INDICE

PLANEACION DE SEGURIDAD EN REDES

Es importante tener una política de seguridad de red bien concebida y efectiva que pueda proteger la inversión y los recursos de información de la compañía. Vale la pena implementar una política de seguridad si los recursos y la información que la organización tiene en sus redes merecen protegerse. La mayoría de las organizaciones tienen en sus redes información delicada y secretos importantes; esto debe protegerse del acceso indebido del mismo modo que otros bienes valiosos como la propiedad corporativa y los edificios de oficinas.

La mayoría de los diseñadores de redes por lo general empiezan a implementar soluciones de firewall antes de que se haya identificado un problema particular de seguridad de red. Quizá una de las razones de esto es que idear una política de seguridad de red efectiva significa plantear preguntas difíciles acerca de los tipos de servicios de Inter.−redes y recursos cuyo acceso se permitirá a los usuarios, y cuales tendrán que restringirse debido a los riesgos de seguridad.

Si actualmente sus usuarios tienen acceso irrestricto a la red, puede ser difícil aplicar una política que limite ese acceso. También debe tomar en cuenta que la política de seguridad que Usted debe usar es tal, que no disminuirla la capacidad de su organización. Una política de red que impide que los usuarios cumplan efectivamente con sus tareas, puede traer consecuencias indeseables: los usuarios de la red quizá encuentren la forma de eludir la política de seguridad, lo cual la vuelve inefectiva.

Una política de seguridad en redes efectiva es algo que todos los usuarios y administradores

de redes pueden aceptar y están dispuestos a aplicar.

POLITICA DE SEGURIDAD DEL SITIO

Una organización puede tener muchos sitios, y cada uno contar con sus propias redes. Sí la organización es grande, es muy probable que los sitios tengan diferente administración de red, con metas y objetivos diferentes. Si esos sitios no están conectados a través de una red interna, cada uno de ellos puede tener sus propias políticas de seguridad de red. Sin embargo, si los sitios están conectados mediante una red interna, la política de red debe abarcar todos los objetivos de los sitios interconectados.

En general, un sitio es cualquier parte de una organización que posee computadoras y recursos

relacionados con redes. Algunos, no todos, de esos recursos son los siguientes:

- Estaciones de trabajo.
- Computadoras host y servidores.
- Dispositivos de interconexión gateway, routers, bridges, repetidores.
- Servidores de terminal.
- Software para conexión de red y de aplicaciones.
- Cables de red
- La información de archivos y bases de datos.

La política de seguridad del sitio debe tomar en cuenta la protección de estos recursos. Debido a que el sitio está conectado a otras redes, la política de seguridad del sitio debe considerar las necesidades y requerimientos de seguridad de todas las redes interconectadas.

Este es un punto importante en el que es posible idear una política de seguridad que salvaguarde sus intereses pero que sea dañina para los de otros. Un ejemplo de esto sería el uso deliberado de direcciones IP, detrás del gateway de las firewall que ya estén siendo usadas por alguien más. En este los ataques que se hicieran contra su red mediante la falsificación de las direcciones IP de su red, se desviarán a la organización a la que pertenecen las direcciones IP que usted está usando. Debe evitarse esta situación, ya que su interés es ser un `buen ciudadano' de Internet.

La RFC 1244 aborda con considerable detalle la política de seguridad del sitio. Muchas de las cuestiones de política de seguridad de este capítulo están basadas en las cuestiones planteadas por esa RFC.

PLANTEAMIENTO DE LA POLITICA DE SEGURIDAD

Definir una política de seguridad de red significa elaborar procedimientos y planes que Salvaguarden los recursos de la red contra perdida y daño. Uno de los enfoques posibles para elaborar dicha política es examinar lo siguiente:

- ¿Qué recursos esta usted tratando de proteger?
- ¿De quiénes necesita proteger los recursos?
- ¿Qué tan posibles son las amenazas?
- ¿Qué tan importante es el recurso?
- ¿Qué medidas puede implementar para proteger sus bienes de forma económica y

oportuna!?

- Examine periódicamente su política de seguridad de red para ver si han cambiado los

objetivos y las circunstancias de la red.

La figura siguiente muestra una hoja de trabajo que puede ayudarle a canalizar sus ideas conforme estos lineamientos.

- La columna Numero de recursos de red es un numero de red de identificación

interna de los recursos que van a ser protegidos (sí se aplica).

- La columna Nombre del recurso de red es la descripción en lenguaje común de los

recursos. La importancia del recurso puede estar en una escala numérica del O al 10,

o en expresiones `Vagas de lenguaje natural como bajo, alto, medio, muy alto, etcétera.

- La columna Tipo de usuario del que hay que proteger al recurso puede tener

designaciones como interno, externo, invitado o nombres de grupos como usuarios

de contabilidad, asistentes corporativos, etcétera.

- La columna Posibilidad de una amenaza' puede estar en una escala numérica del O al

10, o en expresiones `Vagas de lenguaje natural como baja, alta, media, muy alta,

etcétera.

- La columna Medidas que se implementarán para proteger el recurso de red puede

tener valores tales como `permisos de sistema operativo para archivos y directorios;

pistas/alertas de auditoria' para servicios de red; routers de selección y firewalls

para hosts y dispositivos para conectividad de red; y cualquier otra descripción del

tipo de control de seguridad.

En general, el costo de proteger las redes de una amenaza debe ser menor que el de recuperación en caso de que se viera afectado por una amenaza de seguridad. Si usted no tiene el conocimiento suficiente de lo que esta protegiendo y de las fuentes de la amenaza, puede ser difícil alcanzar un nivel aceptable de seguridad.

No dudar en contar con la ayuda de otros con conocimientos especializados respecto de los bienes de la red y de las posibles amenazas en su contra.

Es importante hacer que en el diseño de la política de seguridad participe la gente adecuada.

Quizá usted ya tenga grupos de usuarios que podrían considerar que su especialidad es la implementación de la política de seguridad de red. Estos grupos podrán incluir a quienes están implicados en el control de auditoria, grupos de sistemas de información de universidades y organizaciones que manejan la seguridad física. Si usted desea que la política de seguridad tenga apoyo universal, es importante hacer participar a estos grupos, de modo que usted obtenga su cooperación y aceptación de la política de seguridad de red.

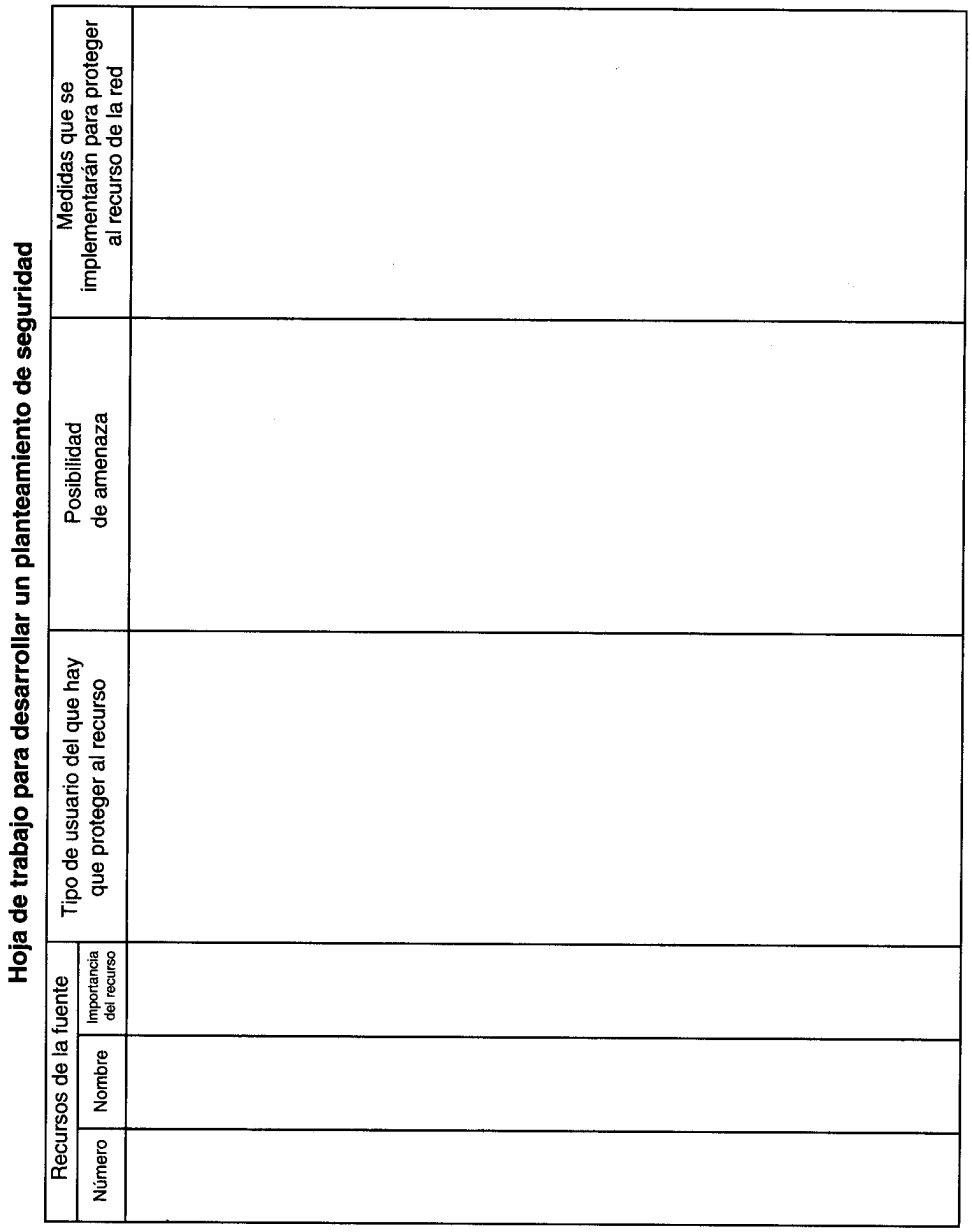

FIGURA 3.1 *Hoja de trabajo para desarrollar un planteamiento de seguridad.*

COMO ASEGURAR LA RESPONSABILIDAD HACIA LA POLTICA DE SEGURIDAD

Un aspecto importante de la política de seguridad de red es asegurar que todos conozcan su propia responsabilidad para mantener la seguridad. Es difícil que una política de seguridad se anticipe a todas las amenazas posibles. Sin embargo, las políticas s pueden asegurar que para cada tipo de problema haya alguien que lo pueda manejar de manera responsable. Puede haber muchos niveles de seguridad relacionados con la política de seguridad. Por ejemplo, cada usuario de la red debe ser responsable de cuidar su contraseña. El usuario que permite que su contraseña se vea comprometida incrementa la posibilidad de comprometer otras cuentas y recursos. Por otra parte, los administradores de la red y del sistema son responsables de administrar la seguridad general de la red.

ANALISIS DE RIESGO

Cuando usted crea una política de seguridad de red, es importante que comprenda que la razón para crear una política es, en primer lugar, asegurar que los esfuerzos dedicados a la seguridad impliquen un costo

razonable. Esto significa que usted debe conocer cuales recursos vale la pena proteger, y cuales son más importantes que otros. También debe identificar la fuente de amenazas de la que usted esta protegiendo a los recursos de la red. A pesar de toda la publicidad acerca de los intrusos que irrumpen en una red, muchos estudios indican que, en el caso de la mayoría de las organizaciones, las verdaderas perdidas causadas por los usuarios internos son mucho mayores.

El análisis de riesgo implica determinar lo siguiente:

- ***¿Que necesita proteger?***
- ***¿De que necesita protegerlo?***
- ***¿Cómo protegerlo?***

Los riesgos deben clasificarse por nivel de importancia y gravedad de la perdida. No debe terminar en una situación en la que gaste más en proteger algo que es de menor valor para usted. En el análisis de riesgo hay que determinar los siguientes dos factores:

1. Estimación del riesgo de perder el recurso (Ri)

2. Estimación de la importancia del recurso (Wi)

Puede asignarse un valor numérico como paso para cuantificar el riesgo de perder un recurso. Por ejemplo, puede asignarse un valor de 0 a 10 al riesgo (Ri) de perder un recurso, en donde 0 representa que no hay riesgo y 10 representa él más alto riesgo. De igual modo, a la importancia de un recurso (Wi) se le puede asignar un valor del 0 al 10, en donde 0 representa que no tiene importancia y 10 representa la máxima importancia. El riesgo evaluado del recurso ser el producto del valor del riesgo y de su importancia (también llamada peso). Esto puede escribirse como sigue:

WRi= Ri*Wi

Wri = Riesgo evaluado del recurso i

Ri = Riesgo del recurso i

Wi = Peso (importancia) del recurso i

Considere la figura que se muestra es una red simplificada con un router, un servidor y un bridge.

Suponga que los administradores de la red y del sistema hayan encontrado las siguientes estimaciones del riesgo y de la importancia de los dispositivos de red.

R3=10

W3=1

Diagrama de una red simplificada, con evaluaciones de peso Y riesgo. Bridge:

Router

- R1=6
- W1=.7

Bridge

- R2=6
- W2=.3

Servidor

- R3=10
- W3=1

El cálculo de los riesgos evaluados de estos dispositivos se muestra a continuación

Router

WR1 = R1 * W1 = 6*0.7 = 4.2

Bridge

WR2 = R2 * W2 = 6*0.3 = 1.8

Servidor

WR3 = R3 * W3 = 10 * 1 = 10

La evaluación de la amenaza y los riesgos no debe ser una actividad de una sola vez; debe realizarse con regularidad, como se defina en la política de seguridad del sitio. El Servicio de Pesca y Fauna de Estados Unidos ha documentado las cuestiones implicadas en la realización de evaluaciones de amenazas y riesgos. El URL del documento de evaluación de amenazas y riesgos es http://www.fws.gov/−pullenl/security/rpamp.html.

Otros factores que hay que considerar al estimar el riesgo de un recurso de red son su disponibilidad, integridad y confidencialidad. La disponibilidad de un recurso es la medida de qué tan importante es tenerlo disponible todo el tiempo. La integridad de un recurso es la medida de que tan importante es que este o los datos del mismo sean consistentes.

Esto es de particular importancia para los recursos de bases de datos. La confidencialidad se aplica a recursos, tales como archivos de datos, a los cuales se desee restringir el acceso.

IDENTIFICACION DE RECURSOS

Al realizar el análisis de riesgo, usted debe identificar todos los recursos que corran el riesgo de sufrir una violación de seguridad. Los recursos como el hardware son bastante obvios para incluirlos en este cálculo, pero en muchas ocasiones se ignoran recursos tales como las personas que en realidad utilizan los sistemas. Es importante identificar a todos los recursos de la red que puedan ser afectados por un problema de seguridad.

La RFC 1244 enlista los siguientes recursos de red que usted debe considerar al calcular las amenazas a la seguridad general

- HARDWARE: procesadores, tarjetas, teclados, terminales, estaciones de trabajo, computadoras personales, impresoras, unidades de disco, líneas de comunicación, servidores terminales, routers.

2. SOFTWARE: programas fuente, programas objeto, utileras, programas de diagnostico, sistemas operativos, programas de comunicaciones.

3. DATOS: durante la ejecución, almacenados en línea, archivados fuera dé línea, respaldos, registros de auditoria, bases de datos, en tránsito a través de medios de comunicación.

4. PERSONAS: usuarios, personas necesarias para operar los sistemas.

5. DOCUMENTACION: Sobre programas, hardware, sistemas, procedimientos administrativos locales.

6. SUMINISTROS: papel, formularios, cintas, medios magnéticos.

IDENTIFICACION DE LAS AMENAZAS

Una vez que se han identificado los recursos que requieren protección, usted debe identificar las amenazas a las que están expuestos. Pueden examinarse las amenazas para determinar que posibilidad de perdida existe. También debe identificar de que amenazas esta usted tratando de proteger a sus recursos.

En la siguiente sección se describen unas cuantas de las posibles amenazas.

DEFINICION DEL ACCESO NO AUTORIZADO

El acceso a los recursos de la red debe estar permitido a los usuarios autorizados. Esto sé llama acceso autorizado. Una amenaza común que afecta a muchos sitios es el acceso no autorizado a las instalaciones de cómputo. Este acceso puede tomar muchas formas, como el uso de la cuenta de otro usuario para tener acceso a la red y sus recursos. En general, se considera que el uso de cualquier recurso de la red sin permiso previo es un acceso no autorizado. La gravedad del acceso no autorizado depende del sitio y de la naturaleza de la perdida potencial. En algunos sitios, el solo hecho de conceder acceso a un usuario no autorizado puede causar daños irreparables por la cobertura negativa de los medios.

Algunos sitios, debido a su tamaño y visibilidad, pueden ser objetivos más frecuentes que otros. El Equipo de Respuesta de Emergencias de Computo (CERT) ha hecho la observación de que, en general, las universidades de prestigio, los sitios del gobierno y las zonas militares parecen atraer más intrusos. En la sección Equipo de respuesta de seguridad, puede encontrarse mayor información acerca de CERT, así como sobre otras organizaciones similares.

RIESGO DE REVELACION DE INFORMACIÓN

La revelación de información, ya sea voluntaria o involuntaria, es otro tipo de amenaza. Usted debe determinar el valor y delicadeza de la información guardada en sus computadoras. En el caso de vendedores de hardware y software, el código fuente, los detalles de diseño, los diagramas y la información especifica de un producto representan una ventaja competitiva.

Los hospitales, las compañías de seguros y las instituciones financieras mantienen información confidencial, cuya revelación puede ser perjudicial para los clientes y la reputación de la empresa. Los laboratorios farmacéuticos pueden tener aplicaciones patentadas y no pueden arriesgarse a perdidas causadas por robos.

A nivel del sistema, la revelación de un archivo de contraseñas de un sistema Unix puede volverlo vulnerable a accesos no autorizados en el futuro. Para muchas organizaciones, un vistazo, a una propuesta o un proyecto de investigación que represente muchos años de trabajo puede darle a su competidor una ventaja injusta.

