CAPÍTULO 18

AUDITORÍA DE REDES

José Ignacio Boixo Pérez-Holanda

18.1. TERMINOLOGÍA DE REDES. MODELO OSI

Para poder auditar redes, lo primero y fundamental es utilizar el mismo vocabulario (más bien jerga) que los expertos en comunicaciones que las manejan. Debido a la constante evolución en este campo, un primer punto de referencia es poder referirse a un modelo comúnmente aceptable. El modelo común de referencia, adoptado por ISO *(International Standards Organization)* se denomina Modelo OSI *(Open Systems Interconection)*, y consta de estas siete capas:

7	Aplicación	Es donde la aplicación que necesita comunicaciones enlaza, mediante *API (Application Program Interface)* con el sistema de comunicaciones.
6	Presentación	Define el formato de los datos que se van a presentar a la aplicación.
5	Sesión	Establece los procedimientos de aperturas y cierres de sesión de comunicaciones, así como información de la sesión en curso.
4	Transporte	Comprueba la integridad de los datos transmitidos (que no ha habido pérdidas ni corrupciones).
3	Red	Establece las rutas por las cuales se puede comunicar el emisor con el receptor, lo que se realiza mediante el envío de paquetes de información.
2	Enlace	Transforma los paquetes de información en tramas adaptadas a los dispositivos físicos sobre los cuales se realiza la transmisión.
1	Físico	Transforma la información en señales físicas adaptadas al medio de comunicación.

La potencia del modelo OSI proviene de que cada capa no tiene que preocuparse de qué es lo que hagan las capas superiores ni las inferiores; cada capa se comunica con su igual en el interlocutor, con un protocolo de comunicaciones específico. Entre cada par de capa N y capa N-1 está perfectamente definido el paso de la información, que se produce *dentro* de la misma máquina, con métodos clásicos de programación en local.

Para establecer una comunicación, la información atraviesa descendentemente la pila formada por las siete capas, atraviesa el medio físico y asciende a través de las siete capas en la pila de destino. Por tanto, cada capa tiene unos métodos prefijados para comunicarse con las inmediatamente inferior y superior.

De esta manera, se aíslan los protocolos que se utilizan en unas capas con los protocolos que se utilizan en otras. Por ejemplo, es posible transmitir tráfico TCP/IP (capas superiores), a través de Ethernet o Token-Ring indistintamente (capas inferiores), gracias a esta independencia entre capas.

Este método de especificar a qué capas corresponde cada protocolo de comunicaciones resulta muy útil a efectos didácticos, pues rápidamente se tiene una visión del alcance y utilidad del protocolo o elemento de comunicaciones en cuestión.

Como regla mnemónica para recordar fácilmente el orden de las siete capas OSI, suele utilizarse la frase "Formemos Esta Red y Todos Seremos Pronto Amigos" (Físico, Enlace, Red, Transporte, Sesión, Presentación y Aplicación).

En los niveles inferiores, habitualmente hasta el nivel tres, es donde se definen las redes LAN (Local Area Network), MAN (Metropolitan Area Network) y WAN (Wide Area Network). Las funcionalidades de estos tres tipos de redes son similares, variando fundamentalmente la distancia que son capaces de salvar entre el emisor y el receptor (LAN: dentro de un edificio, MAN: dentro de un campus o zona urbana, WAN: cualquier distancia), siendo la velocidad inversamente proporcional a la distancia.

La red LAN más extendida, Ethernet, está basada en que cada emisor envía, cuando desea, una trama al medio físico, sabiendo que todos los destinatarios están permanentemente en escucha. Justo antes de enviar, el emisor se pone a la escucha, y si no hay tráfico, procede directamente al envío. Si al escuchar detecta que otro emisor está enviando, espera un tiempo aleatorio antes de volverse a poner a la escucha. Según crece el tráfico, se incrementa la probabilidad de que dos emisores hayan escuchado que el medio está libre y se pongan a transmitir simultáneamente. En ese caso, se habrá producidos una colisión y las tramas enviadas se destruirán mutuamente, creándose una alteración que es percibido físicamente como colisión de tramas. Cada emisor procede entonces a dar la trama como no enviada y a esperar un

tiempo aleatorio antes de ponerse de nuevo a escuchar, exactamente igual que cuando el medio estaba ocupado. Las tecnologías de Ethernet (10 Megabits por segundo - Mbps), Fast Ethernet (100 Mbps) y Giga Ethernet (1.000 Mbps) se basan en el mismo principio, incrementando sucesivamente la velocidad de transmisión. La Ethernet fue normalizada por el norteamericano Institute of Electric and Electronic Engineers con el nombre IEEE 802.3.

El cable que físicamente conecta a equipos Ethernet se denomina segmento. En vez de tender un único cable que recorra todos los equipos del segmento, se suele tender un cable por equipo y juntar todos los cables en un concentrador pasivo ("lau") o activo ("hub"). Cada segmento admite un número máximo de equipos, por lo que los segmentos han de ser conectados entre sí mediante dispositivos que hagan que la información pase del segmento origen al segmento de destino, pero confinando en cada segmento la información que no deba salir de él y así evitar anegar los segmentos adyacentes.

La LAN Token-Ring, desarrollada por IBM, está normalizada como IEEE 802.5, tiene velocidades de 4 y 16 Mbps y una mejor utilización del canal cuando se incrementa el tráfico. La FDDI es otra LAN, basada en transmisión a través de fibras ópticas, a velocidades de centenas de Mbps, que se suele utilizar para interconectar segmentos de LAN.

