



Universidad Nacional de la Matanza

*Departamento de Ingeniería e Investigaciones
Tecnológicas*



Ingeniería en Informática

Taller de SEGURIDAD INFORMATICA

**Estrategias de Privacidad y
Seguridad en PC individuales y
Redes**

MOTIVACION

El área de sistemas de cualquier empresa, ocupa en las últimas dos décadas, y en particular desde la difusión de Internet, un espacio clave en las comunicaciones, por ello se deben conocer las amenazas a la privacidad y seguridad, tanto a nivel de usuario individual, como en redes, con el fin de asegurar integridad, confidencialidad y control en el intercambio de información.

¿PORQUE ES IMPORTANTE ESTE CURSO?

En este curso se podrá obtener conocimiento sobre seguridad y experiencia práctica en detección y prevención de ataques derivados del intercambio de información. Desde un simple mail, una conversación de chat, navegación en Internet, hasta transacciones bancarias online, todo intercambio de datos presenta riesgos que deben ser prevenidos y controlados. Los tiempos del mercado, obligan a mantenerse constantemente actualizados, ya que la información es un bien de intercambio para usuarios particulares y empresas. Los usuarios individuales, necesitan proteger sus datos y documentos personales, y las empresas para funcionar en forma segura, implementan estrategias que tienden a la protección en el tráfico de datos, puesto que la vulnerabilidad en este aspecto, se paga con altos costos materiales o de imagen.

OBJETIVOS:

Aprender los principales conceptos y habilidades relacionados con la seguridad en informática y sus implicaciones para el ambiente Internet. Proporcionar las herramientas, técnicas y conceptos que permitan a los usuarios particulares y encargados de administrar los servicios de información en redes, analizar riesgos de seguridad, prevenir incidentes y detectar ataques y fallas en la seguridad de dichos servicios.

Adquisición de conocimientos acerca de los riesgos que implica el intercambio electrónico de datos, los mecanismos de defensa y el establecimiento de políticas de seguridad.

CONTENIDO

Introducción a la Seguridad Informática. Seguridad Física y Lógica en PC individuales.

Pérdida de archivos y Software de recuperación. Evaluación y configuración de Software Antivirus.

Seguridad y Privacidad en la navegación en Internet. Control de Acceso, confidencialidad, e integridad. Cookies. Monitoreo remoto.

Tráfico de datos invisible al usuario. Firewall de usuario.

Intercambio seguro de la información. Seguridad en Correo Electrónico. SPAM. Criptografía. Métodos de Autenticación. Firma Electrónica. PGP. Transacciones Seguras SSL.

Seguridad en Redes de Area Local. Monitoreo de red y herramientas de libre acceso. Intranet, Extranet. Control de flujo de información mediante Proxy.

Administración de Redes. Detección y protección de intrusos. Redes Privadas Virtuales (VPN). Túneles encriptados.

Privilegios del Administrador de Redes. Derechos del usuario. Etica profesional. Legislación vigente.

REQUISITOS

Sin Requisitos Previos

FECHAS DE PRESENTACIÓN

Sábado 3 de marzo de 2001, a las 11:30 hs.

Sábado 10 de marzo de 2001, a las 13:30 hs.

LUGAR: Laboratorio de Electrónica UNLM

Dictado por:

Ing. Rubén C. Rodriguez

Sr. Miguel Iwanciw

Consultas via E-mail: labelec@uol.com.ar

INTRODUCCION A LA SEGURIDAD INFORMATICA

Antecedentes y definiciones

¿ Qué es la seguridad en cómputo, o seguridad informática ?

En realidad es un concepto cuya definición exacta es difícil de proporcionar, debido a la gran cantidad de factores que intervienen.

Sin embargo es posible enunciar que Seguridad es el conjunto de recursos (metodologías, documentos, programas y dispositivos físicos) encaminados a lograr que los recursos de cómputo disponibles en un ambiente dado, sean accedidos única y exclusivamente por quienes tienen la autorización para hacerlo.

Existe una medida cualitativa para la Seguridad que dice **"Un sistema es seguro si se comporta como los usuarios esperan que lo haga"** (Dr. Eugene Spafford).