Muchas veces, la gente supone que los accesos no autorizados de terceros a las redes y computadoras son realizadas por individuos que trabajan por su cuenta. No siempre es así. Los peligros del espionaje industrial gubernamental sistemático son realidades desafortunadas de la vida.

Además, cuando se logra uno de estos accesos no autorizados, por lo general la información fluye por Internet en muy poco tiempo. Hay grupos de noticias y canales de difusión, en Internet (IRC) en los que los usuarios comparten la información que lograron extraer de estas intromisiones.

NEGACION DEL SERVICIO

Las redes vinculan recursos valiosos, como computadoras y bases de datos, y proporcionan servicios de los cuales depende la organización. La mayoría de los usuarios depende de estos servicios para realizar su trabajo con eficacia. Si no están disponibles estos servicios, hay una pérdida correspondiente de productividad. Un ejemplo clásico de esto es el incidente del gusano de Internet, que ocurrió el 2 y 3 de noviembre de 1988, en el que se volvieron inservibles un gran numero de computadoras de la red.

Es difícil predecir la forma en que se produzca la negación del servicio. Los siguientes son algunos ejemplos de cómo la negación de servicios puede afectar una red.

- La red puede volverse inservible por un paquete extraviado.
- La red puede volverse inservible por inundación de trafico.
- La red puede ser fraccionada al desactivar un componente importante, como el router

que enlaza los segmentos de la red.

- Un virus puede alentar o invalidar un sistema de cómputo al consumir los recursos

del sistema.

- Los dispositivos reales que protegen a la red podrán alterar el funcionamientose.

Usted debe determinar que servicios son absolutamente esenciales y, para cada uno de ellos, determinar el efecto de su perdida. También debe contar con políticas de contingencia para recuperarse de tales perdidas.

USO Y RESPONSABILIDADES DE LA RED

Existen numerosas cuestiones que deben abordarse al elaborar una política de seguridad:

1. ¿Quién esta autorizado para usar los recursos?

2. ¿Cuál es el uso adecuado de los recursos?

3. ¿Quién esta autorizado para conceder acceso y aprobar el uso?

4. ¿Quién puede tener privilegios de administración del sistema?

5. ¿Cuáles son los derechos y las responsabilidades del usuario?

6. ¿Cuáles son los derechos y las responsabilidades del administrador del sistema, en

comparación con los de los usuarios!

7. ¿Qué hace usted con la información delicada?

IDENTIFICACION DE QUIEN ESTA AUTORIZADO PARA USAR LOS RECURSOS DE LA RED

Debe hacerse una lista de los usuarios que necesitan acceso a los recursos de la red. No es necesario enlistar a cada usuario. La mayoría de estos pueden dividirse en grupos como usuarios de contabilidad, abogados corporativos, ingenieros, etcétera. También debe tomar en cuenta una clase llamada usuarios externos esta se compone de los usuarios que tengan acceso a su red desde otras partes, como estaciones de trabajo autónomas y otras redes; pueden no ser empleados, o bien, pueden ser empleados que tengan acceso a la red desde sus hogares o durante un viaje.

IDENTIFICACION DEL USO ADECUADO DE LOS RECURSOS

Una vez determinados los usuarios autorizados a tener acceso a los recursos de la red, usted debe establecer los lineamientos del uso aceptable de dichos recursos. Los lineamientos dependen de la clase de usuarios, como desarrolladores de software, estudiantes, profesores, usuarios externos, etcétera. Debe tener lineamientos aparte para cada clase. La política debe establecer que tipo de uso es aceptable y cual es inaceptable, así como que tipo de uso esta restringido. La política que usted elabore será la Política de Uso Aceptable (AUP) de esa red. Si el acceso a un recurso de la red esta restringido, debe considerar el nivel de acceso que tendrá cada clase de usuario.

Su AUP debe establecer con claridad que cada usuario es responsable de sus acciones. La responsabilidad de cada usuario existe al margen de los mecanismos de seguridad implantados. No tiene caso construir costosos mecanismos de seguridad con firewalls si un usuario puede revelar la información copiando archivos en disco o cinta y poner los datos a disposición de individuos no autorizados.

Aunque parezca obvio, la AUP debe establecer claramente que no esta permitido irrumpir en las cuentas o pasar por alto la seguridad. Esto puede ayudar a evitar cuestiones legales planteadas por empleados que pasan por alto la seguridad de la red y después aseguran que no se les informa o capacita adecuadamente acerca de la política de la red. A continuación se muestran los lineamientos que deben escribirse al desarrollar la AUP:

- ¿Se permite introducirse en las cuentas?
- ¿Se permite descifrar las contraseñas?
- ¿Se permite interrumpir servicios?
- ¿Los usuarios deben suponer que, si un archivo tiene permiso general de lectura, eso

los autoriza a leerlo?

- ¿Debe permitirse que los usuarios modifiquen archivos que no sean suyos, aun cuando

dichos usuarios tengan permiso de escritura?

- ¿Los usuarios deben compartir cuentas?

A menos que usted tenga requerimientos especiales, la respuesta a estas preguntas, en la mayoría de las organizaciones, debe ser no. Además, quizá usted quiera incorporar en sus políticas una declaración respecto al software registrado y patentado. En general, los procedimientos del uso de red deben ser tales que se dificulte que los usuarios bajen software no autorizado de la red. En la mayoría de los pases occidentales, copiar software en forma ilegal esta penado por la ley. Las organizaciones grandes tienen políticas muy estrictas respecto a las licencias, debido al riesgo de demandas judiciales y el daño causado por la publicidad de los incidentes.

Muchos productos de software con licencia para redes determinan su uso y restringen el número de usuarios que pueden tener acceso a la red. Sin embargo, algunos acuerdos de licencia quizá requieran que usted vigile su uso para que no se viole el acuerdo.

Quizá se desee incluir información con respecto al software con derechos de autor o con licencia en su AUP. Los siguientes son ejemplos de los puntos que necesita abordar:

1 No se puede reproducir el software con derechos de autor y con licencia, a menos que

se exprese en forma explícita.

2 Indicar métodos de trasmitir información acerca de la situación del software con

derechos de autor y con licencia.

3 Conceda el beneficio de la duda a la precaución. Si tiene dudas, no lo copie.

Si la AUP no establece claramente lo que esta prohibido, será difícil demostrar que un usuario ha violado la política. Los miembros de los llamados equipos tigre pueden estar exentos de esta política, ya que son responsables de sondear las debilidades de seguridad de las redes. Debe identificarse claramente a los miembros de los equipos tigre. En ocasiones, quizá se tenga que tratar con usuarios que sean miembros auto designados de estos equipos y que quieran sondear los puntos débiles de la seguridad, con fines de investigación o para demostrar algo.

La AUP debe abordar las siguientes cuestiones acerca de los sondeos de seguridad:

- ¿Está permitido el vandalismo en el ámbito de usuarios?
- ¿Qué tipo de actividades de sondeos de seguridad se permiten?
- ¿Qué controles deben implantarse para asegurar que los sondeos no se salgan de control?
- ¿Qué controles deben implantarse para proteger a otros usuarios de la red para que

no sean victimas de las actividades de sondeos de seguridad?

- ¿Quién debe tener permiso de realizar sondeos de seguridad, y cuál es el procedimiento

para la obtención del permiso para realizar esas pruebas!

Si quiere permitir sondeos legítimos de seguridad, debe tener segmentos separados de red y hosts en la red para esas pruebas. En general, es muy peligroso probar gusanos y virus.

Si debe realizar esas pruebas, seria tanto hacerlo en una red activa. En cambio, debe aislar físicamente a los hosts y a los segmentos de red que se utilicen para la prueba, y después de cada prueba volver a cargar, por completo y con cuidado, todo el software.

Evaluar los puntos débiles de la seguridad y tomar las medidas adecuadas puede ser eficaz para repeler ataques de hackers. Algunas organizaciones recurren a asesores externos para que evalúen la seguridad de sus servicios. Como parte de esta evaluación, ellos tendrá el derecho de realizar vandalismo. La política debe tener margen para estas situaciones.

QUIEN ESTA AUTORIZADO PARA CONCEDER ACCESO Y APROBAR EL USO

La política de seguridad de red debe identificar quien esta autorizado para conceder acceso a sus servicios. También se debe determinar que tipo de acceso puede conceder dichas personas. Si no puede controlar a quien se le dá acceso a sistema, será difícil controlar quien use la red. Si puede identificar a las personas encargadas de conceder acceso a la red, puede rastrear qué tipo de acceso o control se ha otorgado. Esto es útil para identificar las causas de las fallas de seguridad como resultado de que se hayan concedido privilegios

excesivos a ciertos usuarios.

Quizá necesite considerar los siguientes factores al determinar quién conceder acceso a los servicios de la red:

- ¿Se otorgara el acceso a los servicios desde un punto central?
- ¿Que métodos se usan para crear cuentas y finalizar accesos?

Si la organización es grande y descentralizada, quizá haya muchos puntos centrales, uno en cada departamento, que sea el responsable de la seguridad de su red departamental. En este caso, se necesitará tener lineamientos globales acerca de los tipos de servicios que se le permitirán a cada clase de usuario. En general, mientras más centralizada este la administración de la red, es más fácil mantener la seguridad. Por otra parte, la administración centralizada puede crear problemas cuando los departamentos deseen tener mayor control sobre sus recursos de red. El grado correcto de centralización o descentralización depender de factores que esté mas allá del alcance de este análisis.

Por supuesto, los administradores del sistema necesitaran tener acceso especial a la red, pero quizá haya otros usuarios que requieran de ciertos privilegios. La política de seguridad de la red debe abordar esta cuestión. Una política universal que restrinja todos los privilegios, si bien es más segura, quizá impida que ciertos usuarios legítimos realicen su trabajo. Se necesita un enfoque más equilibrado.

El reto es equilibrar el acceso restringido a los privilegios especiales para hacer más segura la red, con el otorgamiento de acceso a las personas que necesitan esos privilegios para realizar sus tareas. En general, se debe conceder solo los privilegios; suficientes para cumplir con las tareas necesarias.

Algunos administradores de sistemas se van por la vía fácil y asignan mas privilegios de los que necesita el usuario, para que estos no los vuelvan a molestar. Asimismo, el administrador del sistema quizá no comprenda las sutilezas de la asignación de seguridad y se vaya por el lado de conceder más privilegios. La capacitación y la educación ayudan a evitar este tipo de problemas. Las personas que tengan privilegios deben ser responsables y rendir cuentas ante alguna autoridad identificada dentro de la propia política de seguridad. Algunos sistemas podrán tener mecanismos de auditorias personales, que pueden usarse para que los usuarios con privilegios no abusen de la confianza.

ADVERTENCIA

Si las personas a las que les conceden privilegios no son responsables ni rinden cuentas, usted corre el riesgo de crear fallas en el sistema de seguridad y de conceder arbitrariamente los permisos a los usuarios. Por lo general, tales sistemas son difíciles de administrar.

Si existe gran número de administradores de red y de sistemas es difícil llevar la cuenta de que permisos se han concedido para los recursos de la red. Puede seguirse una manera formal de solicitudes de otorgamiento. Una vez que el usuario hace la solicitud y esta es autorizada por el supervisor del usuario, el administrador del sistema debe documentar las restricciones de seguridad o de acceso a las que esta sujeto el usuario.

También debe examinar el procedimiento que seguir para crear cuentas nuevas y asignar permisos. En el caso menos restrictivo, las personas que están autorizadas para otorgar acceso deben poder ir directamente al sistema y crear una cuenta a mano o mediante mecanismos suministrados por el proveedor. Estos mecanismos le dan mucha confianza a la persona que los ejecuta, la cual, por lo general, tiene gran cantidad de privilegios, como el usuario raíz (Root) en Unix. En esas circunstancias, necesita seleccionar a alguien confiable para llevar a cabo esa tarea.

Debe elaborar procedimientos específicos para la creación de cuentas. En Unix existen numerosas formas que pueden usarse para crear cuentas. Sin importar el procedimiento que usted decida seguir, este debe estar bien

documentado para evitar confusiones y reducir errores. Como resultado de errores cometidas por el administrador del sistema pueden producirse puntos vulnerables en la seguridad. Si tiene procedimientos bien documentados, eso le ayudar a reducir los errores.

COMO DISEÑAR UNA POLITICA DE RED

Estos procedimientos también permiten capacitar fácilmente a futuros administradores de sistemas acerca de las peculiaridades de un sistema determinado. Otra cuestión que hay que considerar es seleccionar un procedimiento de creación de cuentas de usuario que sea él más sencillo y fácil de entender. Esto asegura que se cometen menos errores y que sea más probable que lo sigan los administradores del sistema (como debe ocurrir normalmente).

También debe tener una política para seleccionar la contraseña inicial. El momento de otorgar la contraseña inicial es muy vulnerable para la cuenta de usuario. Las políticas como aquellas donde la contraseña inicial sea igual al nombre del usuario, o que se quede en blanco, pueden dejar al descubierto las cuentas. Asimismo, evite establecer la contraseña inicial como una función del nombre de usuario, o parte de este, o alguna contraseña generada por un algoritmo que pueda adivinarse con facilidad. La selección de la contraseña inicial no debe ser tan obvia.

El CERT Equipo de Respuesta a Emergencias de Cómputo (CERT, Computer Emergency Response Team), en avisos publicados calcula que 80 por ciento de todos los problemas de seguridad en redes son creados por contraseñas inseguras.

Algunos usuarios empiezan a usar su cuenta mucho tiempo después de haber sido creada; otros nunca se registran. En esas circunstancias, si no es segura la contraseña inicial, la cuenta y el sistema son vulnerables. Por esta razón, usted debe tener una política para desactivar las cuentas en las que no haya habido acceso durante cierto periodo. El usuario se ve obligado a pedir que se le active su cuenta.

También es un error permitir que los usuarios sigan usando su contraseña inicial en forma indefinida. Si el sistema lo permite, usted debe obligar al usuario a cambiar de contraseña la primera vez que se registre. Muchos sistemas cuentan con una política de caducidad de contraseñas, lo cual es útil para protegerlas. También hay utilerías Unix, que pueden usarse para probar la seguridad de las contraseñas como las siguientes:

Password es una aplicación para analizar contraseñas. Puede encontrarse en ftp: llftp.dartmouth.edu/pub/security/passwd+.atr.

Npasswd es un reemplazo compatible para el comando password. Incorpora un sistema de verificación de contraseñas que inhabilita las contraseñas sencillas.

Npasswd puede encontrarse en ftp:llrtp.usa.edulpub/security/npaccwd.tar.gz.

DETERMINACION DE LAS RESPONSABILIDADES DEL USUARIO

La política de seguridad de la red debe definir los derechos y las responsabilidades de los usuarios que utilizan los recursos y servicios de la red. La siguiente es una lista de los aspectos que usted puede abordar respecto de las responsabilidades de los usuarios:

1. Lineamientos acerca del uso de los recursos de red, tales como que los usuarios estén restringidos

2. Que constituye un abuso en términos de usar recursos de red y afectar el desempeño del sistema y de la red.

3. Esta permitido que los usuarios compartan cuentas o permitan a otros usar la suya.

4. Pueden los usuarios revelar su contraseña en forma temporal, para permitir que otros que trabajen en un proyecto tengan acceso a sus cuentas.

5. Política de contraseña de usuario: con que frecuencia deben cambiar de contraseña los usuarios y que otras restricciones o requerimientos hay al respecto.

6. Los usuarios son responsables de hacer respaldos de sus datos o es esto responsabilidad del administrador del sistema.

7. Consecuencias para los usuarios que divulguen información que pueda estar patentada. Que acciones legales u otros castigos pueden implantarse.

8. Una declaración sobre la privacidad del correo electrónico (Ley de Privacidad en las Comunicaciones Electrónicas)

9. Una política respecto a correo o publicaciones controversiales en las listas de correo o grupos de discusión.

10. Una política sobre comunicaciones electrónicas, tales como falsificación de correo.

La Asociación de Correo Electrónico (EMA, Electrónica Mail Asociación) recomienda que todo sitio debe tener una política acerca de la protección de la privacidad de los empleados.

Las organizaciones deben establecer políticas que no se limiten a correo electrónico, sino que también abarque otros medios, como discos, cintas y documentos impresos. La EMA sugiere cinco criterios para evaluar cualquier política:

1. ¿La política cumple con la ley y con las obligaciones hacia otras empresas?

2. La política compromete innecesariamente los intereses del empleado, del patrón o

de otras empresas!

3. ¿La política es funcional, práctica y de posible cumplimiento?

4. La política aborda apropiadamente todas las formas de comunicación y

mantenimiento de archivo en la oficina!

5. ¿La política fue anunciada por anticipado y aceptada por todos los interesados?

DETERMINACIONES DE LAS RESPONSABILIDADES DE LOS ADMINISTRADORES DE SISTEMAS

Muchas veces, el administrador del sistema necesita recabar información del directorio privado de un usuario para diagnosticar problemas del sistema. Los usuarios, por otra parte, tienen el derecho de conservar su privacidad. Existe, por lo tanto, una contradicción entre el derecho del usuario a la privacidad y las necesidades del administrador del sistema. Cuando se presentan amenazas a la seguridad de la red, el administrador del sistema tendrá mayor necesidad de recabar información de los archivos, incluidos los del directorio base de los usuarios.

La política de seguridad de la red debe especificar el grado al que el administrador del sistema pueda examinar los directorios y archivos privados de los usuarios para diagnosticar problemas del sistema e investigar violaciones de la seguridad. Si la seguridad de la red esta en riesgo, la política debe permitir mayor flexibilidad para que el administrador corrija los problemas de seguridad. Otros aspectos relacionados que usted debe abordar son los siguientes:

1. Puede el administrador revisar o leer los archivos de un usuario por alguna razón.

2. Los administradores de la red tienen el derecho de examinar el tráfico de la red o del host.

3. Cuáles son las responsabilidades legales de los usuarios, los administradores del sistema y de la organización por tener acceso no autorizado a los datos privados de otras personas.

