repudio significa que un emisor no pueda negar haber remitido un mensaje (cuando realmente lo ha emitido) y que un receptor no pueda negar su recepción (cuando realmente lo ha recibido).

De todo lo que hasta el momento hemos comentado podemos concluir que la información es de vital importancia para las empresas y por tanto se debe proteger. Existen muchas formas de proteger la información y a continuación hablaremos de cada una de ellas.

Seminario (seguridad en desarrollo del software)

1. Copias de seguridad o de respaldo-backup

Como su nombre lo indica, es realizar una copia de la información de la empresa. Las copias de seguridad pueden ser:

- Copia de seguridad completa: se copian todos los datos.
- Copias de seguridad incremental: sólo se copian los archivos creados o modificados desde el último backup.

Igualmente, es importante elaborar un plan de backup en función del volumen de información generada; se deben definir los tipos de copias. ¿Cuál ciclo de esta operación (diaria, semanal, mensual)? ¿Cómo se identificará esta información (etiqueta)? ¿Quién debe realizar la copia? ¿Cómo lo hará? ¿En qué momento se hará? ¿Donde quedarán guardados estos datos?

Sabía usted…

Muchas de las empresas ubicadas en las torres gemelas pudieron ser reconstituidas después del fatal ataque del 11 de septiembre del 2001, con solo recuperar la información que tenían guarda en sus sistemas de backup ubicados fuera de las torres.

2. Políticas de seguridad

Una política de seguridad especifica qué está permitido y a quién se le permite. A esto comúnmente se le conoce con el nombre de control de acceso.

Cuando se define una política se debe tener en cuenta:

- A quién se le da acceso.
- De qué naturaleza es este y quién lo autoriza.

- Quién es el responsable de la seguridad, de las actualizaciones, de realizar las copias de respaldo o backup.
- Qué tipo de servicios están permitidos.
- A qué sitios y usuarios externos se les permite el acceso a los recursos.
- Cómo y cuándo deben actualizarse las políticas.

Un usuario tiene acceso a los recursos de acuerdo al rol que tenga asignado; un rol debe ser definido de acuerdo a las funciones de trabajo, y los permisos que se le otorgan al usuario deben ser definidos en función de la autoridad y responsabilidad que este debe asumir.

Muchas veces se agrupa un conjunto de usuarios bajo un mismo grupo, esto es un conjunto de usuarios que comparten los mismos privilegios o permisos.

3. Seguridad a nivel de redes

A nivel de redes existen varias formas de proteger los sistemas. A continuación se explican algunas de ellas:

- **Uso de *Firewalls***. Un *firewall* es un elemento de hardware o software utilizado en una red de computadores para controlar las comunicaciones, permitiéndolas o prohibiéndolas según las políticas de red que haya definido la organización responsable de la red.

  La ubicación habitual de un *firewalls* es el punto de conexión de la red interna de la organización con la red exterior, que normalmente es Internet; de este modo se protege la red interna de intentos de acceso no autorizados desde Internet, que puedan aprovechar vulnerabilidades de los sistemas de la red interna.

Para que sirve un *firewalls*

- Protege contra accesos no autenticados desde el exterior.
- Protege contra tráfico no autorizado desde el exterior.
- Permite la salida a servicios desde el interior de una institución.
- Proporciona un único punto para implantar una política de seguridad y auditoría.

Para que NO sirve un *firewalls*

- Para proteger contra ataques desde el interior.
- Para proteger contra virus, troyanos, túneles…
- Para proteger contra salida de información por otros medios como CD, memorias.

- **Arquitectura DMZ**: los sistemas *firewall* permiten definir las reglas de acceso entre dos redes; en la práctica, sin embargo, las empresas cuentan generalmente con varias subredes con diferentes políticas de seguridad. Por esta razón, es necesario configurar arquitecturas de *firewall* que aíslen las diferentes redes de una compañía. Esto se denomina "aislamiento de la red" o DMZ.

