Trabajo Práctico final

Seguridad

Índice

Página

Introducción general sobre Seguridad

Hasta finales de 1988 muy poca gente tomaba en serio el tema de la seguridad en redes de computadoras. Mientras que por una parte Internet iba creciendo exponencialmente, por otra el auge de la informática de consumo iba produciendo un aumento espectacular en el numero de piratas informáticos.

Sin embargo, el 22 de noviembre de 1988 Robert T. Morris protagonizo el primer gran incidente de la seguridad informática: uno de sus programas se convirtió en el famoso *worm* o gusano de Internet. Miles de computadoras conectados a la red se vieron inutilizados durante días, y las perdidas se estiman en millones de dólares. Desde ese momento el tema de la seguridad en sistemas operativos, redes, seguridad física y lógica ha sido un factor a tener muy en cuenta por cualquier organización.

¿ Qué es *seguridad?*

Podemos entender como **seguridad** una característica de cualquier sistema (informático o no) que nos indica que ese sistema esta libre de todo peligro, daño o riesgo, y que es, en cierta manera, infalible.

Es muy difícil de conseguir seguridad total, entonces podemos hablar de **fiabilidad** (probabilidad de que un sistema se comporte tal y como se espera de el). Más que de *seguridad*, se habla de *sistemas fiables* en lugar de hacerlo de *sistemas seguros*.

A grandes rasgos se entiende que mantener un sistema *seguro* (o fiable) consiste básicamente en garantizar tres aspectos:

- **Confidencialidad**
- **Integridad**
- **Disponibilidad**.

¿Qué queremos proteger?

Los tres elementos principales a proteger en cualquier sistema informático son:

- *Software*
- *Hardware*
- *Datos*

Por **hardware** entendemos el conjunto formado por todos los elementos físicos de un sistema informático, como CPUs, terminales, cableado, medios de almacenamiento secundario (cintas, CDROMs, diskettes. . .) o tarjetas de red.

Por **software** entendemos el conjunto de programas lógicos que hacen funcional al *hardware*, tanto sistemas operativos como aplicaciones.

Por datos el conjunto de información lógica que manejan el *software* y el *hardware.*

Habitualmente los datos constituyen el principal elemento de los tres a proteger, ya que es el más amenazado y seguramente el más difícil de recuperar.

Con toda seguridad una maquina esta ubicada en un lugar de acceso físico restringido, o al menos controlado, y además en caso de pérdida de una aplicación este software se puede restaurar sin problemas desde su medio original (por ejemplo, el CDROM con el sistema operativo que se utilizo para su instalación. Sin embargo, en caso de perdida de una base de datos o de un proyecto de un usuario, no tenemos un medio `original' desde el cual restaurar: debemos pasar obligatoriamente por un sistema de copias de seguridad, y a menos que la política de copias sea muy estricta, es difícil devolver los datos al estado en que se encontraban antes de la

perdida.

Contra cualquiera de los tres elementos descritos anteriormente se pueden realizar multitud de ataques, los mismos están expuestos a diferentes amenazas.

Generalmente, la taxonomía más elemental de estas amenazas las divide en cuatro grandes grupos:

- Interrupción
- Interceptación
- Modificación
- Fabricación.

Un ataque se clasifica como **interrupción** si hace que un objeto del sistema se pierda, o sea que quede inutilizable o no disponible.

En el caso de una **interceptación** si un elemento no autorizado consigue un acceso a un determinado objeto del sistema, y una **modificación o destrucción** si además de conseguir el acceso se consigue modificar el objeto o destruirlo. Por último, se dice que un ataque es una **fabricación** si se trata de una modificación destinada a conseguir un objeto similar al atacado de forma que sea difícil distinguir entre el objeto original y el `fabricado'.

¿De qué nos queremos proteger?

Se suele identificar a los atacantes únicamente como personas; esto tiene sentido si hablamos por ejemplo de responsabilidades por un delito informático. Pero nuestro sistema puede verse perjudicado por múltiples entidades aparte de humanos, como por ejemplo programas, catástrofes naturales.

Personas

La mayoría de ataques a nuestro sistema van a provenir en última instancia de personas que, intencionada o inintencionadamente, pueden causarnos enormes perdidas.

Generalmente se tratara de piratas que intentan conseguir el máximo nivel de privilegio posible aprovechando alguno de los riesgos lógicos de los que después mencionaremos, especialmente agujeros del *software*.

Pero con demasiada frecuencia se suele olvidar que los piratas `clásicos' no son los únicos que amenazan nuestros equipos: es especialmente preocupante que mientras que hoy en día cualquier administrador mínimamente preocupado por la seguridad va a conseguir un sistema relativamente fiable de una forma lógica (permaneciendo atento a vulnerabilidades de su *software*, restringiendo servicios, utilizando cifrado de datos, y demás mecanismos)

Pocos administradores tienen en cuenta factores como la ingeniería social o él basureo a la hora de diseñar una política de seguridad.

Aquí se describen brevemente los diferentes tipos de personas que de una u otra forma pueden constituir un riesgo para nuestros sistemas; generalmente se dividen en dos grandes grupos: los atacantes **pasivos**, son aquellos que curiosean por el sistema pero no lo modifican o destruyen, y los **activos**, aquellos que dañan el objetivo atacado, o lo modifican en su favor.

Generalmente los curiosos y los *crackers* realizan ataques pasivos (que se pueden convertir en activos), mientras que los terroristas y ex empleados realizan ataques activos puros; los intrusos remunerados suelen ser atacantes pasivos si nuestra red o equipo no es su objetivo, y activos en caso contrario, y el personal realiza

ambos tipos indistintamente, dependiendo de la situación concreta.

TIPOS

DE

ATACANTES

Personal

Las amenazas a la seguridad de un sistema provenientes del personal de la propia organización rara vez son tomadas en cuenta; se presupone un entorno de confianza donde a veces no existe, por lo que se pasa por alto el hecho de que casi cualquier persona de la organización, incluso el personal ajeno a la infraestructura informática (secretariado, personal de seguridad, personal de limpieza y mantenimiento) puede comprometer la seguridad de los equipos.

Aunque los ataques pueden ser intencionados, (en cuyo caso sus efectos son extremadamente dañinos), lo normal es que más que de ataques se trate de **accidentes** causados por un error o por desconocimiento de las normas básicas de seguridad: un empleado de mantenimiento que corta el suministro eléctrico para hacer una reparación puede llegar a ser tan peligroso como el más experto de los administradores que se equivoca al teclear una orden y borra todos los sistemas de archivos.

Otro gran grupo de personas potencialmente interesadas en atacar nuestro sistema son los antiguos empleados de la mismo, especialmente los que no abandonaron el entorno por voluntad propia (y en el caso de redes de empresas, los que pasaron a la competencia).

Curiosos

Junto con los *crackers*, los curiosos son los atacantes más habituales de sistemas.

Aunque en la mayoría de situaciones se trata de ataques no destructivos (a excepción del borrado de huellas para evitar la detección), parece claro que no benefician en absoluto al entorno de fiabilidad que podamos generar en un determinado sistema.

Crackers

Los entornos de seguridad media son un objetivo típico de los intrusos, ya sea para fisgonear, para utilizarlas como enlace hacia otras redes o simplemente por diversión.

Terroristas

Por `terroristas' no debemos entender simplemente a los que se dedican a poner bombas; bajo esta definición se engloba a cualquier persona que ataca al sistema simplemente por causar algún tipo de daño en el. Por ejemplo, alguien puede intentar borrar las bases de datos de un partido político enemigo o destruir los sistemas de archivos de un servidor que alberga paginas *web* de algún grupo religioso, típicos ataques son la destrucción de sistemas de practicas o la modificación de paginas *web* de algún departamento o de ciertos profesores, generalmente por parte de alumnos descontentos.

Intrusos remunerados

Este es el grupo de atacantes de un sistema más peligroso, aunque por suerte el menos habitual en redes normales; suele afectar más a las grandes empresas o a organismos de defensa. Se trata de piratas con gran

experiencia en problemas de seguridad y un amplio conocimiento del sistema, que son pagados por una tercera parte generalmente para robar secretos, información confidencial etc. O simplemente para dañar la imagen de la entidad afectada.

TIPOS

DE

AMENAZAS

Amenazas lógicas

Bajo la etiqueta de `amenazas lógicas' encontramos todo tipo de programas que de una forma u otra pueden dañar a nuestro sistema, creados de forma intencionada para ello o simplemente por error.

Software incorrecto

Las amenazas más habituales a un sistema provienen de errores cometidos de forma involuntaria por los programadores de sistemas o de aplicaciones. Una situación no contemplada a la hora de diseñar el sistema de red del *kernel* o un error accediendo a memoria en un archivo *setuidado* pueden comprometer local o remotamente a cualquier sistema.

A estos errores de programación se les denomina *bugs*, y a los programas utilizados para aprovechar no de estos fallos y atacar al sistema, *exploit.*

Bombas lógicas

Las bombas lógicas son partes de código de ciertos programas que permanecen sin realizar ninguna función hasta que son activadas; en ese punto, la función que realizan no es la original del programa, sino que generalmente se trata de una acción perjudicial.

Los activadores más comunes de estas bombas lógicas pueden ser la ausencia o presencia de ciertos archivos, la ejecución bajo un determinado UID o la llegada de una fecha concreta; cuando la bomba se activa va a poder realizar cualquier tarea que pueda realizar la persona que ejecuta el programa: si las activa el *root (en el caso del UNIX)*, o el programa que contiene la bomba esta setuidado a su nombre, los efectos obviamente pueden ser fatales.

Canales cubiertos

Son canales de comunicación que permiten a un proceso transferir información de forma que viole la política de seguridad del sistema; dicho de otra forma, un proceso transmite información a otros (locales o remotos) que no están autorizados a leer dicha información.

Virus

Un virus es una secuencia de código que se inserta en un archivo ejecutable (denominado *huésped*), de forma que cuando el archivo se ejecuta, el virus también lo hace, insertándose a si mismo en otros programas.

Gusanos

Un gusano es un programa capaz de ejecutarse y propagarse por si mismo a través de redes, en ocasiones portando virus o aprovechando *bugs* de los sistemas a los que conecta para dañarlos.

Al ser difíciles de programar su numero no es muy elevado, pero el daño que pueden causar es muy grande: el mayor incidente de seguridad en Internet fue precisamente el *Internet Worm*, un gusano que en 1988 causo perdidas millonarias al infectar y detener más de 6000 máquinas conectadas a la red.

Este año hubo uno muy conocido con el nombre de Sircam32 que también causó mucho daño no sólo aquí sino en la defensa de EEUU, conociendo la forma de combatirlo prácticamente una semana más tarde, el mismo circulaba a través de los correos electrónicos, reenviándose a nuestra libreta de direcciones, adjuntando archivos de la carpeta mis documentos.

Un gusano puede automatizar y ejecutar en unos segundos todos los pasos que seguiría un atacante humano para acceder a nuestro sistema: mientras que una persona, por muchos conocimientos y medios que posea, tardaría como mínimo horas en controlar nuestra red completa (un tiempo más que razonable para detectarlo), un gusano puede hacer eso mismo en pocos minutos: de ahí su enorme peligro y sus devastadores efectos.

Caballos de Troya

Los troyanos o caballos de Troya son instrucciones escondidas en un programa de forma que este parezca realizar las tareas que un usuario espera de el, pero que realmente ejecute funciones ocultas (generalmente en detrimento de la seguridad) sin el conocimiento del usuario; como el Caballo de Troya de la mitología griega, al que deben su nombre, ocultan su función real bajo la apariencia de un programa inofensivo que a primera vista funciona correctamente.

Programas conejo o bacterias

Bajo este nombre se conoce a los programas que no hacen nada útil, sino que simplemente se dedican a reproducirse hasta que el numero de copias acaba con los recursos del sistema (memoria, procesador, disco. . .), produciendo una negación de servicio. Por si mismos no hacen ningún daño, sino que lo que realmente perjudica es el gran numero de copias suyas en el sistema, que en algunas situaciones pueden llegar a provocar la parada total de la maquina.

Técnicas salami

Por técnica salami se conoce al robo automatizado de pequeñas cantidades de bienes (generalmente dinero) de una gran cantidad origen. El hecho de que la cantidad inicial sea grande y la robada pequeña hace extremadamente difícil su detección.

Las técnicas salami no se suelen utilizar para atacar sistemas normales, sino que su uso más habitual es en sistemas bancarios; sin embargo, como en una red con requerimientos de seguridad medios es posible que haya computadoras dedicados a contabilidad, facturación de un departamento o gestión de nominas del personal, comentamos esta potencial amenaza contra el *software* encargado de estas tareas.

Catástrofes

Las catástrofes (naturales o artificiales) son la amenaza menos probable contra los entornos habituales: simplemente por su ubicación geográfica, a nadie se le escapa que la probabilidad de sufrir un terremoto o una inundación que afecte a los sistemas informáticos en una gran ciudad, es relativamente baja, al menos en comparación con el riesgo de sufrir un intento de acceso por parte de un pirata o una infección por virus. Sin embargo, el hecho de que las catástrofes sean amenazas poco probables no implica que contra ellas no se tomen unas medidas básicas, ya que si se produjeran generarían los mayores daños.

Un subgrupo de las catástrofes es el denominado de **riesgos poco probables**. Obviamente se denomina así al conjunto de riesgos que, aunque existen, la posibilidad de que se produzcan es tan baja (menor incluso que la

del resto de catástrofes) que nadie toma, o nadie puede tomar, medidas contra ellos.

Ejemplos habituales de riesgos poco probables son un ataque nuclear contra el sistema, el impacto de un satélite contra la sala de operaciones. Nada nos asegura que este tipo de catástrofes no vaya a ocurrir, pero la probabilidad es tan baja y los sistemas de prevención tan costosos que no vale la pena tomar medidas contra ellas.