QUE HACER CON LA INFORMACION DELICADA

Usted debe determinar que tipo de datos delicados pueden almacenarse en un sistema específico. Desde el punto de vista de la seguridad, la información en extremo delicada, como nóminas y planes, debe estar restringida a unos cuantos hosts y administradores de sistemas.

Para concederle a un usuario acceso a un servicio de un host, usted debe considerar que otros servicios e información se proporcionan y a los cuales el usuario podrá tener acceso. Si el usuario no tiene necesidad de manejar información delicada, no debe tener una cuenta en un sistema que contenga dicho material.

También debe considerar si existe una seguridad adecuada en el sistema para proteger la información delicada. En general, usted no desear que los usuarios guarden información muy delicada en un sistema que usted no planee asegurar bien. Por otra parte, asegurar un sistema puede implicar hardware, software y costos adicionales de administración, por lo cual puede no ser rentable asegurar datos en un host que no sea muy importante para la organización o los usuarios.

La política también debe tomar en cuenta el hecho de que usted necesita decirle a los usuarios que podrán guardar información delicada que servicios son apropiados para el almacenamiento de dichos datos.

PLAN DE ACCION CUANDO SE VIOLE LA POLITICA DE SEGURIDAD

Cada vez que se viola la política de seguridad, el sistema esta sujeto a amenazas. Si no se producen cambios en la seguridad de la red cuando esta sea violada, entonces debe modificarse la política de seguridad para eliminar aquellos elementos que no sean seguros.

La política de seguridad y su implementación deben ser lo menos obstructivas posible. Si la política de seguridad es demasiado restrictiva, o esta explicada inadecuadamente, es muy probable que sea violada o desactivada.

Al margen del tipo de política que se implemente, algunos usuarios tienen la tendencia a violarla. En ocasiones las violaciones a la política son evidentes; otras veces estas infracciones no son detectadas. Los procedimientos de seguridad que usted establezca deben reducir al mínimo la posibilidad de que no se detecte una infracción de seguridad.

Cuando usted detecte una violación a la política de seguridad, debe determinar si esta ocurrió debido a la negligencia de un individuo, a un accidente o error, por ignorancia de la política vigente o si deliberadamente la política fue pasada por alto. En este último caso, la violación quizás haya sido efectuada no solo por una persona, sino por un grupo que a sabiendas realiza un acto en violación directa de la política de seguridad. En cada una de estas circunstancias, la política de seguridad debe contar con lineamientos acerca de las medidas

que se deben tomar.

Debe llevarse a cabo una investigación para determinar las circunstancias en torno a la violación de seguridad, y cómo y por que ocurrió. La política de seguridad debe contener lineamientos acerca de las acciones correctivas para las fallas de seguridad. Es razonable esperar que el tipo y severidad de la acción dependen de la gravedad de la violación.

RESPUESTA A LAS VIOLACIONES DE LA POLÍTICA

Cuando ocurre una violación, la respuesta puede depender del tipo de usuario responsable del acto. Las violaciones a la política pueden ser cometidas por gran variedad de usuarios; algunos pueden ser locales y otros externos. Los usuarios locales son llamados usuarios internos y los externos, usuarios foráneos. Por lo general, la distinción entre ambos tipos están basada en los límites de red, administrativos, legales o políticos. El tipo de limite determina cual debe ser la respuesta a la violación de la seguridad. Los ejemplos de respuestas pueden ir desde una reprimenda o advertencia verbal, una carta formal o la presentación de cargos judiciales.

Usted necesita definir la acción según el tipo de violación. Estas acciones requieren ser definidas con claridad, con base en el tipo de usuario que haya violado la política de seguridad de computo. Los usuarios internos y externos de su red deben estar conscientes de la política de seguridad.

Si hay usuarios externos que utilicen legalmente la red, es responsabilidad de usted verificar que esas personas conozcan las políticas que se han establecido. Esto es de particular importancia si usted tiene que emprender acciones legales en contra de los transgresores.

Si se ha producido una perdida significativa, quizá usted tendrá que tomar acciones mas drásticas. Si todo esto implica una publicidad negativa, quizás usted prefiera arreglar la falla de seguridad y no emprender acción judicial.

El documento de la política de seguridad también debe contener procedimientos para manejar cada tipo de incidente de violación. Debe llevarse un registro apropiado de tales violaciones, el cual ha de revisarse periódicamente para observar tendencias y tal vez ajustar la política de seguridad para que dicha política tome en cuenta cualquier nuevo tipo de amenaza.

RESPUESTA A LAS VIOLACIONES DE LA POLITICA POR USUARIOS LOCALES

Se podría tener una violación de la política de seguridad en la que el agresor sea un usuario interno. Esto podrá ocurrir en las siguientes situaciones:

- Un usuario local viola la política de seguridad de un sitio local.
- Un usuario local viola la política de seguridad de un sitio remoto.

En el primer caso, debido a que se viola la política de seguridad interna, usted tendrá mas control sobre el tipo de respuesta ante esta violación de seguridad. En el segundo caso, un usuario local ha violado la seguridad de la política de seguridad de otra organización.

Esto podrá ocurrir a través de una conexión como Internet. Esta situación se complica por el hecho de que esto implicada otra organización, y cualquier respuesta que usted tome tendrá que discutirse con la organización cuya política de seguridad fue violada por un usuario local de usted. También deber consultar con el abogado de su empresa o con especialistas en seguridad legal de computo.

ESTRATEGIAS DE RESPUESTA

Existen dos tipos de estrategias de respuesta ante incidentes de seguridad:

- **Proteja y continúe**
- **Persiga y demande**

Si los administradores de la política de seguridad sienten que la compañía es bastante vulnerable, quizás se decidan por la estrategia de proteger y continuar. El objetivo de esta política es proteger de inmediato a la red y restablecerla a su situación normal, para que los usuarios puedan seguir usándola. Para hacer esto, usted tendrá que interferir activamente con las acciones del intruso y evitar mayor acceso. A esto debe seguir el análisis del daño causado.

En ocasiones no es posible restablecer la red de inmediato a su funcionamiento normal; quizás tenga que aislar sus segmentos y apagar sistemas, con el objeto de evitar más accesos no autorizados en el sistema.

La desventaja de este procedimiento es que los intrusos saben que ya fueron detectados y tomaran medidas para evitar que sean rastreados. Asimismo, el intruso puede reaccionar a su estrategia de protección atacando el sitio con otro método; por lo menos, es probable que el intruso contiene su vandalismo en otro sitio.

La segunda estrategia −perseguir y demandar− adopta el principio de que el objetivo principal es permitir que los intrusos contienen sus actividades mientras usted los vigila.

Esto debe hacerse en forma lo más discreta posible, de modo que los intrusos no se den cuenta de que usted los esta vigilando. Deben registrarse las actividades de los intrusos, para que haya pruebas disponibles en la fase de demanda de esta estrategia. Éste es el enfoque recomendado por las dependencias judiciales y los fiscales, ya que rinde evidencias que pueden usarse para demandar a los intrusos.

La desventaja es que el intruso seguirá robando información o haciendo otros daños, y de todos modos usted estar sujeto a demandas legales derivadas del daño al sistema y la perdida de información.

Una forma posible de vigilar a los intrusos sin causarle daño al sistema, es construir una cárcel. Una cárcel, en este caso, se refiere a un ambiente simulado para que lo usen los intrusos, de modo que puedan vigilarse sus actividades. El ambiente simulado presenta datos falsos, pero el sistema esta configurado de tal modo que se registran las actividades del intruso.

Para construir una cárcel, se necesita acceso al código fuente del sistema operativo y alguien interno con talento de programación que sepa simular ese ambiente. Lo mas seguro es construir la cárcel sacrificando una maquina en un segmento aislado de la red, para reducir el riesgo de contaminación hacia otros segmentos y sistemas por las actividades de los intrusos. También es posible construir la cárcel mediante un ambiente simulado de software; sin embargo, esto es más difícil de preparar.

En un sistema Unix, el mecanismo de root puede ser muy útil para preparar la cárcel. Este mecanismo confina irrevocablemente los procesos a una sola rama del sistema de archivos.

Para todos los fines prácticos, la raíz de esta rama del sistema de archivos parece la raíz del sistema de archivos para el proceso. Este mecanismo evita el acceso a archivos de dispositivo y al archivo de contraseñas reales (/etc/passwd).

Si usted no desea que otros usuarios se conecten con la máquina sacrificada, tendrán que actualizar periódicamente el archivo utmp, que contiene el registro de los usuarios conectados, de modo que la cárcel parezca real. También debe eliminar las utilerías que revelen que la cárcel es un ambiente simulado. Ejemplos de estas utileras son netstat, ps, who y w.

Alternativamente, usted puede proporcionar versiones falsas de estas utilerías, para hacer que el ambiente simulado parezca real.

Arquitectura general de una cárcel.

Una vez que tenga suficientes evidencias contra un intruso, quizá desee demandarlo.

Sin embargo, los pleitos judiciales no son siempre los mejores resultados. Si el intruso es un usuario interno o un invitado, como un estudiante, las acciones disciplinarias adecuadas pueden ser igualmente eficaces, sin necesidad de los costos adicionales de la demanda judicial y la correspondiente publicidad.

La política de seguridad de red debe contemplar estas opciones y ofrecer lineamientos acerca de cuando deben ejercerse.

La siguiente lista puede usarse como lineamiento para ayudar a determinar cuando el sitio debe usar una política de proteger y continuar, y cuando una de perseguir y demandar.

La estrategia de proteger y continuar puede usarse en las siguientes circunstancias:

- Si los recursos de la red no están bien protegidos de los intrusos.
- Si la continua actividad del intruso pudiera resultar en daños y riesgos financieros considerables.
- Si el costo de la demanda es demasiado elevado, o si no existe voluntad o posibilidad de demandar.
- Si existen considerables riesgos para los usuarios actuales de la red.
- Si en el momento del ataque no se conocen los tipos de usuario de una gran red interna.
- Si el sitio esta sujeto a demandas judiciales por parte de los usuarios. Esto se aplica a las compañías de seguros, bancos, formas de seguridad, proveedores de red, etc.

En las siguientes circunstancias puede seguir la estrategia de perseguir y demandar.

- Si los recursos del sistema están bien protegidos.
- Si el riesgo de la red es incrementado por los disturbios creados por las intrusiones presentes y futuras.
- Si se trata de un ataque concentrado y ya ha ocurrido antes.
- Si el sitio es muy notorio y ha sido víctima de ataques anteriores.
- Si el hecho de no demandar acarrear más intrusiones.
- Si el sitio esta dispuesto a arriesgar los recursos de la red permitiendo que continúe la intrusión.
- Si puede controlarse el acceso del intruso.
- Si las herramientas de vigilancia están bien desarrolladas para crear registros adecuadas y recabar evidencias para la demanda.
- Si cuenta con personal capacitado interno para construir rápidamente herramientas especializadas.
- Si los programadores, administradores del sistema y de la red son tan listos y

conocedores acerca del sistema operativo, utilerías del sistema y los sistemas para que valga la pena el juicio.

- Si la administración de la empresa tiene disposición a demandar.
- Si los administradores del sistema saben que tipo de evidencias presentar en un juicio y pueden crear los registros adecuados de las actividades del intruso.
- Si hay contactos establecidos con agencias judiciales conocedoras.
- Si existe un representante del sitio versado en las cuestiones legales relevantes.
- Si el sitio esta preparado para las posibles acciones legales que emprendieran los usuarios si sus datos o sistemas se vieran comprometidos durante la demanda.
- Si se dispone de buenos respaldos.

DEFINICION DE RESPONSABILIDADES PARA SER BUEN CIUDADANO DE INTERNET

Internet es una asociación cooperativa y se espera que los sitios que tengan redes conectadas a ella sigan reglas de buen comportamiento hacia los otros sitios. Esto es similar al funcionamiento de una sociedad moderna exitosa. Su política de seguridad debe contener una declaración que especifique que los intentos deliberados de violar las redes de otro sitio constituyen una violación de la política de la compañía.

También debe definir que tipo de información debe difundirse. Quizás sea mas económico publicar documentos acerca de la organización en un servidor FTP. En este caso, debe decidir que tipo y que cantidad de información deber difundirse.

CONTACTOS Y RESPONSABILIDADES CON ORGANIZACIONES EXTERNAS

La política de seguridad de red debe definir los procedimientos para interactuar con organizaciones externas. Dichas organizaciones podrían incluir dependencias judiciales, especialistas legales, otros sitios afectados por incidentes de violación de seguridad, organizaciones externas con equipos de respuesta, como el Equipo de Respuesta a Emergencias de Computo (CERT, Computer Emergency Response Team) y la Capacidad de Asesoría en Incidentes de Computadoras (CIAC, Computer Incident Advisory Capability) y, de ser necesario, agencias de noticias.

Debe identificarse a las personas autorizadas para tener contacto con estas organizaciones.

Usted debe identificar a más de una persona en cada área para cubrir situaciones en las que la persona designada no se encuentre. Entre las cuestiones que usted debe abordar están las siguientes:

- ***Identificar los tipos de relaciones publicas de quienes están versados para hablar con la prensa.***
- ***¿Cuándo debe ponerse en contacto con dependencias judiciales locales y federales, como con las dependencias investigadoras.***
- ***Qué tipo de información puede ser divulgada.***

Deben seguirse ciertas reglas respecto al manejo de pruebas durante la investigación.

De no seguirse estas reglas, se podría perder el caso. En consecuencia, es esencial que usted se ponga en contacto con las autoridades de su país, encargadas de delitos de computo y pedirles que lo ayuden para planear la investigación. Muchas dependencias judiciales ofrecen capacitación en manejo de pruebas y hay compañías que ofrecen servicios en el rea de investigación.

INTERPRETACION Y PUBLICACION DE LA POLITICA DE SEGURIDAD

Es importante identificar a las personas que interpretan la política. Generalmente no es aconsejable que sea una sola persona, ya que podrá no estar disponible en el momento de la crisis.

Se puede designar a un comité, pero también se recomienda que no esta constituido por muchos miembros. De vez en cuando, se convocar al comité de política de seguridad para interpretar, repasar y revisar el documento.

Una vez que se haya redactado la política de seguridad y se haya alcanzado el consenso en sus puntos, el sitio debe asegurarse de que la declaración de política se divulgue y discuta ampliamente.

Podrán utilizarse listas de correo o una pagina web interna. Puede reforzarse la nueva política mediante educación interna, como seminarios de capacitación, sesiones informativas, talleres, reuniones personales con el administrador, o todo esto dependiendo del tamaño de la institución y de las necesidades existentes.

Implementar una política de seguridad efectiva es un esfuerzo colectivo. Por lo tanto, debe permitirse que los usuarios comenten la política durante cierto tiempo. Será conveniente que se organizaran reuniones para obtener comentarios y asegurarse de que la política se entienda correctamente. Esto también puede ayudarle a aclarar el texto de la política y evitar ambigüedades e inconsistencias.

Las reuniones deben estar abiertas a todos los usuarios de la red y a los miembros de la administración de alto nivel, quienes pueden ser necesarios para tomar decisiones globales cuando surjan preguntas importantes. La participación y el interés de los usuarios asegura que la política se comprender mejor y que será más probable que se siga.

Si los usuarios sienten que la política reduce su productividad, se les debe permitir que argumenten el porque. Si es necesario, habrá que agregar recursos adicionales a la red para asegurarse de que los usuarios puedan realizar su trabajo sin pérdida de productividad. Para crear una política efectiva de seguridad, usted necesita lograr un delicado equilibrio entre protección y productividad.

En ocasiones, los nuevos programas son recibidos con entusiasmo al principio, cuando todos están conscientes de la política. Con el tiempo, empero, existe la tendencia a olvidar el contenido.

Los usuarios necesitan recordatorios periódicos. Asimismo, cuando llegan usuarios nuevos a la red, estos necesitan conocer la política de seguridad.

Los recordatorios periódicos (debidamente programados) y la capacitación continua acerca de la política, incrementan las posibilidades de que los usuarios sigan dicha política de seguridad. Debe incluirse la política de seguridad en el paquete de información de los usuarios nuevos. Algunas organizaciones requieren que cada usuario de la red firme una declaración en la que se especifique que han leído y comprendido la política. Si posteriormente se necesita emprender acción legal contra un usuario por graves violaciones de seguridad, esta declaración firmada le ayudar a entablar exitosamente la demanda.

IDENTIFICACION Y PREVENCION DE PROBLEMAS DE SEGURIDAD

La política de seguridad define lo que necesita protegerse, pero no señala explícitamente como deben protegerse los recursos y el enfoque general para manejar los problemas de seguridad. En una sección separada de la política de seguridad deben abordarse los procedimientos generales que deben implementarse para evitar problemas de seguridad.

La política de seguridad debe remitirse a la guía del administrador de sistemas del sitio respecto a detalles adicionales acerca de la implementación de los procedimientos de seguridad.

Antes de establecer los procedimientos de seguridad, debe evaluar el nivel de importancia de los recursos de la red y su grado de riesgo.

En muchas ocasiones es tentador empezar a implementar procedimientos como el siguiente, sin haber definido la política de seguridad de la red: Nuestro sitio necesita ofrecer a los usuarios acceso telnet a los hosts internos y externos, evitar acceso NFS a los hosts internos, pero negarlo a los usuarios externos, tener tarjetas inteligentes para registrarse desde afuera, tener módems de contestación de Llamada...

Si no se conocen adecuadamente los recursos más importantes y los que están expuestos a mayores riesgos, el enfoque anterior hará que ciertas áreas tengan mas protección de la que necesitan, y que otras áreas más importantes no tengan suficiente protección.

Establecer una política de seguridad eficaz requiere considerable esfuerzo. Se necesita cierto esfuerzo para considerar todos los aspectos y cierta disposición para establecer las políticas en papel y hacer lo necesario

para que los usuarios de la red la entiendan adecuadamente.

Además de realizar el análisis de riesgo de los recursos de la red, usted debe identificar otros puntos vulnerables. La siguiente lista es un intento de describir algunas de las tareas más problemáticas. Esta lista lo puede orientar en la dirección correcta, pero de ningún modo esta completa, ya que es probable que su sitio tenga algunos puntos vulnerables particulares.

