Seguridad Fisica COMO

Jose María López Hernández

Table of Contents

1. Sobre Seguridad Física COMO

Seguridad Física COMO es un tutorial dedicado a la Seguridad Física de Sistemas, que intenta clarificar términos y técnicas en este área de la Seguridad Informática. El tutorial trata sobre la seguridad física de los sistemas informáticos (ordenadores, hardware de red, dispositivos electrónicos, etc), de todo el entorno que los rodea en el lugar donde se hallan ubicados (edificio, sistemas eléctricos, conducciones de gas y agua, seguridad de las cerraduras, etc) y de las personas que están encargadas de su vigilancia o de la vigilancia del acceso a estos sistemas informáticos (administradores, personal externo, vigilantes, etc). Todo este entorno configura la Seguridad Física que vamos a tener en un sistema y es por tanto imprescindible tener en cuenta todos estos aspectos para conseguir una seguridad física aceptable.

2. Sobre los autores de este tutorial

El tutorial Sobre Seguridad Física COMO ha sido creado por Jose María López Hernández <jkerouac@bgsec.com (mailto:jkerouac@bgsec.com)> y bgSEC (www.bgsec.com (http://www.bgsec.com/)) y liberado bajo licencia FDL. bgSEC Beat Generation Seguridad y Consultoría de Sistemas Informáticos se dedica a la Consultoría de Sistemas Informáticos en todas sus formas, sobre todo a la Consultoría de Sistemas de Software Libre. Uno de nuestros servicios es la Consultoría de Seguridad Física de Sistemas, y es en este trabajo donde hemos recopilado la experiencia y la información que se intenta plasmar en este documento.

3. Introducción

Sobre Seguridad Física COMO tratará la seguridad física como un conjunto integrado de capacidades y soluciones que deben proveerse en una empresa o centro de computación para mantener la seguridad en un nivel aceptable, intentando ir de lo global a lo específico. Este punto es extremadamente importante, porque una acumulación de actuaciones puntuales sobre una serie de sistemas o dispositivos no nos proveerán de una seguridad física aceptable si no tenemos en cuenta el aspecto global del problema y el entorno físico y social donde estas máquinas van a cumplir su función. Es un error muy común en los estudios de seguridad física el centrarse en el hardware específicamente, asegurando las máquinas y dispositivos de red, pero descuidando el entorno donde estas máquinas han de trabajar, que es tan importante como el mismo hardware que ha de soportar las aplicaciones.

Trataremos por tanto de ir desde lo global a lo específico, desde el edificio donde se alojará el hardware y el suministro de energía o el control de accesos hasta lo más específico del hardware que ha de soportar nuestras aplicaciones, llegando incluso a la redundancia en las placas base de los ordenadores o el acceso físico a las bocas de red de los concentradores que proporcionan acceso a nuestra red local.

Debemos hacer notar que lo más importante en un estudio de seguridad física es el encontrar los posibles puntos de fallo dentro del sistema. Es un caso parecido al estudio de los sistemas de alta disponibilidad, donde se buscan los puntos únicos de fallos (SPOF). Esto se realizará estudiando la estructura del sistema y su funcionamiento. Es esencial comprender como funciona el sistema para conocer los puntos de fallo que puedan aparecer tanto en el funcionamiento normal del sistema como ante posibles situaciones anómalas, así como las debilidades que ante intrusos o atacantes exteriores pueda ofrecer.

4. El edificio

El estudio del edificio donde se encuentra ubicado el hardware y los dispositivos que han de soportar nuestras aplicaciones es el primer paso en cualquier estudio de seguridad física, y también suele ser el más problemático, puesto que nos encontramos con un entorno ya construido, no modificable y que suele tener un uso compartido por nuestros sistemas hardware y otro tipo de sistemas. Se intentará siempre resaltar todos los fallos de seguridad que se puedan encontrar, y se tendrá en cuenta si estos son subsanables o inherentes a la estructura del edificio. En cualquier caso se realizará un informe de las

posibilidades de modificación para subsanar fallos y de las precauciones que sea posible tomar para minimizar los riesgos de seguridad física cuando no sea posible subsanarlos.

También suele ser interesante estudiar el impacto económico de las modificaciones que aconsejemos puesto que la entidad física de los sistemas que vamos a supervisar suele implicar un gasto considerable si han de realizarse modificaciones de cualquier tipo. Nunca se debe dejar de lado ningún defecto que observemos al realizar el estudio, pero es aceptable el dejar a consideración de la empresa las modificaciones que impliquen un gasto considerable. Deberá en este caso intentar buscar formas alternativas de minimizar los riesgos o recurrir en su caso a aseguradoras que puedan atenuar la gravedad de un incidente que implique a instalaciones del edificio.

4.1. Los suministros de energía del edificio

El primero de los puntos que debemos observar al realizar el estudio del edificio es el suministro de energía. Debemos centrarnos en los sistemas de suministro de energía que puedan afectar a los sistemas que queremos proteger, dejando de lado otras consideraciones como la disponibilidad de servicios para el personal y similares. Por ejemplo es asunto nuestro la disponibilidad de aire acondicionado en la Sala de Computación, pero no lo es la disponibilidad en la Sala de Reuniones.

El suministro de energía suele tener dos partes, una parte externa que provee y gestiona la compañía eléctrica y que llega justo hasta el punto donde se encuentra el sistema de tarificación, detrás del cual se suele encontrar nuestro sistema de protecciones y todo nuestro cableado y dispositivos, la parte interna.

La parte externa está protegida por un fusible y un limitador de potencia que instala la compañía eléctrica y que deben estar calculados para la potencia que vaya a consumir nuestro edificio. Normalmente no deberemos preocuparnos por estos dispositivos, que suelen estar sobredimensionados para evitar cortes de energía y que tienen como principal función la protección de la red eléctrica de la compañía. Por otro lado deberemos observar la disponibilidad del suministro de energía a nuestro edificio, teniendo en cuenta la redundancia que pueda tener la red eléctrica y por tanto nuestro suministro eléctrico. Esta información es posible obtenerla llamando al teléfono de información de la compañía eléctrica, que nos informará de la redundancia de la red para nuestro sector en concreto, que suele depender del número de lineas de media o alta tensión de que disponga la compañía en la subestación para proveer de energía al sector donde se encuentre nuestro edificio. Este es un punto donde no podemos actuar de ninguna forma, simplemente podemos advertir a la empresa para la que realizamos el trabajo de consultoría de las posibilidades de que se produzca un corte eléctrico general.

Otro aspecto a tener en cuenta es la posible redundancia que estructuralmente se pueda proporcionar al edificio. Este suele ser un aspecto complicado, pues no es común el tener más de una conexión eléctrica para un edificio. Con todo, el sistema ideal sería el que proporcionara redundancia por medio del suministro de energía eléctrica por dos compañías diferentes que operen en el mismo sector, lo que es una opción a considerar para sistemas críticos. Es posible solicitar este tipo de servicios a través de algunas compañías eléctricas y es imposible en otras, pero si necesita este tipo de servicio recomiendeló y soliciteló, puede ser esencial para sistemas críticos. La disponibilidad de este sistema suele ser nula en la mayoría de los sitios, pues aunque se cuente con un mercado de energía liberalizado que permita la

contratación del suministro eléctrico eligiendo entre varias compañías la red eléctrica que ha de transportar esa energía hasta nuestro edificio suele ser propiedad de una de las compañías o de propiedad estatal, con lo que no tendríamos redundancia en el suministro de energía.

La opción más común para proporcionar redundancia en el sistema de suministro de energía es la utilización de generadores eléctricos (grupos electrógenos), que funcionan con combustible y pueden proporcionar energía a todo un edificio durante un periodo largo de tiempo durante un corte de energía o una interrupción del suministro por un desastre natural. Estos sistemas son bastante comunes en los hospitales y son una buena opción (aunque cara) de asegurar el suministro de energía eléctrica.

El suministro de gas y agua es menos crítico que el suministro de energía eléctrica para la seguridad de los sistemas hardware del edificio. Debe tenerse en cuenta el suministro de gas porque algunos sistemas de calefacción funcionan con gas, y pueden ser necesarios en climas muy fríos para mantener una temperatura mínima en nuestros centros de datos. El frío no suele ser un problema para los sistemas hardware, por lo que el gas no será una preocupación en la mayor parte de los casos.