Como ejemplos de catástrofes hablaremos de terremotos, inundaciones, incendios, humo o atentados de baja magnitud (más comunes de lo que podamos pensar); obviamente los riesgos poco probables los trataremos como algo anecdótico.

MECANISMOS

DE

SEGURIDAD

¿Cómo nos podemos proteger?

Para proteger nuestro sistema tenemos que realizar un análisis de las amenazas potenciales que puede sufrir, las perdidas que podrían generar, y la probabilidad de su ocurrencia; a partir de este análisis vamos a diseñar una política de seguridad que defina responsabilidades y reglas a seguir para evitar tales amenazas o minimizar sus efectos en caso de que se produzcan. A los mecanismos utilizados para implementar esta política de seguridad se les denomina **mecanismos de seguridad**; son la parte más visible de nuestro sistema de seguridad, y se convierten en la herramienta básica para garantizar la protección de los sistemas o de la propia red.

Los mecanismos de seguridad se dividen en tres grandes grupos:

- de prevención
- de detección
- de recuperación.

Los mecanismos **de prevención** son aquellos que aumentan la seguridad de un sistema durante el funcionamiento normal de este, previniendo la ocurrencia de violaciones a la seguridad; por ejemplo, el uso de cifrado en la transmisión de datos se puede considerar un mecanismo de este tipo, ya que evita que un posible atacante escuche las conexiones hacia o desde un sistema en la red.

Por mecanismos **de detección** se conoce a aquellos que se utilizan para detectar violaciones de la seguridad o intentos de violación; ejemplos de estos mecanismos son los programas de auditoria como *Tripwire*.

Finalmente, los mecanismos **de recuperación** son aquellos que se aplican cuando una violación del sistema se ha detectado, para retornar a este a su funcionamiento correcto; ejemplos de estos mecanismos son la utilización de copias de seguridad o el *hardware* adicional. Dentro de este último grupo de mecanismos de seguridad encontramos un subgrupo denominado **mecanismos de análisis forense**, cuyo objetivo no es simplemente retornar al sistema a su modo de trabajo normal, sino averiguar el alcance de la violación, las actividades de un intruso en el sistema, y la puerta utilizada para entrar; de esta forma se previenen ataques posteriores y se detectan ataques a otros sistemas de nuestra red.

MECANISMOS

DE

PREVENCION

Mecanismos de prevención

- *Mecanismos de autenticación e identificación*

Estos mecanismos hacen posible identificar entidades del sistema de una forma única, y posteriormente, una vez identificadas, autenticarlas (comprobar que la entidad es quien dice ser).

Son los mecanismos más importantes en cualquier sistema, ya que forman la base de otros mecanismos que basan su funcionamiento en la identidad de las entidades que acceden a un objeto.

Un grupo especialmente importante de estos mecanismos son los denominados Sistemas de Autenticación de Usuarios.

- *Mecanismos de control de acceso*

Cualquier objeto del sistema debe estar protegido mediante mecanismos de control de acceso, que controlan todos los tipos de acceso sobre el objeto por parte de cualquier entidad del sistema.

- *Mecanismos de separación*

Cualquier sistema con diferentes niveles de seguridad implementa mecanismos que permitan separar los objetos dentro de cada nivel, evitando el flujo de información entre objetos y entidades de diferentes niveles siempre que no exista una autorización expresa del mecanismo de control de acceso.

Los mecanismos de separación se dividen en cinco grandes grupos, en función de como separan a los objetos: separación física, temporal, lógica, criptográfica y fragmentación.

- *Mecanismos de seguridad en las comunicaciones*

Es especialmente importante para la seguridad de nuestro sistema el proteger la integridad y la privacidad de los datos cuando se transmiten a través de la red. Para garantizar esta seguridad en las comunicaciones, utilizamos ciertos mecanismos, la mayoría de los cuales se basan en la Criptografia: cifrado de clave publica, de clave privada, firmas digitales.

SEGURIDAD

FÍSICA DE LOS SISTEMAS

Introducción

La seguridad física de los sistemas informáticos consiste en *la aplicación de barreras físicas y procedimientos de control como medidas de prevención y contramedidas contra las amenazas a los recursos y la información confidencial*.

Por seguridad física podemos entender todos aquellos mecanismos generalmente de prevención y detección destinados a proteger físicamente cualquier recurso del sistema; estos recursos son desde un simple teclado hasta una cinta de *backup* con toda la información que hay en el sistema, pasando por la propia cpu de la maquina.

Desgraciadamente, la seguridad física es un aspecto olvidado con demasiada frecuencia a la hora de hablar de

seguridad informática en general; en muchas organizaciones se suelen tomar medidas para prevenir o detectar accesos no autorizados o negaciones de servicio, pero rara vez para prevenir la acción de un atacante que intenta acceder físicamente a la sala de operaciones o al lugar donde se depositan las impresiones del sistema. Esto motiva que en determinadas situaciones un atacante se decline por aprovechar vulnerabilidades físicas en lugar de lógicas, ya que posiblemente le sea más fácil robar una cinta con una imágen completa del sistema que intentar acceder a el mediante fallos en el *software*. Tenemos que ser conscientes de que la seguridad física es demasiado importante como para no tenerla en cuenta: un ladrón que roba una computadora para venderla, un incendio o un pirata que accede sin problemas a la sala de operaciones nos pueden hacer mucho más daño que un intruso que intenta conectar remotamente con una máquina no autorizada; no importa que utilicemos los más avanzados medios de cifrado para conectar a nuestros servidores, ni que hayamos definido una política de *firewalling* muy restrictiva: si no tenemos en cuenta factores físicos, estos esfuerzos para proteger nuestra información no van a servir de nada. Además, en el caso de organismos con requerimientos de seguridad medios, unas medidas de seguridad físicas ejercen un efecto disuasorio sobre la mayoría de piratas: como casi todos los atacantes de los equipos de estos entornos son casuales (esto es, no tienen interés especifico sobre *nuestros* equipos, sino sobre *cualquier* equipo), si notan a través de medidas físicas que nuestra organización esta preocupada por la seguridad probablemente abandonaran el ataque para lanzarlo contra otra red menos protegida.

Pero tenemos que recordar que cada sitio es diferente, y por tanto también lo son sus necesidades de seguridad; de esta forma, no se pueden dar recomendaciones especificas sino pautas generales a tener en cuenta, que pueden variar desde el simple sentido común (como es el cerrar con llave la sala de operaciones cuando salimos de ella) hasta medidas mucho más complejas, como la prevención de radiaciones electromagnéticas de los equipos.

En entornos habituales suele ser suficiente con un poco de sentido común para conseguir una mínima seguridad física; de cualquier forma, en cada institución se debe analizar el valor de lo que se quiere proteger y la probabilidad de las amenazas potenciales, para en función de los resultados obtenidos diseñar un plan de seguridad adecuado.

Protección del hardware

El *hardware* es frecuentemente el elemento más caro de todo sistema informático. Por tanto, las medidas encaminadas a asegurar su integridad son una parte importante de la seguridad física de cualquier organización.

Son muchas las amenazas al *hardware* de una instalación informática; aquí se vamos a presentar algunas de ellas, sus posibles efectos y algunas soluciones, si no para evitar los problemas si al menos para minimizar sus efectos.

Acceso físico

La posibilidad de acceder físicamente a una maquina hace inútiles casi todas las medidas de seguridad que hayamos aplicado sobre ella.

Un atacante puede llegar con total libertad hasta una estación, puede por ejemplo abrir la CPU y llevarse un disco duro; sin necesidad de privilegios en el sistema.

El atacante podrá seguramente modificar la información almacenada, destruirla o simplemente leerla. Incluso sin llegar al extremo de desmontar la maquina, que quizás resulte algo exagerado en entornos clásicos donde hay cierta vigilancia, como un laboratorio o una sala de informática, la persona que accede al equipo puede pararlo o arrancar una versión diferente del sistema operativo sin llamar mucho la atención.

Visto esto, parece claro que cierta seguridad física es necesaria para garantizar la seguridad global de la red y los sistemas conectados a ella; evidentemente el nivel de seguridad física depende completamente del entorno donde se ubiquen los puntos a proteger (no es necesario hablar solo de equipos), sino de cualquier elemento físico que se pueda utilizar para amenazar la seguridad, como una toma de red apartada en cualquier rincón de un edificio de nuestra organización. Mientras que parte de los equipos estarán bien protegidos, por ejemplo los servidores de un departamento o las máquinas de los despachos, otros muchos estarán en lugares de acceso semipúblico, como laboratorios de practicas; es justamente sobre estos últimos sobre los que debemos extremar las precauciones, ya que lo más fácil y discreto para un atacante es acceder a uno de estos equipos y, en segundos, lanzar un ataque completo sobre la red.

PREVENCIÓN

DE

ATAQUES

FISICOS

Prevención

¿Cómo prevenir un acceso físico no autorizado a un determinado punto?

Existen muchas soluciones también de todos los precios: desde analizadores de retina hasta videocámaras, pasando por tarjetas inteligentes o control de las llaves que abren determinada puerta.

Todos los modelos de autenticación de usuarios son aplicables, aparte de para controlar el acceso lógico a los sistemas, para controlar el acceso físico; de todos ellos, quizás los más adecuados a la seguridad física sean los biométricos y los basados en algo poseído; aunque suelen resultar algo caros para utilizarlos masivamente en entornos de seguridad media.

Pero no hay que irse a sistemas tan complejos para prevenir accesos físicos no autorizados; normas tan elementales como cerrar las puertas con llave al salir de un laboratorio o un despacho o bloquear las tomas de red que no se suelan utilizar y que estén situadas en lugares apartados son en ocasiones más que suficientes para prevenir ataques. También basta el sentido común para darse cuenta de que el cableado de red es un elemento importante para la seguridad, por lo que es recomendable apartarlo del acceso directo.

Concretamente, el uso de lectores de tarjetas para poder acceder a ciertas dependencias es algo muy a la orden del ida; la idea es sencilla: alguien pasa una tarjeta por el lector, que conecta con un sistema por ejemplo una computadora en la que existe una base de datos con información de los usuarios y los recintos a los que se le permite el acceso. Si la tarjeta pertenece a un usuario capacitado para abrir la puerta, esta se abre, y en caso contrario se registra el intento y se niega el acceso. Aunque este método quizás resulte algo caro para extenderlo a todos y cada uno de los puntos a proteger en una organización, no seria tan descabellado instalar pequeños lectores de códigos de barras conectados a una maquina Linux en las puertas de muchas áreas, especialmente en las que se maneja información más o menos sensible. Estos lectores podrían leer una tarjeta que todos los miembros de la organización poseerían, conectar con la base de datos de usuarios, y autorizar o denegar la apertura de la puerta. Se trataría de un sistema sencillo de implementar, no muy caro, y que cubre de sobra las necesidades de seguridad en la mayoría de entornos: incluso se podría abaratar si en lugar de utilizar un mecanismo para abrir y cerrar puertas el sistema se limitara a informar al administrador del área o a un guardia de seguridad mediante un mensaje en pantalla o una luz encendida: de esta forma los únicos gastos serian los correspondientes a los lectores de códigos de barras, ya que como equipo con la base de datos se puede utilizar una maquina vieja o un servidor de propósito general.

Detección

Cuando la prevención es difícil por cualquier motivo (técnico, económico, humano. . .) es deseable que un potencial ataque sea detectado cuanto antes, para minimizar así sus efectos. Aunque en la detección de problemas, generalmente accesos físicos no autorizados, intervienen medios técnicos, como cámaras de vigilancia de circuito cerrado o alarmas, en entornos más normales el esfuerzo en detectar estas amenazas se ha de centrar en las personas que utilizan los sistemas y en las que sin utilizarlos están relacionadas de cierta forma con ellos; sucede lo mismo que con la seguridad lógica: se ha de ver toda la protección como una cadena que falla si falla su eslabón más débil.

Ejemplo: un usuario autorizado detecta presencia de alguien de quien sospecha que no tiene autorización para estar en un determinado lugar debe avisar inmediatamente al administrador o al responsable de los equipos, que a su vez puede avisar al servicio de seguridad si es necesario. No obstante, utilizar este servicio debe ser solamente un último recurso: generalmente en la mayoría de entornos no estamos tratando con terroristas, sino por suerte con elementos mucho menos peligrosos. Si cada vez que se sospecha de alguien se avisa al servicio de seguridad esto puede repercutir en el ambiente de trabajo de los usuarios autorizados estableciendo cierta presión que no es en absoluto recomendable; un simple *`¿puedo ayudarte en algo?'* suele ser más efectivo que un guardia solicitando una identificación formal.

Esto es especialmente recomendable en lugares de acceso restringido, como laboratorios de investigación o centros de cálculo, donde los usuarios habituales suelen conocerse entre ellos y es fácil detectar personas ajenas al entorno.

TIPOS

DE

DESASTRES

NATURALES

Terremotos

Los terremotos son el desastre natural menos probable en la mayoría de organismos ubicados en Argentina, simplemente por su localización geográfica: no nos encontramos en una zona donde se suelan producir temblores de intensidad considerable; incluso en zonas del oeste de Argentina, como Mendoza, donde la probabilidad de un temblor es más elevada, los terremotos no suelen alcanzan la magnitud necesaria para causar daños en los equipos. Por tanto, no se suelen tomar medidas serias contra los movimientos sísmicos, ya que la probabilidad de que sucedan es tan baja que no merece la pena invertir dinero para minimizar sus efectos.

De cualquier forma, aunque algunas medidas contra terremotos son excesivamente caras para la mayor parte de organizaciones en Argentina (evidentemente serian igual de caras en zonas como Los Angeles, pero allí el costo estaría justificado por la alta probabilidad de que se produzcan movimientos de magnitud considerable), no cuesta nada tomar ciertas medidas de prevención; por ejemplo, es muy recomendable no situar nunca equipos delicados en superficies muy elevadas (aunque tampoco es bueno situarlos áreas de suelo, como veremos al hablar de inundaciones. Si lo hacemos, un pequeño temblor puede tirar desde una altura considerable un complejo *hardware*, lo que con toda probabilidad lo inutilizara; puede incluso ser conveniente y barato utilizar fijaciones para los elementos más críticos, como las CPUs, los monitores o los *routers*. De la misma forma, tampoco es recomendable situar objetos pesados en superficies altas cercanas a los equipos, ya que si lo que cae son esos objetos también dañaran el *hardware*.