PROPIEDADES DE LA INFORMACIÓN QUE PROTEGE LA SEGURIDAD INFORMÁTICA

La Seguridad Informática debe vigilar principalmente por las siguientes propiedades:

Privacidad - La información debe ser vista y manipulada únicamente por quienes tienen el derecho o la autoridad de hacerlo. Un ejemplo de ataque a la Privacidad es la Divulgación de Información Confidencial.

Integridad - La información debe ser consistente, fiable y no propensa a alteraciones no deseadas. Un ejemplo de ataque a la Integridad es la modificación no autorizada de saldos en un sistema bancario o de calificaciones en un sistema escolar.

Disponibilidad - La información debe estar en el momento que el usuario requiera de ella. Un ataque a la disponibilidad es la negación de servicio (En Inglés Denial of Service o DoS) o tirar el servidor

DIVISIÓN DE LAS ÁREAS DE ADMINISTRACIÓN DE LA SEGURIDAD.

Para simplificar, es posible dividir las tareas de administración de seguridad en tres grandes rubros. Estos son:

Autenticación .- Se refiere a establecer las entidades que pueden tener acceso al universo de recursos de cómputo que cierto medio ambiente puede ofrecer.

Autorización .- Es el hecho de que las entidades autorizadas a tener acceso a los recursos de cómputo, tengan efectivamente acceso únicamente a las áreas de trabajo sobre las cuales ellas deben tener dominio.

Auditoría .- Se refiere a la continua vigilancia de los servicios en producción. Entra dentro de este rubro el mantener estadísticas de acceso, estadísticas de uso y políticas de acceso físico a los recursos.

Para ejemplificar lo anterior, tomemos el ejemplo de una compañía ficticia a la que llamaremos "Servicios de Cómputo". Esta compañía dispone de un servidor donde corre el software a través del cual se lleva a cabo el procesamiento de las nóminas y el control de recursos humanos. (Ambos muy relacionados)

Autenticación se refiere a que sólo las personas de esos departamento tengan cuentas de acceso a dichos equipos, puesto que sería peligroso que algún otro departamento lo tuviera. El responsable de los equipos de cómputo llevaría a cabo la labor de Autorización, al no permitir que todas las personas responsables de recursos humanos tuvieran acceso a las Bases de Datos de Nóminas, si no lo necesitan.

La Auditoría se lleva a cabo al establecer políticas de uso y acceso a los recursos, así como reglamentos que rijan la no-divulgación de información confidencial. También aquí se debe llevar un registro de los recursos utilizados para prevenir, por ejemplo, que un uso del 100% en un disco provoque que el sistema deje de funcionar. Debe vigilarse también los intentos de acceso legal e ilegal al mismo.

¿Cómo se pueden clasificar los factores que intervienen en seguridad?

La clasificación dentro de cada una de las áreas arriba expuestas es también un tanto compleja. Pero a grandes rasgos podemos decir que la seguridad en un sistema está determinada por:

EL FACTOR ORGANIZACIONAL:

a) Usuarios

- Tipo de usuarios que se tienen
- Reglamentos y políticas que rigen su comportamiento
- Vigilar que esos reglamentos y políticas se cumplan, y no quede sólo en papel

b) La alta dirección

- Inversión en capacitación de los administradores
- Apoyo económico orientado a la adquisición de tecnología de seguridad
- Negociar acuerdos de soporte técnico con los proveedores de equipo.

EL FACTOR SOFTWARE:

a) La aplicación

- Vigilar que tenga mecanismos para control de acceso integrados
- Observar las facilidades de respaldo de información que se tienen
- Establecer qué tan crítica es la aplicación y desprender su disponibilidad de ahí

b) El sistema operativo

- Mostrar preferencias por los sistemas abiertos (UNIX)
- Vigilar que soporte estándares de seguridad como C2
- Observar las recomendaciones del fabricante y aplicar los parches que libere...
- Vigilar siempre las bitácoras
- Mantenerse informado sobre las alertas de seguridad

c) Software de red

- Vigilar de cerca las estadísticas de acceso y tráfico de la red
- Procurar implementar cortafuegos (firewalls), pero no confiar en ellos
- En la medida de lo posible, apoyar las conexiones cifradas.