  [1]Cuando algunas máquinas de la red interna deben ser accesibles desde una red externa (servidores Web, servidores de correo electrónico, servidores FTP); a veces es necesario crear una nueva interfaz hacia una red separada a la que se pueda acceder tanto desde la red interna como por vía externa sin correr el riesgo de comprometer

[1] [1] Tomado de: http://es.kioskea.net/contents/protect/dmz-cloisonnement.php3

la seguridad de la compañía. El término "zona desmilitarizada" o DMZ hace referencia a esta zona aislada que posee aplicaciones disponibles para el público.

Por lo general, la política de seguridad para la DMZ es la siguiente:

- El tráfico de la red externa a la DMZ está autorizado
- El tráfico de la red externa a la red interna está prohibido
- El tráfico de la red interna a la DMZ está autorizado
- El tráfico de la red interna a la red externa está autorizado
- El tráfico de la DMZ a la red interna está prohibido
- El tráfico de la DMZ a la red externa está denegado

De esta manera, la DMZ posee un nivel de seguridad intermedio, el cual no es lo suficientemente alto para almacenar datos imprescindibles de la compañía.

Debe observarse que es posible instalar las DMZ en forma interna para aislar la red interna con niveles de protección variados y así evitar intrusiones internas.

- **Minimización de servicios.** Otra forma de asegurar la información consiste en reducir el riesgo de ataque minimizando servicios que se ofrecen.

Servicios	Motivo
DNS	Existen implementaciones de este servicio que pueden usarse para desproteger un servidor.

SMTP	Errores en *sendmail* y otros programas que interrumpen el sistema.
Finger	Este protocolo puede usarse para obtener información del SO.
Netstat, systtat	Pueden revelar la configuración y patrones del uso del sistema
Chargen, echo	Pueden iniciar ataques dirigidos por los datos y de negación de servicios.
FTP	El ftp estándar envía información sin encriptar.
Telnet	No se debe permitir sesiones interactivas a menos que sea un administrador. Se debe usar telnet con encriptación (ssh o telnet kerberizado) o un sistema de clave de acceso no reutilizable S/Key, Security ID.
Comandos: rlogin, rsh	Estos comandos utilizan direcciones IP para autenticarse.

Tabla 1: Servicios que pueden ser riesgosos

- **VPN (*Virtual Private Network* o Red Privada Virtual)**

  Las redes privadas virtuales son tecnologías que permiten la extensión de las redes de área local o LAN (redes internas de las empresas),

sobre redes externas. Con ellas se hace posible el acceso de usuarios remotos a redes de área local como si estuvieran en la misma empresa.

Para que sirve una VPN

- Permite la autenticación; es decir, comprobar la identidad de los servidores que intervienen en la comunicación (no comprueba la identidad de los usuarios).
- Permite la privacidad de las comunicaciones.
- Proporciona un canal de comunicaciones seguro a través de redes públicas como Internet.
- Permite la extensión de una red corporativa interconectando oficinas o instalaciones geográficamente dispersas.

Usualmente, una VPN usa una tecnología denominada *tunneling* a la hora de establecer la comunicación entre dos puntos. El *tunneling* simplemente hace uso de un protocolo especial (normalmente SSH) para crear un "túnel" por el que circulan todos los datos desde un extremo a otro. Este "túnel" en realidad es la misma información que se manda, pero encriptada por la acción del protocolo seguro de comunicación, lo cual hace que nuestros datos no puedan ser vistos por agentes externos.

Las VPN impiden que usuarios no autorizados puedan ver información; igualmente no permiten la manipulación y la falsificación de las comunicaciones en aplicaciones de Internet.

Sistemas de Detección de Intrusos (IDS) y Sistemas de Prevención de Intrusos (IPS).

IDS (Sistemas de detección de intrusos) consiste en un conjunto de métodos y técnicas para revelar actividades sospechosas sobre un recurso o conjunto de recursos computacionales.

Los IDS tienen dos funciones principales:

1. Detectar los posibles ataques o intrusiones, lo cual se realiza mediante un conjunto de reglas que se aplican sobre los paquetes del tráfico entrante.
2. Registrar todos los eventos sospechosos, añadiendo información útil (como puede ser la dirección IP de origen del ataque), a una base de datos o a un archivos de registro.