- Puntos de acceso
- Sistemas configurados inadecuadamente
- Problemas de software
- Amenazas internas
- Seguridad física

A continuación presentamos una explicación de estos aspectos.

PUNTOS DE ACCESO

Los puntos de acceso son los puntos de entrada (también llamados de ingreso) para los usuarios no autorizados. Tener muchos puntos de acceso incrementa los riesgos de seguridad de la red.

La siguiente figura muestra una red simplificada de una organización en la que existen varios puntos de ingreso a la red. Los puntos de acceso son el servidor terminal y el router del segmento A de la red. La estación de trabajo del segmento A tiene un módem privado, que se usa para conexiones telefónicas. El host B de segmento B de la red también es un punto de ingreso a este segmento. Ya que el router une los dos segmentos de la red, cualquier intruso puede usar estos puntos de acceso en cada segmento de la red para penetrar a la red completa.

Se puede asegurar los puntos de acceso en la figura, pero es fácil que se olvide de la estación de trabajo del segmento A, que iba a ser usada para conexiones telefónicas al exterior, quizá para simples boletines electrónicos.

Considere la siguiente situación: el usuario de la estación de trabajo del segmento A puede tener una cuenta con un proveedor de acceso a Internet. Suponga que este usuario utiliza una conexión de Protocolo Internet de Línea Serial (SLIP, Serial Line Internet Protocol) o de Protocolo de Punto a Punto (PPP, Point to Point Protocol) para acceder a este proveedor de acceso a Internet.

Si el software TCP/IP que este usuario ejecuta en la estación de trabajo está configurado también como router es posible que un intruso tenga acceso a toda la red. Así mismo, si en la estación de trabajo se habilita un protocolo de enrutamiento como el protocolo de información de enrutamiento (RIP, Routing Information Protocol) o el de Abrir Primero la Ruta más Corta (OSPF, Open, Shortest Path First), la estación de trabajo puede exponer a la red interna a ataques basados en los protocolos de enrutamiento.

Observe que quizá el usuario no haya habilitado deliberadamente a la estación de trabajo como router el sistema operativo de la estación de trabajo podría estar habilitado como router en forma predeterminada. Este es el caso de muchos sistemas Unix, así como de los paquetes TCP/IP para DOS y Windows. Aún cuando la estación de trabajo haya sido configurada adecuadamente por el personal de la red, el usuario podrá conectar su computadora laptop a la red y usar un módem para tener acceso telefónico al proveedor de acceso a Internet. Si el usuario estuviera utilizando acceso telefónico (también llamado cuenta shell), donde el usuario ejecuta software de emulación de terminal en la estación de trabajo y no software TCP/IP, quizás no producirá daños. Sin embargo, si el usuario empleara una conexión SLIP o PPP, creara otro punto de acceso sin darse cuenta, el cual podrá pasar inadvertido para el personal de administración de la red.

Esto podrá representar un riesgo para la seguridad de toda la red. Puede evitarse la situación de la figura anterior si la política de seguridad de la red le informa al usuario que están prohibidas las conexiones privadas a través de las estaciones de trabajo individuales. Esta situación también subraya la importancia de tener una política de seguridad en la que se define con claridad la política de uso aceptable para la red.

Si quiere conectarse a Internet, debe tener por lo menos un vínculo con redes fuera de la organización. Él vinculo de red hace disponibles numerosos servicios de red, tanto dentro como fuera de esta, y cada servicio es susceptible de ser comprometido.

Los servidores terminales pueden representar un riesgo si no están protegidos adecuadamente. Muchos de los servidores terminales que hay en el mercado no requieren ningún tipo de autentificación. Pregúntele a su distribuidor acerca de la capacidad de autentificación del servidor terminal. Los intrusos pueden utilizar a dichos servidores para disfrazar sus acciones, marcando al servidor terminal y teniendo acceso a la red interna. Si el servidor terminal lo permite, el intruso puede tener acceso a la red interna desde dicho servidor, y después utilizar telnet para salir de nuevo, lo que dificulta rastrearlo. Asimismo, si el intruso lo utiliza para atacar a otra red, parecer que el ataque se origen en la red de usted.

Según su configuración, las líneas telefónicas pueden dar acceso tan solo a un puerto de conexión de un solo sistema. Si esta conectada a un servidor terminal, la línea de telefónica puede dar acceso a toda la red. Como se menciona al explicar la figura 3.6, una línea telefónica en una estación de trabajo que ejecute software TCP/IP puede dar acceso a toda la red.

SISTEMAS MAL CONFIGURADOS

Cuando los intrusos penetran en la red, por lo general tratan de alterar el funcionamiento los hosts del sistema.

Los blancos preferidos son los hosts que actúan como servidores telnet. Si el host esta mal configurado, el sistema puede ser alterado con facilidad. Los sistemas mal configurados son responsables de numerosos problemas de seguridad de red.

ANTECEDENTES DE LA SEGURIDAD EN REDES

Los modernos sistemas operativos y su software correspondiente se han vuelto tan complicados, que entender cómo funciona el sistema no solo es un trabajo de tiempo completo, sino que requiere conocimientos especializados. Los distribuidores también pueden ser responsables de la mala configuración de los sistemas. Muchos distribuidores envían los sistemas con la seguridad totalmente abierta. Las contraseñas de cuentas importantes pueden no estar establecidas, o usar combinaciones de contraseñas y logins fácilmente descifrables. El libro The Cuckoo's Egg, de Cliff Stoll, narra la historia real de una cacería global de un espía de computadoras y menciona cómo el intruso obtuvo el acceso a los sistemas mediante una combinación de logins y contraseñas como `Sistema / administrador campo / servicio, etcétera.

PROBLEMAS DE SOFTWARE

Al aumentar la complejidad del software, también aumenta el número y la complejidad de los problemas de un sistema determinado. A menos que se encuentren formas revolucionarias de crear software, éste nunca estar por completo libre de errores. Las fallas de seguridad conocidas públicamente se vuelven métodos comunes de acceso no autorizado. Si la implementación de un sistema es abierta y muy conocida (como es la de Unix), el intruso puede usar los puntos débiles del código de software que se ejecuta en modo privilegiado para tener acceso privilegiado al sistema. Los administradores de sistemas deben estar conscientes de los puntos débiles de sus sistemas operativos y tienen la responsabilidad de obtener las actualizaciones y de implementar las correcciones cuando se descubran esos problemas. También usted debe tener la política de reportar al proveedor los problemas cuando se encuentren, de modo que pueda implementarse y distribuirse la

solución.

AMENAZAS INTERNAS

Por lo general, los usuarios internos tienen más acceso al software de la computadora y de la red que al hardware. Si un usuario interno decide alterar el funcionamiento la red, puede representar una considerable amenaza a la seguridad de la red. Si usted tiene acceso físico a los componentes de un sistema, este es fácil de alterar el funcionamiento. Por ejemplo, pueden manipularse fácilmente las estaciones de trabajo para que otorguen acceso privilegiado. Puede ejecutarse fácilmente decodificación de protocolo y software de captura para analizar él trafico de protocolo. La mayoría de los servicios de aplicación estándar TCP/IP como telnet, rlogin y ftp, tienen mecanismos de autentificación muy débiles, en los que las contraseñas se envían en forma clara. Debe evitarse el acceso a estos servicios desde cuentas privilegiadas, ya que esto puede comprometer fácilmente las contraseñas de dichas cuentas.

SEGURIDAD FÍSICA

Si la computadora misma no esta físicamente segura, pueden ignorarse fácilmente los mecanismos de seguridad del software. En el caso de las estaciones de trabajo DOS(Windows ni siquiera existe un nivel de contraseña de protección. Si se deja desatendida una estación de trabajo Unix, sus discos pueden ser cambiados o si se deja en modo privilegiado, la estación estar por completo abierta. Asimismo, el intruso puede parar la máquina y regresarla a modo privilegiado, y después plantar programas tipo caballo de Troya, o tomar cualquier medida para dejar al sistema abierto para ataques futuros.

Todos los recursos importantes de la red, como las backbons, los vínculos de comunicación, los hosts, los servidores importantes y los mecanismos clave deben estar ubicados en una rea físicamente segura. Por ejemplo, el mecanismo de autentificación Kerberos requiere que su servidor está físicamente seguro. Físicamente seguro significa que la máquina está guardada en una habitación o colocada de tal modo que se restrinja el acceso fisco a ella.

En ocasiones no es fácil asegurar físicamente las máquinas. En esos casos, debe tenerse cuidado para no confiar demasiado en esas máquinas. Usted debe limitar el acceso desde máquinas no seguras hacia las más seguras. En particular, usted no debe permitir acceso a hosts que usen mecanismos de acceso confiable como las utileras Berkeley−r* (rsh, rlogin, rcp, rexec).

Aún cuando la máquina está segura físicamente, debe tener cuidado en quién tiene acceso a ella. Las tarjetas electrónicas inteligentes para tener acceso a la habitación en la que están aseguradas las máquinas pueden limitar el número de personas con acceso y proporcionar un registro de la identidad y hora de las personas que entraron en la habitación. Debe establecer en la política que los empleados con acceso no podrán introducir a otras personas en la sala segura cuando está abierta la puerta, aun cuando se conozca la identidad de esas personas.

Si usted permite que entre alguien junto con una persona autorizada, no podrá llevar un registro adecuado de quién y cuando entre en la habitación.

Recuerde que el personal de mantenimiento y limpieza del edificio quizá tenga acceso a la sala de seguridad. Asegúrese de tomar esto en cuenta al diseñar el sistema de seguridad.

CONFIDENCIALIDAD

La confidencialidad puede definirse como el hecho de mantener las cosas ocultas o secretas. Esta es una consideración muy importante para varios tipos de datos delicados.

Las siguientes son algunas de las situaciones en las que la información es vulnerable de ser divulgada:

- ***Cuado la información está almacenada en un sistema de cómputo.***
- ***Cuando la información está en tránsito hacia otro sistema en la red.***
- ***Cuando la información está almacenada en cintas de respaldo.***

El acceso a la información que está almacenada en una computadora está controlado mediante los permisos de archivo, las listas de control de acceso (ACL) y otros mecanismos similares.

La información en tránsito puede protegerse mediante la encriptación o los gateways de las firewalls. La encriptación puede usarse para proteger la información en las tres situaciones. El acceso a la información almacenada en cintas puede controlarse mediante la seguridad física, como puede ser guardar las cintas en una caja de seguridad o en un rea inaccesible.

IMPLEMENTACION DE CONTROLES ECONOMICOS VIABLES PARA LA POLÍTICA

Deben seleccionarse los controles y los mecanismos de protección de modo que estos puedan hacer frente adecuadamente a las amenazas detectadas en la evaluación de riesgos. Estos controles deben implementarse en forma económicamente viable. Tiene poco sentido gastar grandes cantidades de dinero y sobreproteger y restringir el uso de un recurso, si especifico el riesgo de exposición.

El sentido común es, en muchas ocasiones, una herramienta muy eficaz para establecer la política de seguridad. Si bien son impresionantes los elaborados planes y mecanismos de seguridad, estos pueden ser bastante costosos. En ocasiones, el costo de esta implementación está oculto. Por ejemplo, usted podría implementar una solución de seguridad mediante software gratuito, sin tomar en cuenta el costo de administrar ese sistema y mantenerlo actualizado.

Además, si la solución de seguridad es muy elaborada, puede ser difícil de implementar y administrar. Si la administración constituye un paso único, los comandos para administrar tal sistema pueden ser fáciles de olvidar.

También debe mantener la perspectiva de que, por muy elaborada que sea la solución, una contraseña débil o robada puede comprometer a todo el sistema.

A continuación damos algunos lineamientos para implementar controles costeadles para la política.

SELECCION DE CONTROLES RELACIONADOS CON LAS POLÍTICAS

Los controles que usted seleccione serán la primera línea de defensa en la protección de su red. Estos controles deben representar con precisión lo que usted intenta proteger, tal como está definido en la política de seguridad. Si las intrusiones externas son una gran amenaza contra su sistema, quizá no sea económicamente emplear dispositivos biométricos para autentificar a los usuarios internos. En cambio, si la amenaza mayor a sus sistemas es el uso no autorizado de los recursos de computadora por los usuarios internos, usted necesitar establecer buenos procedimientos de contabilidad automatizados. Si la amenaza principal a la red son los usuarios externos, usted tendrá que construir routers de selección y firewalls.

USO DE ESTRATEGIAS DE RESERVA

Si el análisis de riesgo indica que proteger un recurso es vital para la seguridad de la red, necesitará usar diversas estrategias para hacerlo, lo cual le da a usted la seguridad de que, si una estrategia falla o es alterada, otra puede entrar en acción y seguir protegiendo el recurso de la red.

Puede resultar más económico y sencillo usar varias estrategias, de fácil implementación pero eficaces, que seguir una sola estrategia complicada y sofisticada. Este último es el principio del todo o nada. Si el mecanismo elaborado es vencido, no hay ninguno de reserva que proteja al recurso.

Ejemplos de controles sencillos son los módems de devolución de llamada, que pueden usarse en combinación con mecanismos tradicionales de conexión. Esto puede reforzarse con tarjetas inteligentes y autentificadotes manuales de un paso.

DETECCION Y VIGILANCIA DE ACTIVIDADES NO AUTORIZADAS

Si ocurre una intrusión o un intento de intrusión, debe detectarse tan pronto como sea posible.

Usted puede implantar varios procedimientos sencillos para detectar el uso no autorizado de un sistema de cómputo. algunos procedimientos se basan en herramientas proporcionadas con el sistema operativo por el proveedor. También se dispone públicamente de tales herramientas en Internet.

INSPECCION DEL USO DEL SISTEMA

El administrador del sistema puede realizar periódicamente la inspección. Si no, puede usarse software elaborado con este fin. La inspección de un sistema implica revisar varias de sus partes y buscar cualquier cosa que sea inusual. En esta sección se explican algunas de las formas para hacer esto.

La inspección debe hacerse con regularidad. No es suficiente hacerla cada mes o cada semana, ya que esto provocaría una brecha de seguridad que no seria detectada en mucho tiempo.

Algunas violaciones de seguridad pueden detectarse unas cuantas horas después de haberse cometido, en cuyo caso no tiene sentido la inspección semanal o mensual. El objetivo de la inspección es detectar la brecha de seguridad en forma oportuna, de modo que se pueda reaccionar adecuadamente a ella.

Si usted utiliza herramientas de inspección, debe examinar periódicamente la información de estas. Si los registros son voluminosos, tal vez necesite usar los scripts awk o perl para analizar la información. Estas herramientas también están disponibles para sistemas que no son Unix.

MECANISMOS DE INSPECCION

Muchos sistemas operativos almacenan la información de conexiones en archivos de registro especiales. El administrador del sistema debe examinar regularmente estos archivos de registro para detectar el uso no autorizado del sistema. La siguiente es una lista de métodos que puede utilizar en su sitio.

Puede comparar las listas de los usuarios que estén conectados en ese momento con los registros de las conexiones anteriores. La mayoría de los usuarios tienen horarios de trabajo regulares y se conectan y desconectan casi a la misma hora todos los días.

- Una cuenta que muestre actividad fuera del horario normal del usuario debe inspeccionarse de cerca. Quizá un intruso este usando esa cuenta. También puede alertarse a los usuarios para que observen el último mensaje de conexión que aparece al momento de hacer su primera conexión. Si notan algún horario inusual, deben avisarle al administrador del sistema.
- Muchos sistemas operativos llevan registros de contabilidad para efectos de cobranza. También pueden examinarse esos registros para detectar cualquier pauta desacostumbrada de uso del sistema. Los registros de contabilidad inusuales pueden indicar una penetración ilegal en el sistema.
- El sistema operativo quizá tenga también utilerías de registro de conexión, como el syslog usado en Unix. Deben revisarse los registros producidos por dichas herramientas para detectar cualquier

mensaje de error desacostumbrado producido por el software del sistema. Por ejemplo, un gran número de intentos fallidos de conexión en un periodo corto puede indicar que alguien está tratando de adivinar contraseñas. También debe inspeccionar el número de intentos de registro de conexión en las cuentas delicadas como root, sysadm, etcétera.

- Muchos sistemas operativos tienen comandos, como el ps de Unix, que enlistan los procesos que se están ejecutando en ese momento. Pueden usarse estos comandos para detectar si los usuarios están ejecutando programas a los cuales no están autorizados, así como para detectar programas no autorizados que quizá hayan sido iniciados por un intruso.
- Pueden usarse los gateways de las firewalls para crear un registro del acceso a la red. Esta debe inspeccionarse con regularidad. Más adelante se explican con detalle las firewalls.
- Si usted tiene recursos especiales que desee inspeccionar, puede construir sus propias herramientas con las utileras estándar del sistema operativo. Por ejemplo, puede combinar los comandos **ls** y **find** de Unix en un script de shell para revisar las configuraciones de propiedades y permisos privilegiados de archivo. Puede guardar la salida de esta actividad de inspección en listas que se pueden comparar y analizar mediante herramientas comunes de Unix como diff, awk o perl. Las diferencias en los permisos de archivos importantes pueden indicar modificaciones no autorizadas en el sistema.

HORARIO DE INSPECCION

Los administradores del sistema deben inspeccionar con frecuencia y regularidad a lo largo de todo el día. Puede resultar muy fastidioso inspeccionar por horarios fijos, pero pueden ejecutarse comandos de inspección a cualquier hora, en los momentos desocupados, por ejemplo, cuando usted está hablando de negocios por teléfono.

Si ejecuta los comandos de inspección con frecuencia, se familiarizará rápidamente con la información normal de estas herramientas de inspección. Esto le ayudar a detectar la información inusual. Es posible intentar automatizar este proceso ejecutando herramientas de búsqueda sobre la información, y se pueden buscar ciertos patrones fijos, pero generalmente es difícil detectar toda la información inusual causada por la intrusión en el sistema. El cerebro humano sigue siendo mejor que la mayoría de los programas para detectar sutiles diferencias en los registros de inspección.