Para redes WAN, está muy extendido el X.25. Se basa en fragmentar la información en paquetes, habitualmente de 128 caracteres. Estos paquetes se entregan a un transportista habitualmente público que se encarga de ir enviándolos saltando entre diversos nodos intermedios hacia el destino. En cada nodo se lleva una cuenta con el nodo inmediato (colateral), para saber que cada paquete se ha recibido correctamente, o si hubo fallo, proceder a su retransmisión. Para su transmisión, cada paquete recibe una cabecera y una cola, y así queda convertida en una trama con control de tráfico y de errores entre cada pareja colateral de nodos. Mediante este salto de nodo a nodo se puede establecer tráfico a cualquier distancia a velocidades típicas de decenas de Kbps.

El Frame-Relay es básicamente lo mismo que el X.25, pero, aprovechando que la fiabilidad entre nodos es muy alta, sólo se comprueba que los paquetes han sido transportados sin errores cuando son recibidos en el destinatario; esto ahorra multitud de comprobaciones en los nodos intermedios, incrementando la velocidad hasta el orden de los cientos de Kbps.

El ATM (Asynchronus Transfer Mode/modo de transferencia asíncrono) utiliza un concepto de alguna manera similar a Frame Relay, con tramas de 53 caracteres (cinco de cabecera y 48 de información a transportar), que se conmutan en nodos

especialmente diseñados, con lógica prácticamente cableada, a muy alta velocidad, desde los cien Mbps.

18.2. VULNERABILIDADES EN REDES

Todos los sistemas de comunicación, desde el punto de vista de auditoría, presentan en general una problemática común: La información transita por lugares físicamente alejados de las personas responsables. Esto presupone un compromiso en la seguridad, ya que no existen procedimientos físicos para garantizar la inviolabilidad de la información.

En las redes de comunicaciones, por causas propias de la tecnología, pueden producirse básicamente tres tipos de incidencias:

1ª Alteración de bits. Por error en los medios de transmisión, una trama puede sufrir variación en parte de su contenido. La forma más habitual de detectar, y corregir en su caso, este tipo de incidencias, es sufijar la trama con un Código de Redundancia Cíclico (CRC) que detecte cualquier error y permita corregir errores que afecten hasta unos pocos bits en el mejor de los casos.

2ª Ausencia de tramas. Por error en el medio, o en algún nodo, o por sobrecarga, alguna trama puede desaparecer en el camino del emisor al receptor. Se suele atajar este riesgo dando un número de secuencia a las tramas.

3ª Alteración de Secuencia. El orden en el que se envían y se reciben las tramas no coincide. Unas tramas han adelantado a otras. En el receptor, mediante el número de secuencia, se reconstruye el orden original.

Por causas dolosas, y teniendo en cuenta que es físicamente posible interceptar la información, los tres mayores riesgos a atajar son:

1º Indagación. Un mensaje puede ser leído por un tercero, obteniendo la información que contenga.

2º Suplantación. Un tercero puede introducir un mensaje espurio que el receptor cree proveniente del emisor legítimo.

3º Modificación. Un tercero puede alterar el contenido de un mensaje.

Para este tipo de actuaciones dolosas, la única medida prácticamente efectiva en redes MAN y WAN (cuando la información sale del edificio) es la criptografía. En

redes LAN suelen utilizarse más bien medidas de control de acceso al edificio y al cableado, ya que la criptografía es muy onerosa todavía para redes locales.

Dada la proliferación de equipos que precisan comunicación de datos dentro de los edificios, es muy habitual plantearse sistemas de cableado integral en vez de tender un cable en cada ocasión. Esto es prácticamente un requisito en edificios con cierto volumen de usuarios.

Los sistemas de cableado suelen dividirse según su ámbito. En cada planta o zona se tienden cables desde un armario distribuidor a cada uno de los potenciales puestos. Este cableado se denomina habitualmente de " planta". Estos armarios están conectados a su vez, entre sí y con las salas de computadores, denominándose a estas conexiones cableado "troncal". Desde las salas de computadores parten las líneas hacia los transportistas de datos (Telefónicas o PTTs), saliendo los cables al exterior del edificio en lo que se denomina cableado de " ruta".

El cableado de planta suele ser de cobre, por lo que es propenso a escuchas ("pinchazos") que pueden no dejar rastro. El cableado troncal y el de ruta cada vez más frecuentemente se tienden mediante fibras ópticas, que son muy difíciles de interceptar, debido a que no provocan radiación electromagnética y a que la conexión física a una fibra óptica requiere una tecnología delicada y compleja.

En el propio puesto de trabajo puede haber peligros, como grabar/retransmitir la imagen que se ve en la pantalla, teclados que guardan memoria del orden en que se han pulsado las teclas, o directamente que las contraseñas estén escritas en papeles a la vista.

Dentro de las redes locales, el mayor peligro es que alguien instale una "escucha" no autorizada. Al viajar en claro la información dentro de la red local, es imprescindible tener una organización que controle estrictamente los equipos de escucha, bien sean éstos físicos ("sniffer") o lógicos ("traceadores"). Ambos escuchadores, físicos y lógicos, son de uso habitual dentro de cualquier instalación de cierto tamaño. Por tanto, es fundamental que ese uso legítimo esté controlado y no devenga en actividad espuria.

El riesgo de interceptar un canal de comunicaciones, y poder extraer de él la información, tiene unos efectos relativamente similares a los de poder entrar, sin control, en el sistema de almacenamiento del computador.

Hay un punto especialmente crítico en los canales de comunicaciones que son las contraseñas de usuario. Mientras que en el sistema de almacenamiento las contraseñas suelen guardarse cifradas, es inhabitual que los terminales u computadores personales sean capaces de cifrar la contraseña cuando se envía al computador central o al servidor.