Otro punto a comprobar debe ser la posibilidad de que un intruso malintencionado quiera cortar nuestro suministro eléctrico. Para esto debe de comprobarse que no es fácil el acceso a los cables que proporcionan energía eléctrica al edificio, por lo menos en un recorrido razonable desde nuestro edificio hasta la caja de conexiones más cercana.

Es imprescindible comprobar que existen todos los dispositivos de protección necesarios para el edificio y la disponibilidad de estos para todo el edificio y para cada planta de este, de forma que pueda aislarse un problema eléctrico lo máximo que sea posible. Idealmente deberíamos tener protecciones en cada planta e incluso en cada sección de cada planta, de forma que un problema eléctrico afecte lo mínimo posible a los sistemas de hardware y a la red. Los sistemas que consuman gran potencia, como los grandes sistemas UPS deberían tener su propia protección, normalmente interna en forma de fusibles u otro tipo de protecciones.

Todos los dispositivos de protección deben estar homologados y la instalación debe cumplir con el reglamento de baja tensión del país donde nos encontremos. Esto nos asegurará una cierta protección contra dispositivos e instalaciones defectuosos. Es importante asegurarnos de que la instalación eléctrica cumple estas condiciones, solicitando la documentación necesaria para comprobarlo. En casos muy críticos se puede contratar a especialistas en sistemas eléctricos que realicen un estudio eléctrico del edificio, del suministro y de las protecciones.

4.2. Los enlaces de comunicaciones del edificio

El caso de los sistemas de comunicaciones del edificio es similar al del suministro eléctrico, deberemos buscar la mayor seguridad y protección en los sistemas y además siempre que sea posible tener redundancia en los sistemas de comunicaciones para preveer el caso de que uno de los enlaces falle.

Los sistemas de comunicaciones suelen ser de dos tipos: públicos y privados. La mayoría de los edificios

usarán sistemas públicos de comunicaciones, como puede ser la red telefónica para el transporte de voz y datos o las conexiones ADSL/DSL/Cable/etc que usan medios compartidos para la transmisión de datos. Es mucho menos común el uso de sistemas privados de comunicaciones como lineas telefónicas o de datos dedicadas o enlaces de microondas entre edificios.

Para los sistemas públicos debemos estudiar sobre todo si existe algún tipo de redundancia en las comunicaciones, puesto que las compañías telefónicas que suelen ser las que proveen los servicios no suelen proporcionar ningún tipo de certeza de que nuestras comunicaciones van a mantenerse, por lo que estamos a expensas de las averías o fallos que se puedan producir en las redes públicas para tener comunicaciones. Las comunicaciones telefónicas son necesarias para permitir el fallo de alguna de estas. Téngase en cuenta que las centralitas suelen tener una única conexión por lo que solo proveen un enlace de comunicaciones compartido por varias lineas telefónicas, si nos falla la conexión nos fallará el acceso telefónico de todos los sistemas telefónicos conectados a la centralita. Es aconsejable por tanto mantener más de una linea y además con diferentes compañías, de forma que tengamos siempre comunicación telefónica aunque alguna de las compañías falle. Es un sistema bastante común en grandes edificios y no debería tener más complicaciones. Es bastante común que las compañías que usan la red telefónica clásica compartan el medio físico para mandar los datos, medio físico que será propiedad pública o de una de las compañías, pero en cambio las compañías de cable suelen tener su propia red para proporcionar la conectividad, por lo que puede ser interesante la contratación de una linea con una compañía tradicional y otra con una compañía de cable para tener dos redes independientes.

Para los sistemas de datos tipo ADSL/DSL/Cable debemos buscar también la redundancia en los sistemas, manteniendo varias conexiones con varios proveedores para mantener siempre un enlace de datos seguro puesto que ninguno nos asegurará una conexión cien por cien fiable. Es necesario que el departamento de administración de red tenga en cuenta esta estructura para poder enrutar el tráfico de forma que si uno de los enlaces falla los datos se transmitan por otro enlace de otra compañía. Esta estructura de acceso a redes es muy común en grandes instalaciones y no debería haber problema en su estudio o en recomendar su instalación.

Para los sistemas privados las consideraciones de seguridad son algo menos severas que para los sistemas compartidos. La compañía que nos suministra el servicio nos asegurará las conexiones con una tasa fija de porcentaje de fallo en el tiempo, lo que nos permite planificar más fácilmente la seguridad del enlace, pues tenemos la seguridad de que el enlace se mantendrá. Lo mismo se aplica para los sistemas de comunicaciones privadas entre edificios usando microondas, donde nosotros mismos podemos asegurar la comunicación y no dependemos de la disponibilidad de una red pública. Para estos sistemas privados se puede realizar un estudio contratando a personal especializado en el estudio de estos enlaces y en su ajuste. Siempre es aconsejable complementar estos sistemas privados con un sistema de comunicación público para proporcionar redundancia en el caso de que nuestro enlace falle.

Se comprobará también la seguridad física del cableado (o la visibilidad de los tambores de microondas en su caso) comprobando que un intruso malintencionado no pueda seccionar los cables de comunicaciones que van desde la centralita más cercana hasta nuestro edificio. Hay que tener en cuenta que esta sección de cable es propiedad de la compañía que proporciona el servicio, por lo que necesitaremos llegar a un acuerdo con esta si queremos realizar algún tipo de modificación en este cable.

4.3. Los accesos físicos al edificio

Debemos tener en cuenta que el edificio tiene una serie de accesos obvios y otros no tan obvios que un intruso puede usar para entrar en nuestras instalaciones. Los obvios son las puertas principales de acceso y las ventanas que se encuentran cercanas a la calle. Los no tan obvios son las puertas de servicio, las ventanas superiores, las claraboyas, los accesos de mantenimiento o los sistemas de ventilación o calefacción.

Debemos realizar un estudio de la estructura del edificio, incluyendo si es necesario el estudio de los planos arquitectónicos de este si es necesario. Es imprescindibles ser paranoicos en este aspecto de la seguridad física del edificio, puesto que un intruso dentro del edificio es la mayor amenaza que podemos tener, incluso con todos nuestros sistemas de seguridad física desplegados. Nuestros sistemas de seguridad física pueden ser difíciles de sobrepasar, pero un intruso con el suficiente tiempo y que pueda usar la fuerza bruta sobre nuestros armarios o racks sin ser detectado tendrá siempre todas las de ganar. Debemos por todos los medios impedir el acceso a los potenciales intrusos, ya sea mediante la utilización de rejillas resistentes en las zonas de acceso y cerraduras de seguridad en las puertas y ventanas de acceso, o ya sea mediante la contratación de una vigilancia suficiente para asegurar que ningún intruso pueda acceder al edificio sin que sea detectado. El nivel de paranoia que debemos emplear para aconsejar estas medidas de seguridad es directamente proporcional a lo críticos que sean los datos que debemos proteger. No es lo mismo un simple edificio de oficinas que la central de un banco, por ejemplo. En el primero aconsejaremos cerraduras de seguridad, rejillas y vigilancia general del edificio, en el segundo aconsejaremos todo tipo de medidas de seguridad físicas como puertas blindadas, rejas de acero o rejillas soldadas, y además vigilancia mediante personas y cámaras en cada una de las plantas del edificio y sobre todo en las salas de máquinas que puedan contener datos críticos o sistemas que puedan dejar el sistema de computación del edificio inutilizado.

Podemos realizar una distinción entre la vigilancia en horas de oficina y cuando el edificio está cerrado. En las primeras centraremos nuestra atención en la vigilancia de los accesos al edificio, utilizando tarjetas de identificación para nuestros empleados y para el personal que deba acceder a zonas con seguridad y controlando a todas las personas que entren y salgan del edificio. Cuando el edificio está cerrado centraremos nuestra atención en la vigilancia por medio de cámaras, en los accesos menos obvios al edificio y en las posibilidades de que un intruso pueda forzar algún medio de entrada al edificio.

Es posible contratar a un especialista en puertas y cerraduras para comprobar la seguridad de los accesos al edificio y dentro del edificio. También es posible aplicar alguna de las Lock Picking Guides que se encuentran en Internet si somos los suficientemente hábiles como para comprobar una cerradura por nosotros mismos, aunque es muy posible que sea más sencillo y eficaz la contratación de un especialista.