Si ejecuta diversos comandos de inspección a diferentes horas del día, será difícil que un intruso prediga sus acciones. El intruso no puede saber cuándo el administrador correrá el comando de inspección para desplegar a los usuarios conectados, por lo que corre mayor riesgo de ser detectado. Por otra parte, si el intruso sabe que todos los días, a las seis de la tarde, el sistema se revisa para ver que todos se hayan desconectado, esperará a que concluya esta revisión antes de conectarse.

La inspección es útil, pero también puede ser alterada. Algunos intrusos pueden darse cuenta de los mecanismos estándar de registro de conexiones que se usen en el sistema y pueden tratar de desactivarlos. La inspección periódica puede detectar a los intrusos, pero no ofrece ninguna garantía de que el sistema esta a salvo. No es un método infalible para detectar a los intrusos.

PROCEDIMIENTOS DE REPORTE

En caso de que se detecte algún acceso no autorizado, debe haber procedimientos para reportar este acceso y a quién será informado. Además, su política de seguridad debe cubrir los siguientes aspectos:

- ***Procedimientos de administración de cuentas***
- ***Procedimientos de administración de configuración***
- ***Procedimientos de recuperación***
- ***Procedimiento de reporte de problemas para los administradores del sistema***

PROCEDIMIENTOS DE ADMINISTRACION DE CUENTAS

Cuando se crean cuentas de usuario, debe tenerse cuidado en no dejar ninguna laguna de seguridad. Si el sistema operativo se esta instalando desde los medios de distribución, debe examinarse que la contraseña no tenga cuentas privilegiadas que usted no necesite.

Algunos vendedores de sistemas operativos proporcionan cuentas para los ingenieros de servicio de campo y servicios de sistemas. Estas cuentas o no tienen contraseña o son de dominio publico. Si usted necesita estas cuentas, debe darles una contraseña nueva; si no, debe eliminarlas o desactivarlas. En general no hay ninguna razón para permitir cuentas que no tienen una contraseña establecida.

Las cuentas sin contraseña son peligrosas aun cuando no ejecuten interpretes de comandos, como la cuenta que existe tan solo para ver quién esta conectado en el sistema. Si estas no están establecidas correctamente, puede comprometerse la seguridad del sistema. Por ejemplo, si no se establece adecuadamente el usuario anónimo de una cuenta FTP a cualquier usuario le estar permitido el acceso al sistema para recuperar archivos. Si se cometen errores al establecer esta cuenta, e inadvertidamente se concede el permiso de escritura al sistema de archivos, un intruso puede cambiar el archivo de contraseñas o destruir el sistema.

El recurso shadow password se utiliza por primera vez en el System V, pero hay otros sistemas Unix que cuentan con el, como SunOS 4.0 y superior, y el 4.3BSD Unix Tahoe. El archivo shadow password permite que la forma encriptada de las contraseñas esta oculta para los usuarios no privilegiados. El intruso, por lo tanto, no puede copiar el archivo de contraseñas y tratar de adivinarlas.

Su política también debe incluir los procedimientos para llevar cuenta de quién tiene cuenta privilegiada, como raíz en Unix y MAINT en VMS. En Unix, si usted conoce la contraseña raíz (Root), puede usar el comando **su** para usurpar privilegios de raíz. Si se descubre la contraseña en forma inadvertida, el usuario puede conectarse con su cuenta personal y usurpar privilegios de raíz. Por lo tanto, usted debe implantar una política que obligue a los usuarios privilegiados a cambiar de contraseña a intervalos periódicos.

Asimismo, cuando un usuario privilegiado abandone la organización, se le debe avisar a usted para que cambie la contraseña de las cuentas privilegiadas.

Además deben cambiarse las cuentas de usuario de quienes salgan de la compañía.

Los servicios de red deben someterse a un estrecho escrutinio. Muchos proveedores proporcionan archivos de permisos de red predeterminados, que suponen que todos los hosts externos son confiables. Éste no es el caso cuando se esta conectado a una red como Internet.

Los mismos intrusos recaban información acerca de los puntos vulnerables de sistemas en particular. En ocasiones hacen circular sus descubrimientos en revistas clandestinas, como las siguientes:

- 2600 Magazine
- Phrack
- Computer Underground Digest

Ciertos administradores de sistemas deberían subscribirse a tales publicaciones, para mantenerse adelante de los intrusos.

PROCEDIMIENTOS DE ADMINISTRACION Y CONFIGURACIÓN

Usted debe mantener actualizadas las versiones del sistema operativo y de utileras importantes.

Por lo general, los puntos débiles de los sistemas anteriores son bien conocidos y es probable que el intruso se dé cuenta de los problemas de seguridad. Desgraciadamente, las nuevas versiones del software, si bien arreglan algunos problemas de seguridad, en muchas ocasiones crean otros.

Por esta razón es importante sopesar los riesgos de no actualizarse con la nueva versión del sistema operativo y dejar descubiertas lagunas de seguridad, contra el costo de actualizarse con un nuevo software.

Aunque puede confiarse en la mayoría de los proveedores en el envío de sus actualizaciones, muchas organizaciones dependen del bienestar del software público desarrollado para cierta actividad dentro de su compañía. Muchas empresas de ***software*** envían su producto con PGP u otras firmas digitales para demostrar que nadie ha alterado su software.

Tripwire es una herramienta que ayuda a administradores de sistemas y usuarios a inspeccionar cualquier cambio en un conjunto designado de archivos. Usado con archivos de sistema en forma regular (es decir, diario), Tripwire puede notificar al administrador acerca de archivos alterados o manipulados, de modo que puedan tomarse medidas de control en forma oportuna.

Tripwire puede encontrarse en el siguiente URL:

ftp://ftp/nordu.net/net−Working/security/tools/tripwire/tripwire−1.2.tar.gz.

Por lo general, puede confiarse en la mayoría de los proveedores, en el sentido de que las nuevas versiones del software arreglen problemas de seguridad anteriores y no generen otros más grandes. Otra complicación es que la nueva versión puede quebrantar software de aplicación del que dependan los usuarios. Quizá tenga que coordinar la campaña de actualización con más de un proveedor.

También se pueden recibir soluciones a través de las listas de correo en la red. Usted debe tener personal competente que examine con cuidado estas soluciones a los problemas y que las implante sólo si son seguras.

Como regla, usted no debe instalar una solución si no conoce las consecuencias de tal solución. Siempre es posible que los autores de la solución tengan un código no evidente que les permita acceso no autorizado a su sistema.

PROCEDIMIENTOS DE RECUPERACIÓN

Siempre que instale una nueva versión del sistema operativo, usted no sólo debe hacer respaldo de la imagen binaria del kernel del sistema operativo, sino también de los archivos usados para compilar y configurar dicho sistema. Lo mismo es válido para todo el software de aplicación y de red.

Los respaldos del sistema de archivos son como una póliza de seguros. No só1o lo protegen en

caso de fallas del disco y de otras partes del hardware, sino también contra eliminaciones accidentales y como medida de reserva cuando el sistema es penetrado. Si usted sospecha que alguien ha irrumpido en su sistema, quizá tenga que restablecerlo desde el respaldo para protegerse de los cambios que pudiera haber hecho el intruso. Si usted no puede detectar cuándo ocurrieron los cambios no autorizados, tendrá que examinar numerosos respaldos. Si no cuenta con una buena copia del software del sistema, ser difícil determinar cómo deben de ser los datos y los archivos del sistema.

Los respaldos diarios, así como los de incremento, pueden ser útiles para ofrecer la historia de las actividades del intruso. Al examinar los respaldos anteriores, puede determinar cuándo se penetró por primera vez en el sistema. Aún cuando hayan sido borrados los archivos del intruso, usted podrá verlos en las cintas de respaldo.

Cuando busque rastros de archivos intrusos, debe buscar nombres de archivo que normalmente no aparecerían en el listado del directorio. En los sistemas Unix, a los intrusos les gusta guardar datos en archivos cuyo nombre empieza con punto (.) o que tengan caracteres no desplegables. Estos archivos son más difíciles de detectar.

Usted debe decidir la estrategia de respaldo, lo cual implica la combinación de los siguientes

métodos:

- ***Respaldo total***
- ***Respaldo de nivel 1***
- ***Respaldo de nivel 2***
- ***Respaldo personalizado***

En los sistemas Unix, al respaldo total también se le llama de nivel 0. En estos sistemas, el respaldo de nivel I respalda todos los archivos que han sido modificados desde el último respaldo de nivel 0. En general, un respaldo de nivel N respalda todos los archivos modificados desde el último respaldo de nivel N−1. En el caso de utileras de respaldo, como dump, el respaldo de nivel N respalda todos los archivos modificados desde el último respaldo N−1 o inferior.

Se puede usar un número arbitrario de niveles, pero en general no tiene sentido, pues se dificulta seguir la pista de los respaldos. Los niveles de respaldo numéricos tienen soporte con comandos de respaldo de tipo BSD, desde el nivel 0 al nivel 9, pero esta idea puede usarse con cualquier sistema y usted quizás tenga que llevar la cuenta a mano. En BSD de Unix el programa de respaldo es dump, y los archivos que se han respaldado en un nivel específico se guardan en el archivo /etc/dump/dates.

En el respaldo total (nivel 0) se respaldan todos los datos, sin importar cuando hayan sido modificados, ni aun cuando no lo hayan sido. Un ejemplo de esto son todos los directorios y archivos de un sistema de archivos. Después de haber respaldado los datos, se elimina el bit de archivero en todos los archivos respaldados.

La estrategia de respaldo total es la más exhaustiva de todas, ya que respalda todos los archivos sin importar si estos fueron modificados o no desde el último respaldo. Si embargo, debido al gran volumen de datos que pueden requerir respaldo, es la más lenta de las estrategias.

En el respaldo de nivel 1 se respaldan todos los archivos que se hayan modificado desde el último respaldo total (de Nivel 0). Esto significa que todos los archivos que hayan sido respaldado en el 1º respaldo de nivel 1 lo serán también en el siguiente respaldo de nivel 1, junto con aquellos que se hayan modificado desde el 1º respaldo de nivel 1. Este proceso continua con cada respaldo de nivel 1 y puede esperarse que, en cada proceso, aumente el número de archivos respaldados.

Existe una lamentable confusión de términos para referirse al respaldo de nivel 1 . En los sistemas Unix el respaldo de nivel 1 es llamado respaldo incremental. En muchos sistemas no Unix (Sistemas operativos DOS / WINDOWS / PC para LAN) este nivel es llamado respaldo diferencial. El término respaldo incremental en muchos sistemas no Unix significa algo por completo diferente. Para evitar confusiones, usted debe establecer claramente en su política que definición está siguiendo.

Para obtener un registro completo de las versiones más actualizadas de los archivos, usted debe empezar con el respaldo completo más reciente (Nivel 1) y agregar a éste los archivos del respaldo de Nivel 1 más reciente. Esto es respaldo más reciente = último respaldo total más d, donde el d es el respaldo de nivel 1 más reciente.

Ya que el último respaldo de nivel 1 contiene todos los archivos modificados desde el último respaldo total,

usted podrá restaurar los datos con tan solo 2 juegos de cintas: una para el respaldo total y otra para el último respaldo de nivel uno.

Si los datos en uno de los últimos respaldos de nivel 1 están corrompidos, usted tendrá que acudir a su reserva del penúltimo respaldo diferencial. Por otra parte, si está corrompido algún dato de otra cinta de respaldo de nivel 1, no importa en tanto que estén bien los datos en el más reciente respaldo diferencial.

Si por cierto tiempo no se ha hecho ningún respaldo total, y ha habido muchos cambios en el archivo, en cada respaldo de nivel 1 tenderá a crecer el tamaño de los datos que requieran respaldo.

Si se han modificado todos los archivos la sesión de respaldo de nivel 1 será igual que la del respaldo total. Esto suele no ser el caso, ya que la mayoría de los sistemas contienen una mezcla de programas y de datos y los programas de archivos suelen no modificarse.

En muchos sistemas no Unix se utiliza el término respaldo incremental para referirse al respaldo de todos los archivos que hayan sido modificados desde el último respaldo (de nivel 0 ó 1). Esto es como el respaldo de nivel 2 en los sistemas Unix. Los archivos que no se hayan modificados no se respaldarán. Para obtener un registro completo de las versiones más actualizadas de los archivos, usted empezaría con el respaldo total más reciente, y agregaría los cambios registrados en cada sesión de respaldo incremental. Esto es:

Respaldo más reciente = último respaldo total + + + n

Último respaldo total + i (i = 1ª n)

Donde cada i es un respaldo incremental.

El respaldo incremental contiene la historia secuencial de los archivos que se han modificado.

Esto significa que, para restaurar los datos usted necesita el último respaldo total y todos los respaldos incrementales posteriores. Si los datos en una de las cintas de respaldo están corrompidos, quizás no pueda restaurarlos. La excepción a esto son las situaciones en la que los respaldos incrementales posteriores tienen los archivos que están inaccesibles en las cintas corrompidas. En este caso, usted podrá restaurar esos datos a partir de las cintas posteriores.

El respaldo personalizado le da el control completo de los archivos que se respaldarán. Usted puede incluir o excluir ciertas partes de la estructura de directorios que serán respaldado, o seleccionar diferentes tipos de elementos de datos que serán respaldados. Los respaldos personalizados son útiles cuando usted quiere respaldar en forma selectiva unos cuantos archivos y directorios y no esperar al respaldo programado.

PROCEDIMIENTO DE REPORTE DE PROBLEMAS PARA LOS ADMINISTRADORES DEL SISTEMA

Ya se abordó el tema de los procedimientos para que los usuarios reporten problemas. Los administradores del sistema deben contar con un procedimiento definido para reportar los problemas de seguridad. En grandes instalaciones de red, esto puede hacerse mediante una lista de correo electrónico que contenga las direcciones de correo electrónico de todos los administradores de la organización. En algunas organizaciones se forma un equipo de respuesta que ofrece un servicio de emergencia.

PROTECCION DE LAS CONEXIONES DE RED

Si es probable que el ataque del intruso se realice a través de una red de conexión externa, como Internet, talvez tenga que proteger las conexiones con la red externa.

Puede usarse un dispositivo de firewall para ofrecer un punto de resistencia a la entrada de intrusos en la red. Además de la firewall puede usarse routers de selección.

Algunos sitios de la organización necesitan conectarse con otros sitios de la misma organización, y está prohibido que se conecten a redes externas. Estas redes son menos susceptibles de amenazas desde fuera de la red de la organización. De todos modos, pueden ocurrir intrusiones inesperadas a través de módems de acceso telefónico situados en las estaciones de trabajo de escritorio de los usuarios.

Una organización podría necesitar conexiones con sus demás sitios a través de redes grandes

como Internet. Si los protocolos que dichos sitios utilizan son diferentes de los de Internet,

puede emplearse una técnica llamada túneles IP. Tales sitios son susceptibles de amenazas externas.

Muchas organizaciones requieren la conexión a Internet debido a los servicios que ésta ofrece.

Deben sopesarse los riesgos de seguridad de conectarse a una red externa contra sus beneficios.

Se debe limitar el número de puntos de acceso a la red. Además, debe conectarse a redes

externas a través de hosts que no guarden material delicado. También deben eliminarse de tales hosts las herramientas de desarrollo de software y otras herramientas privilegiadas que podría ser usadas para sondear su red. La idea es proporcionar un grado de aislamiento o una firewall entre su red y la externa. Los servicios importantes requeridos por la organización pueden mantenerse detrás del segmento aislado de la red.

Debe considerar seriamente la posibilidad de restringir el acceso a una red externa a través de un solo sistema. Si todo el acceso a la red externa se realiza a través de un solo host, éste actúa como firewall entre usted y la red externa. El sistema de firewall debe estar estrictamente controlado y protegido con contraseña. Los usuarios externos que necesiten acceso a la red interna tendrán que pasar por la firewall. El host de firewall puede seleccionar adecuadamente las llamadas de entrada.

El sistema de firewall no es garantía contra el éxito de los ataques de intrusos. Si un intruso logra comprometer la seguridad de la firewall, tendrá acceso a la red interna detrás de esa barrera.

USO DE LA ENCRIPTACION PARA PROTEGER LA RED

Puede usarse la encriptación para proteger los datos en tránsito, así como los almacenados.

Algunos proveedores ofrecen dispositivos de encriptación de hardware que pueden usarse para encriptar y desencriptar datos en conexiones de punto a punto.

La ***encriptación*** puede definirse como el proceso de tomar información que se encuentra en cualquier forma legible y convertirla a una forma que no pueda ser entendida por otros.

Si el receptor de los datos encriptados desea leerlos, debe convertirlos a su forma original en un proceso llamado ***desencriptación,*** el cual es el inverso del proceso de encriptación. Para llevar a cabo la desencriptación, el receptor debe contar con un dato especial llamado clave.

La clave debe guardarse y distribuirse con cuidado. La ventaja de usar encriptación es que, aun si el intruso logra vencer otros métodos de protección de datos (listas de control de acceso, permisos de archivo, contraseñas, etcétera), los datos no tendrán significado para él.

Existen muchos tipos de paquetes de encriptación, tanto en hardware como en software. Los paquetes de software de encriptación están disponibles en forma comercial o gratuita. El hardware de encriptación por lo general se construye en torno a procesadores dedicados y es mucho más rápido que su equivalente en software.

Por otra parte, si el intruso tiene acceso al hardware puede elaborar esquemas de desencriptación basados en el mismo hardware que utilizará para un ataque intenso contra la información encriptada.

Los datos que están en tránsito en una red son vulnerables a la intercepción. En algunos sitios se prefiere encriptar todo el archivo, como paso adicional antes de enviarlo. Esto en ocasiones se llama encriptación de extremo a extremo. En otros sitios se prefiere encriptar los datos en forma dinámica conforme llegan a la red, mediante hardware de encriptación que crea un vínculo seguro.

Si todo el paquete se encripta antes de enviarse, como en el hardware de encriptación, los routers con protocolo IP que no entienden el paquete encriptado lo rechazarán. Si desea usar encriptación en Internet, debe encriptar los datos en un paso aparte y pasarlos al proceso de aplicación.