Para evitar males mayores ante un terremoto, también es muy importante no situar equipos cerca de las ventanas: si se produce un temblor pueden caer por ellas, y en ese caso la perdida de datos o *hardware* pierde importancia frente a los posibles accidentes incluso mortales que puede causar una pieza voluminosa a las personas a las que les cae encima. Además, situando los equipos alejados de las ventanas estamos dificultando las acciones de un potencial ladrón que se descuelgue por la fachada hasta las ventanas, ya que si el equipo estuviera cerca no tendría más que alargar el brazo para llevárselo.

No debemos entender por terremotos únicamente a los grandes desastres que derrumban edificios y destrozan vías de comunicación; quizás seria más apropiado hablar incluso de **vibraciones**, desde las más grandes (los terremotos) hasta las más pequeñas (un simple motor cercano a los equipos. Las vibraciones, incluso las más imperceptibles, pueden dañar seriamente cualquier elemento electrónico de nuestras máquinas, especialmente si se trata de vibraciones continuas: los primeros efectos pueden ser problemas con los cabezales de los discos duros o con los circuitos integrados que se dañan en las placas. Para hacer frente a pequeñas vibraciones podemos utilizar plataformas de goma donde situar a los equipos, de forma que la plataforma absorba la mayor parte de los movimientos; incluso sin llegar a esto, una regla común es evitar que entren en contacto equipos que poseen una electrónica delicada con *hardware* más mecánico, como las impresoras: estos dispositivos no paran de generar vibraciones cuando están en funcionamiento, por lo que situar una pequeña impresora encima de la CPU de una maquina es una idea nefasta. Como dicen algunos expertos en seguridad, el espacio en la sala de operaciones es un problema sin importancia comparado con las consecuencias de fallos en un disco duro o en la placa base de una computadora.

Tormentas eléctricas

Las tormentas con aparato eléctrico, especialmente frecuentes en verano cuando mucho personal se encuentra de vacaciones, lo que las hace más peligrosas, generan subidas súbitas de tensión infinitamente superiores a las que pueda generar un problema en la red eléctrica.

Si cae un rayo sobre la estructura metálica del edificio donde están situados nuestros equipos es casi seguro que podemos ir pensando en comprar otros nuevos; sin llegar a ser tan dramáticos, la caída de un rayo en un lugar cercano puede inducir un campo magnético lo suficientemente intenso como para destruir *hardware* incluso protegido contra voltajes elevados.

Sin embargo, las tormentas poseen un lado positivo: son predecibles con más o menos exactitud, lo que permite a un administrador parar sus máquinas y desconectarlas de la línea eléctrica .

Aparte de las propias tormentas, el problema son los responsables de los equipos: la caída de un rayo es algo poco probable pero no imposible en una gran ciudad donde existen pararrayos destinados justamente a atraer rayos de una forma controlada; por lo que directamente tiende a asumir que eso no le va a suceder nunca, y menos a sus equipos. Por tanto, muy pocos administradores se molestan en parar máquinas y desconectarlas ante una tormenta; si el fenómeno sucede durante las horas de trabajo y la tormenta es fuerte, quizás si que lo hace, pero si sucede un sábado por la noche nadie va a ir a la sala de operaciones a proteger a los equipos, y nadie antes se habrá tomado la molestia de protegerlos por una simple previsión meteorológica.

Otra medida de protección contra las tormentas eléctricas hace referencia a la ubicación de los medios magnéticos, especialmente las copias de seguridad; lo más alejados posible de la estructura metálica de los edificios. Un rayo en el propio edificio, o en un lugar cercano, puede inducir un campo electromagnético lo suficientemente grande como para borrar de golpe todas nuestras cintas o discos, lo que añade a los problemas por daños en el *hardware* la perdida de toda la información de nuestros sistemas.

Inundaciones y humedad

Cierto grado de humedad es necesario para un correcto funcionamiento de nuestras máquinas: en ambientes

extremadamente secos el nivel de electricidad estática es elevado, lo que, como veremos más tarde, puede transformar un pequeño contacto entre una persona y un circuito, o entre diferentes componentes de una maquina, en un daño irreparable al *hardware* y a la información. No obstante, niveles de humedad elevados son perjudiciales para los equipos porque pueden producir condensación en los circuitos integrados, lo que origina cortocircuitos que evidentemente tienen efectos negativos sobre cualquier elemento electrónico de una maquina.

Controlar el nivel de humedad en los entornos habituales es algo innecesario, ya que por norma nadie ubica estaciones en los lugares más húmedos o que presenten situaciones extremas; no obstante, ciertos equipos son especialmente sensibles a la humedad, por lo que es conveniente consultar los manuales de todos aquellos de los que tengamos dudas. Quizás sea necesario utilizar alarmas que se activan al detectar condiciones de muy poca o demasiada humedad, especialmente en sistemas de alta disponibilidad o de altas prestaciones, donde un fallo en un componente puede ser crucial.

Cuando ya no se habla de una humedad más o menos elevada sino de completas inundaciones, los problemas generados son mucho mayores. Casi cualquier medio que entre en contacto con el agua queda automáticamente inutilizado, bien por el propio liquido o bien por los cortocircuitos que genera en los sistemas electrónicos.

Evidentemente, contra las inundaciones las medidas más efectivas son las de prevención; podemos utilizar detectores de agua en los suelos o falsos suelos de las salas de operaciones, y apagar automáticamente los sistemas en caso de que se activen. Tras apagar los sistemas podemos tener también instalado un sistema automático que corte la corriente: algo muy común es intentar sacar los equipos previamente apagados o no de una sala que se esta empezando a inundar; esto, que a primera vista parece lo lógico, es el mayor error que se puede cometer si no hemos desconectado completamente el sistema eléctrico, ya que la mezcla de corriente y agua puede causar incluso la muerte a quien intente salvar equipos. Por muy caro que sea el *hardware* o por muy valiosa que sea la información a proteger, nunca serán magnitudes comparables a lo que supone la perdida de vidas humanas

Medidas de protección menos sofisticadas pueden ser la instalación de un falso suelo por encima del suelo real, o simplemente tener la precaución de situar a los equipos con una cierta elevación respecto al suelo, pero sin llegar a situarlos muy altos por los problemas que ya hemos comentado al hablar de terremotos y vibraciones.

Desastres del entorno

Electricidad

Quizás los problemas derivados del entorno de trabajo más frecuentes son los relacionados con el sistema eléctrico que alimenta nuestros equipos; cortocircuitos, picos de tensión, cortes de flujo que a diario amenazan la integridad tanto de nuestro *hardware* como de los datos que almacena o que circulan por el.

El problema menos común en las instalaciones modernas son las subidas de tensión, conocidas como `picos' porque generalmente duran muy poco: durante unas fracciones de segundo el voltaje que recibe un equipo sube hasta sobrepasar el limite aceptable que dicho equipo soporta. Lo normal es que estos picos apenas afecten al *hardware* o a los datos gracias a que en la mayoría de equipos hay instalados fusibles, elementos que se funden ante una subida de tensión y dejan de conducir la corriente, provocando que la maquina permanezca apagada. Disponga o no de fusibles el equipo a proteger (lo normal es que si los tenga) una medida efectiva y barata es utilizar tomas de tierra para asegurar aun más la integridad; estos mecanismos evitan los problemas de sobre tensión desviando el exceso de corriente hacia el suelo de una sala o edificio, o simplemente hacia cualquier lugar con voltaje nulo. Una toma de tierra sencilla puede consistir en un buen conductor conectado a los chasis de los equipos a proteger y a una barra maciza, también conductora, que se

introduce lo más posible en el suelo; el coste de la instalación es pequeño, especialmente si lo comparamos con las perdidas que supondría un incendio que afecte a todos o a una parte de nuestros equipos.

Incluso teniendo un sistema protegido con los métodos anteriores, si la subida de tensión dura demasiado, o si es demasiado rápida, podemos sufrir daños en los equipos; existen acondicionadores de tensión comerciales que protegen de los picos hasta en los casos más extremos, y que también se utilizan como filtros para ruido eléctrico. Aunque en la mayoría de situaciones no es necesario su uso, si nuestra organización tiene problemas por el voltaje excesivo quizás sea conveniente instalar alguno de estos aparatos.

Un problema que los estabilizadores de tensión o las tomas de tierra no pueden solucionar es justamente el contrario a las subidas de tensión: las bajadas, situaciones en las que la corriente desciende por debajo del voltaje necesario para un correcto funcionamiento del sistema, pero sin llegar a ser lo suficientemente bajo para que la maquina se apague.

En estas situaciones la maquina se va a comportar de forma extraña e incorrecta, por ejemplo no aceptando algunas instrucciones, no completando escrituras en disco o memoria, etc.

Otro problema, muchísimo más habituales que los anteriores en redes eléctricas modernas, son los cortes en el fluido eléctrico que llegan a nuestros equipos. Aunque un simple corte de corriente no suele afectar al *hardware*, lo más peligroso (y que sucede en muchas ocasiones) son las idas y venidas rápidas de la corriente; en esta situación, aparte de perder datos, nuestras máquinas pueden sufrir daños.

La forma más efectiva de proteger nuestros equipos contra estos problemas de la corriente eléctrica es utilizar una SAI (Servicio de Alimentación Ininterrumpido) conectada al elemento que queremos proteger.

Estos dispositivos mantienen un flujo de corriente correcto y estable de corriente, protegiendo así los equipos de subidas, cortes y bajadas de tensión; tienen capacidad para seguir alimentando las máquinas incluso en caso de que no reciban electricidad .

Un último problema contra el que ni siquiera las SAIs nos protegen es la corriente estática, un fenómeno extraño del que la mayoría de gente piensa que no afecta a los equipos, solo a otras personas. Nada más lejos de la realidad: simplemente tocar con la mano la parte metálica de teclado o un conductor de una placa puede destruir un equipo completamente. Se trata de corriente de muy poca intensidad pero un altísimo voltaje, por lo que aunque la persona no sufra ningún daño − solo un pequeño calambrazo − la computadora sufre una descarga que puede ser suficiente para destrozar todos sus componentes, desde el disco duro hasta la memoria RAM. Contra el problema de la corriente estática existen muchas y muy baratas soluciones: *spray* antiestético, ionizadores antiestéticos. . . No obstante en la mayoría de situaciones solo hace falta un poco de sentido común del usuario para evitar accidentes: no tocar directamente ninguna parte metálica, protegerse si debe hacer operaciones con el *hardware*, no mantener el entorno excesivamente seco. . .

Ruido eléctrico

Este problema no es una incidencia directa de la corriente en nuestros equipos, sino una incidencia relacionada con la corriente de otras máquinas que pueden afectar al funcionamiento de la nuestra. El ruido eléctrico suele ser generado por motores o por maquinaria pesada, pero también puede serlo por otras computadoras o por multitud de aparatos, especialmente muchos de los instalados en los laboratorios de organizaciones, y se transmite a través del espacio o de líneas eléctricas cercanas a nuestra instalación.

Para prevenir los problemas que el ruido eléctrico puede causar en nuestros equipos lo más barato es intentar no situar *hardware* cercano a la maquinaria que puede causar dicho ruido; si no tenemos más remedio que hacerlo, podemos instalar filtros en las líneas de alimentación que llegan hasta las computadoras. También es recomendable mantener alejados de los equipos dispositivos emisores de ondas, como teléfonos móviles,

transmisores de radio o *walkietalkies*; estos elementos pueden incluso dañar permanentemente a nuestro *hardware* si tienen la suficiente potencia de transmisión, o influir directamente en elementos que pueden dañarlo como detectores de incendios o cierto tipo de alarmas.

Incendios y humo

Una causa casi siempre relacionada con la electricidad son los incendios, y con ellos el humo; aunque la causa de un fuego puede ser un desastre natural, lo habitual en muchos entornos es que el mayor peligro de incendio provenga de problemas eléctricos por la sobrecarga de la red debido al gran numero de aparatos conectados al tendido. Un simple cortocircuito o un equipo que se calienta demasiado pueden convertirse en la causa directa de un incendio en el edificio, o al menos en la planta, donde se encuentran invertidos miles de pesos en equipamiento.

Un método efectivo contra los incendios son los extintores situados en el techo, que se activan automáticamente al detectar humo o calor. Algunos de ellos, los más antiguos, utilizaban agua para apagar las llamas, lo que provocaba que el *hardware* no llegara a sufrir los efectos del fuego si los extintores se activaban correctamente, pero que quedara destrozado por el agua expulsada.

Visto este problema, a mitad de los ochenta se comenzaron a utilizar extintores de halon; este compuesto no conduce electricidad ni deja residuos, por lo que resulta ideal para no dañar los equipos. Sin embargo, también el halon presentaba problemas: por un lado, resulta excesivamente contaminante para la atmósfera, y por otro puede asfixiar a las personas a la vez que acaba con el fuego. Por eso se han sustituido los extintores de halon (aunque se siguen utilizando mucho hoy en día) por extintores de dióxido de carbono, menos contaminante y menos perjudicial. De cualquier forma, al igual que el halon el dióxido de carbono no es precisamente sano para los humanos, por lo que antes de activar el extintor es conveniente que todo el mundo abandone la sala; si se trata de sistemas de activación automática suelen avisar antes de expulsar su compuesto mediante un pitido.

Aparte del fuego y el calor generado, en un incendio existe un tercer elemento perjudicial para los equipos: el humo, un potente abrasivo que ataca especialmente los discos magnéticos y ópticos.