EL FACTOR HARDWARE:

a) Hardware de red

- Elegir adecuadamente el tipo de tecnología de transporte (Ethernet, FDDI, etc)
- Proteger muy bien el cableado, las antenas y cualquier dispositivo de red
- Proporcionar periódicamente mantenimiento a las instalaciones

b) Servidores

- Mantenerlos en condiciones de humedad y temperatura adecuadas.
- Establecer políticas de acceso físico al servidor.
- El mantenimiento también es importante aquí.

¿Cuáles serían algunos métodos de protección ?

Por regla general, las políticas son el primer paso que dispone a una organización para entrar en un ambiente de seguridad, puesto que reflejan su voluntad de hacer algo que permita detener un posible ataque antes de que éste suceda (proactividad).

Hecha la aclaración, enumeremos algunos otros métodos:

I - Sistemas de detección de intrusos.- Son sistemas que permiten analizar las bitácoras de los sistemas en busca de patrones de comportamiento o eventos que puedan considerarse sospechosos, en base a la información con la que han sido previamente alimentados. Pueden considerarse como monitores.

II.- Sistemas orientados a conexión de red.- Monitorean las conexiones de red que se intentan establecer con una red o un equipo en particular, siendo capaces de efectuar una acción en base a métricas como: origen de la conexión, destino de la conexión, servicio solicitado, etc. Las acciones que pueden emprender suelen ir desde el rechazo de la conexión hasta alerta al administrador vía correo electrónico o vía pager. En esta categoría están los cortafuegos (firewalls) y los wrappers.

III.- Sistemas de análisis de vulnerabilidades.- Analizan sistemas en busca de vulnerabilidades conocidas anticipadamente. La desventaja de estos sistemas es que pueden ser utilizados tanto por personas autorizadas como por personas que busquen acceso no autorizado al sistema

IV.- Sistemas de protección a la privacidad de la información.-

Herramientas que utilizan criptografía para asegurar que la información sólo es visible a quien tiene autorización de verla. Su aplicación es principalmente en las comunicaciones entre dos entidades. Dentro de este tipo de herramientas podemos situar a Pretty Good Privacy (PGP), Secure Sockets Layer (SSL) y los certificados digitales tipo X.509

V.- Sistemas de protección a la integridad de información.-

Sistemas que mediante criptografía o sumas de verificación tratan de asegurar que no ha habido alteraciones indeseadas en la información que se intenta proteger. Algunos ejemplos son los programas que implementan algoritmos como Message Digest 5 (MD5) o Secure Hash Algorithm 1 (SHA-1), o bien sistemas que utilizan varios de ellos como Tripwire.

Algunos consejos aplicables en cualquier ambiente:

a) Informar al usuario/administrador

Si usted es un administrador, notifique a sus usuarios de los mecanismos de seguridad que usted tiene implementados, y anímelos a utilizarlos haciendo de su conocimiento las posibles consecuencias de no cumplir con ellos. Así pues hágalos saber que si prestan su password están cometiendo una falta, y que igualmente serán responsables por los actos, de buena o mala fe, que alguien más realice con su cuenta si logra adivinar dicho password.

Si usted es un usuario por otra parte, observe siempre una conducta acorde a lo que su administrador ha determinado como válida para el sistema al que tiene acceso. Así mismo, dé a conocer a su administrador, cualquier sospecha de violación a cualquier recurso al que usted tiene acceso legítimo.

b) Respaldo siempre.-

Sin embargo no basta con efectuar respaldos.