A continuación damos una breve explicación de los diferentes métodos de encriptación. En la política de seguridad de red, usted debe especificar cuál de estas técnicas de encriptación va a utilizar, si va a emplear alguna.

ESTANDAR DE ENCRIPTACION DE DATOS (DES)

El DES es un mecanismo de encriptación de datos muy utilizado y del cual existen varias implementaciones tanto en software como en hardware. El DES transforma información de texto llano en datos encriptados, llamado *texto cifrado,* mediante un algoritmo especial y un valor *semilla* llamado clave. Si el receptor conoce la clave, puede usarla para convertir el texto cifrado en los datos originales.

Un punto débil potencial de todos los sistemas de encriptación es la necesidad de recordar la clave mediante la cual fueron encriptados los datos. En este sentido, es similar al problema de recordar la contraseña. Si la clave está por escrito y una persona no autorizada la llega a conocer, los datos originales podrán ser leídos. Si se olvida la clave, entonces no se podrán recuperar los datos originales.

Hay muchos sistemas que soportan el comando DES, o utilerías y bibliotecas de código que pueden ser usadas por DES.

CRYPT

En los sistemas Unix el comando crypt también puede usarse para encriptar datos. El algoritmo usado por crypt está basado en el dispositivo *Enigma,* de tiempos de la Segunda Guerra Mundial, y es muy inseguro. Los archivos encriptados con crypt pueden desencriptarse fácilmente *con un* ataque intenso en cuestión de horas. Por esta razón debe *evitarse el* comando crypt para los datos delicados y dejarse para tareas de encriptación triviales.

CORREO DE PRIVACIDAD MEJORADA(PEM)

El correo electrónico por lo general se envía en Internet mediante el Protocolo Simple de Transferencia de Correo (SMTP, Simple Mail Transfer Protocol). Este protocolo es muy sencillo y transmite los datos a la vista. Además, puede usarse para trasmitir sólo textos ASCII. Si usted desea enviar un mensaje encriptado, debe usar medios indirectos. Primero debe encriptar el mensaje, con lo que lo convierte en archivo binario. Debido a que no puede usarse SMTP para trasmitir datos binarios −sólo transmite datos de texto− tiene que codificar los datos binarios como texto.

Una forma muy común de hacer esto en Internet es con una utilería llamada uuencode. El receptor del mensaje tiene que usar una utilería llamada uudecode para convertir el texto a su forma binaria encriptada original. Si el receptor conoce la clave, puede desencriptar el mensaje. Si bien es posible asegurar el correo a través del método que acabamos de esbozar, es incómodo y laborioso. Asimismo, está el problema de distribuir la clave a los receptores del mensaje. Usted debe considerar si esto se debe hacer a través de Internet o de algún otro método de distribución.

Un enfoque que ha atraído gran interés es el Correo de Privacidad Mejorada (PEM, Privacy Enhanced Mail), el cual constituye una forma de encriptar los mensajes de correo electrónico en forma automática, antes de que sean enviados. No hay procedimientos separados que haya que seguir para encriptar el mensaje de correo. Por lo tanto, aun si el mensaje es interceptado en un host de distribución de correo, quien lo haga no podrá leerlo.

PRIVACIDAD BASTANTE BUENA(PGP)

La Privacidad Bastante Buena (PGP, Pretty Good Privacy) fue elaborada por Phil Zimmerman para abordar la cuestión de la encriptación de archivos de clave pública, o asimétrica, y de las firmas digitales. La PGP constituye una forma sólida de protección criptográfica de la que antes no se disponía y que se utiliza para proteger correo electrónico, archivos y documentos con firma digital; está disponible en forma comercial y no comercial.

Los residentes de Estados Unidos y Canadá pueden obtener la PGP en el sitio del MIT. http://web.mit.edu/network>1pgp.form.html. También se encuentra en otros lugares de Internet.

Hay gran variedad de formatos y programas de firma digital. Algunos de ellos están a disposición pública, lo que significa que, si usted tiene algún problema, debe resolverlo por su cuenta o esperar a que alguien lo ayude. Una alternativa es usar un producto comercial que tenga soporte de encriptación de archivos y firmas digitales como el producto Entrust de Northern Telecom Secure Network (URL http: //www.entrust.com) o la versión comercial de PGP de Viacrypt (teléfono (602) 944−0773). La ventaja de usar un producto comercial es que se le pueden reportar los problemas al fabricante para que éste los resuelva. Además, usted obtiene soporte de usuario y actualizaciones de¡ software y la documentación cuando éstos se publican, lo que asegura que la aplicación no será afectada por nuevos problemas.

AUTENTIFICACIÓN DE ORIGEN

Cuando se recibe un mensaje de correo electrónico, el encabezado de éste indica el origen del mensaje. La mayoría de los usuarios del correo de Internet dan por hecho que el encabezado del mensaje realmente indica el remitente. Sin embargo, si uno es lo bastante astuto, es posible falsificar el encabezado de modo que éste indique que fue enviado desde otra dirección de correo electrónico. A esto se le llama *suplantación* de la dirección de correo electrónico. Para evitar este tipo de falsificaciones puede usarse una técnica llamada autentificación de origen.

La autentificación de origen constituye un medio de garantizar que el remitente de un mensaje realmente sea quien dice ser. Puede considerar la autentificación de origen como un servicio notarial electrónico, similar al notario público que verifica las firmas en los documentos legales. Por lo general, la autentificación de origen se implementa mediante un cripto sistema de clave pública.

Los cripto sistemas usan dos claves, las cuales son independientes en el sentido de que una no puede derivarse de la otra mediante procedimientos matemáticos o algorítmicos. Una de ellas es la *clave pública,* lo que significa que cualquiera la puede encontrar fácilmente y que no se hace ningún intento por ocultarla. La otra es la llamada *clave privada,* lo que significa que sólo es conocida por el dueño. La clave privada debe guardarse con mucho cuidado.

En un cripto sistema de clave pública, el originador utiliza una clave privada para encriptar el mensaje. El receptor utiliza una clave pública, que recibe del originador, para desencriptar el mensaje. La clave pública se usa para auntentificar que sólo el originador pudo haber usado su clave privada. Hay varios criptosistemas públicos que están disponibles.

La implementación más conocida del cripto sistema de clave pública es el sistema RSA (Rivest Shamir Adleman). El estándar Internet del correo de privacidad mejorada utiliza el sistema RSA.

INTEGRIDAD DE LA INFORMACIÓN

Cuando se envían archivos o documentos a través de la red, usted debe tener alguna forma de verificar que éstos no hayan sido alterados. Esto es lo que se llama integridad de la información y se refiere al proceso de verificar que la información enviada esté completa y sin cambios con respecto de la última vez que se verificó. La integridad de la información es importante para instituciones militares, de gobierno y financieras. También puede ser importante que no se revele información clasificada, ya sea con o sin modificaciones. La información que se modifica en forma maliciosa puede crear malas interpretaciones, confusiones y conflictos.

Si la información se envía en forma electrónica a través de la red, una forma de asegurar que no se modifique es mediante *sumas de verificación.* Cualquier forma de encriptación también ofrece la integridad de la información, ya que el interceptor tendría que descifrarla primero, antes de modificarla.

SUMAS DE VERIFICACIÓN

Las sumas de verificación son un mecanismo sencillo y efectivo para verificar la integridad de los archivos. Puede usarse un sencillo procedimiento de sumas de verificación para computar el valor de un archivo y después compararlo con el valor anterior. Si ambas sumas coinciden, es muy probable que el archivo no haya cambiado. Si no coinciden, el archivo ha sido alterado. Muchas utilerías de compresión y descompresión, usadas para conservar espacio en disco y reducir el costo de trasmisión de archivos, generan sumas internas de verificación para verificar sus algoritmos de compresión y descompresión.

Es fácil implementar las sumas de verificación aritméticas. Éstas se forman agregando elementos de 16 o 32 bits al archivo, para llegar al número de sumas de verificación. Aunque son fáciles de implementar, las sumas de verificación aritméticas son débiles desde el punto de vista de la seguridad. Un atacante determinado puede agregarle datos al archivo, de modo que las sumas aritméticas computen el valor correcto.

La CRC (suma de verificación de redundancia cíclica), también llamada *suma de verificación polinomial*, es más segura que la aritmética y su implementación es bastante sencilla. Sin embargo, al igual que la aritmética, puede estar comprometida por un interceptor determinado.

Las sumas de verificación dificultan que el interceptor altere imperceptiblemente la información. Sin embargo, no pueden evitar que se hagan cambios. Usted podría usar otros mecanismos, como los controles de acceso del sistema operativo y la encriptación. Los controles de acceso al sistema operativo sólo protegen los datos cuando éstos están guardados en el sistema de archivos y no los pueden proteger cuando se transmiten en la red.

Las sumas de verificación criptográficas representan un avance con respecto a las aritméticas y a las CRC. Este tipo de sumas se explican a continuación.

SUMAS DE VERIFICACION CRIPTOGRAFICA

En las sumas de verificación criptográfica, también llamadas de *cripto sellado*, los datos se dividen en series pequeñas y se calcula una suma de verificación CRC por cada una de las series. Después se suman las CRCs

de todas las series de datos.

Este método dificulta alterar los datos, ya que el interceptor no conoce el tamaño de las series de datos que se están usando. Este tamaño puede ser variable y se computa mediante técnicas seudo aleatorias, lo que hace en extremo difícil que el interceptor altere los datos. La desventaja de este mecanismo es que en ocasiones requiere muchos recursos de cómputo.

Puede usarse otro método para detectar modificaciones en un archivo, llamado *Código de Detección de Manipulación* (MDC) o función de cálculo (hash function) de una vía. Esta función es llamada así porque no hay dos salidas que puedan producir el mismo valor. Los datos de un archivo se usan como entrada de la función para producir un valor calculado. Si se modifican los datos de un archivo, éste tendrá un valor calculado diferente. Las funciones de cálculo de una vía pueden implementarse con bastante eficiencia y posibilitan la integridad de las verificaciones. Ejemplos de estas funciones son la MD2 (compendio de mensaje 2) y la MD5 (compendio de mensaje 5), que se describen en las RFCs 1319 y 132 1, respectivamente.

COMO USAR SISTEMAS DE AUTENTIFICACIÓN

La autentificación puede definirse como el proceso de proporcionar una identidad declarada a la satisfacción de una autoridad que otorga permisos.

En la mayoría de los sistemas, el usuario tiene que especificar la contraseña de su cuenta para que se le permita registrarse. El propósito de la contraseña es verificar que el usuario sea quien dice ser. En otras palabras, la contraseña actúa como mecanismo que autentifica al usuario. Sin embargo, las contraseñas pueden ser robadas y alguien puede imitar al usuario. Debido a que no se toman las medidas adecuadas con la frecuencia necesaria, las contraseñas robadas son causa de gran número de brechas de seguridad en Internet.

Los sistemas de autentificación son una combinación de hardware, software y procedimientos que permiten al usuario el acceso a los recursos de cómputo. La política de su sitio debe establecer el tipo de mecanismo de autentificación que usted debe adoptar. Si los usuarios se van a registrar en sus cuentas desde un sitio externo, usted deberá usar mecanismos de autentificación más potentes que la contraseña.

Los mecanismos de autentificación van desde las tarjetas inteligentes hasta los dispositivos biométricos como los dispositivos lectores de huellas digitales, lectores de frecuencia de voz y exploradores de retina.

Los mecanismos de autentificación pueden reforzarse mediante mecanismos de desafío/ respuesta. Estos mecanismos le piden al usuario que suministre un dato compartido para la computadora y el usuario, como el nombre de soltera de la madre o algún otro dato especial conocido por el usuario y el sistema.

COMO UTILIZAR TARJETAS INTELIGENTES

Las tarjetas inteligentes son dispositivos manuales y portátiles (HHP) que tienen un microprocesador, puertos de entrada y salida y algunos kilobytes de memoria no volátil. El usuario debe tener uno de estos dispositivos para poder registrarse en el sistema. Esta autentificación se basa en "algo conocido". La computadora host le pregunta al usuario un valor que se obtiene de la tarjeta, cuando la computadora le pide la contraseña. En ocasiones, la máquina host le da al usuario algún dato que éste debe registrar en la tarjeta inteligente. Después, la tarjeta despliega una respuesta que deberá introducirse en la computadora. Si la respuesta es aceptada, se establece la sesión. Algunas tarjetas inteligentes despliegan un número que cambia con el tiempo, pero que está sincronizado con el software de autentificación de la computadora.

COMO UTILIZAR Kerberos

Muchos sistemas pueden mortificarse para usar el mecanismo de autentificación Kerberos. Este mecanismo,

cuyo nombre proviene del perro que en la mitología griega cuidaba las puertas del Hades, es una colección de software que se usa en redes grandes para establecer la presunta identidad del usuario. Creado en el Instituto de Tecnología de Massachusetts (MIT), Kerberos se basa en una combinación de encriptación y bases de datos distribuidas, de modo que los usuarios de las instalaciones universitarias puedan registrarse e iniciar una sesión desde cualquier computadora situada en las instalaciones.

COMO MANTENERSE ACTUALIZADO

Su política de seguridad, además de identificar a las agencias con las que debe hacer contacto en caso de incidentes de seguridad, debe también designar a las personas que deban mantenerse actualizadas con las cuestiones y problemas de seguridad.

Si su organización está conectada a Internet, quizá tenga que inscribirse en las listas de correo o grupos de noticias en los que se discuten temas de seguridad que son de interés para usted.

Recuerde que se requiere tiempo para mantenerse al día con la información de las listas de correo y grupos de noticias. A menos que usted identifique a las personas que deban mantener esta información, y que esta tarea sea parte de su trabajo, el administrador del sistema probablemente no tendrá tiempo para hacerlo.

LISTAS DE CORREO

Las listas de correo son mantenidas por servidores de listas en Internet. Cuando usted se une a una de ellas, puede comunicarse con los demás usuarios a través del correo electrónico. Para enviar sus respuestas u opiniones acerca de un tema, puede enviar correo electrónico a la lista. Todos los que estén en la lista de correo recibirán el mensaje. La solicitud para unirse en una lista de correo se envía a otra dirección, la cual es diferente *de* la dirección de correo electrónico de la lista. La solicitud de suscripción debe enviarse a la dirección de solicitudes y no a la dirección de correo electrónico de la lista. Los miembros de la lista, que pueden ser miles, no apreciarán recibir solicitudes para unirse a una lista de correo. Algunos administradores de listas de correo compilan una lista especial de preguntas frecuentes (FAQs), las cuales constituyen un buen lugar para empezar a buscar más información.

Las listas de correo pueden ser moderadas o no moderadas. En las moderadas, el dueño de la lista actúa de moderador y descarta las respuestas que no estén de acuerdo con los objetivos de la lista.

Se dispone de gran variedad de administradores de listas. Algunos son automáticos y otros se procesan a mano. Si usted tiene dudas de cómo suscribirse o retirarse de una lista, envíe el siguiente comando, en el que *nombrelista* representa el nombre de la lista de la cual usted desea información: *INFO <nombrelista>*

En las listas no moderadas no existe proceso de selección. En consecuencia, la proporción entre señal y ruido puede ser muy baja. Si decide que esa lista de correos no es para usted, envíe una solicitud de "eliminación de suscripción" a la dirección electrónica de solicitudes de la lista (¡y no a la lista en sí!). Esta solicitud debe incluir lo siguiente en el cuerpo principal:

UNSUBSCRIBE listname

El término *proporción entre señal y ruido*, usado en correo electrónico, es un concepto tomado del audio. La señal representa mensajes de correo electrónico reales y significativos; el *ruido* representa los mensajes inútiles, como los de suscripción y prueba, que obstruyen las comunicaciones normales entre quienes utilizan la lista de correo.

LISTAS DE CORREO DE SEGURIDAD DE UNIX

El objetivo de la lista de correo de seguridad de Unix es notificar a los administradores de sistemas acerca de problemas de seguridad, antes de que éstos se hagan de dominio público, así como proporcionar información acerca de temas relacionados con la seguridad. Debido a que la información de este tipo puede resultar dañina si cae en manos de quien no debe, la lista de seguridad de Unix es de acceso restringido. Esta lista está abierta sólo a aquellas personas de las que pueda comprobarse que son los administradores principales de un sitio.

Para suscribirse a esta lista, la solicitud debe originarse desde el contacto del sitio listado en la base de datos VMOIS del Centro de Información sobre Redes de la Red de Datos de la Defensa (DDN NIC, Defense Data Network's Network Information Center), o desde la cuenta raíz de una de las máquinas principales del sitio. Usted debe incluir la dirección destinataria de correo electrónico que desee en la lista. Debe indicar si quiere estar en la lista reflectora de correo o recibir compendios semanales. También debe incluir la dirección de correo electrónico y el número de teléfono del contacto del sitio.

La dirección de correo electrónico para enviar la solicitud de suscripción es la siguiente:
security−request@cpd.com

LA LISTA DEL FORO DE RIESGOS

El foro de riesgos es un componente del Comité de Computadoras y Políticas Públicas ACM. Se trata de una lista moderada en la que se discuten los riesgos para el público de computadoras y sistemas relacionados. También se discuten aspectos de seguridad de interés específico, grandes incidentes internacionales relacionados con la seguridad de computadoras, problemas de sistemas de control de tráfico aéreo y ferroviario, ingeniería de software, etcétera.