Por tanto, alguien que intercepte la información puede hacerse con las contraseñas en claro. Además, dado que las carátulas iniciales donde se teclea la contraseña son siempre las mismas, se facilita la labor de los agentes de interceptación, pues proporcionan un patrón del paquete de información donde viaja la contraseña a interceptar.

18.3. PROTOCOLOS DE ALTO NIVEL

Como protocolos de alto nivel, los más importantes por orden de aparición en la industria son: SNA, OSI, Netbios, IPX y TCP/IP.

SNA

System Network Architecture. Fue diseñado por IBM a partir de los años setenta, al principio con una red estrictamente jerarquizado, y luego pasando a una estructura más distribuida, fundamentalmente con el tipo de sesión denominado LU 6.2.

El SNA se encuentra fundamentalmente en los computadores centrales IBM, donde sigue gozando de un extraordinario vigor, especialmente para comunicación con terminales no inteligentes de tipo 3270, y para sesiones establecidas entre computadores centrales y componentes software IBM.

OSI

Fue diseñado por el antiguo Comité Consultivo Internacional de Teléfonos y Telégrafos –CCITT–, actualmente Unión Internacional de Telecomunicaciones –ITU– básicamente compuesto por las compañías telefónicas nacionales (llamadas PTT). Se diseñaron todas las capas, desde los medios físicos hasta las aplicaciones como trasferencia de archivos o terminal virtual. Donde ha tenido éxito es en el protocolo de Red X.25 y en el correo electrónico X.400.

Netbios

Este protocolo fue el que se propuso, fundamentalmente por Microsoft, para comunicar entre sí computadores personales en redes locales. Es una extensión a red ("net") del "Basic Input/Output System" del sistema operativo DOS. Está muy orientado a la utilización en LAN, siendo bastante ágil y efectivo.

IPX

Es el protocolo propietario de Novell que, al alcanzar en su momento una posición de predominio en el sistema operativo en red, ha gozado de gran difusión. Su suerte está ligada a la de ese fabricante.

TCP/IP

(Transfer Control Protocol/Internet Protocol). Diseñado originalmente en los años setenta, para sobrevivir incluso a ataques nucleares contra los EE.UU., e impulsado desde los ámbitos académicos, la enorme versatilidad de este protocolo y su aceptación generalizada le ha hecho el paradigma de protocolo abierto, siendo la base de interconexión de redes que forman la Internet. Es el protocolo que está imponiéndose, por derecho propio, como gran unificador de todas las redes de comunicaciones.

Lamentablemente, no existe una independencia *de facto* entre las aplicaciones y los protocolos de alto nivel. Es todavía poco habitual que los clásicos programas de computador central IBM se usen con protocolo distinto de SNA. Por su parte el TCP/IP posee una gran cantidad de aplicaciones, ampliamente difundidas, pero que no pueden funcionar con otros protocolos.

Por ejemplo, la transmisión de archivos FTP *(File Transfer Protocol),* el correo electrónico SMTP *(Simple Mail Transfer Protocol)* o el terminal virtual Telnet han de correr precisamente sobre una "pila" de protocolo TCP/IP. Se establece así una retroalimentación donde las utilidades refuerzan al protocolo TCP/IP, que se vuelve cada vez más atractivo para que los desarrolladores escriban nuevas utilidades a él orientadas. Además, precisamente por su apertura, el TCP/IP es el preferido por organismos reguladores y grandes empresas, pues permiten evitar, al ser abierto, la dependencia de ningún fabricante en concreto.

Una solución que está teniendo éxito es "encapsular" un protocolo sobre otro. Así, el Netbios puede ser transportado sobre TCP/IP; la capa inferior, Netbeui, puede ser sustituida por TCP/IP, quedando el Netbios "encapsulado" sobre TCP/IP. Sin embargo, han de tenerse muy en cuenta las vulnerabilidades que se crean al encapsular. En el caso de Netbios sobre TCP/IP son vulnerabilidades serias, pues facilitan el tomar control remoto de recursos que se pensó que sólo se accederían en local, confiando, al menos en parte, en la protección física.

Al ser los sistemas de comunicaciones, procesos "sin historia", donde no se almacenan permanentemente datos de ningún tipo, los sistemas de recuperación se ven especialmente beneficiados por esta característica. Si una sesión cae, una vez que se

vuelve a establecer la sesión, el incidente queda solucionado. Es responsabilidad de la aplicación volver a reinicializar si la interrupción se produjo en mitad de una unidad de proceso.

Por ejemplo, si la interrupción de la sesión se ha producido a mitad de una transferencia de archivo, será misión de la aplicación, cuando la sesión se reanude, determinar si vuelve a comenzar la transmisión del archivo desde el principio o si reutiliza la parte que ya se ha transmitido.

Si es una persona quien ha sufrido el incidente, cuando se reanude la sesión deberá volver a identificarse con su nombre de usuario y contraseña, comprobando hasta qué punto la aplicación en la que estaba operando recogió los últimos datos que introdujeron.

Esta restricción fundamental, de que los sistemas de comunicaciones no almacenan datos, permite una mayor facilidad a la hora de duplicar equipamiento. Dado que una vez cerrada la sesión no queda ninguna información a retener (salvo obviamente estadísticas y pistas de auditoría), la sesión, al reanudarse, puede utilizar la misma o diferente ruta. Si existen diversos nodos y diversos enlaces entre ellos, la caída de un nodo sólo ha de significar la interrupción de las sesiones que por él transiten, que se podrán reiniciar a través de los restantes nodos. Por ello, es una norma generalmente aceptada, al menos en redes de cierto tamaño, tener nodos y enlaces replicados para prevenir situaciones de contingencia.