4.4. El acceso al centro de computación

Si contamos en el edificio con un centro de computación o datacenter deberemos comprobar la seguridad física específica de esa habitación en concreto, por ser esta crítica para nuestros sistemas. Un centro de computación debe tener unas características especiales en cuanto a seguridad que no son necesarias en otros puntos del edificio. Debe tener un sistema de acceso suficientemente seguro,

preferiblemente con una puerta blindada y siempre que sea posible con personal de vigilancia que compruebe el acceso por medio de tarjetas de identificación o medios similares. También es posible el uso de sistemas de identificación biométrica, por medio de claves temporales tipo Opie o similares. El acceso físico debe ser todo lo seguro que sea posible, vigilando que la puerta sea lo suficientemente sólida y la cerradura los suficientemente segura. No es difícil el estudio de seguridad física del acceso a un datacenter, pero es complicado el crear un sistema seguro de control de acceso, siendo aconsejable el tener personal de vigilancia que compruebe las identificaciones de forma inequívoca y que apunte en un sistema todos los accesos que se produzcan al datacenter.

En cuanto a la estructura física deberemos tener un suministro eléctrico asegurado, para lo que tomaremos las medidas que hemos indicado más arriba para el edificio, incluido un panel de protecciones para el datacenter que pueda protegerlo y aislarlo de otras secciones del edificio. Deberemos tener también un sistema de conexión a la red corporativa asegurado, mediante varias conexiones redundantes que permitan que una falle y que el edificio pueda seguir accediendo al centro de computación. Si el sistema debe tener conexión a redes públicas se proporcionará una conexión redundante que permita el fallo de al menos una de las vías de acceso.

Es imprescindible un sistema de aire acondicionado si tenemos suficiente hardware en el centro de computación. Es aconsejable tener algún método de monitorización de la temperatura y la humedad de la sala para mantener unas condiciones óptimas para los equipos que mantengamos en la sala de computación. También es imprescindible un sistema de detección de incendios, que pueda avisar rápidamente al personal encargado si se produce algún incendio en la sala. Siempre que sea posible se tendrá alimentación redundante para todo el sistema de computación y luego para cada equipo en particular.

4.5. La estructura del edificio

El estudio de la estructura del edificio es beneficioso para todos los demás estudios que vayamos a realizar sobre la seguridad física del edificio. Siempre que sea posible estudiaremos los planos del edificio para observar la estructura, el reparto del espacio dentro del edificio, los accesos, los sistemas de seguridad (salidas de emergencia, sistemas antiincendios, etc), el suministro de energía, las canalizaciones de agua y gas, etc.

En lugares donde sea probable la incidencia de terremotos se estudiará especialmente la estructura física del edificio y los sistemas de seguridad implementados para tales casos. Se puede pedir ayuda a un arquitecto para que estudie los planos del edificio y pueda señalarnos los puntos más críticos o que debamos vigilar.

4.6. La seguridad contra incendios y otros desastres

Los sistemas de seguridad contra incendios y otros desastres naturales deben ser instalados normalmente cuando el edificio es construido, y son difíciles de instalar después. En nuestro caso estudiaremos la disponibilidad de sistemas de detección y prevención de incendios, de rotura de tuberías o escapes de

agua y en el caso de disponer de antenas de cualquier tipo o sistemas de comunicaciones como tambores de microondas estudiaremos la resistencia de estos a vientos fuertes.

Los sistemas de detección de incendios pueden ser instalados después de construido el edificio y no suponen una gran inversión, pueden avisar rápidamente de pequeños incendios y permitir al personal el sofocarlos antes de que alcancen mayor entidad. Puesto que el agua es enemigo del hardware informático no podemos implantar ningún tipo de sistema para sofocar incendios basado en agua, es preferible el comprobar que se dispone de suficientes extintores de CO2 o de espuma.

Como hemos dicho otro problema para el hardware informático es el agua. La rotura de una tubería puede producir un verdadero desastre en el sistema informático de una empresa, estropeando todos los sistemas de una red, por lo que es aconsejable la instalación de detectores de líquidos a ras de suelo para detectar rápidamente cualquier fuga de agua.

En cualquier caso siempre que tengamos un sistema de computación lo suficientemente crítico ninguno de estos sistemas puede sustituir al personal de vigilancia, que deberá velar por la seguridad física de los sistemas también en estos aspectos, para lo que deberá tener una serie de protocolos claros a seguir cuando se produce una de estas contingencias.

4.7. Planes de evacuación del personal

Consideraciones éticas aparte debemos tener en cuenta que una parte esencial del sistema computacional de una empresa o edificio son los administradores, las personas que usan el sistema y en general los empleados de la empresa. Por eso dentro del estudio de la seguridad física del sistema debemos tener en cuenta a las personas, manteniendo una serie de planes claros e inequívocos de evacuación de estos si se produce cualquier tipo de desastre dentro del edificio. Como consultores de seguridad estudiaremos los planes existentes para este tipo de evacuaciones, teniendo en cuenta que sean realmente aplicables en un momento de desconcierto general como puede ser un incendio y que sean el máximo de eficaces.

4.8. Seguridad física de los backups

De nada sirve mantener un perfecto sistema de backups si cuando es necesario restaurarlos estos no están disponibles. La seguridad física de las cintas o dispositivos de backup debe ser una preocupación para un consultor en seguridad física, y por tanto se debe tener previsto cualquier incidente que se pueda producir, como incendios, terremotos, robos y así cualquier evento que se nos pueda ocurrir.

Los armarios ignífugos son eficaces hasta cierto punto contra los incendios. Si estos son de pequeña magnitud probablemente nuestros backups sobrevivirán, pero si tenemos un incendio de cierta entidad la temperatura que se alcanzará dentro del armario destruirá los datos de los backups, por lo que son sólo relativamente eficaces contra este tipo de eventos. Lo mismo es aplicable para los terremotos y otros accidentes naturales.

El sistema más eficaz para mantener los backups seguros es mantenerlos fuera del edificio, o al menos mantener una copia de estos, ya sea en otro edificio o en un centro de almacenamiento de backups. Estos últimos son centros que proporcionan almacenamiento de las cintas de backup con todas las medidas de seguridad física imaginables y que son una buena alternativa a el mantenimiento de los backups cerca de las máquinas de las que se ha hecho backup. Puede contratarse uno de estos servicios y mandar los backups o copias de estos a uno de estos servicios, que velará por la seguridad de nuestros backups. Normalmente este tipo de servicios se encarga de ir a la empresa en los periodos de tiempo concertados para recoger las cintas de backup.

Otra alternativa es mantener backups distribuidos, replicando los backups entre edificios o entre sistemas informáticos, para prevenir la perdida de datos por culpa de un problema de seguridad física en alguno de los sistemas o edificios.

4.9. Sistemas de redundancia de servidores y almacenamiento de datos

Una opción que siempre deberemos considerar cuando realizamos estudios de seguridad física es la posibilidad de mantener varias copias de los datos e incluso tener redundancia para los servidores corporativos. Con los nuevos sistemas de almacenamiento distribuido es sencillo mantener los datos sincronizados en varias localizaciones, con lo que disminuye enormemente la probabilidad de pérdida de datos. Y teniendo suficiente ancho de banda de red para interconexionar los sistemas corporativos de varios edificios podemos tener redundancia de los servidores de datos o aplicaciones, con lo que podremos tener la seguridad de que nuestros sistemas informáticos siempre estarán disponibles, aunque no sea en la localización física que estamos estudiando.

La redundancia de servidores y del almacenamiento de los datos, sobre todo cuando está situada en diferentes edificios mejora la seguridad física de un sistema de computación en gran medida, y es una opción a tener en cuenta incluso aunque implementemos otro tipo de sistemas de seguridad física en el edificio.