Quizás ante un incendio el daño provocado por el humo sea insignificante en comparación con el causado por el fuego y el calor, pero hemos de recordar que puede existir humo sin necesidad de que haya un fuego: por ejemplo, en salas de operaciones donde se fuma. Aunque muchos no apliquemos esta regla y fumemos demasiado delante de nuestros equipos, seria conveniente no permitir esto; aparte de la suciedad generada que se deposita en todas las partes de una computadora, desde el teclado hasta el monitor, generalmente todos tenemos el cenicero cerca de los equipos, por lo que el humo afecta directamente a todos los componentes; incluso al ser algo más habitual que un incendio, se puede considerar más perjudicial para los equipos y las personas el humo del tabaco que el de un fuego.

En muchos manuales de seguridad se insta a los usuarios, administradores, o al personal en general a intentar controlar el fuego y salvar el equipamiento; esto tiene, como casi todo, sus pros y sus contras. Evidentemente, algo lógico cuando estamos ante un incendio de pequeñas dimensiones es intentar utilizar un extintor para apagarlo, de forma que lo que podría haber sido una catástrofe sea un simple susto o un pequeño accidente. Sin embargo, cuando las dimensiones de las llamas son considerables lo último que debemos hacer es intentar controlar el fuego nosotros mismos, arriesgando vidas para salvar *hardware*; como sucedía en el caso de inundaciones, no importa el precio de nuestros equipos o el valor de nuestra información: nunca serán tan importantes como una vida humana. Lo más recomendable en estos casos es evacuar el lugar del incendio y dejar su control en manos de personal especializado.

Temperaturas extremas

No hace falta ser un genio para comprender que las temperaturas extremas, ya sea un calor excesivo o un frío intenso, perjudican gravemente a todos los equipos. Es recomendable que los equipos operen entre 10 y 32 grados Celsius , aunque pequeñas variaciones en este rango tampoco han de influir en la mayoría de sistemas.

Para controlar la temperatura ambiente en el entorno de operaciones nada mejor que un acondicionador de aire, aparato que también influirá positivamente en el rendimiento de los usuarios (las personas también tenemos rangos de temperaturas dentro de los cuales trabajamos más cómodamente).

Otra condición básica para el correcto funcionamiento de cualquier equipo que este se encuentre correctamente ventilado, sin elementos que obstruyan los ventiladores de la CPU.

La organización física de la computadora también es decisiva para evitar sobrecalentamientos: si los discos duros, elementos que pueden alcanzar temperaturas considerables, se encuentran excesivamente cerca de la memoria RAM, es muy probable que los módulos acaben quemándose.

Protección de los datos

La seguridad física también implica una protección a la información de nuestro sistema, tanto a la que esta almacenada en el como a la que se transmite entre diferentes equipos.

Hay ciertos aspectos a tener en cuenta a la hora de diseñar una política de seguridad física que afectan principalmente, aparte de a los elementos físicos, a los datos de nuestra organización; existen ataques cuyo objetivo no es destruir el medio físico de nuestro sistema, sino simplemente conseguir la información almacenada en dicho medio.

Interceptación o Eavesdropping

La interceptación o *eavesdropping*, también conocida por *passive wiretapping* es un proceso mediante el cual un agente capta información − en claro o cifrada − que no le iba dirigida; esta captación puede realizarse por muchísimos medios (por ejemplo, capturando las radiaciones electromagnéticas.

Aunque es en principio un ataque completamente pasivo, lo más peligroso del *eavesdropping* es que es muy difícil de detectar mientras que se produce, de forma que un atacante puede capturar información privilegiada y claves para acceder a más información sin que nadie se de cuenta hasta que dicho atacante utiliza la información capturada, convirtiendo el ataque en activo. Un medio de interceptación bastante habitual es el *sniffing*, consistente en capturar tramas que circulan por la red mediante un programa ejecutándose en una máquina conectada a ella o bien mediante un dispositivo que se engancha directamente el cableado.

Estos dispositivos, denominados *sniffers* de alta impedancia, se conectan en paralelo con el cable de forma que la impedancia total del cable y el aparato es similar a la del cable solo, lo que hace difícil su detección. Contra estos ataques existen diversas soluciones; la más barata a nivel físico es no permitir la existencia de segmentos de red de fácil acceso, lugares idóneos para que un atacante conecte uno de estos aparatos y capture todo nuestro trafico. No obstante esto resulta difícil en redes ya instaladas, donde no podemos modificar su arquitectura; en estos existe una solución generalmente gratuita pero que no tiene mucho que ver con el nivel físico: el uso de aplicaciones de cifrado para realizar las comunicaciones o el almacenamiento de la información. Tampoco debemos descuidar las tomas de red libres, donde un intruso con un portátil puede conectarse para capturar trafico; es recomendable analizar regularmente nuestra red para verificar que todas las máquinas activas están autorizadas.

Como soluciones igualmente efectivas contra la interceptación a nivel físico podemos citar el uso de

dispositivos de cifra, generalmente *chips* que implementan algoritmos. Esta solución es muy poco utilizada, ya que es muchísimo más cara que utilizar implementaciones *software* de tales algoritmos y en muchas ocasiones la única diferencia entre los programas y los dispositivos de cifra es la velocidad. También se puede utilizar, como solución más cara, el cableado en vacío para evitar la interceptación de datos que viajan por la red: la idea es situar los cables en tubos donde artificialmente se crea el vacío o se inyecta aire a presión; si un atacante intenta `pinchar' el cable para interceptar los datos, rompe el vacío o el nivel de presión y el ataque es detectado inmediatamente.

Backups

La protección de los diferentes medios donde residen nuestras copias de seguridad es muy importante. Hemos de tener siempre presente que si las copias contienen toda nuestra información tenemos que protegerlas igual que protegemos nuestros sistemas.

Un error muy habitual es almacenar los dispositivos de *backup* en lugares muy cercanos a la sala de operaciones, cuando no en la misma sala; esto, que en principio puede parecer correcto (y cómodo si necesitamos restaurar unos archivos) puede convertirse en un problema: imaginemos simplemente que se produce un incendio de grandes dimensiones y todo el edificio queda reducido a cenizas. En este caso extremo tendremos que unir al problema de perder todos nuestros equipos − que seguramente cubrirá el seguro, por lo que no se puede considerar una catástrofe − el perder también todos nuestros datos, tanto los almacenados en los discos como los guardados en *backups* (esto evidentemente no hay seguro que lo cubra). Como podemos ver, resulta recomendable guardar las copias de seguridad en una zona alejada de la sala de operaciones, aunque en este caso descentralicemos la seguridad y tengamos que proteger el lugar donde almacenamos los *backups* igual que protegemos la propia sala o los equipos situados en ella, algo que en ocasiones puede resultar caro.

También suele ser común etiquetar las cintas donde hacemos copias de seguridad con abundante información sobre su contenido (sistemas de archivos almacenados, día y hora de la realización, sistema al que corresponde); esto tiene una parte positiva y una negativa. Por un lado, recuperar un archivo es rápido: solo tenemos que ir leyendo las etiquetas hasta encontrar la cinta adecuada.

Igual que para un administrador es fácil encontrar el *backup* deseado también lo es para un intruso que consiga acceso a las cintas, por lo que si el acceso a las mismas no esta bien restringido un atacante lo tiene fácil para sustraer una cinta con toda nuestra información; no necesita saltarse nuestro contrafuegos, conseguir una clave del sistema o chantajear a un operador: nosotros mismos le estamos poniendo en bandeja toda nuestros datos. No obstante, ahora nos debemos plantear la duda habitual: *si no etiqueto las copias de seguridad, ¿cómo puedo elegir la que debo restaurar en un momento dado?* Evidentemente, se necesita cierta información en cada cinta para poder clasificarlas, pero esa información **nunca** debe ser algo que le facilite la tarea a un atacante; por ejemplo, se puede diseñar cierta codificación que solo conozcan las personas responsables de las copias de seguridad, de forma que cada cinta vaya convenientemente etiquetada, pero sin conocer el código sea difícil imaginar su contenido. Aunque en un caso extremo el atacante puede llevarse todos nuestros *backups* para analizarlos uno a uno, siempre es más difícil disimular una carretilla llena de cintas de 8mm que una pequeña unidad guardada en un bolsillo. Y si aun pensamos que alguien puede sustraer todas las copias, simplemente tenemos que realizar *backups* cifrados. . . y controlar más el acceso al lugar donde las guardamos.

Radiaciones electromagnéticas

El acceso no autorizado a los datos a través de las radiaciones que el *hardware* emite; es un tema que ha cobrado especial importancia (especialmente en organismos militares) a raíz del programa tempest, un termino (*Transient ElectroMagnetic Pulse Emanation STandard*) que identifica una serie de estándares del gobierno estadounidense para limitar las radiaciones eléctricas y electromagnéticas del equipamiento

electrónico, desde estaciones de trabajo hasta cables de red, pasando por terminales, *mainframes*, ratones. . .

La idea es sencilla: la corriente que circula por un conductor provoca un campo electromagnético alrededor del conductor, campo que varia de la misma forma que lo hace la intensidad de la corriente. Si situamos otro conductor en ese campo, sobre el se induce una señal que también varia proporcionalmente a la intensidad de la corriente inicial; de esta forma, cualquier dispositivo electrónico (no solo el informático) emite continuamente radiaciones a través del aire o de conductores, radiaciones que con el equipo adecuado se pueden captar y reproducir remotamente con la consiguiente amenaza a la seguridad que esto implica. Conscientes de este problema − obviamente las emisiones de una batidora no son peligrosas para la seguridad, pero si que lo pueden ser las de un dispositivo de cifrado o las de un teclado desde el que se envíen mensajes confidenciales − en la década de los 50 el gobierno de Estados Unidos introdujo una serie de estándares para reducir estas radiaciones en los equipos destinados a almacenar, procesar o transmitir información que pudiera comprometer la seguridad nacional. De esta forma, el *hardware* certificado tempest se suele usar con la información clasificada y confidencial de algunos sistemas gubernamentales para asegurar que el *eavesdropping* electromagnético no va a afectar a privacidad de los datos. Casi medio siglo después de las primeras investigaciones sobre emanaciones de este tipo, casi todos los países desarrollados y organizaciones militares internacionales tienen programas similares a tempest con el mismo fin: proteger información confidencial. Para los gobiernos, esto es algo reservado a informaciones militares, nunca a organizaciones `normales' y mucho menos a particulares (la NRO, *National Reconnaissance Office*, elimino en 1992 los estándares tempest para dispositivos de uso domestico); sin embargo, y como ejemplo − algo extremo quizás − de hasta que punto un potencial atacante puede llegar a comprometer la información que circula por una red o que se lee en un monitor, vamos a dar aquí unas nociones generales sobre el problema de las radiaciones electromagnéticas.

Existen numerosos tipos de señales electromagnéticas; sin duda las más peligrosas son las de vídeo y las de transmisión serie, ya que por sus características no es difícil interceptarlas con el equipamiento adecuado.

Otras señales que *a priori* también son fáciles de captar, como las de enlaces por radiofrecuencia o las de redes basadas en infrarrojos, no presentan tantos problemas ya que desde un principio los diseñadores fueron conscientes de la facilidad de captación y las amenazas a la seguridad que una captura implica; esta inseguridad tan palpable provoco la rápida aparición de mecanismos implementados para dificultar el trabajo de un atacante, como el salto en frecuencias o el espectro disperso, o simplemente el uso de protocolos cifrados.

Este tipo de emisiones quedan fuera del alcance de tempest, pero son cubiertas por otro estándar denominado nonstop, también del Departamento de Defensa estadounidense.

Sin embargo, nadie suele tomar precauciones contra la radiación que emite su monitor, su impresora o el cable de su módem. Y son justamente las radiaciones de este *hardware* desprotegido las más preocupantes en ciertos entornos, ya que lo único que un atacante necesita para recuperarlas es el equipo adecuado.

¿Cómo podemos protegernos contra el *eavesdropping* de las radiaciones electromagnéticas de nuestro *hardware*?

Existe un amplio abanico de soluciones, desde simples medidas de prevención hasta complejos − y caros − sistemas para apuntalar los equipos. La solución más barata y simple que podemos aplicar es la **distancia**: las señales que se transmiten por el espacio son atenuadas conforme aumenta la separación de la fuente, por lo que si definimos un perímetro físico de seguridad lo suficientemente grande alrededor de una máquina, será difícil para un atacante interceptar desde lejos nuestras emisiones. No obstante, esto no es aplicable a las señales inducidas a través de conductores, que aunque también se atenúan por la resistencia e inductancia del cableado, la perdida no es la suficiente para considerar seguro el sistema.

Otra solución consiste en la **confusión**: cuantas más señales existan en el mismo medio, más difícil será para un atacante filtrar la que esta buscando; aunque esta medida no hace imposible la interceptación, si que la dificulta enormemente. Esto se puede conseguir simplemente manteniendo diversas piezas emisoras (monitores, terminales, cables. . .) cercanos entre si y emitiendo cada una de ellas información diferente (si todas emiten la misma, facilitamos el ataque ya que aumentamos la intensidad de la señal inducida. También existe *hardware* diseñado explícitamente para crear ruido electromagnético, generalmente a través de señales de radio que enmascaran las radiaciones emitidas por el equipo a proteger; dependiendo de las frecuencias utilizadas, quizás el uso de tales dispositivos pueda ser ilegal: en todos los países el espectro electromagnético esta dividido en bandas, cada una de las cuales se asigna a un determinado uso, y en muchas de ellas se necesita una licencia especial para poder transmitir.