Una vez más, el protocolo TCP/IP demuestra en este caso su utilidad. Al haber sido este protocolo diseñado para encontrar rutas remanentes, inclusive ante caídas masivas, está especialmente bien orientado para facilitar la reestructuración de una red ante fallos de parte de sus componentes, sean éstos líneas, nodos o cualquier otro tipo de equipamiento. Cada vez más se está orientando los equipos de red a manejar prioritariamente tráfico TCP/IP y añadir facilidades de gestión de sobrecargas, rutas alternativas, tratamientos de contingencias y todo tipo de situaciones que acontecen en una red en funcionamiento.

18.4. REDES ABIERTAS (TCP/IP)

Ante el auge que está tomando el protocolo TCP/IP, como una primera clasificación de redes, se está adoptando la siguiente nomenclatura para las redes basadas en este protocolo:

- Intranet: Es la red interna, privada y segura de una empresa, utilice o no medios de transporte de terceros.

- Extranet: Es una red privada y segura, compartida por un conjunto de empresas, aunque utilice medios de transporte ajenos e inseguros, como pudiera ser Internet.

- Internet: Es la red de redes, "metared" a donde se conecta cualquier red que se desee abrir al exterior, pública e insegura, de alcance mundial, donde puede comunicar cualquier pareja o conjunto de interlocutores, dotada además de todo tipo de servicios de valor añadido. Infovía es la Internet que soporta Telefónica, con peculiaridades fundamentalmente comerciales.

El mayor peligro que representa un acceso TCP/IP no autorizado viene precisamente por la mayor virtud del TCP/IP: su amplia disponibilidad de utilidades. Dada la estandarización de las utilidades TCP/IP, es muy razonable suponer que cada máquina con acceso TCP/IP tenga "puertos abiertos", que a su vez tienen direcciones normalizadas donde encontrar transmisores de archivos, servidores de correo, terminales virtuales y todo tipo de servicios de utilidad. Una ausencia de protección significaría que un tercero puede utilizar estos servicios normalizados, de común existencia en cualquier máquina, en beneficio propio.

Un dispositivo específicamente dedicado a la protección de una Intranet ante una Extranet, y fundamentalmente ante Internet, es el cortafuegos (Firewall). Ésta es una máquina dedicada en exclusiva a leer cada paquete que entra o sale de una red para permitir su paso o desecharlo directamente. Esta autorización o rechazo está basada en unas tablas que identifican, para cada pareja de interlocutores (bien sea basado en el tipo de interlocutor o inclusive en su identificación individual) los tipos de servicios que pueden ser establecidos. Para llevar a cabo su misión, existen diversas configuraciones, donde se pueden incluir encaminadores (routers), servidores de proximidad (proxy), zonas desmilitarizadas, bastiones, y demás parafernalia, a veces copiada de modelos militares.

Las políticas de protección en un cortafuegos suelen denominarse desde "paranoicas" hasta "promiscuas", pasando por todo tipo de gamas intermedias. Dícese de la política paranoica cuando está prohibido absolutamente todo, requiriéndose una autorización específica para cada servicio en concreto entre cada par de interlocutores concretos. Dícese de política promiscua cuando todo está autorizado, identificándose específicamente aquellos servicios concretos entre parejas concretas de interlocutores que se prohíben. Lo más habitual es autorizar específicamente servicios (por ejemplo, correo electrónico) para ciertos tipos genéricos de usuarios (por ejemplo, a todos), otros servicios (por ejemplo, terminal virtual) a ciertos usuarios específicos (por ejemplo, servidor de terminales virtuales) y el resto no autorizarlo.