Los sistemas de gestión y los servidores de aplicaciones comerciales distribuidos son caros y difíciles de mantener hoy en día, pero es posible implementar mediante software libre sistemas distribuidos con precios razonables y con un gran rendimiento. Algunas grandes empresas están liberando bajo licencias de software libre sistemas de gestión de datos distribuidos que pueden ser de gran ayuda en estos casos. Para los sistemas de almacenamiento distribuido existen varias opciones tanto de software libre como de software comercial, por lo que sólo deberemos ocuparnos de tener el sistema adecuado y el ancho de banda suficiente para poder replicar los datos.

El único punto de fallo con estos sistemas es el enlace de comunicación entre los sistemas a replicar, sobre todo cuando manejamos datos críticos. Para solucionar esto debemos aplicar otro tipo de redundancia, tanto en los sistemas como en los enlaces de red entre sistemas, como hemos explicado más arriba.

4.10. Sistemas distribuidos con localización en diferentes edificios

En el punto anterior hablábamos principalmente de redundancia entre sistemas de gestión o servidores de aplicaciones, así como de redundancia en el almacenamiento de datos. En este vamos a hablar de algo diferente, el estudio de sistemas de computación distribuidos localizados en diferentes edificios, con o sin replicación de datos.

Lo que antes se volvía un punto a nuestro favor ahora se vuelve un punto en nuestra contra. Al tener varios sistemas distribuidos en varios edificios deberemos realizar el estudio de seguridad física para cada uno de los edificios en todos los aspectos que puedan afectar a nuestros servidores. Esto supone más trabajo para el consultor en seguridad física, pero proporciona a la empresa una forma de aprovechar óptimamente su capacidad de calculo y almacenamiento de datos e incluso de de centralizar sistemas y servicios antes dispersos.

4.11. Alojamiento y backup de datos críticos fuera del edificio

La elección de un sistema de alojamiento para backups es una decisión del personal de administración, teniendo en cuenta una serie de razones como la necesidad disponibilidad inmediata de los backups o el tiempo que estos deben almacenarse. Como regla general deberemos mantener al menos una copia de los backups principales fuera del edificio, o incluso mantener fuera todos los backups. Como hemos indicado en la sección dedicada a los backups existen empresas dedicadas al almacenamiento de datos que proveerán a nuestros backups de todas las medidas de seguridad física necesarias. Medidas como el almacenamiento de los backups en el domicilio particular de los administradores son contraproducentes, pues no suelen tener ni las medidas de seguridad necesarias ni la capacidad de mantener un entorno óptimo para los backups.

4.12. Control de marcado de edificios y Warchalking

En el mundo hacker es una práctica común el marcado de edificios para indicar que en determinado edificio es posible acceder a la red o a los datos corporativos mediante técnicas de hacking, sobre todo con la cada vez mayor implantación de tecnología inalámbrica para la transmisión de datos, y que permite el acceso a los datos en bruto e incluso la comunicación desde el exterior de la empresa.

Deberá estudiarse la fachada del edificio de forma que no encontremos signos de Warchalking u otro tipo de marcado sospechoso. El Warchalking es una técnica de marcado que mediante símbolos realizados con tiza en la fachada de un edificio indica que el edificio cuenta con una red wireless y las características de esta, como pueda ser la posibilidad de obtener una IP valida por medio de DHCP desde fuera del edificio utilizando un portátil con una tarjeta wireless, la posibilidad de acceder a la red interna de la empresa por este método o la salida a Internet a través de la red de la empresa. El Warchalking es extremadamente peligroso, pues expone las vulnerabilidades que un hacker haya encontrado en nuestra red a cualquier otro intruso que pase por delante de nuestro edificio.

La primera medida contra el marcado y el Warchalking es la implementación de plena seguridad en la red interna de la empresa, incluso evitando tecnologías que permitan el acceso indiscriminado a nuestros datos desde el exterior como las redes wireless. Como el tener plena seguridad informática es siempre un objetivo difícil de cumplir y debemos tener en cuenta que siempre será necesaria la vigilancia por parte del personal de seguridad o de control de accesos a posibles signos de marcado o Warchalking.

Los símbolos de Warchalking cambian con el tiempo e incluso son diferentes entre diferentes escuelas de hackers, por lo que deberemos sospechar de cualquier marca o símbolo que encontremos en el edificio y que pueda tener algún sentido. Si encontramos signos manifiestos de Warchalking tendremos que asumir que además del riesgo en la seguridad física que supone el Warchalking que hemos detectado tenemos un problema de seguridad informática, porque sabemos que alguien se ha preocupado de marcarnos como objetivo de ataques que son en teoría posibles.

5. El entorno físico del hardware

Entendemos como entorno físico del hardware el entorno en el que está situado nuestro hardware, dispositivos de red y centros de computación. Es el paso siguiente en el estudio de la seguridad física al estudio del edificio. Supone el estudio de la localización del hardware, el acceso físico que las personas puedan tener a este, todo el cableado que interconecta el hardware o que le provee de energía, el control de la temperatura y demás condiciones climáticas del entorno donde se encuentra el hardware, el estudio del tipo de montaje de este hardware dentro de nuestra infraestructura y los métodos de administración y gestión del hardware y de su entorno.

5.1. Suministro de energía para el hardware

Después de haber estudiado el suministro de energía al edificio debemos realizar un estudio del suministro de energía a los centros de computación o en el entorno inmediato donde se encuentra situado nuestro hardware. Es imprescindible el asegurar un suministro estable y continuo de energía eléctrica al hardware, utilizando normalmente sistemas UPS (Sistema de suministro ininterrumpido de energía) que regularán la tensión evitando los picos de voltaje que pueda traer la red y proporcionarán un tiempo de autonomía por medio de baterías en caso de cortes del suministro eléctrico.

Hay que tener en cuenta siempre que no solo es necesario proveer de un suministro estable y continuo de energía a los ordenadores y a los sistemas de almacenamiento, deberemos proporcionar el mismo tratamiento al hardware de red, incluidos concentradores, enrutadores, pasarelas y todos los dispositivos que sean necesarios para el funcionamiento normal de la empresa. Estas medidas pueden incluir también otro tipo de hardware como impresoras láser o fotocopiadoras.

Para evitar puntos de fallo es conveniente el no depender únicamente de un sistema UPS para todo el hardware a proteger, siendo más conveniente la instalación de varios UPS que puedan suministrar energía a parte del sistema en el caso de que uno de los UPS fallara. Se estudiará la autonomía de los

UPS y las protecciones que proporcionan al hardware y se recomendará en su caso la instalación de más sistemas UPS o la redundancia de alguno de ellos.

Deberá estudiarse también las protecciones como fusibles, automáticos y diferenciales que tengamos en cada una de las concentraciones de hardware, como centros de computación, racks o armarios con varios sistemas montados.

5.2. Comunicaciones: Interconexión de redes y sistemas

En este momento del estudio de la seguridad física deberemos centrarnos sobre todo en la estructura física general de la red y no en los dispositivos en concreto. Deberemos comenzar estudiando el diseño de la red del edificio, observando las troncales de red que intercomunicarán las diferentes plantas y secciones del edificio. Intentaremos centrarnos en la estructura física y no lógica de la red, buscando los puntos de fallo que puedan afectar a toda la red.

Una red típica de un edificio consta de uno o varios grandes enrutadores que proporcionan la conectividad con el exterior, una red troncal (normalmente Gigabit Ethernet) que se extiende por la estructura del edificio, un gran concentrador por planta que distribuye el tráfico desde la red troncal y luego varios concentradores más pequeños que conformarán las diferentes redes departamentales.

El primer paso a estudiar es buscar los puntos de fallo que puedan provocar una caída total de la red, estudiando los grandes enrutadores que proporcionan conexión con el exterior, donde deberemos buscar dispositivos fiables y dotados de redundancia tanto en su estructura física interior como en la funcionalidad que proporcionan, incorporando varias conexiones preferiblemente con varios proveedores que nunca dejen a nuestra red troncal sin conexión al exterior. Se estudiará el entorno donde están situados los dispositivos enrutadores, observando que cumplan con todas las normas y que dispongan de un suministro continuo y estable de energía.