Existen dos tipos de IDS:

- Los IDS basados en el *host* (HISD) solamente procesan información de las actividades de los usuarios y servicios en una máquina determinada. Por ejemplo: creación de archivos, llamadas al sistema operativo, llamadas a servicios de red.
- Los IDS basados en la red (NIDS) hacen *snifing* sobre algún punto de la red, analizan el tráfico capturado en busca de intrusiones.

Arquitectura de un IDS[2]

A continuación se describe la arquitectura general de un IDS:

- Fuente de recogida de datos: estas fuentes pueden ser un *log*, dispositivo de red, o como en el caso de los IDS basados en *host*, el propio sistema.

[2] Tomado de : http://www.maestrosdelweb.com/editorial/snort/

- Reglas que contienen los datos y patrones para detectar anomalías de seguridad en el sistema.
- Filtros que comparan los datos snifados de la red o de *logs* con los patrones almacenados en las reglas.
- Detectores de eventos anormales en el tráfico de red.
- Dispositivos generadores de informes y alarmas. En algunos casos con la funcionalidad de enviar alertas vía mail, o SMS.

Snort

Snort es uno de los NIDS más popular. Inicialmente fue desarrollado por Martin Roesh, quien lo llamó de esta forma basado en su rol: "*Sniffer and more*". Actualmente *Snort* es un software de código abierto por *SourceFire*. Mayor información

IPS (Sistemas de Prevención de Intrusos): consiste en dispositivos de hardware o software, encargados de revisar el tráfico de red con el propósito de detectar y responder a posibles ataques o intrusiones.

De alguna manera el comportamiento de los IPS se asemeja al comportamiento de los *firewalls*, ya que ambos toman decisiones con respecto a la aceptación de un paquete de un sistema. Sin embargo, la diferencia radica en el hecho de que los *firewalls* basan sus decisiones en los encabezados del paquete entrante, en particular los de capa de red y transporte, mientras que los IPS basan sus decisiones tanto en los encabezados como en el contenido de datos del paquete.

Para varios autores los sistemas de prevención de intrusos son una evolución de los sistemas de detección de intrusos, particularmente se dice que los primeros ofrecen un manejo más efectivo de las intrusiones

al tiempo que superan las dificultades inherentes de los IDS, en particular, la permisividad de los IDS ante las intrusiones.

El IDS se limita a detectar y notificar la intrusión a la persona encargada de recibir y responder las alertas (en este caso el administrador), quien deberá tomar la acción correctiva pertinente.

Por su parte, una vez el IPS detecta la intrusión la detiene de algún modo. Como quien dice, el IPS se encarga de la situación y genera una alerta sólo si se le configura explícitamente para tal fin o cuando la criticidad del evento lo amerite.

Hay que tener en cuenta que entre los IDS y los IPS hay una categoría especial de IDS que se denominan IDS con respuesta activa, que cumplen la tarea de detener intrusiones, descartando los paquetes del ataque.

Según los autores R.Alder, J.Foster, M.Rash, la principal diferencia entre los IDS con respuesta activa y los IPS es que estos últimos están en capacidad de inutilizar los paquetes involucrados en el ataque, modificando su contenido, pero tal distinción parece no estar muy difundida, y la mayor parte de la bibliografía catalogó los IDS con respuesta activa como un tipo particular de IPS.

- **Protocolos de seguridad**

Un protocolo no es más que un conjunto de reglas formales que permiten a dos dispositivos intercambiar datos de forma no ambigua. Para que este intercambio se efectúe es necesario:

a. Todos los dispositivos deben conocer los pasos del protocolo de antemano.

b. Todos deben estar de acuerdo en seguir el protocolo.

c. El protocolo no debe admitir ambigüedades.

d. El protocolo debe ser completo, o sea, definir qué hacer en cualquier circunstancia posible.

Un protocolo de seguridad define las reglas que son necesarias para que un sistema pueda soportar ataques de carácter malicioso. A nivel de seguridad de redes existen muchos protocolos; para este curso sólo mencionaremos los protocolos de seguridad que existen a nivel de transporte.