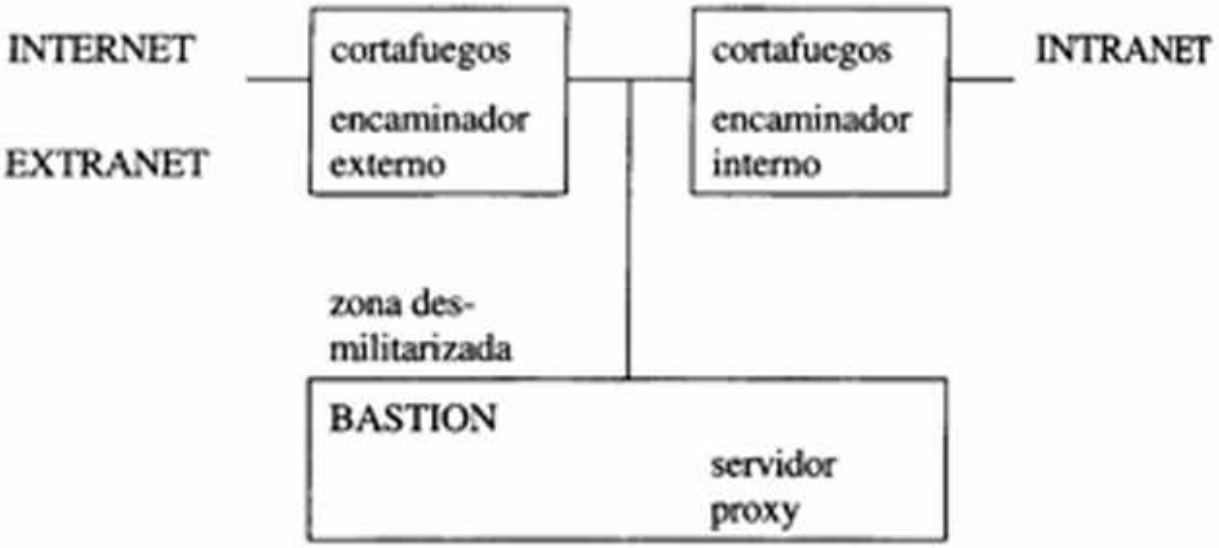

Figura 18.1. Protección de una red Intranet

Para proteger la red interna "Intranet" del exterior suele utilizarse el esquema expuesto en la figura 18.1, o bien variaciones del mismo. Se parte de la base de que la información que viaja entre la Intranet y el exterior ha de atravesar la "zona desmilitarizada" (DMZ de sus siglas inglesas), pasando por dos encaminadores. Un encaminadór protege los accesos desde el exterior hacia la zona desmilitarizada (encaminador externo) y otro protege los accesos desde la zona desmilitarizada hacia la Intranet (encaminador interno). En la zona desmilitarizada se instalan aquellos servicios a los que haya que acceder desde el exterior y desde el interior, en una máquina especialmente segura, denominada *bastión,* que debe ser dedicada exclusivamente a este fin.

Por ejemplo, un servidor proxy accede a un servidor Internet, recuperando la información que haya solicitado un usuario interno, y almacenándola para que pueda ser recuperada desde la Intranet. De esta manera se evita una conexión directa desde una máquina interna a un servidor Internet. Del mismo modo, el correo electrónico podría recibirse en un servidor instalado en la zona desmilitarizada y reexpedirse hacia el interior. El objetivo es evitar establecer sesiones directas entre una máquina Intranet y una maquina externa. Los encaminadores impedirán que se establezcan conexiones de este tipo, salvo aquellas que específicamente se determinen. El encaminador externo sólo permitirá que atraviese tráfico autorizado entre el exterior y el bastión, y el encaminador interno hará lo propio con el tráfico entre el bastión y la red interna.

Este esquema de protección puede ser simplificado, a costa de disminuir funcionalidades y solidez, prescindiendo en primer lugar del encaminador interno, y en segundo lugar del bastión. Abrir al exterior, sin protección, una red interna, queda fuera de la buena práctica informática.

El peligro más clásico es que un extraño se introduzca desde el exterior hacia la red interna. Dado que las técnicas para saltar los procedimientos de seguridad son públicas y se puede acceder a ellas desde Internet, una primera preocupación debiera ser, periódica, controlada y preventivamente, intentar saltar los procedimientos de seguridad antes de que un extraño los ponga a prueba.

Para comprobar los controles de acceso desde el exterior, así como las vulnerabilidades en la red interna, cortafuegos, servidores, etc. existen programas específicos ya comercializados, como por ejemplo SAFEsuite, Satan, Cops... que facilitan esta tarea, comprobando las vulnerabilidades ya conocidas. Las nuevas versiones de estos programas, que aparecen regularmente, incluyen comprobaciones de las nuevas debilidades detectadas. Como en el caso de los anti-virus, se deben tener estos programas actualizados a fecha reciente.

Un primer ataque es conseguir la identificación de un usuario. Para ello pueden utilizarse técnicas de indagación, leyendo el tráfico hasta encontrar nombres de usuario y contraseñas, poner a prueba la buena fe de los usuarios mandándoles un mensaje del tipo "soy su administrador, por favor, cambie su contraseña a *manzana*" o directamente intentar encontrar identificaciones habituales de usuarios ("prueba", "opel", "master"...), o que ya vienen por defecto en muchos sistemas.

Aunque los archivos de contraseñas están cifrados, habitualmente utilizando como clave de cifrado de cada contraseña la propia contraseña, como los métodos de cifra se conocen, existen programas que son capaces de probar miles de contraseñas usuales ya cifradas para ver si corresponden con alguna del archivo de contraseñas cifradas. Por ello es fundamental evitar que los archivos con las contraseñas cifradas caigan en manos de terceros.

En los sistemas distribuidos, se suele utilizar la técnica de "confianza entre nodos", de manera que si un usuario está autorizado para el nodo A, y solicita desde el nodo A un servicio al nodo B, como el nodo B "confía" en que el nodo A ya ha hecho la autenticación del usuario, el nodo B admite la petición del usuario sin exigirle la contraseña. Un intruso que sea capaz de entrar en un nodo puede por tanto entrar en todos los nodos que "confíen" en el nodo ya accedido.

También aparece diversa "fauna maligna" como "gusanos", mensajes de correo electrónico que se reproducen y acaban por colapsar la red; "caballos de Troya", programas aparentemente "inocuos" que llevan código escondido; virus, que se autocopian de un programa/documento "infectado" a otros programas/documentos "limpios"; "puertas falsas", accesos que muchas veces se quedan de la etapa de instalación/depuración de los sistemas.

18.5. AUDITANDO LA GERENCIA DE COMUNICACIONES

Cada vez más las comunicaciones están tomando un papel determinante en el tratamiento de datos, cumpliéndose el lema "el computador es la red" .

No siempre esta importancia queda adecuadamente reflejada dentro de la estructura, organizativa de proceso de datos, especialmente en organizaciones de tipo "tradicional", donde la adaptación a los cambios no se produce inmediatamente. Mientras que comúnmente el directivo informático tiene amplios conocimientos de proceso de datos, no siempre sus habilidades y cualificaciones en temas de comunicaciones están a la misma altura, por lo que el riesgo de deficiente anclaje de la gerencia de comunicaciones en el esquema organizativo existe. Por su parte, los informáticos a cargo de las comunicaciones suelen autoconsiderarse exclusivamente técnicos, obviando considerar las aplicaciones organizativas de su tarea.