Para unirse a esta lista de correo, envíe un mensaje por correo electrónico a la siguiente dirección:

risks−request@csl.sri.com

En el cuerpo del mensaje incluya la siguiente línea:

subscribe risks Nombre Apellido

Si desea recibir la versión compendiada, en lugar de respuestas de correo electrónico individuales, incluya la siguiente línea:

set risks digest

La lista de riesgos también está disponible a través del grupo de noticias Usenet, con el siguiente nombre:

comp.risks

LA LISTA VIRUS−L

En la lista VIRUS−L se habla de experiencias con virus de computación, software de protección y temas relacionados. La lista está abierta al público y está implementada como un compendio moderado. La mayoría de la información se relaciona con las computadoras personales, aunque parte de ella puede aplicarse a sistemas más grandes. Para suscribirse, envíe un mensaje de correo electrónico a la siguiente dirección:

listserv%lehiibml.bitnet@mitvma.mit.edu

0 bien, a:

listserv@lehiibml.bitnet

En el cuerpo del mensaje incluya la siguiente línea:

subscribe virus−L Nombre Apellido

Si desea recibir una versión compendiada, en lugar de respuestas de correo electrónico individuales, incluya la siguiente línea:

set virus−L digest

Esta lista también está disponible a través del grupo de noticias Usenet, con el siguiente nombre:

comp.virus

LA LISTA BUGTRAQ

En la lista Bugtraq se habla de problemas de software y lagunas de seguridad. Usted puede usar esto para evaluar el riesgo de seguridad de su sistema. También se habla de la forma de arreglar las lagunas de seguridad, así que puede utilizar dicha información para resolver ese tipo de problemas en su sistema.

Para suscribirse, envíe un mensaje de correo electrónico a la siguiente dirección:

bugtraq−request@crimelab.com

En el cuerpo del mensaje incluya la siguiente línea:

subscribe bugtraq−list Nombre Apellido

Si desea recibir una versión compendiada, en lugar de respuestas de correo electrónico individuales, incluya la siguiente línea:

set bugtraq−list digest

EL COMPENDIO NO COMERCIAL DE LA COMPUTACIÓN

El compendio no comercial de la computación tiene como objetivo ser "un foro abierto dedicado a compartir información entre gente dedicada a la computación y a la presentación y el debate de diversas opiniones".

Este compendio contiene discusiones acerca de la privacidad y otros temas relacionados con la seguridad. Se le localiza en el siguiente UR−L:

http://sun.soci.nui.edul−cudigest/

Para suscribirse, envíe un mensaje de correo electrónico a la siguiente dirección:

cu−digest−request@weber.ucsd.edu

En el cuerpo del mensaje incluya la siguiente línea: SUB CuD

También incluya los temas SUB CuD en el mensaje.

Esta lista también está disponible a través del grupo de noticias Usenet, con el siguiente nombre:

comp.s ociety.cu−digest

LA LISTA DE CORREO CERT

El Equipo de Respuesta a Emergencias de Cómputo (CERT, Computer Emergency Response Team) publica avisos. En una sección anterior de este capítulo hablamos del CERT, como una organización con la que usted puede ponerse en contacto para obtener ayuda relacionada con la seguridad.

Para suscribirse, envíe un mensaje de correo electrónico a la siguiente dirección:

cert−request@cert.sei.cmu.edu

En el cuerpo del mensaje incluya la siguiente línea:

subscribe cert Nombre Apellido

Si desea recibir una versión compendiada, en lugar de respuestas de correo electrónico individuales, incluya la siguiente línea:

set cert digest

LA LISTA DE CORREO CERT−TOOLS

El CERT también mantiene la lista CERT−TOOLS con el fin de intercambiar información acerca de herramientas y técnicas que retuercen la operación de seguridad de los sistemas Internet. CERT/CC no reseña ni endosa las herramientas descritas en la lista.

Para suscribirse, envíe un mensaje de correo electrónico a la siguiente dirección:
cert−tools−request@cert.sei.cmu.edu

En el cuerpo del mensaje incluya la siguiente línea: subscribe cert−tools *Nombre Apellido*

Si desea recibir una versión compendiada, en lugar de respuestas de correo electrónico individuales, incluya la siguiente línea:

set cert−tools digest

El sitio Web del CERT contiene un cúmulo de información acerca de seguridad, incluyendo todos los avisos del CERT. Puede consultarlo en *http://www.cert. org.*

LA LISTA DE CORREO TCP/IP

La lista de correo TCP/IP es un foro de discusión para desarrolladores y mantenedores de implementaciones del conjunto de protocolos TCP/IP Sin embargo, muchas de las preguntas que se reciben en la lista provienen de usuarios de diversos paquetes TCP/IP, o de quienes buscan ayuda acerca de las aplicaciones de TCP/IP En esta lista también se discuten problemas de seguridad en redes.

Para suscribirse, envíe un mensaje de correo electrónico a la siguiente dirección:

tcp−ip−request@nisc.sri.com

En el cuerpo del mensaje incluya la siguiente línea:

subscribe tcp−ip Nombre Apellido

Si desea recibir una versión compendiada, en lugar de respuestas de correo electrónico individuales, incluya la siguiente línea:

set tcp−ip digest

Esta lista también está disponible a través del grupo de noticias Usenet, con el siguiente nombre:

como.protocolos.tcp−ip

LA LISTA DE CORREOSSUN−NETS

En la lista SUN−NETS se discuten temas relacionados con redes en sistemas de estaciones de trabajo de SUN Microsystems. La discusión se centra en torno a cuestiones de red y de seguridad que tengan que ver con NFS, NIS y servidores de nombre.

Para suscribirse, envíe un mensaje de correo electrónico a la siguiente dirección:

sun−nets−request@umiacs.umd.edu

En el cuerpo del mensaje incluya la siguiente línea:

subscribe sun−nets Nombre Apellido

Si desea recibir una versión compendiada, en lugar de respuestas de correo electrónico individuales, incluya la siguiente línea:

set sun−nets digest

GRUPOS DE NOTICIAS

Los grupos de noticias son foros de discusión que intercambian información a través de programas especiales de lectura de noticias. Para unirse a un grupo, debe utilizar un programa especial de lectura, como nn y tin para sistemas Unix. Los sistemas DOS y Windows cuentan con numerosos paquetes comerciales, así como software compartido y gratuito. El lector de noticias le proporciona gran flexibilidad para manejar mensajes.

Al igual que las listas de correo, los grupos de noticias pueden ser moderados o no moderados. Los grupos Usenet que abordan temas de seguridad son:

misc.security

alt.security

comp.security.announce

El grupo misc.security es moderado y también incluye la discusión de la seguridad física y candados. El grupo alt.security es no moderado. El grupo de noticias comp.security.announce contiene los mensajes enviados a la lista de correo del CERT.

Algunas de las listas de correo también tienen acceso a través de los grupos de noticias. Esto se mencionó en la sección acerca de las listas de correo y las presentamos aquí para su consulta.

comp.risks

comp.virus

alt.society.cu−digest

comp.protocols.tcp−ip

EQUIPOS DE RESPUESTA DE SEGURIDAD

Algunas organizaciones han formado grupos de especialistas en seguridad que manejan los problemas de seguridad de las computadoras. Estos equipos recaban información acerca de las posibles lagunas de seguridad en el sistema y la difunden y reportan a las personas adecuadas. Dichos equipos pueden ayudar a rastrear intrusos y proporcionan ayuda y lineamientos para recuperarse de una violación de seguridad. Los equipos pueden tener listas de distribución de correo electrónico y números telefónicos especiales a los que usted puede llamar para reportar problemas. Algunos de estos equipos son miembros del sistema CERT.

EQUIPO DE RESPUESTA A EMERGENCIAS DE COMPUTO

El Equipo de Respuesta a Emergencias de Cómputo/Centro de Coordinación (CERT/CC) fue establecido en diciembre de 1988 por la Agencia de Proyectos de Investigación Avanzada de la Defensa (DARPA). El objetivo de este equipo es abordar las preocupaciones acerca de seguridad de cómputo de los investigadores en Internet. El CERT es coordinado por el Instituto Nacional de Estándares y Tecnología de Estados Unidos (NIST), y existe para facilitar el intercambio de información entre diversos equipos.

Una de las principales motivaciones para promover el equipo CERT/CC fue evitar y manejar incidentes como el del gusano de Internet, del que hablamos anteriormente en este capítulo.

El CERT es manejado por el Instituto de Ingeniería de Software (SEI) de la Universidad Carnegie Mellon (CMU). Este equipo tiene la capacidad de hablar inmediatamente con expertos para diagnosticar y resolver problemas de seguridad. También pueden ayudar a establecer y mantener la comunicación entre un sitio y las autoridades del gobierno.

Cuando no está dedicado a atender emergencias, el CERT/CC sirve de centro de intercambio para identificar y reparar puntos vulnerables en los principales sistemas operativos. También puede proporcionar evaluaciones informales de sistemas existentes y orientar para mejorar la capacidad de respuesta a emergencias. Debido a esto, puede ayudarlo indirectamente a formular una política eficaz de seguridad de redes. También se sabe que este equipo ha trabajado con proveedores de sistemas de software para coordinar las soluciones a los problemas de seguridad.

El CERT mantiene una línea telefónica de emergencias las 24 horas, a la que se puede llamar para reportar problemas de seguridad, como el que alguien irrumpa en un sistema. También puede llamar a este número para obtener información actualizada acerca de los rumores sobre problemas de seguridad. El número del teléfono de emergencias de 24 horas del CERT es el (412)268−7090.

El CERT/CC le envía avisos de seguridad a la lista de correo CERT−ADVISORY siempre que es apropiado. Para unirse a CERT−ADVISORY, envíe un mensaje de correo electrónico a la siguiente dirección:

cert−requestCacert.sei.cmu.edu

La información sobre seguridad que se envía a esta lista también aparece en el siguiente grupo de noticias Usenet:

comp.security.announce

Los avisos anteriores están disponibles para FTP anónimo desde el host cert.sei.cmu.edu. El servidor FTP de¡ host cert.sei.cmu.edu contiene otra información útil acerca de temas de seguridad. El archivo README de este servidor puede informarle qué está disponible. Si desea mayor información, comuníquese a:

CERT

Software Engineering Institute

Carnegie Mellon University

Pittsburgh, PA, 15213−3890

(412)268−7090

cert@cert.sei.cmu.edu

http://~.cert.org

CENTRO DE COORDINACION DE SEGURIDAD

DDN

Para los usuarios de la Red de Datos de la Defensa (DDN), el Centro de Coordinación de Seguridad (SCC, Security Coordination Center) sirve como una oficina central para discutir los problemas y soluciones de seguridad para usuarios y hosts, y trabaja en combinación con la Oficina de Seguridad de Redes DDN. En este sentido, el DDN SCC ofrece una función similar al CERT.

El SCC publica el Boletín de Seguridad DDN. En este boletín se discuten temas que se relacionan con seguridad de redes y de hosts, soluciones de seguridad, y se interesa por la seguridad y el personal administrativo de las instalaciones DDN. El Boletín de Seguridad DDN está disponible en línea, por medio de transferencias Kermit o mediante FTP anónimo desde el host NIC.DDN.MIL. Los boletines de seguridad están en archivos con el siguiente formato:

SCC:DDN−SECURITY−aa−nn.TXT

Donde aa representa el año y nn el número del boletín.

El SCC ofrece asistencia para problemas de seguridad de host relacionados con la DDN a través de su número telefónico de emergencias (800)235−3155 (de 6 a.m. a 5 p.m., hora del Pacífico).

Para ponerse en contacto con el SCC a través de correo electrónico, envíe un mensaje a:

SCC@NIC.DDN.MIL.

Para cobertura de 24 horas, puede llamar al Escritorio de Problemas MILNET, en el teléfono al (800)451−7413.

CENTRO DE RECURSOS Y RESPUESTA DE SEGURIDAD EN COMPUTADORAS DEL NIST

El Instituto Nacional de Estándares y Tecnologías (NIST), además de manejar las cuestiones de estándares, también tiene la responsabilidad, dentro del gobierno estadounidense, de actividades de ciencia y tecnología de computación. El NIST ha desempeñado un papel importante en la organización del sistema CERT y funciona como la Secretaría del Sistema CERT.

El NIST maneja el Centro de Recursos y Respuesta de Seguridad en Computadoras (CSRC), el cual ofrece ayuda e información acerca de incidentes de seguridad de computadoras. También está interesado en despertar la conciencia acerca de la vulnerabilidad de seguridad de las computadoras. El equipo del CSRC maneja un teléfono de emergencias las 24 horas del día el (301)975−5200.

El NIST ofrece publicaciones en línea e información sobre seguridad de computadoras, que puede bajarse mediante FTP anónimo desde el host csrc.nist.gov. La información también está disponible en World Wide Web, en el URL http://csrc.nist.gov.

Además del servidor FTP, el NIST opera un boletín electrónico en computadoras personales, que contiene información acerca de virus de computadoras, así como sobre otros aspectos de la seguridad de computadoras. Para tener acceso a este boletín electrónico, use la siguiente información:

Línea del boletín electrónico: 301−948−5717 8 bits, sin paridad, 1 bit de parada

Cuando usted se registre por primera vez en el boletín electrónico, debe registrar su nombre de usuario y su dirección.

El NIST también produce publicaciones especiales relacionadas con la seguridad y los virus de computadoras. Éstas pueden bajarse a través del boletín electrónico o del servidor FTR Si desea información adicional, póngase en contacto con el NIST en la siguiente dirección:

Computer Security Resource and Response Center

A~216 Technology

Gaithersburg, MD 20899

(301)975−3359

csrc@nist.gov

http://csrc.nist.gov

CAPACIDAD DE ASESORIA EN INCIDENTES DE COMPUTADORAS DEL DOE

La CIAC es la Capacidad de Asesoría en Incidentes de Computadoras del Departamento de Energía y *se formó* para constituir una capacidad de respuesta centralizada y un centro *de asistencia* técnica para *los sitios* del DOE.

La CIAC consiste en un equipo de cuatro científicos de computación del Laboratorio Nacional Lawrence Livermore (LLNL). La responsabilidad básica de este grupo es ayudar a los sitios del DOE que se enfrentan a incidentes de seguridad, como ataques de intrusos, infecciones de virus, ataques de gusanos, etcétera. La CIAC mantiene a los sitios informados de los eventos actuales relacionados con la seguridad y mantiene enlaces con otros equipos y agencias de respuesta.

La CIAC ayuda a los sitios mediante asistencia técnica directa, proporcionando información, o remitiendo las consultas a otros expertos técnicos. También sirve de centro de información acerca de amenazas de seguridad, incidentes conocidos de seguridad y puntos vulnerables. Además, establece lineamientos para el manejo de incidentes de seguridad y desarrolla software para reaccionar a tales incidentes.

La CIAC analiza incidentes y tendencias de seguridad, y organiza actividades de capacitación y concientización para alertar y asesorar a *los sitios* acerca de puntos vulnerables y ataques potenciales.

El número telefónico, la dirección de correo electrónico y el URL del CIAC son los siguientes:
(415)422−8193

ciac@tiger.llnl.gov

http://ciac.llnl.gov

EQUIPO DE RESPUESTA DE SEGURIDAD DE RED DE COMPUTADORAS AMES DE LA NASA

El Equipo de Respuesta de Seguridad de Red de Computadoras (CNSRT) fue formado por el Centro de Investigación Ames de la NASA en agosto de 1989. El objetivo primordial del equipo es ofrecer ayuda a los usuarios de Ames, pero también se ha involucrado para ayudar a otros centros de la NASA y agencias federales.

El CNSRT es el equivalente del CERT en la NASA. El CNSRT mantiene enlaces con el equipo CIAC del DOE y con el DARPA CERT, y es miembro fundador del sistema CERT.

Puede ponerse en contacto con el CNSRT las 24 horas del día en el teléfono (415)694−0571. La dirección de correo electrónico del CNSRT es:

cnsrt@ames.arc.nasa.gov

RESUMEN

Se habló de los factores y aspectos que usted debe tomar en cuenta para diseñar una red segura. Estos factores se formalizan en la política de seguridad, que le ayuda a identificar las amenazas, a realizar análisis de riesgos y a determinar cómo va a proteger sus recursos de red.

Usted necesita formular una política efectiva de seguridad antes de construir una firewall para conectar a su red con el resto de Internet. Es importante que conozca exactamente qué recursos y servicios de su red desea proteger.

La política de seguridad es un documento que describe los intereses de seguridad de la organización. Este documento constituye el primer paso para construir Firewalls efectivas.

APÉNDICE

Política de Uso del Correo Electrónico

Es responsabilidad de todos los usuarios del Correo Electrónico (E−Mail), seguir los procedimientos establecidos para asegurar un efectivo y eficiente uso del sistema de correo corporativo.

El uso indiscriminado del correo causa degradación en el desempeño del sistema y peor aún, puede resultar en la indisponibilidad del servicio. El sistema de E−Mail depende de la disponibilidad de espacio en disco en los

servidores y de las comunicaciones y su uso no adecuado sobrecarga estos recursos.

Es política del Grupo que el sistema de correo (E−Mail) sea para USO DEL NEGOCIO. Por lo tanto, los usuarios deberán abstenerse de enviar mensajes no oficiales, como por ejemplo, videos de saludos/bromas, cartas de cadenas, avisos económicos, etc ya que estos incrementan el uso de recursos escasos como el espacio en disco y el ancho de banda de las líneas de comunicaciones y además pueden resultar en la diseminación de virus aparte de consumir tiempo productivo del personal.

Para asegurar el uso eficiente del sistema del correo electrónico, se debe seguir las siguientes recomendaciones:

- **Envío de Información Confidencial:** En el interés de la seguridad, los empleados del SCC deben abstenerse de enviar correos confidenciales y/o críticos para el negocio, a través de Internet. Todo envío de información confidencial debe hacerse vía Fax, que es la herramienta del Grupo para estos efectos.

- **Tratar la Internet como un Dominio Público**, donde cualquier dicho o juicio hecho por los empleados, necesariamente refleja la posición del SCC. Por lo tanto, sólo personas autorizadas por el SCC para actuar en su representación (p.e. Asuntos Públicos) pueden responder o comentar en Internet, sobre aquellas materias relacionados con la empresa.

- **Evite Anexar Grandes Archivos:** Cuando requiera anexar grandes archivos, hágalo fuera de los horarios de alto tráfico o en casos extremos utilice el fax. Enviar un archivo muy grande a través de la red toma considerable tiempo y como consecuencia produce congestión y demoras en la entrega de los demás correos. Para minimizar los tamaños use siempre la compresión de archivos utilizando la herramienta que se encuentre disponible, teniendo en cuenta en cuenta que sobre 2 MB los correos son rechazados.