El siguiente punto a estudiar es el cableado de la red, comenzando por la red troncal. La red troncal suele ser Ethernet Grueso en sistemas antiguos y Gigabit Ethernet en los sistemas más modernos. En ambos casos deberemos estudiar el cableado mediante dispositivos al efecto y observando mediante planos o esquemas como han sido entubados y distribuidos por el edificio. En el caso de redes troncales de fibra óptica necesitaremos instrumental específico para el estudio de la red y de las interconexiones que esta pueda tener, y es posible que necesitemos contratar a personal especializado si queremos estudiar la fiabilidad del medio físico, lo que no suele ser necesario, pues realizando un estudio de la velocidad de conexión entre los diferentes concentradores en cada planta o departamento y con los enrutadores que dan conexión al exterior podremos comprobar la salud del medio físico. Debe estudiarse el tipo de fibra óptica instalada y la calidad del cableado, observando la documentación que hayan dejado los instaladores de la red troncal.

El tercer punto a estudiar es la posibilidad de fallo de los concentradores que conectan la red troncal con los concentradores de los distintos departamentos o secciones dentro del edificio. Lo más común es encontrar uno de estos dispositivos por planta, al cual se conectan todos los demás concentradores

proporcionando conexión a las distintas redes departamentales del edificio. Para estos concentradores se deberán tomar las mismas precauciones que para los enrutadores principales, proporcionando siempre que sea posible redundancia en las conexiones entre la red troncal y los concentradores de las redes departamentales.

El cuarto punto son los concentradores que interconectan las redes locales departamentales con los concentradores conectados a la red troncal. Estos dispositivos son menos críticos que los anteriores, puesto que un fallo en ellos sólo afectaría a la red local departamental a la que proveen conexión. Para estos concentradores no suele ser necesario proporcionar redundancia, simplemente cuidaremos de que se encuentran en un entorno no hostil y correctamente alimentados. Mas adelante veremos las medidas que deben tomarse con el dispositivo en concreto en materia de seguridad física.

Para todos los dispositivos indicados se estudiará su ubicación y el acceso que un intruso pueda tener a ellos, sobre todo deberemos tener control de acceso a los enrutadores principales y también a los concentradores de cada planta, que son críticos en la seguridad física de todo el sistema.

Se deberá estudiar también la posibilidad de que un intruso malintencionado provoque algún tipo de fallo en la red cortando el cableado de red o manipulando alguno de los dispositivos de red. Contra la contingencia de un corte en el cableado de red es interesante la posibilidad en edificios nuevos de que el cableado de red sea integrado en la estructura del edificio, aunque esto siempre supondrá una merma en las posibilidades de ampliación de la red. En otro caso deberemos procurar que los cables de red estén lo más agrupados posible para facilitar su vigilancia. Se entubarán siempre que sea posible los cables de red utilizando medios rígidos que no sean fáciles de seccionar. Los dispositivos de red estarán también agrupados y preferiblemente protegidos en armarios ignífugos o racks con ventilación suficiente que permita una fácil vigilancia.

5.3. Acceso físico al hardware

El acceso físico al hardware sea este computadoras o dispositivos de red deberá ser restringido, teniendo en cuenta las necesidades de cada departamento o usuario. Se debe hacer aquí una distinción entre los equipos de red y servidores departamentales o corporativos y las máquinas de usuario final.

Los equipos de red importantes como routers, pasarelas y concentradores deberán estar en un lugar donde exista un control de acceso, ya sea mediante vigilancia por medio de personas o mediante el aislamiento de las salas o armarios donde estos se encuentren por medio de cerraduras o sistemas de control de acceso mediante tarjetas, claves o control biométrico. Para cada acceso deberá reflejarse una entrada en un sistema de control que puede ser desde un simple libro donde se vayan apuntando las personas y el acceso que han tenido a los equipos hasta un sistema informático que deje reflejado en sus logs el acceso al hardware y quien lo ha hecho. Es importante controlar y reflejar siempre en los apuntes quien ha accedido al hardware, con que motivo y las modificaciones físicas o lógicas que en su caso pueda haber realizado sobre este hardware. Los dispositivos de red que permitan un acceso remoto deberán ser protegidos por medio de claves y cortafuegos para limitar el acceso a las personas que tienen a su cargo la administración de estos sistemas. Se deberá preveer la posibilidad de que intrusos o atacantes intenten cambiar la configuración del hardware de red, sobre todo en el caso de enrutadores y

concentradores que proporcionen funcionalidad de VPN, para esto se seguirán las medidas de seguridad informática indicadas para cada caso, que dependerán del tipo de dispositivo y de sus posibilidades de configuración. Es esencial el control físico de estos dispositivos porque algunos de ellos permiten el acceso a la configuración por medio de conexión a puertos serie y proporcionan una seguridad menor cuando se accede de esta forma. Se deberá preveer también la posibilidad de atacantes con el tiempo suficiente para realizar ataques de fuerza bruta sobre las claves de los sistemas o denegaciones de servicio por medio de envío de tráfico masivo o construido contra los dispositivos. Se debe preveer también la posibilidad hoy en día de que estos dispositivos sean hackeados, pues muchos de estos dispositivos tienen su propio sistema operativo o están directamente basados en hardware estándar que es más susceptible a ser atacado por medio de ataques informáticos. Incluso las más modernas impresoras láser cuentan con su propio sistema operativo, que puede ser hackeado y que puede proveer a un atacante de un medio de acceso a la red prácticamente no tenido nunca en cuenta por los administradores encargados de la seguridad.

Para los servidores departamentales o corporativos se deberá tener en cuenta las mismas premisas que para los dispositivos de red y además las propias de cualquier computadora que necesite una seguridad física e informática. Se tendrá en cuenta también la localización física de las máquinas y en su caso se proveerá el mismo control de acceso que para los dispositivos de red importantes.

Una de las medidas más eficaces contra los ataques tanto físicos como informáticos sobre todo este tipo de sistemas es la monitorización continua de los dispositivos mediante sistemas de monitorización basados en hardware o software. Los administradores de la red y de los servidores deberán mantener bajo observación estos dispositivos mediante esta monitorización buscando fallos y deberá evaluarse en cada caso si el fallo ha sido fortuito o se ha debido a algún tipo de manipulación sobre el hardware o sobre el software de los dispositivos.

Las maquinas de usuario final donde han de trabajar los empleados son paradójicamente las más importantes y las mas difíciles de proteger, porque normalmente han de estar situadas en el entorno del usuario, donde están expuestas a los errores o manipulaciones que un usuario poco cuidadoso o mal informado pueda realizar sobre ellas. En secciones posteriores de este manual se explicará como proteger este tipo de máquinas, pero a nivel corporativo puede ser interesante algún tipo de monitorización también de estas máquinas para detectar fallos o manipulaciones del hardware o el software. La localización de estas máquinas deberá ser idealmente centralizada, en forma de racks o de armarios donde se agrupen las máquinas y donde se pueda controlar el acceso a estas, siempre que los usuarios finales no deban manipular físicamente las máquinas, como en el caso de utilización de lectores de CDROM, grabadoras de CDs o disqueteras. Se intentará siempre que sea posible que el usuario final trabaje de forma remota sobre los servidores de la empresa, implementando soluciones de acceso remoto a las aplicaciones y los datos, o manteniendo como hemos dicho las máquinas en una localización segura donde el usuario no pueda manipularlas.

5.4. Localización física del hardware

La localización física del hardware puede afectar enormemente a la seguridad física del sistema, pues un sistema donde las máquinas estén expuestas a la manipulación del usuario final o de supuestos intrusos

será un sistema poco seguro. Es aconsejable mantener los dispositivos de red y los servidores en un lugar centralizado, idealmente un centro de datos donde podamos tener las medidas de seguridad física indicadas anteriormente y donde el control de acceso permita saber quien, cuando y porqué ha accedido físicamente a alguno de los dispositivos.

Se aconseja el uso de armarios ignífugos correctamente ventilados con racks donde se instalarán los dispositivos de red y los servidores, correctamente cableados y teniendo en cuenta la seguridad física de este cableado. Estos armarios deben tener cerraduras lo suficientemente seguras para impedir el acceso a un supuesto intruso malintencionado y con la capacidad de realizar Lock Picking (Manipulación de cerraduras). Mas adelante se hablará de las medidas que se pueden implementar para impedir este tipo de comportamientos. El acceso a los armarios deberá estar controlado y se deberá crear una política de acceso a los armarios, donde se apuntará de alguna de las formas anteriormente indicadas cada acceso a los dispositivos de red y servidores alojados en el armario, la persona que ha accedido y las manipulaciones que en su caso pueda haber realizado. Siempre que se realice algún tipo de ampliación de equipos o modificación del hardware en los armarios por personal externo a la empresa o al departamento encargado de la administración del hardware deberá dejarse muy claro mediante una serie de políticas de acceso lo que puede o no puede hacerse.