Todos estos factores convergen en que la auditoría de comunicaciones no siempre se practique con la frecuencia y profundidad equivalentes a las de otras áreas del proceso de datos.

Por tanto, el primer punto de una auditoría es determinar que la función de gestión de redes y comunicaciones esté claramente definida, debiendo ser responsable, en general, de las siguientes áreas:

- Gestión de la red, inventario de equipamiento y normativa de conectividad.
- Monitorización de las comunicaciones, registro y resolución de problemas.
- Revisión de costes y su asignación de proveedores y servicios de transporte, balanceo de tráfico entre rutas y selección de equipamiento.
- Participación activa en la estrategia de proceso de datos, fijación de estándares a ser usados en el desarrollo de aplicaciones y evaluación de necesidades en comunicaciones.

Como objetivos del control, se debe marcar la existencia de:

- Una gerencia de comunicaciones con autoridad para establecer procedimientos y normativa.
- Procedimientos y registros de inventarios y cambios.
- Funciones de vigilancia del uso de la red de comunicaciones, ajustes de rendimiento, registro de incidencias y resolución de problemas.

- Procedimientos para el seguimiento del coste de las comunicaciones y su reparto a las personas o unidades apropiadas.

- Procedimientos para vigilar el uso de la red de comunicaciones, realizar ajustes para mejorar el rendimiento, y registrar y resolver cualquier problema.

- Participación activa de la gerencia de comunicaciones en el diseño de las nuevas aplicaciones *on line* para asegurar que se sigue la normativa de comunicaciones.

Lista de control

Comprobar que:

* G.1. La gerencia de comunicaciones despache con el puesto directivo que en el organigrama tenga autoridad suficiente para dirigir y controlar la función.

* G.2. Haya coordinación organizativa entre la comunicación de datos y la de voz, en casa de estar separadas estas dos funciones.

* G.3. Existan descripciones del puesto de trabajo, competencias, requerimientos y responsabilidades para el personal involucrado en las comunicaciones.

* G.4. Existan normas en comunicaciones al menos para las siguientes áreas:

    - Tipos de equipamiento, como adaptadores LAN, que pueden ser instalados en la red.

    - Procedimientos de autorización para conectar nuevo equipamiento en la red.

    - Planes y procedimientos de autorización para la introducción de líneas y equipos fuera de las horas normales de operación.

    - Procedimientos para el uso de cualquier conexión digital con el exterior, como línea de red telefónica conmutada o Internet.

    - Procedimientos de autorización para el uso de exploradores físicos (sniffers) y lógicos (traceadores).

- Control físico de los exploradores físicos (sniffers), que deben estar guardados.

- Control de qué máquinas tienen instalados exploradores lógicos (traceadores), y de que éstos sólo se pueden invocar por usuarios autorizados.

* G.5. Los contratos con transportistas de información y otros proveedores tienen definidas responsabilidades y obligaciones.

* G.6. Existan planes de comunicaciones a largo plazo, incluyendo estrategia de comunicaciones de voz y datos.

* G.7. Existen, si fueren necesarios, planes para comunicaciones a alta velocidad, como fibra óptica, ATM, etc.

* G. 8. Se planifican redes de cableado integral para cualquier nuevo edificio o dependencia que vaya a utilizar la empresa.

* G.9. El plan general de recuperación de desastres considera el respaldo y recuperación de los sistemas de comunicaciones.

* G.10. Las listas de inventario cubren todo el equipamiento de comunicaciones de datos, incluyendo módems, controladores, terminales, líneas y equipos relacionados.

* G.11. Se mantienen los diagramas de red que documentan las conexiones físicas y lógicas entre las comunicaciones y otros equipos de proceso de datos.

* G.12. Se refleja correctamente, en el registro de inventario y en los diagramas de red, una muestra seleccionada de equipos de comunicaciones, de dentro y de fuera de la sala de computadores.

* G.13. Los procedimientos de cambio para equipos de comunicaciones, así como para añadir nuevos terminales o cambios en direcciones, son adecuados y consistentes con otros procedimientos de cambio en las operaciones de proceso de datos.

* G.14. Existe un procedimiento formal de prueba que cubre la introducción de cualquier nuevo equipo o cambios en la red de comunicaciones.

* G.15. Para una selección de diversas altas o cambios en la red, de un período reciente, los procedimientos formales de control han sido cumplidos.

* G.16. Están establecidos ratios de rendimiento que cubren áreas como la de tiempos de respuesta en los terminales y tasas de errores.

* G.17. Se vigila la actividad dentro de los sistemas *on line* y se realizan los ajustes apropiados para mejorar el rendimiento.

* G.18. Existen procedimientos adecuados de identificación, documentación y toma de acciones correctivas ante cualquier fallo de comunicaciones.

* G.19. La facturación de los transportistas de comunicaciones y otros vendedores es revisada regularmente y los cargos con discrepancias se conforman adecuadamente.

* G.20. Existe un sistema comprensible de contabilidad y cargo en costes de comunicaciones, incluyendo líneas, equipos y terminales.

* G.21. Los gestores de comunicaciones están informados y participan en la planificación pre-implementación de los nuevos sistemas de información que puedan tener impacto en las comunicaciones.

* G.22. Las consideraciones de planificación de capacidad en comunicaciones son tomadas en cuenta en el diseño e implementación de nuevas aplicaciones.

18.6. AUDITANDO LA RED FÍSICA

En una primera división, se establecen distintos riesgos para los datos que circulan dentro del edificio de aquellos que viajan por el exterior. Por tanto, ha de auditarse hasta qué punto las instalaciones físicas del edificio ofrecen garantías y han sido estudiadas las vulnerabilidades existentes.