- **Evite Enviar Correos a Grandes Grupos de Usuarios:** Envíe, copie, replique o re−rutee mensajes sólo a aquellos usuarios relacionados con cada tema. Operar sobre la base estrictamente necesario−de−conocer.

- **Practique Frecuente Limpieza de su Directorio de Correo:** Existe una cuota para su espacio en correo, por lo tanto éstos deben ser borrados o si revisten importancia, guardados en archivos personales residentes en la red. De esta forma evitará interrupciones en su servicio por falta de capacidad en disco.

- **No Use la Funcionalidad Replicar o Re−Rutear Para Recipientes de Correo Internacional:** Envíe un mensaje nuevo (es decir, no anexe el historial de los mensajes que generan esta respuesta). Tome en cuenta que el costo de los correos internacionales esta basado en el tamaño de los mismos.

- **Uso de Direcciones Personales:** Estas no son actualizadas cuando se producen cambios en las listas oficiales de correo, por lo que es responsabilidad de cada uno su permanente actualización.

- **Envío de Mensajes Urgentes:** De acuerdo al BCP (Business Communications Procedures) todo mensaje URGENTE debe ir acompañado de un llamado telefónico.

- **Escriba sus Mensajes Directamente en el Correo:** En la medida de lo posible escriba sus mensajes directamente en el correo. Escribir mensajes en Word y luego anexarlos genera mensajes que ocupan un mayor espacio y hacen más lenta su lectura consumiendo más recursos del sistema.

Política de Administración de Passwords

Uno de los componentes básicos de la Tecnología de la Información es la Confidencialidad,

es decir la protección de la información sensible del acceso de personas no autorizadas.

Los computadores personales usados para llevar a cabo los negocios de la compañía, en la mayoría de los casos contienen información sensible la cual debe estar protegida de accesos de terceros o más aún de accesos involuntarios. Los hackers no están interesados en los PC's como tal, sino en la valiosa información que ellos contienen en sus medios magnéticos.

En vista de lo anterior, se ha preparado esta política para lograr que su cumplimiento garantice la seguridad de la información residente tanto en nuestros PC's como en otras facilidades IT y debe ser adherida por todos los usuarios. A continuación se resume las principales responsabilidades de cada sector:

Para los Administradores de Seguridad: (p.e. Administrador de LAN, Administrador JDE)

- Ningún sistema debe desplegar la password al momento de ser ingresada.
- Todos los sistemas deben obligar (donde sea posible) a que el largo de la password tenga un mínimo de 6 caracteres y en aquellos usuarios con privilegios, un largo mínimo de 8.
- El acceso a los sistemas se bloquea después de tres intentos fallidos de ingreso de la password.
- Todos los sistemas deben obligar, donde sea posible, a cambiar la password una vez transcurridos 30 días.
- Los administradores o Soporte a Usuarios, según corresponda, darán de alta o revocarán passwords existentes con passwords genéricas, solo cuando esto haya sido solicitado vía mail por el jefe inmediato del usuario a quién se le revoca la password. Los sistemas obligarán al usuario a cambiarla inmediatamente luego del primer ingreso.
- Todos los sistemas, donde sea posible, mantendrán un registro de las 13 últimas passwords usadas con el objeto de prevenir que los usuarios las re−utilicen.
- Las passwords con privilegios se encuentran en sobres cerrados, no son conocidas por nadie y se encuentran guardadas en áreas restringidas.

Para los Usuarios:

- Mantener la password de encendido del PC activada. Esta se establece al momento de instalar cada PC por el Departamento de Informática del SCC.
- Configurar el protector de pantalla con password y activación después de cinco minutos sin actividad. Cada vez que el PC quede desatendido se debe activar manualmente el protector de pantalla evitando así que personas no autorizadas tengan acceso a la información.
- Seleccionar una password con un largo mínimo de 6 caracteres utilizando letras y números, siguiendo las reglas establecidas.
- Seleccione passwords robustas difíciles de adivinar.
- Nunca construya su password basado en alguno de los siguientes factores:
- fechas asociadas con el usuario (p.e. cumpleaños, nacimiento, etc.)
- números telefónicos
- indicador de cargo
- series de caracteres numéricos o alfabéticos iguales
- Evite escribir su password y manténgala confidencial.
- Cambie su password a la primera sospecha de que alguien la conozca.
- Evite re−utilizar antiguas passwords aunque el sistema se lo permita.
- Cambie la password después de 30 días de uso aún si el sistema no se lo exige.(p.e. la password de encendido del PC).
- En caso de haber perdido la password su jefe inmediato deberá solicitar vía mail a soporte a usuarios revocar la password existente.

Para los Supervisores y RR HH

- De acuerdo al procedimiento respectivo, es responsabilidad de los Supervisores avisar prontamente a IT sobre aquellos empleados que dejan de prestar servicios a la compañía.
- IT bloqueará inmediatamente, según las instrucciones de los Supervisores, el acceso a la red y computadoras centrales, deshabilitando los User Id. y contraseñas de los empleados involucrados.

Política de Acceso a Internet

La Internet ha llegado a ser un poderoso medio de comunicación y una importante herramienta de búsqueda de información. En reconocimiento a esto, el Southern Cone Cluster (SCC) ha establecido los mecanismos para permitir el acceso a Internet para uso exclusivo del negocio y bajo una apropiada justificación.

El acceso a Internet es otorgado, a través de las facilidades tanto locales como internacionales de la compañía, para ayudar a los empleados a ser más efectivos en su trabajo. Su uso está sujeto al monitoreo y revocación a la sola discreción del SCC. A todos aquellos con acceso, se les insta fuertemente a ejercitar el buen juicio cada vez que utilicen Internet. Las gerencias de líneas tienen la responsabilidad de hacer efectivas las sanciones que correspondan, a todos aquellos que infrinjan cualquiera de las condiciones enumeradas a continuación. Toda la organización debe adherirse a esta política para asegurar el uso seguro y productivo de la Internet en el South Cone Cluster.

- Dado el costo y los riesgos de seguridad que el acceso a internet involucra, éste sólo debe ser otorgado por el Director respectivo y basado en una fuerte justificación de necesidad del negocio.
- El acceso a Internet provisto por el SCC debe ser usado sólo para propósitos del negocio.
- Está estrictamente prohibido la difusión en Internet de documentos relacionados con la compañía, programas, objetos y gráficos sin la debida autorización. Los empleados tienen la responsabilidad de proteger toda aquella información comercial y/o propietaria que sea propiedad intelectual de la empresa.
- Toda información extraída a través de Internet, a menos que sea de fuentes confiables confirmadas, debe ser validada antes de ser utilizada para fines del negocio.
- Tratar la Internet como un dominio público, donde cualquier dicho o juicio hecho por los empleados, necesariamente refleja la posición del SCC. Por lo tanto, sólo personas autorizadas por el SCC para actuar en su representación (p.e. Asuntos Públicos) pueden responder o comentar en Internet, sobre aquellas materias relacionados con la empresa.
- Todos los archivos extraídos desde internet deben ser scaneados y limpiados de virus. De acuerdo a la política de Control de Virus, acciones disciplinarias se tomarán contra todos aquellos que fallen en tomar precauciones que conduzcan a difundir virus en las redes.
- Cualquier texto, foto, sonido, video u otro objeto gráfico que pueda ser considerado ofensivo (p.e. material pornográfico) o en alguna forma discriminatorio, no debe ser desplegado, almacenado ni transmitido sobre los equipos de propiedad de la compañía. Como empleados, se espera que nos conduzcamos en una forma decente y profesional.
- Está estrictamente prohibido el acoso a individuos, corporaciones u organizaciones y el acceso a cualquier sistema o computador de un tercero sin el expreso consentimiento del propietario. Al cometer tales actos, se queda expuesto a reclamos de tipo legal como individuo.
- Re−publicar o distribuir material bajo licencia, sin el permiso del propietario está prohibido, ya que esto infringe el derecho de propiedad intelectual de otras entidades.
- Los usuarios de Internet deben reportar todos los problemas de seguridad a Soporte a Usuarios.

Política de Clasificación de la Información

Esta política está basada en el nuevo sistema de clasificación de la información diseñada por la empresa. Ella ha sido encarada con un enfoque hacia el compartir información en el más amplio sentido, pero por otro lado

asegurando que toda aquella información que requiera un mayor nivel de protección sea debidamente identificada.

Estas definiciones establecen claramente los ítems de información que van en cada clasificación. En el hoy creciente mundo del compartir información es más necesario que nunca tener estas clasificaciones claramente identificadas. Sub−clasificación de información sensible puede llegar a tener serias consecuencias − datos sensibles podrían ser interceptados si no hay adecuadas protecciones al momento de la transmisión. Sobre−clasificación también puede ser dañina en términos de eficiencia y pérdida de oportunidades al no disponer de la información en el momento correcto, por otro lado puede hacer perder credibilidad al sistema de clasificación.

Variaciones en la definición de clasificaciones no están permitidas ya que ello provocaría confusión

en relación a las medidas de protección y grados de disponibilidad de la información.

La siguiente tabla resume las definiciones y guías generales sobre distribución, protección y rotulamiento de la información que esta política adhiere y que se espera sea cumplida por todo el staff del South Cone Cluster (SCC) y compañías asociadas:

	Desclasificada (Unclassified)	**Restringida (Restricted)**	**Confidencial (Confidential)**	**Muy Confidencial (Most Confidential)**
Definición:	Información que puede ser **compartida sin ninguna restricción** ya que su divulgación a terceros no implica que los intereses de la compañía pudieran ser dañados.	Información que puede ser **libremente compartida internamente entre los empleados del SCC y compañías asociadas** (*), pero no con terceros .	Información que debe ser **compartida sólo por grupos reducidos de empleados** ya que eventualmente su divulgación a personas no autorizadas podría dañar los intereses de la compañía y/o del Grupo.	Información que sólo debe estar disponible sobre la base **estrictamente necesario−de−conocer,** ya que de lo contrario, en caso que esta información llegue a manos de personas inescrupulosas, se podría producir un daño muy grave a la propia compañía y eventualmente a otras áreas del Grupo.
Difusión:	No hay restricciones pero Asuntos Públicos debe ser consultado previo a su publicación externa.	Puede ser libremente compartida entre los empleados del SCC y compañías del Grupo, pero no con terceros.	Debe ser solamente compartida sólo con los empleados y contratistas que realmente requieran conocer	Debe estar estrictamente controlado y limitado a una mínima lista de individuos.
Niveles de protección:	**No se requiere una protección específica** contra accesos no autorizados.	Aplicar **due diligence** para prevenir acceso de terceros.	Aplicar medidas que sean lo suficientemente poderosas para **detener los intentos** de obtener accesos no autorizados	Aplicar el **mayor nivel de protección** disponible dentro del ambiente del negocio.
Volumen Típico:	Alrededor del 10−20% de la información	Alrededor del 80−90% de la información	Alrededor del 5−10% de la información generada.	Menos del 1% de la información generada.

	generada.	generada.		
Ejemplos:	E−mails de rutina relacionados con temas no sensibles. Material de paneles de noticias. Información recibida de socios comerciales o gobierno y que está libremente disponible al dominio público.	Por defecto todos los reportes, minutas de negocios, cartas, etc. Directorios de la compañía. Best Practices Publicaciones técnicas internas Material no clasificado recibido de socios comerciales y/o gobierno que no es de dominio público.	Posiciones de negociaciones. Informaciones de mercado. Estudios sobre la competencia. Información de clientes. Información de los empleados (p.e. ficha médicas) Cuando revelar información pudiera costar pérdidas significativas. (hasta USD $ 5 millones) Minutas de trabajo y programas de viajes de ejecutivos seniors. Material gubernamental marcado como RESTRINGIDO.	Detalles de adquisiciones mayores o fusiones. Cuando un revelamiento pudiera afectar el precio de la acción. Items de alta sensibilidad política o social. Planes de negocios de alto nivel. Itinerarios de viajes de ejecutivos seniors en países de alto riesgo. Planes de reorganizaciones mayores que puedan tener un alto impacto en los empleados. Cuando revelar información pudiera costar grandes pérdidas. (hasta USD $ 50 millones) Material gubernamental marcado como CONFIDENCIAL
Rotulación:	No es necesario rotular	Use la rotulación Restringida en la medida que se requiera.	Despliegue el rótulo Confidencial en un lugar destacado. (p.e. tapa de informes, parte superior hojas)	Despliegue el rótulo Muy Confidencial en partes destacadas del material.

(*):**Empleados (staff) compañía**, incluye a todos los empleados, a contratistas con un contrato a plazo fijo, a individuos específicos no pertenecientes a la empresa que sean requeridos por el negocio, autorizados por una gerencia de línea de y hayan firmado un acuerdo de confidencialidad.

Compañías Asociadas, son aquellas en que por la naturaleza de los negocios compartidos, se les ha otorgado acceso a información Restringida a ciertos niveles de categorías, con la aprobación del regional business adviser.

Política de Respaldo y Recupero de Datos

Política de Respaldo y Recupero de Datos

El respaldo/recupero tiene como objetivo asegurar la continuidad del negocio ante pérdida de los datos operacionales guardados en los dispositivos de almacenamiento.

Todo archivo productivo, tendrá una política de back−ups y restore definida por el Responsable de Definir y ejecutada por el Responsable de Ejecutar (Ambos definidos mas abajo).

Los discos rígidos de las PC's de cada usuario no están ubicadas en áreas bajo la custodia del departamento de informática del cluster, con todas las protecciones que esto significa, por lo tanto no es considerado seguro. Adicionalmente, los datos guardados en el disco rígido, no forman parte del proceso centralizado de back−ups.

Los back−ups serán mantenidos en un edificio distinto al del lugar de procesamiento, en condiciones seguras.

La definición de los respaldo/recupero debe estar incluida en la documentación del pase a operativa y debe contener los siguientes ítems:

- Instructivo de como procesar el back−up.
- Instructivo de como procesar el restore.
- Especificación y Lay out de dispositivos de back−up / restore.
- Cuando tomar el back−up dentro del flujo de procesos de producción.
- Periodicidad del mismo.
- Instrucciones de rotulado.
- Período de Almacenamiento
- Flujo de procesos de recuperos.

Los responsables de definir respaldo/recupero son:

Sistemas Aplicativos: Project Managers / Project Leaders (Según el sistema). En el caso particular de los recuperos, es responsabilidad del Project Leader asegurarse que para todos los respaldos existan las aplicaciones compatibles correspondientes.

Plataformas: Tecnología (Administrador de la plataforma en cuestión).

PC's (Discos Rígidos): Usuarios.

Los responsables de administrar y ejecutar los respaldo/recupero son:

Sistemas residentes en computadoras ubicadas en áreas bajo la custodia del departamento de informática del cluster: Operaciones.

PC's (Discos Rígidos): Usuarios

CONCLUSIONES

A lo largo de este trabajo ha quedado demostrado que nuestros problemas no están solucionados simplemente con la implementación de un esquema de seguridad basada en firewalls; de hecho si en realidad no forma parte de una política de seguridad integral de la organización de nada servirá tener la configuración más segura en lo que a firewall respecta.

A partir del hecho ya consumado que constituye la interconectividad a través de Internet, es fundamental la utilización de filtros debido a que seguramente nuestra organización estará también accediendo a los servicios que Internet nos ofrece. Qué arquitectura es la más apropiada tendrá que ver seguramente con la criticidad de nuestros servicios, lo valioso de nuestra información, los servicios que ofreceremos y obtendremos de Internet, y de los recursos con los cuales contemos para llevar adelante este desafío.

Y por último, debemos tener en cuenta que este tema no consiste solo en implementar una política de seguridad y problema resuelto. La importancia operativa es tal que debemos estar constantemente revisando las políticas, los logs, etc. para poder determinar si estamos siendo vulnerables en algún aspecto. Por otro lado una política de seguridad debe asemejarse a un antivirus, el cual si no se actualiza constantemente deja de ser seguro. Tengamos en cuenta que la seguridad de nuestra empresa constituye la puerta de acceso a nuestra información vital, por ende a nuestro negocio y por último a nuestro dinero.

GLOSARIO DE TÉRMINOS

- AUP: Política de Uso Aceptable
- CIAC: Computer Incident Advisory Capability (Capacidad de Asesoría en Incidentes de Computadoras)
- EMA: Electrónica Mail Asociación (Asociación de Correo Electrónico).
- Firewall: Sistema o grupo de ellos enfocados hacia una política de control de acceso entre la red de la organización y redes externas (por ej: Internet).

- Host: En líneas generales, servidor o estación de trabajo conectado a la red
- Red: Conjunto de máquinas interconectadas entre sí que comparten recursos.
- Proxy: Servicio de propósito especial, código de aplicación instalado en un firewall. El proxy server permite que el administrador de la red permita o rechace determinados servicios de una aplicación en particular.
- RFC: Request for Comment. Se utiliza para establecer y documentar estándares en Internet.
- CERT: Equipo de Respuestas de Emergencias de Cómputo
- NFS: Network File System. Capacidad del sistema operativo Unix de compartir su estructura de directorios a través de una red.
- TCP/IP: TCP o *Transfer Control Protocol* / IP: *Internet Protcol*, conjunto de Protocolos utilizados en Internet.
- PPP: Point to Point Protocol. Protocolo comúnmente utilizado para conexiones por modem.
- SLIP: Serial Line Interface Protocol. Protocolo comúnmente utilizado para conexiones por modem.
- LAN: Local Área Network o Red de Área Local.

WAN: Wide Área Network o Red de Área Amplia.*BIBLIOGRAFIA CONSULTADA*

- ***Internet y Seguridad en Redes***. Karanjit SIYAN, Ph. D. Y Chris HARE. Editorial Prentice Hall.
- ***Hackers Secretos Y Soluciones Para La Seguridad De Redes.*** Mc Clure STUART. Editorial MCGRAW−HILL.
- ***Web Sites corporativos:***

www.3com.com

www.scrc.ncsl.nist.gov

www.interhack.com

www.icsa.com

www.cisco.com

www.hp.com

ftp.tis.com