Una buena política de respaldos contempla, entre otras cosas: tiempos óptimos de respaldo y recuperación, periodicidad del respaldo verificación de integridad (de nada sirve un respaldo no íntegro), necesidad de duplicidad y expiración de los respaldos. Si es usted un usuario, haga además un respaldo propio adicional al que hace el administrador siempre que le sea posible, dependiendo también de la importancia de su información.

c) Realizar verificaciones no predecibles.-

Si un ladrón conoce las horas a las que la guardia de un banco hace su rondín, seguramente decidirá no robarlo a esas horas. Lo mismo sucede con los sistemas: si se hacen verificaciones periódicas, y alguien más conoce qué y cuándo se realizan, será necesario además hacer verificaciones de periodicidad no predecible, a fin de obtener una estadística más real del comportamiento del sistema.

d) Leer las bitácoras.- Las bitácoras del sistema reflejan lo que ocurre en el mismo. De nada sirve tenerlas si no son leídas. Ahí es donde pueden descubrirse ataques no exitosos perpetrados contra su sistema, por ejemplo.

e) Aplicar parches o tener las últimas versiones del software.- Las vulnerabilidades sobre algún producto o plataforma, pueden dar la vuelta al mundo rápidamente gracias a internet. Es recomendable por ello contar siempre con la versión más actualizada del software, o bien aplicar los parches respectivos cuando son liberados. En este rubro, el software libre (Como Linux o Apache) cuenta con una ventaja sobre software comercial, pues el tiempo de respuesta es dramáticamente más rápido para el software libre.

f) Leer noticias sobre seguridad: Si su proveedor mantiene una lista de seguridad, únase a ella. Así mismo suscríbase a listas que le informen sobre seguridad en general de modo que obtenga un panorama amplio pero conciso sobre el tema. Seg-I es en este sentido una excelente opción ;)

g) Cancelación de cuentas.- Todo lo anterior no sirve si personas que han trabajado para la organización poseen sus cuentas de acceso después de haber dejado de colaborar con ella. Las estadísticas demuestran que un 85% de los ataques de seguridad son realizados desde dentro de la organización, o bien a través de cuentas de personal que estuvo dentro de ella.

Organismos de seguridad

Equipo de Respuesta a Incidentes

Es una organización, que investiga sobre seguridad a nivel técnico y difunde información a la comunidad en general sobre el tema. Se les conoce como CERTs (Computer Emergency Response Team ó Equipo de Respuesta a Emergencias de Cómputo) o IRT (Incident Response Team) Equipo de Respuesta a Incidentes.

Certs y equipos de respuesta

ESPAÑA

ESCERT

ESCERT, Cl. Jordi Girona 1-3 Módul D6, CP 08034. Barcelona, España

<http://escert.upc.es/>

e-mail: cert@escert.upc.es

Tel: +34-3-4015795, +34-3-4016984

Fax: +34-3-4017055

IRIS-CERT (Ámbito Académico)

<http://www.rediris.es/cert/>

mail: cert@rediris.es

MÉXICO

MxCERT - DINF - DTCI:

ITESM, Campus Monterrey

Suc. de Correos J, C.P. 64849

Monterrey, N.L.; México

<http://www.mxcert.org.mx/> e-mail: mxcert@mxcert.org.mx

Tel: (8) 328-4088 Atención personal días hábiles de 8:00-13:00 y 15:00-18:00 GMT-0600/GMT-0500.(8) 319-0779 PIN No.628 0508 >> Emergencia 24h << Fax: (8) 328-4129

Area de Seguridad en Cómputo UNAM
Dirección General de Servicios de Cómputo Académico
Circuito Exterior, C. U. (frente a la FCA) 04510 México D. F.
<http://www.asc.unam.mx>
e-mail: asc@asc.unam.mx
Tel: (5) 622-81-69
Fax: (5) 622-80-43

E.E.U.U

CERT/CC: (Centro coordinación CERTs)
<http://www.cert.org/>
e-mail: cert@cert.org
Tel: +1 412 268-7090

FIRST [Forum of Incident and Response Teams]:
<http://www.first.org/>
email: first-sec@first.org
Asociación que aglutina a los equipos de Incidencia y respuesta de todo el mundo (no solo a los CERTs públicos).

Listado CERTs Europeos:

<http://www.cert.dfn.de/eng/csir/europe/certs.html>

Extraído de F.A.Q. DE SEG-L (LISTA DE SEGURIDAD EN CASTELLANO)