En general, muchas veces se parte del supuesto de que si no existe acceso físico desde el exterior a la red interna de una empresa las comunicaciones internas quedan a salvo. Debe comprobarse que efectivamente los accesos físicos provenientes del exterior han sido debidamente registrados, para evitar estos accesos. Debe también comprobarse que desde el interior del edificio no se intercepta físicamente el cableado ("pinchazo").

En caso de desastre, bien sea total o parcial, ha de poder comprobarse cuál es la parte del cableado que queda en condiciones de funcionar y qué operatividad puede soportar. Ya que el tendido de cables es una actividad irrealizable a muy corto plazo, los planes de recuperación de contingencias deben tener prevista la recuperación en comunicaciones.

Ha de tenerse en cuenta que la red física es un punto claro de contacto entre la gerencia de comunicaciones y la gerencia de mantenimiento general de edificios, que es quien suele aportar electricistas y personal profesional para el tendido físico de cables y su mantenimiento.

Como objetivos de control, se debe marcar la existencia de:

- Áreas controladas para los equipos de comunicaciones, previniendo así accesos inadecuados.
- Protección y tendido adecuado de cables y líneas de comunicaciones, para evitar accesos físicos.
- Controles de utilización de los equipos de pruebas de comunicaciones, usados para monitorizar la red y su tráfico, que impidan su utilización inadecuada.
- Atención específica a la recuperación de los sistemas de comunicación de datos en el plan de recuperación de desastres en sistemas de información.
- Controles específicos en caso de que se utilicen líneas telefónicas normales con acceso a la red de datos para prevenir accesos no autorizados al sistema o a la red.

Lista de control

Comprobar que:

* F. 1. El equipo de comunicaciones se mantiene en habitaciones cerradas con acceso limitado a personas autorizadas.

* F.2. La seguridad física de los equipos de comunicaciones, tales como controladores de comunicaciones, dentro de las salas de computadores sea adecuada.

* F.3. Sólo personas con responsabilidad y conocimientos están incluidas en la lista de personas permanentemente autorizadas para entrar en las salas de equipos de comunicaciones.

* F.4. Se toman medidas para separar las actividades de electricistas y personal de tendido y mantenimiento de tendido de líneas telefónicas, así como sus autorizaciones de acceso, de aquéllas del personal bajo control de la gerencia de comunicaciones.

* F.5. En las zonas adyacentes a las salas de comunicaciones, todas las líneas de comunicaciones fuera de la vista.

* F.6. Las líneas de comunicaciones, en las salas de comunicaciones, armarios distribuidores y terminaciones de los despachos, estarán etiquetadas con un código gestionado por la gerencia de comunicaciones, y no por su descripción física o métodos sin coherencia.

* F.7. Existen procedimientos para la protección de cables y bocas de conexión que dificulten el que sean interceptados o conectados por personas no autorizadas.

* F.8. Se revisa periódicamente la red de comunicaciones, buscando intercepciones activas o pasivas.

* F.9. Los equipos de prueba de comunicaciones usados para resolver los problemas de comunicación de datos deben tener propósitos y funciones definidos.

* F.10. Existen controles adecuados sobre los equipos de prueba de comunicaciones usados para monitorizar líneas y fijar problemas incluyendo:

  - Procedimiento restringiendo el uso de estos equipos a personal autorizado.

  - Facilidades de traza y registro del tráfico de datos que posean los equipos de monitorización.

  - Procedimientos de aprobación y registro ante las conexiones a líneas de comunicaciones en la detección y corrección de problemas.

* F.11. En el plan general de recuperación de desastres para servicios de información presta adecuada atención a la recuperación y vuelta al servicio de los sistemas de comunicación de datos.

* F.12. Existen planes de contingencia para desastres que sólo afecten a las comunicaciones, como el fallo de una sala completa de comunicaciones.

* F. 13. Las alternativas de respaldo de comunicaciones, bien sea con las mismas salas o con salas de respaldo, consideran la seguridad física de estos lugares.

* F.14. Las líneas telefónicas usadas para datos, cuyos números no deben ser públicos, tienen dispositivos/procedimientos de seguridad tales como retrollamada, códigos de conexión o interruptores para impedir accesos no autorizados al sistema informático.

18.7. AUDITANDO LA RED LÓGICA

Cada vez más se tiende a que un equipo pueda comunicarse con cualquier otro equipo, de manera que sea la red de comunicaciones el substrato común que les une. Leído a la inversa, la red hace que un equipo pueda acceder legítimamente a cualquier otro, incluyendo al tráfico que circule hacia cualquier equipo de la red. Y todo ello por métodos exclusivamente lógicos, sin necesidad de instalar físicamente ningún dispositivo. Simplemente si un equipo, por cualquier circunstancia, se pone a enviar indiscriminadamente mensajes, puede ser capaz de bloquear la red completa y, por tanto, al resto de los equipos de la instalación.

Es necesario monitorizar la red, revisar los errores o situaciones anómalas que se producen y tener establecidos los procedimientos para detectar y aislar equipos en situación anómala. En general, si se quiere que la información que viaja por la red no pueda ser espiada, la única solución totalmente efectiva es la encriptación.

Como objetivos de control, se debe marcar la existencia de:

- Contraseñas y otros procedimientos para limitar y detectar cualquier intento de acceso no autorizado a la red de comunicaciones.

- Facilidades de control de errores para detectar errores de transmisión y establecer las retransmisiones apropiadas.

- Controles para asegurar que las transmisiones van solamente a usuarios autorizados y que los mensajes no tienen por qué seguir siempre la misma ruta.

- Registro de la actividad de la red, para ayudar a reconstruir incidencias y detectar accesos no autorizados.