Siempre que sea posible se preveerá la posibilidad de atacantes o intrusos malintencionados que tengan acceso físico al hardware, pues aunque tomemos todas las medidas posibles contra el acceso físico al hardware siempre deberemos asegurar también el mismo hardware en previsión de accesos no deseados.

5.5. Control de acceso al hardware. Control de acceso del personal

El control de acceso al hardware se realizará preferiblemente mediante personal que verifique mediante algún tipo de identificación a las personas que tienen permiso para acceder al hardware o mediante dispositivos electrónicos (claves, sistemas biométricos) o físicos (puertas blindadas, cerraduras seguras, etc) que permitan controlar quien tiene acceso al hardware y quien no. Es muy útil en estos casos tener una política clara y concisa sobre quien, como, cuando y para que puede tener acceso al hardware. Estas normativas deberán ser conocidas por todo el personal con acceso al hardware y deberán estar plasmadas sobre papel para poder ser consultadas en caso de duda.

Siempre será preferible la intervención de personal encargado del acceso al hardware que la utilización de llaves, tarjetas o dispositivos electrónicos, pues estos últimos son más susceptibles de ser burlados mediante varios sistemas, mientras que los primeros simplemente deberán ser entrenados para evitar el Hacking Social y para seguir la política de acceso al hardware de manera estricta. En sistemas muy críticos se puede poner personal de vigilancia o cámaras para controlar el acceso al hardware. La rigidez de las políticas de acceso al hardware son inversamente proporcionales a la facilidad de administración de los sistemas, pero normalmente son necesarias si queremos mantener una política de seguridad física alta.

Los dispositivos y servidores situados fuera de los centros de datos o de computación o en las zonas departamentales deberán ser protegidos mediante armarios o racks cerrados con llave y deberá imponerse una política en el departamento de acceso a estos sistemas.

Es importante que en todos los casos siempre tengamos una persona encargada del control del acceso al hardware y que tenga responsabilidades asociadas a este cometido. Puede tratarse de los mismos administradores, de los usuarios (mediante políticas de acceso) o de personal contratado para este cometido. Estas personas deberán responsabilizarse personalmente de todos los accesos al hardware que se produzcan y apuntar en los libros o logs detalladamente todas las manipulaciones realizadas.

Un punto poco conocido pero muy a tener en cuenta en la seguridad física de los sistemas es el control de acceso del personal de mantenimiento del edificio. El personal de limpieza, de mantenimiento del edificio y personal similar debe pasar por los mismos sistemas de control de acceso que los administradores o usuarios de las máquinas. Todo el mundo confía en el personal de limpieza o de mantenimiento, probablemente todo el mundo los conoce y llevan años trabajando en la empresa, pero si nuestros datos son suficientemente críticos haremos bien en desconfiar de todo el mundo, y también de ellos. Alguien puede ofrecer una cantidad de dinero o extorsionar de alguna forma al personal para que extraiga datos o provoque daños en el hardware, todo depende de lo importante que sean nuestros datos y de su valor económico. Incluso pueden producir daños graves por simple desconocimiento, pues no es la primera vez que el personal de limpieza desenchufa un servidor crítico de la empresa para enchufar la aspiradora. Y no es una broma, ocurre de verdad. Lo ideal es que personal de vigilancia acompañe al personal de limpieza y mantenimiento cuando este deba acceder a los centros de computación o a los sitios donde estén alojados servidores o sistemas de almacenamiento de datos. También se puede usar otro tipo de control de acceso como tarjetas o sistemas biométricos, que prevengan este tipo de comportamientos.

5.6. Interacción del hardware con el suministro de energía y agua

Aunque parte de la seguridad física del edificio deberá también tenerse en cuenta en los centros de computación o de almacenamiento de datos la seguridad física asociada a las canalizaciones de energía y agua. Las canalizaciones de energía pueden provocar cortocircuitos o fallos que provoquen incendios y las canalizaciones de agua pueden romperse y estropear el hardware. Se deberá estudiar que estas canalizaciones cumplan las normas que al efecto deben seguirse en cada país, pues existen reglamentos que indican la distancia a la que deben de estar estas canalizaciones unas de otras y de los dispositivos eléctricos como el hardware.

Se puede usar aquí dispositivos de monitorización como detectores de humo o de líquidos, que deberán situarse estratégicamente para proporcionar una máxima superficie de cobertura y sobre todo para proteger a los sistemas más críticos. Puede ser aconsejable en algunos casos mantener los sistemas críticos o redundantes en varias habitaciones, disminuyendo así la posibilidad de que una contingencia de este tipo pueda afectar a un grupo grande de máquinas, y deberá aprovecharse la estructura física del edificio para proveer aislamiento entre estas salas o secciones donde se ha de situar el hardware. La mayoría de las veces es preferible mantener algo más de cableado que mantener todo el hardware en una misma localización física donde esté expuesta a situaciones de riesgo como incendios o inundaciones.

Los sistemas de backup y almacenamiento de datos deberán estar en localizaciones seguras dentro del edificio y lejos de canalizaciones de energía o agua, por ser crítico su funcionamiento para la seguridad de los datos. Como en casi todos los casos la redundancia en estos sistemas, sobre todo si tenemos varios

sistemas distribuidos en distintas secciones del edificio o incluso en diferentes edificios, nos proveerá de una seguridad adicional contra este tipo de accidentes.

5.7. Sistemas de control del hardware y su integridad

Los sistemas de control de las condiciones de trabajo del hardware suelen ir integradas en los racks o armarios que usemos para protegerlos, indicando normalmente una serie de parámetros como la temperatura de trabajo, la humedad relativa del ambiente dentro del rack o armario y otros parámetros. Los sistemas UPS de cierta entidad suelen tener algún medio de monitorización remota mediante SNMP o avisos de algún tipo. Deberá estudiarse la implantación de racks, armarios y sistemas UPS que proporcionen monitorización de las condiciones de funcionamiento del hardware para mantener las máquinas en un nivel óptimo de seguridad y para poder reaccionar rápidamente cuando se produce algún problema.

La integridad del hardware debe ser vigilada normalmente mediante software, ya sea mediante software de monitorización o sistemas de gestión de redes basados en SNMP. Por esto es muy interesante que nuestros dispositivos de red dispongan de funcionalidad SNMP suficiente para poder monitorizar la salud de los dispositivos y su estado. En condiciones normales de funcionamiento será suficiente con un sistema de monitorización a través de la red que permita ver si los dispositivos están funcionando correctamente y cumpliendo con su cometido, en los sistemas críticos puede ser necesaria una monitorización adicional por medio de personal que verifique que los racks y armarios están funcionando correctamente y que los dispositivos de red están físicamente protegidos.

5.8. Seguridad contra incendios y otros desastres a nivel de hardware

La seguridad contra incendios y otros desastres ha sido tratada a nivel estructural anteriormente, pero ahora hablaremos de la seguridad a nivel de hardware, que proporcionará un segundo nivel de protección física. Lo más normal es usar racks o armarios ignífugos para proteger a los sistemas contra pequeños incendios o desastres naturales, aunque deberemos tener siempre en mente que la temperatura que se alcanzará en un incendio en los racks y dentro de los armarios ignífugos es suficiente para destruir el hardware y los datos que este hardware pueda contener. Nada es más eficaz contra este tipo de imprevistos que un sistema eficaz de backup, donde los backups sean guardados fuera del edificio o al menos fuera de la sección que contiene el hardware o los dispositivos de almacenamiento de datos. La eficacia de un sistema de backup es una cuestión de seguridad informática, por lo que no la trataremos aquí, simplemente haremos notar que un backup no es eficaz si no está disponible cuando ocurre un incidente y es necesaria su restauración. La frecuencia de los backups también es un factor a tener en cuenta, puesto que no siempre es posible el llevar fuera del edificio o sección los backups en un espacio de tiempo suficientemente corto como para asegurar la mínima perdida de datos y trabajo cuando se produce un desastre de este tipo. Los backups remotos son una opción a tener en cuenta en estos casos, usando sistemas que realizan backups a través de red en máquinas situadas en otros edificios, posiblemente con replicación de los datos, para mantener varias copias de los datos y los backups y preveer así la contingencia de un incendio o un desastre natural en uno de los edificios.