Por último, la solución más efectiva, y más cara, consiste en el uso de dispositivos certificados que aseguran mínima emisión, así como de instalaciones que apuntalan las radiaciones. En el *hardware* hay dos aproximaciones principales para prevenir las emisiones: una es la utilización de circuitos especiales que apenas emiten radiación (denominados de fuente eliminada, *source suppressed*), y la otra es la contención de las radiaciones, por ejemplo aumentando la atenuación; generalmente ambas aproximaciones se aplican conjuntamente. En cuanto a las instalaciones utilizadas para prevenir el *eavesdropping*, la idea general es aplicar la contención no solo a ciertos dispositivos, sino a un edificio o a una sala completa. Quizás la solución más utilizada son las jaulas de Faraday sobre lugares donde se trabaja con información sensible; se trata de separar el espacio en dos zonas electromagnéticamente aisladas (por ejemplo, una sala y el resto del espacio) de forma que fuera de una zona no se puedan captar las emisiones que se producen en su interior. Para implementar esta solución se utilizan materiales especiales, como algunas clases de cristal, o simplemente un recubrimiento conductor conectado a tierra.

Antes de finalizar este punto quizás es recomendable volver a insistir en que todos los problemas y soluciones derivados de las radiaciones electromagnéticas no son aplicables a los entornos o empresas normales, sino que están pensados para lugares donde se trabaja con información altamente confidencial, como ciertas empresas u organismos militares o de inteligencia. Aquí simplemente se han presentado como una introducción para mostrar hasta donde puede llegar la preocupación por la seguridad en esos lugares. La radiación electromagnética **no** es un riesgo importante en la mayoría de organizaciones ya que suele tratarse de un ataque costoso en tiempo y dinero, de forma que un atacante suele tener muchas otras puertas para intentar comprometer el sistema de una forma más fácil.

Apéndice A

Productos

de

Backups

Bakup Remoto

La última tecnología en materia de backup remoto, que permite reducir el tamaño de los backups diferenciales e incrementales en un entorno del 85 al 99.9%, obteniendo **tiempos mínimos de transferencia de información**, y dándole la posibilidad de guardar todas las versiones de sus archivos que desee en el menor espacio posible.

¿Cómo funciona?

Después de la instalación del programa, se selecciona los archivos que desea respaldar . Se puede crear tantos grupos de archivos como desee, y asignar diferente periodicidad a cada uno de ellos.

Al llegar la hora que se eligió para realizar el respaldo, la computadora comprime, reduce y encripta los archivos, y los envía al servidor seguro de **inforNet**. Toda la tarea es realizada de modo 100% automático, sin requerir de ningún tipo de supervisión.

Los archivos son conservados durante el tiempo que Ud. decida, y pueden ser recuperados en el momento que Ud. quiera, durante las 24 horas del día, los 7 días de la semana.

Compresión y reducción de archivos

Antes de ser enviados al servidor, los archivos son comprimidos.
Se puede optar entre 3 diferentes niveles de compresión.

Por otra parte, antes de enviar un archivo que ya ha sido backupeado, el programa hace un análisis binario de las diferencias existentes entre una y otra versión, y crea un "patch" que expresa esas diferencias. Esto es lo que le permite tener a su disposición todas las versiones de sus archivos, por el tiempo que Ud. decida, en un espacio tan reducido.

Encriptación y confidencialidad

Su información es encriptada antes de ser almacenada en nuestro servidor, para lo cual puede optar entre 3 niveles de seguridad, con algoritmos de 128, 192, o 448 bits. Esto significa que se obtiene la misma seguridad que la de la encriptación utilizada en Estados Unidos para proteger los secretos militares.

Nadie que no conozca la clave puede acceder a los datos.

El proceso FastBIT! es la tecnología central detrás de nuestro revolucionario programa.

El proceso de *patching* involucra la comparación de dos versiones diferentes del mismo archivo y la extracción de las diferencias entre ellas. Estas diferencias se graban en un nuevo archivo conocido como *patch* (parche) que es, con frecuencia, entre un 85% y un 99.9 % mas chico que el archivo original.

La aplicación de esta tecnología al proceso de respaldo reducirá el tiempo de las comunicaciones y el espacio necesario para almacenamiento físico. Todo esto apunta a una sola cosa: **reducción de costos**

Reduce sus costos sin sacrificar la integridad de su copia de seguridad.

Cómo esta tecnología se aplica al proceso de backup

Cuando el programa de backup encuentra un archivo por primera vez, lo comprime y lo envía en forma segura a nuestro servidor. No se volverá a enviar el archivo entero, sino que sólo se transmitirán las modificaciones que sufra a partir de ese momento. Estos cambios son almacenados por separado, permitiendo la actualización y recuperación del archivo a la fecha que el usuario desee.

Esta tecnología se utiliza por primera vez en sistemas de backup remoto pero, lejos de ser nueva, es la forma en que las grandes empresas de software IBM, Microsoft, Novell, etc. actualizan las aplicaciones que

distribuyen comercialmente.

Recuperación de datos

La recuperación de datos se puede realizar de dos formas:

- **Directamente desde el sistema**, utilizando el mismo programa que

realiza los respaldos.

Se puede conectar en cualquier momento, y seleccionar en modo gráfico los archivos que se desea recuperar, o buscarlos por fecha de respaldo, o nombre del archivo o de la carpeta.

También podrá recuperar distintos archivos desde otros equipos sin importar en dónde estén ubicados los originales lo que le permite, por ejemplo, acceder a los datos desde un notebook, o desde una computadora , etc.

- Si la pérdida de datos es total (robo, incendio, desperfecto del disco duro), **suministran toda su información en CD−ROM** en menos de 24hs, por un costo mínimo.

En todos los casos tendrá la opción de grabar su información en su ubicación original, o en cualquier otra.

APÉNDICE B

CISCO IOS FIREWALL*Software Cisco IOS:* Conjunto de características Firewall

(www.Cisco.com)

A medida que la seguridad se va haciendo cada vez más crucial para asegurar las transacciones comerciales, las empresas deben integrarla en el diseño y en la infraestructura de las redes. El respeto de las normas de seguridad es más eficaz cuando es un componente inherente de la red.

El software Cisco IOS® se ejecuta en más del 80 por ciento de los routers de la backbone de Internet, y se ha convertido en el componente fundamental en la infraestructura actual de las redes. La seguridad basada en el Cisco IOS ofrece la mejor solución de seguridad de extremo a extremo para redes Internet, intranets y de acceso remoto.

Cisco IOS Firewall forma parte de la familia de productos Cisco Secure y es una opción diseñada específicamente para la seguridad del software Cisco IOS. Integra la resistente funcionalidad de firewall y la detección de intrusiones para todos los perímetros de la red y enriquece las capacidades de seguridad ya existentes de Cisco IOS. Añade una mayor profundidad y flexibilidad a las soluciones de seguridad ya existentes de Cisco IOS, como por ejemplo autenticación, cifrado y recuperación de fallos, implementando características de seguridad de vanguardia como el filtro basado en aplicaciones; la autenticación y la autorización dinámica por usuario; la defensa contra ataques a la red; el bloqueo Java y alertas en tiempo real. Cuando se combina con el software Cisco IOS IP Security (IPSec) y otras tecnologías basadas en el software Cisco IOS como el protocolo de tunneling de Capa 2 (L2TP) y la calidad de servicio (QoS), el conjunto de características Cisco IOS Firewall proporciona una completa solución de red privada virtual (VPN) integrada.

Funcionalidad Firewall basada en routers

Disponible en una gran variedad de routers basados en el software Cisco IOS, el Cisco IOS Firewall ofrece una sofisticada seguridad y aplicación de normativas para conexiones dentro de una organización (intranet) o entre redes asociadas (extranets), así como para asegurar la conexión a Internet de sucursales y oficinas remotas.

El Cisco IOS Firewall es la mejor elección para integrar el enrutamiento multiprotocolo con la aplicación de normativas de seguridad y permitir que los administradores configuren un router Cisco como firewall. Se puede ampliar para que los clientes puedan elegir la plataforma de los routers en base a su ancho de banda, la densidad de la LAN/WAN y los requisitos multiservicio a la vez que sacan partido de la seguridad avanzada. A la hora de elegir el router Cisco apropiado para diferentes entornos de seguridad, tome como referencia la siguiente pauta.

- Oficinas pequeñas/en casa: routers de las series Cisco 800, UBR900, 1600 y 1720
- Entornos extranet y sucursales: routers de las series Cisco 2500, 2600 y 3600
- Puntos de agregación de VPN y WAN u otros entornos de alto rendimiento: Cisco 7100, 7200, 7500, y routers de la serie Route Switch Module (RSM)

Ventajas principales

Cisco IOS Firewall funciona a la perfección con el software Cisco IOS, proporcionando un gran valor añadido y excepcionales ventajas, entre las que se incluyen:

Flexibilidad: instalada en un router Cisco, la solución integrada con capacidad de ampliación Cisco IOS Firewall lleva a cabo enrutamiento multiprotocolo, seguridad de perímetro, detección de intrusiones, funcionalidad VPN y autenticación y autorización por usuario.

Protección de la inversión: la integración de la funcionalidad firewall en un router multiprotocolo saca partido de la inversión existente en routers sin el costo y la curva de aprendizaje asociados con una nueva plataforma.

Soporte VPN: la instalación de Cisco IOS Firewall, con cifrado Cisco IOS y características VPN de calidad de servicio, hace posible transmisiones extremadamente seguras a bajo costo a través de redes públicas y garantiza que el tráfico de las aplicaciones de importancia crucial reciba la más alta prioridad.

Instalación ampliable: disponible para una gran variedad de plataformas de routers, el Cisco IOS Firewall se puede ampliar para satisfacer los requisitos de ancho de banda y de rendimiento de cualquier red.

Administración más sencilla: con el software Cisco ConfigMaker, un administrador de redes puede configurar características de seguridad de Cisco IOS (incluyendo Cisco IOS Firewall, conversión de direcciones de red y Cisco IPSec) desde una consola central a través de la red.

Cisco IOS Firewall está disponible para los routers de las series Cisco 800, 900, 1400, 1600, 1700, 2500, 2600, 3600, 7100, 7200 y 7500. También está disponible para el switch Catalyst® 5000, que ofrece integración multiservicio (datos/voz/vídeo/conexión telefónica), seguridad avanzada para conexiones por acceso telefónico y, para las series 7x00, 7500 y RSM, seguridad y enrutamiento integrados en el gateway Internet para grandes empresas y equipamiento en las instalaciones del abonado de los proveedores de servicios.

¿Qué novedades ofrece esta última versión? (Software Cisco IOS Firewall Software 12.1(4)T)

Contabilidad de proxy de autenticación para HTTP

La contabilidad es un medio de realizar un seguimiento sobre las acciones del usuario. Por lo general, la información de contabilidad consiste en la acción del usuario y su duración. La información de contabilidad se envía a los servidores de contabilidad, donde se almacena un formato de registro. Los administradores de sistemas utilizan la información de contabilidad para propósitos de facturación, seguridad o asignación de recursos. El servidor de contabilidad proporciona registros contables de "inicio a fin" con suficiente información para la auditoría de facturación y seguridad. Además de la autenticación, la autorización y la

contabilidad (AAA) del proxy de autenticación ayudarán a que los clientes puedan controlar las acciones de los usuarios de este servicio.

Implementación Cisco Firewall

Cuando se crea una caché de proxy de autenticación y las listas de control de acceso (ACL) asociadas, el proxy de autenticación empieza a hacer un seguimiento del tráfico del host autenticado. AAA almacena los datos de este evento. Si la opción se encuentra habilitada, en este momento puede generarse un registro de contabilidad o "registro de inicio". El firewall también proporciona un comando de usuario para ver este dato. Cuando la caché del proxy de autenticación caduca y se borra, los datos adicionales (como el periodo de tiempo transcurrido) se añaden a la información de contabilidad, y se envía al servidor un registro de "finalización". En este punto, la información se elimina de AAA.

Características principales de Cisco IOS Firewall

Cisco IOS Firewall ofrece una funcionalidad integrada de firewall para las redes Cisco y aumenta la flexibilidad y la seguridad de los routers Cisco. La Tabla 1 presenta un resumen de las características principales.

Tabla 1 Descripción general de Cisco IOS Firewall

Caracteristica	Descripción
Control de acceso basado en contexto (CBAC)	**Ofrece a los usuarios internos un control de acceso seguro por aplicación para todo el tráfico a través de los perímetros, como por ejemplo perímetros entre redes empresariales privadas e Internet**
Detección de intrusiones	**Proporciona control, intercepción y respuesta en tiempo real a la mala utilización de la red con un amplio conjunto de firmas de detección de intrusiones de ataque y recopilación de información más comunes**
Proxy de autenticación	**Autenticación y autorización dinámica por usuario para las comunicaciones basadas en LAN y de acceso telefónico; autentica a los usuarios contra los protocolos de autenticación estándar de la industria TACACS+ y RADIUS; los administradores de las redes pueden definir normas de seguridad individuales por usuario**
Detección y prevención de denegación de servicio	**Defiende y protege los recursos del router de los ataques más comunes; verifica las cabeceras de los paquetes eliminando los paquetes sospechosos**
Asignación dinámica de puertos	**Permite que los administradores de las redes ejecuten aplicaciones compatibles con CBAC en puertos que no sean estándares**
Bloqueo de aplicaciones Java	**Protege a la red de aplicaciones Java malintencionadas**
Cifrado de VPN e IPSec y soporte de calidad de servicio	**Funciona con las características de cifrado, tunneling y QoS de Cisco IOS para garantizar las VPN** **Proporcionan túneles cifrados con capacidad de ampliación en el router a la vez que integran una potente seguridad de perímetro, una administración avanzada del ancho de banda, detección de intrusiones y validación a nivel de servicio**