Secure Sockets Layer (SSL)

Proporciona autenticación y privacidad de la información entre extremos, sobre Internet, mediante el uso de técnicas de cifrado.

El SSL requiere un protocolo de transporte confiable (e.g. TCP) para transmisión y recepción de datos. La ventaja del protocolo es que es independiente de la aplicación; esto es, un protocolo de aplicación de "nivel superior" (por ejemplo: HTTP, FTP, TELNET, etc) puede colocarse arriba del SSL de manera transparente.

El protocolo se encarga de negociar el algoritmo de encripción y una llave de sesión, también se autentica el servidor antes de que el protocolo de aplicación transmita o reciba el primer byte de datos. Todos los datos del protocolo de aplicación a transmitir son encriptados.

En el primer módulo de cifrado profundizaremos acerca de este tema.

Secure Shell (SSH)

El SSH, o *Secure Shell* es tanto una aplicación como un protocolo que permite conectar dos computadores a través de una red, ejecutar comandos de manera remota y mover archivos entre los mismos.

Proporciona autentificación fuerte y comunicaciones seguras sobre canales no seguros y pretende ser un reemplazo seguro para aplicaciones tradicionales no seguras, como telnet, rlogin, rsh y rcp. Su versión 2 (SSH2) proporciona también sftp, que es un reemplazo seguro para FTP.

Además de esto, SSH permite establecer conexiones seguras a servidores X-Windows, realizar conexiones TCP seguras y realizar acciones como sincronización de sistemas de archivos y copias de seguridad por red, de manera segura.

El SSH permite, además, solventar problemas de seguridad que pueden ocasionarse debido a que los usuarios que tengan acceso como administradores a ordenadores de la red o acceso al punto de red puedan interceptar contraseñas que se transmitan por la red. Esto no puede ocurrir con SSH, ya que SSH nunca envía texto plano, sino que la información siempre viaja cifrada.

Existen dos versiones de SSH (SSH1 y SSH2) con diferentes funcionalidades e incompatibles entre sí (SSH2 soluciona problemas detectados de SSH1).

4. Seguridad a nivel del canal

Hasta el momento hemos mencionado varias técnicas o protocolos que son usados para proteger el canal de comunicación entre dos ordenadores, y hemos mencionado más de una vez el término “cifrado”. Pero, ¿qué significa que la información este cifrada?

Seminario (seguridad en desarrollo del software)

El cifrado es un método que permite aumentar la seguridad de un mensaje o de un archivo mediante la codificación del contenido, de manera que sólo pueda leerlo la persona que cuente con la clave de cifrado adecuada para descodificarlo. Por ejemplo, si realiza una compra a través de Internet, la información de la transacción (como su dirección, número de teléfono y número de tarjeta de crédito) suele cifrarse a fin de mantenerla a salvo. El cifrado se usa cuando se desea un alto nivel de protección de la información.

Por otro lado, la criptografía es la ciencia que utiliza la técnica del cifrado y descifrado para que dos ordenadores puedan intercambiar mensajes que sólo pueden ser vistos de manera privada.

Este curso dedica dos de sus unidades para revisar el tema de cifrado y criptografía. En la primera unidad tiene como objetivo dar a conocer todos los conceptos relacionados con el arte del cifrado y, la segunda unidad, tiene como objetivo dar a conocer cuáles son las mejores prácticas y los aspectos que se deben tener en cuenta para el diseño y desarrollo de aplicaciones seguras.

Seminario (seguridad en desarrollo del software)

Bibliografía

William Stallings, Fundamentos de seguridad en redes

Teresa F. Lunt. Detecting Intruders in Computer Systems. In Proceedings of the Sixth Annual Symposium and Technical Displays on Physical and Electronic Security

S. Kent and R. Atkinson, \Security Architecture for the Internet Protocol," RFC 240

Caballero, P. Introducción a la Criptografía. Ed. Ra-Ma. Madrid.

http://www.fing.edu.uy/inco/cursos/fsi/teorico/2008/FSI-2008-Introduccion.pdf

http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.127.5591&rep=rep1&type=pdf

http://tec.upc.es/sda/Fundamentos%20Criptografia.pdf