La implementación de los sistemas de seguridad contra incendios, inundaciones, terremotos y demás desastres naturales deberá ser más estricta cuanto más críticos sean los datos que debemos proteger. Se debe mantener un equilibrio entre el presupuesto dedicado a la seguridad física para este tipo de eventos y las pérdidas que puedan darse si uno de estos eventos se produce. Estas pérdidas pueden ser económicas, en horas de trabajo o en la integridad de datos críticos como datos económicos, datos de clientes o proveedores y datos secretos referidos a la empresa o a nuestros clientes o proveedores. En el caso de que los datos sean críticos e irrecuperables o que su perdida pueda dañar la imagen corporativa de la empresa se empleará todo el presupuesto necesario para mantener copias de los datos distribuidas en varios edificios, mediante sistemas de backup o almacenamiento distribuido, porque esté será el único sistema que nos asegurará el mantener siempre copias de los datos físicamente seguras.

5.9. Planes de evacuación de hardware y equipos

Aunque no sea muy común es interesante estudiar la posibilidad de que el hardware deba ser evacuado del edificio por diversas razones. Es posible que tengamos que mover nuestro sistema a otro edificio por razones corporativas o que debamos hacerlo por razones de fuerza mayor, como desastres naturales, incendios parciales o cualquier otra contingencia imaginable. Para preveer este tipo de evacuación deberemos crear un plan de evacuación del hardware que nos permita llevar los equipos críticos a otro edificio o departamento en un mínimo de tiempo y siguiendo un plan predeterminado que tenga en cuenta la importancia de cada sistema.

Deberemos tener en cuenta al realizar el estudio y el plan de evacuación la importancia de los equipos y sobre todo de los datos que albergan estos equipos, de forma que los equipos y datos más importantes sean evacuados primero, y los menos importantes puedan esperar. Se deberá plantear la necesidad de tener personal preparado para este cometido y la facilidad con que estos datos se pueden mover de un lugar a otro.

Lo principal normalmente en una empresa será evacuar los datos corporativos (datos de la empresa, datos de facturación y contabilidad, del personal que trabaja en la empresa, de los clientes y de los proveedores), que estarán en forma de discos duros, sistemas de almacenamiento NAS o cintas de backups. Para los discos duros se facilita enormemente su evacuación si se dispone de discos duros hotswap (extracción en caliente) que puedan extraerse fácilmente del equipo y tengan una cierta protección física contra golpes o movimientos bruscos. Para los sistemas NAS se intentará que estos tengan también discos hotswap o que sean fácilmente desmontables y transportables. Las cintas de backup suelen ser fáciles de transportar, pero deberá tenerse en cuenta que son sensibles a los campos magnéticos y a las temperaturas extremas.

El plan de evacuación debe continuar con la evacuación de los backups y datos de trabajo de los usuarios para perder el mínimo de horas de trabajo posibles. Se debe tener en cuenta que normalmente es más caro el tiempo de trabajo del personal que trabaja en la empresa que la infraestructura informática de esta, por lo que antes de evacuar otro tipo de equipos deberán evacuarse los datos de trabajo del personal. Después se podrán evacuar todos los demás equipos que sea posible, teniendo en cuenta las consideraciones que la empresa encuentre más importantes, que pueden ser el valor económico de los equipos, la necesidad de disponibilidad inmediata de una infraestructura mínima para continuar con el

trabajo o la necesidad de disponer de un sistema mínimo para la prestación de servicios a clientes y proveedores.

5.10. El entorno de trabajo del personal y su interacción con el hardware

Deberá tenerse en cuenta cuando se estudie el entorno de trabajo del personal de la empresa la formación que este personal ha recibido sobre seguridad informática y física de los sistemas sobre los que debe trabajar o que están localizados en su entorno más cercano. Es fundamental que los empleados tengan los conocimientos necesarios para mantener el entorno del hardware físicamente seguro, y para esto deberán crearse normas de acceso y de uso de los dispositivos hardware que el empleado deba manipular, poniendo especial incapié en la seguridad de los datos y de su propio trabajo. Tendremos en cuenta dos tipos de trabajadores para nuestro estudio: los trabajadores con responsabilidad en la administración del hardware y software y los usuarios finales de estos sistemas.

Para los administradores deberemos crear unas normas de acceso y uso de los dispositivos servidores y de red donde se expliquen claramente los pasos que se deberán seguir para acceder al hardware y realizar modificaciones sobre este. Para este personal es esencial el conocimiento de las implicaciones en la seguridad física de los sistemas que su trabajo diario pueda tener y las medidas de precaución que deberán tomar para implementar esta seguridad. Se debe crear junto con el personal de administración las normas a seguir para acceder y modificar el hardware y el software. Esto es importante pues nuestras ideas sobre las medidas que han de tomarse para asegurar físicamente los sistemas pueden chocar frontalmente con las prácticas necesarias en la administración normal del sistema. Los administradores deben por tanto implicarse en crear las normas de seguridad física, haciendo notar las normas que puedan entorpecer su trabajo y la mejor forma de realizar las prácticas de administración sin afectar a la seguridad física del sistema. Una vez creadas las normas y aprobadas por el personal de administración deberá responsabilizarse ya sea a una persona o el conjunto del equipo de administración de la seguridad del sistema, implicando así a todo el personal de administración en las prácticas de seguridad de la red. Las normas una vez aprobadas deberán ser prácticamente inamovibles, y cualquier caso excepcional que tenga implicaciones sobre la seguridad física de los sistemas deberá ser observado con lupa y aceptado por una persona con capacidad de decisión ejecutiva y con los conocimientos técnicos necesarios para aprobar o denegar una determinada práctica puntual. Es muy aconsejable que todo acceso o modificación sobre el hardware quede reflejado de alguna forma para que pueda ser comprobado posteriormente en el supuesto de fallos o problemas de funcionamiento del sistema.

Para los usuarios finales de los sistemas se debe crear una normativa de uso de la red y del hardware, donde se indicará de forma clara y fácil de entender y cumplir las normas que se deben seguir para el uso de los dispositivos hardware y de la red corporativa. Respecto a la red corporativa haremos notar que las normas se referirán a el acceso físico a las bocas de red, a los concentradores y al cableado de red, no a el uso informático que se realice de la red, para lo que deberá elaborarse otra normativa por parte del personal de administración y que no tendrá relación con la seguridad física. Puede ser conveniente la impartición de un seminario donde se explique a los usuarios las normas que deben seguir para evitar la manipulación del hardware y el acceso a este.

Es complicado el implicar totalmente a los usuarios finales en la seguridad tanto física como informática de las máquinas y la red, en determinados casos por falta de información o capacidad técnica y en otros por errores o intentos de manipulación para llevar a cabo prácticas en principio prohibidas o desaconsejadas en la normativa de la red pero que el usuario puede encontrar atractivas. Debemos ser conscientes de que el peso de la responsabilidad de mantener la seguridad física de los sistemas informáticos del usuario final debe recaer sobre el equipo de administración y sobre nosotros como consultores. Todo error o manipulación que un usuario final realice sobre el hardware o la red es responsabilidad nuestra, pues debemos preveer todos los casos posibles que se puedan dar y que puedan afectar a la seguridad del sistema. En caso de tener una normativa que los empleados deben cumplir, estando estos debidamente informados, y sobre todo si se tiene la certeza de que determinada manipulación del hardware o de la red ha sido hecha a sabiendas de las implicaciones en la seguridad deberemos en su caso avisar al infractor y si la conducta se repite deberemos comunicar la infracción a la persona que tenga capacidad ejecutiva para imponer sanciones sobre el usuario.

5.11. Planificación de espacio para hardware y dispositivos. Montaje en racks

Una mala planificación del espacio destinado a contener nuestro hardware o nuestros dispositivos de red puede llevarnos a prácticas contrarias a la consecución de una buena seguridad física. Por ejemplo si no hemos planificado suficiente espacio en uno de nuestros armarios o racks para montar un dispositivo de red podemos vernos obligados a montar este dispositivo fuera del armario con lo que cualquiera podrá acceder a las conexiones y puertos del dispositivo.