	Basada en estándares para su interoperatividad
Alertas en tiempo real	**Registra las alertas en caso de ataques de denegación de servicio u otros casos configurados de antemano; ahora se puede configurar por aplicación o por característica**
Registros de auditoría	**Detalla las transacciones; registra el sello de hora, el anfitrión de origen, el anfitrión de destino, los puertos, la duración y el total de bytes transmitidos para realizar un informe detallado; ahora se puede configurar por aplicación o por característica**
Registro de eventos	**Permite a los administradores controlar en tiempo real posibles intrusiones u otras actividades no estándares, registrando el resultado de los mensajes de error enviados en una terminal de consola o servidor syslog, determinando niveles de gravedad y registrando otros parámetros**
Administración Firewall	**Las herramientas de configuración de la red basadas en asistentes ofrecen ayuda paso a paso durante el diseño de la red, la asignación de direcciones y la configuración de las normas de seguridad Cisco IOS Firewall; disponible en los routers Cisco 1600, 1720, 2500, 2600 y 3600; compatible también con las configuraciones NAT e IPSec**
Integración con el software Cisco IOS	**Funciona conjuntamente con las características de Cisco IOS, integrando la puesta en práctica de normas de seguridad en la red**
Filtrado de tráfico básico y avanzado	**Listas de control de acceso estándares y extendidas (ACL): aplican controles sobre el acceso a segmentos específicos de la red y definen el tráfico que puede pasar a través de un segmento de la red** **Bloqueo: las ACL dinámicas otorgan acceso temporal a través de firewalls mediante la identificación del usuario (nombre de usuario/contraseña)**
Soporte para varias interfaces basado en normativas	**Permite controlar el acceso de los usuarios por dirección IP e interfaz, tal y como determina el sistema de seguridad**
Redundancia/recuperación de fallos	**Encamina automáticamente el tráfico a un router de respaldo si tiene lugar un fallo**
Conversión de direcciones de la red	**Oculta la red interna de la externa para mejorar la seguridad**
Listas de acceso basadas en tiempo	**Define las normas de seguridad por hora del día y día de la semana**
Autenticación de router par	**Asegura que los routers reciben una información de enrutamiento fiable de fuentes solventes**
Mejora la detección y la defensa ante los ataques en los servidores de correo electrónico	**La nueva detección de intrusiones se ha diseñado específicamente para los ataques orientados a SMTP.**

Control de acceso basado en contexto (CBAC)

El motor CBAC de Cisco IOS Firewall proporciona control de acceso por aplicaciones a través de los perímetros de la red. Mejora la seguridad para aplicaciones TCP y de protocolo de datagrama de usuario

(UDP) que usan puertos conocidos, como por ejemplo el tráfico FTP y de correo electrónico, mediante el escrutinio de las direcciones de origen y de destino. CBAC permite que los administradores puedan poner en práctica inteligencia de firewall como parte de un producto integrado.

Por ejemplo, en las sesiones con un socio de extranet que impliquen aplicaciones Internet, multimedia o bases de datos Oracle ya no será necesario abrir una entrada en la red a la que se podría acceder mediante fallos en la red del socio. CBAC permite que redes muy seguras ejecuten el tráfico de las aplicaciones básicas actuales, así como de aplicaciones avanzadas (por ejemplo, multimedia o videoconferencia) con la seguridad de un router.

El impacto CBAC en la seguridad de la red

CBAC es un mecanismo de control por aplicación para el tráfico IP, incluyendo aplicaciones Internet TCP y UDP estándares, aplicaciones multimedia (aplicaciones H.323 y otras aplicaciones de vídeo) y bases de datos Oracle. CBAC examina los paquetes TCP y UDP y hace un seguimiento de su "estado" o del estado de la conexión.

TCP es un protocolo orientado a la conexión. Antes de transmitir los datos, un host de origen negocia una conexión con un destino en un proceso que se denomina "saludo a tres bandas". Este proceso de saludo garantiza que se obtengan conexiones TCP válidas y transmisiones libres de errores. Durante el establecimiento de la conexión, TCP pasa a través de varios estados o fases, las cuales pueden identificarse fácilmente en las cabeceras de los paquetes. Las ACL extendidas y estándares leen los estados en las cabeceras de los paquetes para determinar si el tráfico puede traspasar un enlace.

CBAC mejora las operaciones de las ACL añadiéndoles inteligencia, ya que lee todo el paquete para obtener la información de estado de la aplicación. Usando esta información, CBAC crea una anotación ACL temporal específica a esta sesión, permitiendo que el tráfico de retorno entre en la red protegida. Esta ACL temporal abre la puerta en el firewall. Cuando una sesión caduca o termina, la anotación ACL se elimina y se cierra la entrada a tráfico adicional. Las listas de control de acceso estándares y ampliadas no pueden crear anotaciones ACL temporales, con lo que, hasta ahora, los administradores han estado obligados a evaluar los riesgos de seguridad con respecto a la necesidad de acceder a la información. Usando las ACL estándares o extendidas, las aplicaciones avanzadas que seleccionan entre varios canales para el tráfico de retorno resultan difíciles de proteger.

CBAC es más seguro que los productos que sólo usan ACL, ya que tiene en cuenta el tipo de aplicación en el momento de decidir si debe permitir el paso de una sesión a través del firewall y determina si selecciona entre varios canales para el tráfico de retorno. Antes de existir CBAC, los administradores sólo podían permitir el tráfico de aplicaciones avanzadas escribiendo listas de control de acceso permanentes que, en esencia, dejaban las puertas del firewall abiertas al tráfico de dichas aplicaciones, por lo que la mayoría optaron por denegar dicho tráfico. Ahora, con CBAC, pueden permitir el paso de tráfico de aplicaciones multimedia y de otro tipo de aplicaciones abriendo el firewall cuando sea necesario y cerrándolo el resto del tiempo. Por ejemplo, si se configura CBAC para permitir el paso de tráfico Microsoft NetMeeting, cuando un usuario interno inicie una conexión, el firewall permitirá el tráfico de retorno. No obstante, si una fuente NetMeeting externa inicia una conexión con un usuario interno, CBAC denegará la entrada e ignorará los paquetes.

Detección de intrusiones

Los sistemas de detección de intrusiones (IDS) proporcionan un nivel de protección más allá del firewall protegiendo a la red de ataques y amenazas tanto internas como externas. La tecnología IDS de Cisco IOS Firewall mejora la protección firewall del perímetro tomando las medidas oportunas sobre los paquetes y flujos que violan la norma de seguridad o representan una actividad malintencionada contra la red.

Las capacidades de detección de intrusiones de Cisco IOS Firewall son ideales para proporcionar mayor visibilidad en los perímetros intranet, extranet e Internet de sucursales. Los administradores de redes disfrutan ahora de una protección más resistente contra los ataques sobre la red y pueden responder de forma automática a amenazas de hosts internos o externos.

Detección y respuesta

IDS de Cisco IOS Firewall identifica 59 ataques habituales utilizando firmas para detectar patrones de uso incorrecto en el tráfico de la red. Las firmas de detección de intrusiones que se incluyen en la nueva versión de Cisco IOS Firewall fueron elegidas entre un amplio espectro de firmas de detección de intrusiones. Las firmas representan importantes violaciones de seguridad, así como los ataques más habituales a la red y en los rastreos que recaban información.

Cisco IOS Firewall actúa como un sensor de la detección de intrusiones en línea, observando paquetes y sesiones a medida que fluyen a través del router, rastreando cada uno de ellos para que concuerden con cualquiera de las firmas IDS. Cuando detecta actividad sospechosa, responde antes de que se pueda poner en peligro la seguridad de la red y registra el evento por medio del syslog de Cisco IOS. El administrador de la red puede configurar el sistema IDS para que elija la respuesta apropiada a diferentes amenazas. Cuando los paquetes de una sesión coinciden con una firma, puede configurarse el sistema IDS para que:

Envíe una alarma a un servidor syslog o al sistema de detección de intrusiones de Cisco Secure (antes denominado sistema NetRanger®)

- Director (interfaz de gestión centralizada)
- Omita el paquete
- Restablezca la conexión TCP

Cisco desarrolló las capacidades de detección de intrusiones de Cisco IOS Firewall, basadas en el software Cisco IOS, teniendo en cuenta la flexibilidad. De ese modo, en caso de falsos positivos, pudieran desactivarse firmas individuales. Aunque es preferible activar tanto las características de firewall como de detección de intrusiones del motor de seguridad CBAC para habilitar una normativa de seguridad en la red, cada una de estas funciones puede desactivarse de forma independiente y en interfaces de routers diferentes. La detección de intrusiones basada en el software Cisco IOS forma parte de Cisco IOS Firewall que se encuentra disponible en los routers de las series Cisco 1720, 2600, 3600, 7100, 7200, 7500 y el RSM para los switches Catalyst 5000. Todas las plataformas con Cisco IOS Firewall detectan los cinco ataques SMTP más habituales.

Cisco Secure: software integrado y sistema de detección de intrusiones

Los clientes de Cisco Secure Intrusion Detection System (IDS) pueden utilizar las firmas IDS basadas en el software Cisco IOS para complementar sus sistemas IDS ya existentes. Ello permite que se utilice un IDS en áreas que no serían capaces de admitir un sensor NetRanger. Las firmas IDS de Cisco IOS pueden utilizarse de manera conjunta o independiente del resto de características de Cisco IOS Firewall.

Cisco IOS Firewall con detección de intrusiones puede añadirse a la pantalla de Cisco Secure IDS Director en forma de icono para proporcionar una vista consistente de todos los sensores de detección de intrusiones a lo largo y ancho de la red. Las capacidades de detección de intrusiones de Cisco IOS Firewall cuentan con un mecanismo mejorado de generación de informes que permite informar a la consola de Cisco Secure IDS Director, además de hacerlo al syslog de Cisco IOS.

Proxy de autenticación

Los administradores de redes pueden crear normas de seguridad específicas para cada usuario con la

autenticación y la autorización dinámicas por usuario basadas en el Cisco IOS Firewall LAN. Con anterioridad, la identidad del usuario y el acceso autorizado relacionado con ella se determinaba por una dirección IP de usuario fija o tenía que aplicarse una única normativa de seguridad a todo un grupo de usuarios o subred. Ahora, es posible descargar una normativa por usuario de forma dinámica al router desde un servidor de autenticación TACACS+ o RADIUS, utilizando los servicios de autenticación, autorización y contabilidad (AAA) del software Cisco IOS.

Los usuarios pueden entrar en la red o en Internet mediante HTTP y se descargarán de forma automática sus perfiles de acceso específicos. Cuando hace falta, están disponibles los privilegios de acceso dinámicos individuales pertinentes, que protegen a la red de una normativa genérica aplicada sobre un grupo de usuarios. La autenticación y la autorización pueden aplicarse a la interfaz de los routers en cualquier dirección para asegurar el uso interno y externo de extranets, intranets e Internet.

Detección y prevención de denegación de servicio

La detección y prevención mejoradas de la denegación de servicio defiende a las redes de ataques generalizados, como por ejemplo sobrecarga SYN (sincronizar/iniciar), rastreos de puertos e inyección de paquetes, mediante la inspección de los números de secuencia de los paquetes en las conexiones TCP. Si los números no están dentro de un rango esperado, el router ignora los paquetes sospechosos. Cuando el router detecta velocidades inusualmente altas de nuevas conexiones, emite un mensaje de alerta, a continuación ignora las tablas de estado de las conexiones TCP medio abiertas para impedir que se consuman los recursos de la red.

Cuando el Cisco IOS Firewall detecta un posible ataque, rastrea el acceso de los usuarios por dirección origen o de destino y pares de puertos. También detalla la transacción, creando un informe de auditoría.

Asignación dinámica de puertos

Esta característica permite que las aplicaciones compatibles con CBAC se ejecuten en puertos no estandarizados. También permite que los administradores de redes personalicen el control de acceso para aplicaciones y servicios específicos a fin de satisfacer las diferentes necesidades de sus redes.

Bloqueo de aplicaciones Java

Con la proliferación de las aplicaciones Java disponibles a través de Internet, la protección de las redes contra aplicaciones malintencionadas es una de las principales preocupaciones de los administradores de redes. La característica de bloqueo de Java puede configurarse para que filtre o deniegue por completo el acceso a aplicaciones Java que no estén incorporadas en archivos o comprimidas en ellos.

Cifrado de VPN e IPSec y compatibilidad de calidad de servicio

Cuando se combina con la tecnología Cisco IPSec, Cisco IOS Firewall proporciona funcionalidad VPN integrada. Las VPN se están desarrollando con gran rapidez para ofrecer transferencias de datos seguras a través de líneas públicas (por ejemplo Internet), reducir los costos de administración y telecomunicaciones para usuarios remotos, sucursales y extranets, y mejorar la fiabilidad y la calidad de servicio.

Cisco IOS Firewall funciona con las características de cifrado, tunneling y QoS del software Cisco IOS para dar seguridad a las VPN. La capacidad de cifrado en la capa de red impide las escuchas o la intercepción de los datos durante la transmisión a través de la red. Cisco IOS Firewall cifra los datos de comunicaciones privadas que se establece a través de redes no fiables, utilizando los estándares de cifrado del protocolo de seguridad Internet (IPSec), tanto en la variedad de 56 bits (DES) como de 168 bits (3DES).

Para una perfecta interoperatividad, el software Cisco IOS admite varios estándares de protocolos de tunneling, aceptando la encapsulación genérica de enrutamiento (GRE), envío de Capa 2 (L2F) y protocolo de tunneling de Capa 2 (L2TP). Las funciones de calidad de servicio clasifican el tráfico, gestionan la congestión y dan prioridad a las aplicaciones cuando éstas lo requieren.

Cisco IOS Firewall puede implementarse con las plataformas que admiten Cisco VPN, específicamente, con los routers de las series Cisco 1720, 2600, 3600 y 7100, que amplían una red existente a la conectividad virtual privada. Cisco entiende que las soluciones VPN deben proporcionar algo más que túneles cifrados y seguros a través de instalaciones de redes públicas. También deben garantizar el envío de datos fiable y oportuno, y proporcionar una importante seguridad de perímetro en el portal empresarial de la red pública. Cisco IOS Firewall, combinado con un router de la serie 7100, proporciona túneles cifrados con capacidad de ampliación, a la vez que integra una potente seguridad de perímetro, administración avanzada del ancho de banda, detección de intrusiones y validación a nivel de servicios.

La característica de proxy de autenticación de Cisco IOS Firewall proporciona también autenticación y autorización de los usuarios para el software de cliente VPN de Cisco.