- Técnicas de cifrado de datos donde haya riesgos de accesos impropios a transmisiones sensibles.

- Controles adecuados que cubran la importación o exportación de datos a través de puertas, en cualquier punto de la red, a otros sistemas informáticos.

Lista de control

Comprobar que:

* L.1. El software de comunicaciones, para permitir el acceso, exige código de usuario y contraseña.

* L.2. Revisar el procedimiento de conexión de usuario y comprobar que:

  - Los usuarios no pueden acceder a ningún sistema, ni siquiera de ayuda, antes de haberse identificado correctamente.

  - Se inhabilita al usuario que sea incapaz de dar la contraseña después de un número determinado de intentos infructuosos.

  - Se obliga a cambiar la contraseña regularmente.

  - Las contraseñas no son mostradas en pantalla cuando se teclean.

  - Durante el procedimiento de identificación, los usuarios son informados de cuándo fue su última conexión para ayudar a identificar potenciales suplantaciones o accesos no autorizados.

* L.3. Cualquier procedimiento del fabricante, mediante hardware o software, que permita el libre acceso y que haya sido utilizado en la instalación original, ha de haber sido inhabilitado o cambiado.

* L.4. Se toman estadísticas que incluyan tasas de errores y de retransmisión.

* L.5. Los protocolos utilizados, revisados con el personal adecuado de comunicaciones, disponen de procedimientos de control de errores con la seguridad suficiente.

* L.6. Los mensajes lógicos transmitidos identifican el originante, la fecha, la hora y el receptor.

* L.7. El software de comunicaciones ejecuta procedimientos de control y correctivos ante mensajes duplicados, fuera de orden, perdidos, o retrasados.

* L.8. La arquitectura de comunicaciones utiliza indistintamente cualquier ruta disponible de transmisión para minimizar el impacto de una escucha de datos sensibles en una ruta determinada.

* L.9. Existen controles para que los datos sensibles sólo puedan ser impresos en las impresoras designadas y vistos desde los terminales autorizados.

* L.10. Existen procedimientos de registro para capturar y ayudar a reconstruir todas las actividades de las transacciones.

* L.11. Los archivos de registro son revisados, si es posible a través de herramientas automáticas, diariamente, vigilando intentos impropios de acceso.

* L.12. Existen análisis de riesgos para las aplicaciones de proceso de datos a fin de identificar aquellas en las que el cifrado resulte apropiado.

* L.13. Si se utiliza cifrado:

  - Existen procedimientos de control sobre la generación e intercambio de claves.
  - Las claves de cifrado son cambiadas regularmente.
  - El transporte de las claves de cifrado desde donde se generan a los equipos que las utilizan sigue un procedimiento adecuado.

* L.14. Si se utilizan canales de comunicación uniendo diversos edificios de la misma organización, y existen datos sensibles que circulen por ellos, comprobar que estos canales se cifran automáticamente, para evitar que una interceptación sistemática a un canal comprometa a todas las aplicaciones.

* L.15. Si la organización tiene canales de comunicación con otras organizaciones se analice la conveniencia de cifrar estos canales.

* L.16. Si se utiliza la transmisión de datos sensibles a través de redes abiertas como Internet, comprobar que estos datos viajan cifrados.

* L.17. Si en una red local existen computadores con módems, se han revisado los controles de seguridad asociados para impedir el acceso de equipos foráneos a la red local.

* L.18. Existe una política de prohibición de introducir programas personales o conectar equipos privados a la red local.

* L.19. Todas las "puertas traseras" y accesos no específicamente autorizados están bloqueados. En equipos activos de comunicaciones, como puentes, encaminadores, conmutadores, etc., esto significa que los accesos para servicio remoto están inhabilitados o tienen procedimientos específicos de control.

* L.20. Periódicamente se ejecutan, mediante los programas actualizados y adecuados, ataques para descubrir vulnerabilidades, que los resultados se documentan y se corrigen las deficiencias observadas. Estos ataques deben realizarse independientemente a:

  - Servidores, desde dentro del servidor.
  - Servidores, desde la red interna.
  - Servidores Web, específicamente.
  - Intranet, desde dentro de ella.
  - Cortafuegos, desde dentro de ellos.
  - Accesos desde el exterior y/o Internet.

18.8. LECTURAS RECOMENDADAS

Andrew S. Tanenbaum. *Redes de computadores*. Prentice-Hall. Es el libro de referencia, por antonomasia, en comunicaciones.

Varios. *COAST. Computer Operations, Audit and Security Technology*. http://www.cs.purdue.edu/coast Un actualizado compendio de conocimientos sobre el tema, con hiperenlaces a lo más significativo del sector.

Steven L. Telleen. *Intranet Organization: Strategies for managing change*. Intranet Partners. http://www.intranetpartners.com/IntranetOrg. Enfoque muy orientado a la práctica empresarial cotidiana.

18.9. CUESTIONES DE REPASO

1. ¿Cuáles son los niveles del modelo OSI?
2. ¿Cuáles son las incidencias que pueden producirse en las redes de comunicaciones?
3. ¿Cuáles son los mayores riesgos que ofrecen las redes?
4. ¿Existe el riesgo de que se intercepte un canal de comunicaciones?
5. ¿Qué suele hacerse con las contraseñas de los usuarios?
6. ¿Cuáles son los protocolos más importantes de alto nivel?
7. Diferencias entre Internet, Intranet y Extranet.
8. ¿Qué es un "cortafuegos"?
9. ¿Qué es un "gusano"?
10. ¿Qué objetivos de control destacaría en la auditoría de la gerencia de comunicaciones?