Alertas configurables en tiempo real, registro de auditoría y registro de eventos

Estas alertas en tiempo real envían mensajes de error syslog a las consolas de administración central al detectar una actividad sospechosa, permitiendo que los administradores de la red puedan responder de inmediato a las intrusiones. Las funciones mejoradas para el registro de auditoría usan syslog para controlar todas las transacciones, registrando sellos de hora, host de origen, host de destino, puertos usados, duración de la sesión y el número total de bytes transmitidos para generar informes avanzados basados en la sesión.

Ahora las características de alerta y registro de auditoría de Cisco IOS Firewall pueden configurarse, posibilitando unos informes y un seguimiento de los errores más flexible. Las características configurables de registro de auditoría admiten el rastreo modular de aplicaciones específicas compatibles con CBAC y el bloqueo Java. Tanto las alertas en tiempo real como las características de auditoría son compatibles con una gran variedad de herramientas de generación de informes de otros fabricantes.

Cuando ocurre un evento de la red, éste genera una alerta al host de registro a través de un mecanismo syslog del software Cisco IOS. Esto permite a los administradores controlar en tiempo real intrusiones potenciales u otras actividades no estándares, registrando el resultado de los mensajes de error enviados a una terminal de consola o servidor syslog, determinando niveles de gravedad y registrando otros parámetros.

Administración Firewall

La implementación de las normativas de seguridad y administración de Cisco IOS Firewall es rápida y eficaz con una gestión basada en la interfaz gráfica de usuario desde una ubicación central. Cisco ConfigMaker 2.1 y versiones posteriores incluyen un asistente de seguridad que ofrece ayuda paso a paso para una rápida configuración de la normativa de seguridad para Cisco IOS Firewall. También son compatibles con la configuración NAT e IPSec.

ConfigMaker es una herramienta de software basada en asistentes de fácil manejo para Microsoft Windows 95, Windows 98 y Windows NT 4.0, y diseñada para configurar una pequeña red de routers, switches, hubs y otros dispositivos de red Cisco desde un único PC. Se encuentra disponible para los routers de las series Cisco 800, 1600, 1720, 2500, 2600 y 3600.

Integración con el software Cisco IOS

Cisco IOS Firewall es una solución de seguridad integrada en la red a través del software Cisco IOS. Una

potente normativa de seguridad implica algo más que el control del perímetro o la configuración y la gestión del firewall: el cumplimiento de las normativas de seguridad debe ser un componente inherente de la propia red. El software Cisco IOS es un vehículo ideal para implementar una normativa de seguridad global. La construcción de una solución Cisco de extremo a extremo permite que los administradores apliquen normativas de seguridad en toda la red a medida que ésta crece.

Cisco IOS Firewall también funciona perfectamente con las características del software Cisco IOS, incluyendo NAT, protocolos de tunneling VPN, Cisco Express Forwarding (CEF), extensiones AAA, tecnología de cifrado de Cisco e IPSec de Cisco IOS.

¿Quién debe plantearse la posibilidad de adquirir Cisco IOS Firewall?

- Los clientes que necesiten una solución integrada que combine una potente seguridad, detección de intrusiones, autenticación y autorización por usuario, funcionalidad VPN y enrutamiento multiprotocolo.
- Los clientes interesados en un método rentable de extender la seguridad del perímetro en todas las fronteras de la red, especialmente perímetros de sucursales, intranets y extranets
- Las pequeñas y medianas empresas que buscan un router rentable con capacidades integradas de firewall y de detección de intrusiones
- Los clientes de los proveedores de servicios que desean utilizarlo como paquete router/firewall para un servicio gestionado
- Los clientes que necesitan una seguridad adicional entre segmentos de la red (por ejemplo, entre sus empresas y la ubicación de un socio de menor confianza)
- Empresas con conexiones de intranet en las que se exige una mayor seguridad
- Ubicaciones de sucursales que se conectan con una oficina de la empresa o con Internet
- Clientes que ya conocen el Cisco IOS y no quieren una plataforma firewall independiente
- Clientes que desean llevar a cabo la protección firewall por toda una infraestructura de redes para crear un entorno de defensa en profundidad

¿Y qué pasa con el soporte de Cisco?

Cisco Systems es bien conocido por sus soluciones de conectividad líderes del mercado, pero también por las soluciones de soporte de extremo a extremo a nivel global que ayudan a que los administradores de redes ofrezcan soporte técnico a sus redes locales o de área extensa Cisco.

Esta cartera de productos de soporte técnico cuenta con servicios avanzados y personalizados de instalación, mantenimiento y marketing para maximizar y proteger su inversión. A través de Cisco Connection Online (CCO), el galardonado sitio Web de Cisco, se pueden conseguir actualizaciones para Cisco IOS Firewall.

Disponibilidad y precios

Cisco IOS Firewall se encuentra disponible como una opción de imagen de software para los routers de las series Cisco 800, UBR900, 1600, 1720, 2500, 2600, 3600, 7100, 7200, 7500 y RSM. Se puede descargar la imagen de software desde el sitio Web de Cisco o solicitarla en CD−ROM. Para obtener más información sobre los precios, póngase en contacto con su oficina de ventas o distribuidor de Cisco, o visite nuestro sitio Web en http: //www.cisco.com

APÉNDICE C

CONSIDERACIONES

SOBRE

BACKUPS

BACKUP

Servidores distribuidos

(Revista Datamation)

En los últimos diez años la presencia de servidores múltiples ha complicado la administración de recursos.

Antes los backup eran lentos y tediosos.

Proteccion de datos: Que debemos hacer a la hora de comprar una solución para un entorno de servidores distribuidos..

Características a contemplar:

- Backups que sean automatizados
- Administración centralizada del proceso backup y recuperación
- Backup de archivos y BD que se encuentres abiertos
- Backup que requieren menos tiempo de operación
- Licencias de software incorporadas a la solución para evitar costos
- Disponer del HW adecuado para alojar datos
- Completo control de archivos y directorios que serán respaldados , con capacidades de filtro de archivos
- Dispositivos para la restauración de archivos especificos en cualquier momento del día.
- Ausencia de datos estacionados en servidores o gateways intermediarios
- Capacidad de restauración indistinta a través de líneas de comunicación
- Capacidad de realizar backup en mas de una plataforma con la misma solución.
- Posibilidad que el usuario maneje el programa de retención de datos backup
- Disponibilidad de datos en sitios de prosesamiento alternativo
- Varios niveles de encriptado de datos
- Capacidad de recomenzar y reconstruir automáticamente el backup por líneas de recuperación
- Registro y reportes al adm
- Informe detallado del uso del sistema
- Capacidad de conseguir datos de retenciones a largo plazo sin requerir de un drive o cinta.

Consideraciones relacionadas con los costos:

- Para eventuales restauraciones totales
- Para realizar restauraciones parciales
- De configuración e instalación
- De comunicaciones
- De cintas de archivos
- De uso, basándose en tiempos, cantidades, frecuencias y otros parámetros
- Por cargos de cancelación por recesión del contrato

Que debemos prever :

- Definir los objetivos de la recuperación y las ventajas disponibles para el backup
- Disponer de información detallada sobre el HW del servidor y su sistema operativo

- Detectar los dispositivos de comunicación que vinculan las diferentes localizaciones
- Establecer el personal disponible para la adm del proceso de backup y especificar ubicación geográfica
- Determinar dónde se encuentra la instalación alternativa en caso de que ocurra un desastre

Que se debe preguntar a los proveedores:

- Si puede indicar su experiencia dentro de la industria
- ¿Por que se eligió a este proveedor ?
- ¿Se ha comprobado la velocidad con que se realizan los backup?
- ¿Se hicieron pruebas de recuperación completa ?
- ¿Funciona esta tecnología de la forma especificada?
- ¿Fue necesario aumentar el ancho de banda de las comunicaciones para soportar lo encriptado?
- ¿Podemos conocer el nivel de experiencia ?
- ¿Son los costos mayores a las estimaciones iniciales?

Puntos a revisar:

- Que el proveedor sea realmente capaz de manejar todos los datos dentro de las ventanas que admiten los procesos de la empresa
- Estar seguro de que la recuperación funciona bien en forma online y con medios renovables
- Verificar que la solución hace copia de respaldo de todos los atributos de seguridad y otros del sistema operativo en relación con los archivos
- Asegurarse de que la solución admita backup de archivos y bases de datos mientras estén abiertos
- Verificar que la solución puede funcionar con la red tal como esta inslalada o con conexión a internet que no requiera el rediseño de la arquitectura de la red
- Verificar que los backup y recuperaciones puedan operarse realmente desde la consola de administración central

Antes de cerrar contrato:

- Configurar una simulación o prueba utilizando un servicio especializado . También se puede elegir la ubicación distribuida en la que se registran más problemas y darle ese sitio al proveedor para que haga una prueba paga
- Extrapolar de la prueba los requerimientos propios de su organización en cuanto a comunicaciones

APÉNDICE D

PLAN DE CONTINGENCIA

Plan de Contingencia

Pasos a seguir para elaborar un plan de contingencia

(*Documento en ingles)*

Preparing For Contingencies and Disasters

A *computer security contingency* is an event with the potential to disrupt computer operations, thereby disrupting critical mission and business functions. Such an event could be a power outage, hardware failure, fire, or storm. If the event is very destructive, it is often called a disaster.

Contingency planning directly supports an organization's goal of continued operations. Organizations

practice contingency planning because it makes good business sense.

To avert potential contingencies and disasters or minimize the damage they cause organizations can take steps early to control the event. Generally called *contingency planning*, this activity is closely related to incident handling, which primarily addresses malicious technical threats such as hackers and viruses.

Contingency planning involves more than planning for a move offsite after a disaster destroys a data center. It also addresses how to keep an organization's critical functions operating in the event of disruptions, both large and small. This broader perspective on contingency planning is based on the distribution of computer support throughout an organization.

This chapter presents the contingency planning process in six steps:

- Identifying the mission− or business−critical functions.
- Identifying the resources that support the critical functions.
- Anticipating potential contingencies or disasters.
- Selecting contingency planning strategies.
- Implementing the contingency strategies.
- Testing and revising the strategy.

Step 1: Identifying the Mission− or Business−Critical Functions

This chapter refers to an organization as having critical *mission* or *business* functions. In government organizations, the focus is normally on performing a mission, such as providing citizen benefits. In private organizations, the focus is normally on conducting a business, such as manufacturing widgets.

Protecting the continuity of an organization's mission or business is very difficult if it is not clearly identified. Managers need to understand the organization from a point of view that usually extends beyond the area they control. The definition of an organization's critical mission or business functions is often called a *business plan*.

Since the development of a business plan will be used to support contingency planning, it is necessary not only to identify critical missions and businesses, but also to *set priorities for* them. A fully redundant capability for each function is prohibitively expensive for most organizations. In the event of a disaster, certain functions will not be performed. If appropriate priorities have been set (and approved by senior management), it could mean the difference in the organization's ability to survive a disaster.

Step 2: Identifying the Resources That Support Critical Functions

In many cases, the longer an organization is without a resource, the more critical the situation becomes. For example, the longer a garbage collection strike lasts, the more critical the situation becomes.

Resources That Support Critical Functions

Human Resources
Processing Capability
Computer−Based Services
Data and Applications
Physical Infrastructure
Documents and Papers

After identifying critical missions and business functions, it is necessary to identify the supporting resources,

the time frames in which each resource is used (e.g., is the resource needed constantly or only at the end of the month?), and the effect on the mission or business of the unavailability of the resource. In identifying resources, a traditional problem has been that different managers oversee different resources. They may not realize how resources interact to support the organization's mission or business. Many of these resources are not computer resources. Contingency planning should address all the resources needed to perform a function, regardless whether they directly relate to a computer.

The analysis of needed resources should be conducted by those who understand how the function is performed and the dependencies of various resources on other resources and other critical relationships. This will allow an organization to *assign priorities* to resources since not all elements of all resources are crucial to the critical functions.

Human Resources

People are perhaps an organization's most obvious resource. Some functions require the effort of specific individuals, some require specialized expertise, and some only require individuals who can be trained to perform a specific task. Within the information technology field, human resources include both operators (such as technicians or system programmers) and users (such as data entry clerks or information analysts).

Processing Capability

Traditionally contingency planning has focused on processing power (i.e., if the data center is down, how can applications dependent on it continue to be processed?). Although the need for data center backup remains vital, today's other processing alternatives are also important. Local area networks (LANs), minicomputers, workstations, and personal computers in all forms of centralized and distributed processing may be performing critical tasks.

Contingency Planning Teams

To understand what resources are needed from each of the six resource categories and to understand how the resources support critical functions, it is often necessary to establish a contingency planning team. A typical team contains representatives from various organizational elements, and is often headed by a contingency planning coordinator. It has representatives from the following three groups:

1. business−oriented groups , such as representatives from functional areas;

2. facilities management; and

3. technology management.

Various other groups are called on as needed including financial management, personnel, training, safety, computer security, physical security, and public affairs.

Automated Applications and Data

Computer systems run applications that process data. Without current electronic versions of both applications and data, computerized processing may not be possible. If the processing is being performed on alternate hardware, the applications must be compatible with the alternate hardware, operating systems and other software (including version and configuration), and numerous other technical factors. Because of the complexity, it is normally necessary to periodically verify compatibility. (See Step 6, Testing and Revising.)

Computer−Based Services

An organization uses many different kinds of computer−based services to perform its functions. The two most important are normally communications services and information services. Communications can be further categorized as data and voice communications; however, in many organizations these are managed by the same service. Information services include any source of information outside of the organization. Many of these sources are becoming automated, including on−line government and private databases, news services, and bulletin boards.

Physical Infrastructure

For people to work effectively, they need a safe working environment and appropriate equipment and utilities. This can include office space, heating, cooling, venting, power, water, sewage, other utilities, desks, telephones, fax machines, personal computers, terminals, courier services, file cabinets, and many other items. In addition, computers also need space and utilities, such as electricity. Electronic and paper media used to store applications and data also have physical requirements.

Documents and Papers

Many functions rely on vital records and various documents, papers, or forms. These records could be important because of a legal need (such as being able to produce a signed copy of a loan) or because they are the only record of the information. Records can be maintained on paper, microfiche, microfilm, magnetic media, or optical disk.

Step 3: Anticipating Potential Contingencies or Disasters

Although it is impossible to think of *all* the things that can go wrong, the next step is to identify a likely range of problems. The development of scenarios will help an organization develop a plan to address the wide range of things that can go wrong.

Scenarios should include small and large contingencies. While some general classes of contingency scenarios are obvious, imagination and creativity, as well as research, can point to other possible, but less obvious, contingencies. The contingency scenarios should address each of the resources described above. The following are *examples* of some of the types of questions that contingency scenarios may address:

Examples of Some Less Obvious Contingencies

***1.* A computer center in the basement of a building had a minor problem with rats. Exterminators killed the rats, but the bodies were not retrieved because they were hidden under the raised flooring and in the pipe conduits. Employees could only enter the data center with gas masks because of the decomposing rats.**

***2.* After the World Trade Center explosion when people reentered the building, they turned on their computer systems to check for problems. Dust and smoke damaged many systems when they were turned on. If the systems had been cleaned *first,* there would not have been significant damage.**

- *Human Resources*: Can people get to work? Are key personnel willing to cross a picket line? Are there critical skills and knowledge possessed by one person? Can people easily get to an alternative site?
- *Processing Capability*: Are the computers harmed? What happens if some of the computers are inoperable, but not all?
- *Automated Applications and Data:* Has data integrity been affected? Is an application sabotaged? Can

an application run on a different processing platform?
- *Computer−Based Services*: Can the computers communicate? To where? Can people communicate? Are information services down? For how long?
- *Infrastructure:* Do people have a place to sit? Do they have equipment to do their jobs? Can they occupy the building?
- *Documents/Paper:* Can needed records be found? Are they readable?

Step 4: Selecting Contingency Planning Strategies

The next step is to plan how to recover needed resources. In evaluating alternatives, it is necessary to consider what controls are in place to prevent and minimize contingencies. Since no set of controls can cost−effectively prevent all contingencies, it is necessary to coordinate prevention and recovery efforts.

A contingency planning strategy normally consists of three parts: emergency response, recovery, and resumption. *Emergency response* encompasses the initial actions taken to protect lives and limit damage. *Recovery* refers to the steps that are taken to continue support for critical functions. *Resumption* is the return to normal operations. The relationship between recovery and resumption is important. The longer it takes to resume normal operations, the longer the organization will have to operate in the recovery mode.

- *Example 1*: If the system administrator for a LAN has to be out of the office for a long time (due to illness or an accident), arrangements are made for the system administrator of another LAN to perform the duties. Anticipating this, the absent administrator should have taken steps beforehand to keep documentation current. This strategy is inexpensive, but service will probably be significantly reduced on both LANs which may prompt the manager of the loaned administrator to partially renege on the agreement.
- *Example 2*: An organization depends on an on−line information service provided by a commercial vendor. The organization is no longer able to obtain the information manually (e.g., from a reference book) within acceptable time limits and there are no other comparable services. In this case, the organization relies on the contingency plan of the service provider. The organization pays a premium to obtain priority service in case the service provider has to operate at reduced capacity.
- *Example #3*: A large mainframe data center has a contract with a hot site vendor, has a contract with the telecommunications carrier to reroute communications to the hot site, has plans to move people, and stores up−to−date copies of data, applications and needed paper records off−site. The contingency plan is expensive, but management has decided that the expense is fully justified.
- *Example #4*. An organization distributes its processing among two major sites, each of which includes small to medium processors (personal computers and minicomputers). If one site is lost, the other can carry the critical load until more equipment is purchased. Routing of data and voice communications can be performed transparently to redirect traffic. Backup copies are stored at the other site. This plan requires tight control over the architectures used and types of applications that are developed to ensure compatibility. In addition, personnel at both sites must be cross−trained to perform all functions.The selection of a strategy needs to be based on practical considerations, including feasibility and cost. The different categories of resources should each be considered. Risk assessment can be used to help estimate the cost of options to decide on an optimal strategy. For example, is it more expensive to purchase and maintain a generator or to move processing to an alternate site, considering the likelihood of losing electrical power for various lengths of time? Are the consequences of a loss of computer−related resources sufficiently high to warrant the cost of various recovery strategies? The risk assessment should focus on areas where it is not clear which strategy is the best.

In developing contingency planning strategies, there are many factors to consider in addressing each of the resources that support critical functions. Some examples are presented in the sidebars.

To ensure an organization has access to workers with the right skills and knowledge, training and documentation of knowledge are needed. During a major contingency, people will be under significant stress and may panic. If the contingency is a regional disaster, their first concerns will probably be their family and property. In addition, many people will be either unwilling or unable to come to work. Additional hiring or temporary services can be used. The use of additional personnel may introduce security vulnerabilities.

Contingency planning, especially for emergency response, normally places the highest emphasis on the protection of human life.

Processing Capability

Strategies for processing capability are normally grouped into five categories: hot site; cold site; redundancy; reciprocal agreements; and hybrids. These terms originated with recovery strategies for data centers but can be applied to other platforms.

- *Hot site*A building already equipped with processing capability and other services.
- *Cold site*A building for housing processors that can be easily adapted for use.
- *Redundant site*A site equipped and configured exactly like the primary site. (Some organizations plan on having reduced processing capability after a disaster and use partial redundancy. The stocking of spare personal computers or LAN servers also provides some redundancy.)
- *Reciprocal agreement*An agreement that allows two organizations to back each other up. (While this approach often sounds desirable, contingency planning experts note that this alternative has the greatest chance of failure due to problems keeping agreements and plans up−to−date as systems and personnel change.)
- *Hybrids*Any combinations of the above such as using having a hot site as a backup in case a redundant or reciprocal agreement site is damaged by a separate contingency.

The need for computer security does not go away when an organization is processing in a contingency mode. In some cases, the need may increase due to sharing processing facilities, concentrating resources in fewer sites, or using additional contractors and consultants. Security should be an important consideration when selecting contingency strategies.

Recovery may include several stages, perhaps marked by increasing availability of processing capability. Resumption planning may include contracts or the ability to place contracts to replace equipment.

Automated Applications and Data

Normally, the primary contingency strategy for applications and data is *regular backup* and secure *offsite storage*. Important decisions to be addressed include how often the backup is performed, how often it is stored off−site, and how it is transported (to storage, to an alternate processing site, or to support the resumption of normal operations).

Computer−Based Services

Service providers may offer contingency services. Voice communications carriers often can reroute calls (transparently to the user) to a new location. Data communications carriers can also reroute traffic. Hot sites are usually capable of receiving data and voice communications. If one service provider is down, it may be possible to use another. However, the type of communications carrier lost, either local or long distance, is important. Local voice service may be carried on cellular. Local data communications, especially for large volumes, is normally more difficult. In addition, resuming normal operations may require another rerouting of communications services.

Physical Infrastructure

Hot sites and cold sites may also offer office space in addition to processing capability support. Other types of contractual arrangements can be made for office space, security services, furniture, and more in the event of a contingency. If the contingency plan calls for moving offsite, procedures need to be developed to ensure a smooth transition back to the primary operating facility or to a new facility. Protection of the physical infrastructure is normally an important part of the emergency response plan, such as use of fire extinguishers or protecting equipment from water damage.

Documents and Papers

The primary contingency strategy is usually backup onto magnetic, optical, microfiche, paper, or other medium and offsite storage. Paper documents are generally harder to backup than electronic ones. A supply of forms and other needed papers can be stored offsite.

Step 5: Implementing the Contingency Strategies

Once the contingency planning strategies have been selected, it is necessary to make appropriate preparations, document the strategies, and train employees. Many of these tasks are ongoing.

Implementation

Much preparation is needed to implement the strategies for protecting critical functions and their supporting resources. For example, one common preparation is to establish procedures for backing up files and applications. Another is to establish contracts and agreements, *if* the contingency strategy calls for them. Existing service contracts may need to be renegotiated to add contingency services. Another preparation may be to purchase equipment, especially to support a redundant capability.

Backing up data files and applications is a critical part of virtually every contingency plan. Backups are used, for example, to restore files after a personal computer virus corrupts the files or after a hurricane destroys a data processing center.

Relationship Between Contingency Plans and Computer Security Plans

For small or less complex systems, the contingency plan may be a part of the computer security plan. For larger or more complex systems, the computer security plan could contain a brief synopsis of the contingency plan, which would be a separate document.

How Many Plans?

Some organizations have just one plan for the entire organization, and others have a plan for every distinct computer system, application, or other resource. Other approaches recommend

a plan for each business or mission function, with separate plans, as needed, for critical resources.

Who Prepares the Plan?

If an organization decides on a centralized approach to contingency planning, it may be best to name a *contingency planning coordinator*. The coordinator prepares the plans in cooperation with various functional and resource managers. Some organizations place responsibility directly with the functional and resource managers.

Documenting

The contingency plan needs to be written, kept up−to−date as the system and other factors change, and stored in a safe place. A written plan is critical during a contingency, especially if the person who developed the plan is unavailable. It should clearly state in simple language the sequence of tasks to be performed in the event of a contingency so that someone with minimal knowledge could immediately begin to execute the plan. It is generally helpful to store up−to−date copies of the contingency plan in several locations, including any off−site locations, such as alternate processing sites or backup data storage facilities.

Training

All personnel should be trained in their contingency−related duties. New personnel should be trained as they join the organization, refresher training may be needed, and personnel will need to practice their skills.

Training is particularly important for effective employee response during emergencies. There is no time to check a manual to determine correct procedures if there is a fire. Depending on the nature of the emergency, there may or may not be time to protect equipment and other assets. Practice is necessary in order to react correctly, especially when human safety is involved.

Step 6: Testing and Revising

A contingency plan should be tested periodically because there will undoubtedly be flaws in the plan and in its implementation. The plan will become dated as time passes and as the resources used to support critical functions change. Responsibility for keeping the contingency plan current should be specifically assigned. The extent and frequency of testing will vary between organizations and among systems. There are several types of testing, including reviews, analyses, and simulations of disasters.

Contingency plan maintenance can be incorporated into procedures for change management so that upgrades to hardware and software are reflected in the plan.

A *review* can be a simple test to check the accuracy of contingency plan documentation. For instance, a reviewer could check if individuals listed are still in the organization and still have the responsibilities that caused them to be included in the plan. This test can check home and work telephone numbers, organizational codes, and building and room numbers. The review can determine if files can be restored from backup tapes or if employees know emergency procedures.

The results of a test often implies a grade assigned for a specific level of performance, or simply pass or fail. However, in the case of contingency planning, a test should be used to improve the plan. If organizations do not use this approach, flaws in the plan may remain hidden and uncorrected.

An a*nalysis* may be performed on the entire plan or portions of it, such as emergency response procedures. It is beneficial if the analysis is performed by someone who did *not* help develop the contingency plan but has a good working knowledge of the critical function and supporting resources. The analyst(s) may mentally follow the strategies in the contingency plan, looking for flaws in the logic or process used by the plan's developers. The analyst may also interview functional managers, resource managers, and their staff to uncover missing or unworkable pieces of the plan.

Organizations may also arrange *disaster simulations*. These tests provide valuable information about flaws in the contingency plan and provide practice for a real emergency. While they can be expensive, these tests can also provide critical information that can be used to ensure the continuity of important functions. In general, the more critical the functions and the resources addressed in the contingency plan, the more cost−beneficial it is to perform a disaster simulation.

Interdependencies

Since all controls help to prevent contingencies, there is an interdependency with all of the controls in the Handbook.

- *Risk Management* provides a tool for analyzing the security costs and benefits of various contingency planning options. In addition, a risk management effort can be used to help identify critical resources needed to support the organization and the likely threat to those resources. It is not necessary, however, to perform a risk assessment prior to contingency planning, since the identification of critical resources can be performed during the contingency planning process itself.
- *Physical and Environmental Controls* help prevent contingencies. Although many of the other controls, such as logical access controls, also prevent contingencies, the major threats that a contingency plan addresses are physical and environmental threats, such as fires, loss of power, plumbing breaks, or natural disasters.
- *Incident Handling* can be viewed as a subset of contingency planning. It is the emergency response capability for various technical threats. Incident handling can also help an organization prevent future incidents.
- *Support and Operations* in most organizations includes the periodic backing up of files. It also includes the prevention and recovery from more common contingencies, such as a disk failure or corrupted data files.
- *Policy* is needed to create and document the organization's approach to contingency planning. The policy should explicitly assign responsibilities.

Cost Considerations

The cost of developing and implementing contingency planning strategies can be significant, especially if the strategy includes contracts for backup services or duplicate equipment. There are too many options to discuss cost considerations for each type.

One contingency cost that is often overlooked is the cost of testing a plan. Testing provides many benefits and should be performed, although some of the less expensive methods (such as a review) may be sufficient for less critical resources.

Bibliografía

Seguridad en Unix y Redes, Antob}nio Villalón Huerta, 2 de Octubre de 2000

Páginas consultadas:

www.cisco.com

www.google.com

www.ddmsa.com.ar

There is no distinct dividing line between disasters and other contingencies.

Other names include disaster recovery, business continuity, continuity of operations, or business resumption planning.

Some organizations include incident handling as a subset of contingency planning. The relationship is further discussed in Chapter 12, Incident Handling.

Some organizations and methodologies may use a different order, nomenclature, number, or combination of steps. The specific steps can be modified, as long as the basic functions are addressed.

However, since this is a computer security handbook, the descriptions here focus on the computer−related resources. The logistics of coordinating contingency planning for computer−related and other resources is an important consideration.

Some organizations divide a contingency strategy into emergency response, backup operations, and recovery. The different terminology can be confusing (especially the use of conflicting definitions of *recovery*), although the basic functions performed are the same.