Es aconsejable sobredimensionar los armarios y racks de montaje de equipos en el momento de su compra preveyendo futuras ampliaciones que impliquen la instalación de nuevos equipos o dispositivos de red, esto solo puede hacerse normalmente en el momento de la compra, obligándonos en otro caso a adquirir otro armario o rack si nos quedamos sin espacio. Es un punto a tener en cuenta cuando se planifica una nueva red o cuando se va a ampliar una red existente.

Si observamos que existen dispositivos de red, servidores NAS o servidores de aplicaciones fuera de los racks protegidos con llave o de los armarios ignífugos se aconsejará siempre la compra de nuevos armarios para contener estos dispositivos.

Uno de los aspectos que se suelen descuidar cuando se adquieren o montan racks o armarios ignífugos es la ubicación de los UPS. Los UPS deberán ir dentro de los armarios, por ser un punto de fallo de todo el sistema y por tanto un sistema a proteger con especial cuidado.

5.12. Control de la temperatura y la humedad del entorno. Monitorización

Se aconseja siempre la instalación de dispositivos de control de la temperatura y de la humedad del entorno. El factor más crítico en los datacenters y en los racks y armarios ignífugos suele ser la

temperatura, siendo la humedad un factor secundario sólo a tener en cuenta en climas muy determinados donde la humedad pueda afectar a los equipos.

Para prevenir una excesiva temperatura en los centros de datos y en los racks y armarios lo fundamental es tener una correcta ventilación y en el caso de habitaciones que alberguen una gran cantidad de máquinas la instalación de aparatos de aire acondicionado. A mayor temperatura menor tiempo entre fallos para todos los dispositivos electrónicos, incluidos los ordenadores, los dispositivos de red y cualquier sistema que genere por si mismo calor. Es fundamental que los ordenadores que montemos tengan una ventilación interior suficiente, incluyendo ventiladores para los discos duros y una fuente de alimentación correctamente ventilada. También son convenientes las cajas que incorporan uno o varios ventiladores para refrigerar las máquinas.

En el caso de los racks por su mayor masificación y por ser los dispositivos más pequeños y con una mayor integración de componentes la ventilación se convierte en un punto importante a tener en cuenta. Existen racks y armarios ventilados que permiten tener las máquinas en un punto de funcionamiento óptimo.

Es importante que además de tomar las medidas necesarias para tener la temperatura dentro de unos límites aceptables tengamos un sistema de monitorización de la temperatura. Este sistema puede ser un simple termómetro electrónico en la sala de computación o en los racks y armarios o un sistema de adquisición de datos conectado a un termómetro que pueda mandar datos de la temperatura a un ordenador que nos permita realizar la monitorización. Un ejemplo de un sistema de este tipo son los diversos aparatos que existen para su integración con el software Nagios y que nos permiten mediante plugins de Nagios la monitorización de la temperatura de cualquier sistema, avisándonos cuando supera los límites preestablecidos.

Debe configurarse también correctamente la bios de los ordenadores para que monitoricen correctamente la temperatura interna y avisen si esta supera los límites marcados. Lo mismo para la velocidad de giro de los ventiladores, que redunda al fin y al cabo en la temperatura que el hardware adquirirá.

5.13. Máquinas y dispositivos de escritorio

Los ordenadores y dispositivos de escritorio (Impresoras, faxes, pequeños concentradores, concentradores usb, etc) son uno de los puntos más difíciles de controlar por el consultor de seguridad física, pues dependen totalmente del uso o mal uso que el usuario final pueda realizar de ellos o sobre ellos. La única solución en este caso es la implantación de una política clara y comprensible para el usuario final de uso de los dispositivos que están a su cargo. Es importante responsabilizar de alguna forma al usuario final del hardware que está a su cargo, sin que esto suponga una carga añadida a su trabajo normal. Encontrar el punto justo entre la facilidad y flexibilidad en el uso de los dispositivos a cargo del usuario final y la seguridad física de estos dispositivos no siempre es fácil de encontrar, pero está es la tarea del consultor de seguridad física.

Para los ordenadores y dispositivos de red daremos más adelante algunos consejos de como mejorar la

seguridad física de estos dispositivos, impidiendo su manipulación por parte del usuario final siempre que sea posible. Cuando el usuario final tenga que tener acceso directo al hardware (disqueteras, CDROMS, impresoras, etc) lo más conveniente es la creación de una política de uso del hardware, donde el usuario pueda saber exactamente lo que puede o no puede hacer.

5.14. Servidores y dispositivos concentradores, enrutadores y pasarelas

Hemos hablado ya profusamente sobre el entorno donde deben encontrarse los servidores y dispositivos de red. Añadiremos que la seguridad física que implementemos para estos dispositivos debe ser directamente proporcional a la importancia de estos, y es tarea del consultor informarse de la importancia que cada dispositivo tiene dentro del conjunto. No es lo mismo un concentrador de un departamento que el router principal que proporciona la conexión a Internet. Tampoco es lo mismo un servidor de backups que un servidor de ficheros. El primero puede dejarnos sin backups y sin cierta seguridad, pero el segundo dejará la red y por tanto las máquinas de los usuarios finales paralizadas, perdiendo gran cantidad de tiempo de trabajo hasta que repongamos el servicio.

Debemos por tanto proteger estos dispositivos según su importancia real. Para los dispositivos críticos lo ideal es mantenerlos alejados del personal o de posibles intrusos en salas con una correcta seguridad y control de acceso, así como con temperatura y otras condiciones óptimas y siempre que sea posible monitorizadas. Para los dispositivos menos críticos puede ser más interesante el mantenerlos más cerca del usuario final en armarios cerrados o en racks bajo llave teniendo en cuenta lo que antes hemos indicado para este tipo de sistemas.

5.15. Cableado eléctrico

Debemos tener en cuenta como consultores en seguridad física el cableado eléctrico en dos vertientes principales, las dos relacionadas pero independientes.

La primera de ellas es el cableado que proporciona energía a nuestros sistemas computacionales y dispositivos de red (e incluso otro tipo de dispositivos como impresoras láser o faxes) y que deben de cumplir como mínimo las normas aplicables a este tipo de cableado según el país donde nos encontremos, normalmente el reglamento de baja tensión. Esto implica que los cables no se encuentren cerca de conducciones de agua o gas y otra serie de apartados que se pueden consultar en los reglamentos de baja tensión de cada país. Esto por supuesto es el mínimo admisible. A partir de aquí debemos buscar los posibles fallos que hipotéticamente pudieran producirse dentro del cableado. Por ejemplo hay que estudiar que los enchufes y clavijas donde se conectan los dispositivos cumplen con las normativas aplicables y que no existe peligro de que pueda saltar una chispa entre terminales. Otro punto a estudiar es el diámetro y la calidad del cableado, para lo cual nos puede asesorar un electricista, calculando la potencia máxima que va a consumir un determinado sistema alimentado por un cableado y calculando a partir de ahí la sección y calidad del cable que debe instalarse. Debe sobredimensionarse siempre este factor por las posibles sobretensiones de la red y para prevenir sobrecargas en el cableado si añadimos más dispositivos al sistema. En cualquier caso hay que hacer notar que el cableado no suele

ser problemático y suele estar bien calculado y muy sobredimensionado para la potencia que ha de transportar.

La segunda de las vertientes son las conducciones ajenas a nuestros sistemas computacionales y que puedan afectar negativamente al funcionamiento de estos. Todo el cableado eléctrico, sobre todo el que transporta una gran cantidad de energía eléctrica (soporta mucha potencia) produce trastornos electromagnéticos en su entorno. Los ordenadores y dispositivos de red, e incluso el cableado de red son bastante sensibles a este tipo de alteraciones electromagnéticas, por lo que intentaremos que el cableado ajeno a nuestros sistemas que deba transportar una gran potencia esté lejos de nuestro cableado eléctrico, de red y de los ordenadores y dispositivos de red. Un correcto aislamiento de este cableado puede mitigar este problema en gran medida. En caso de duda siempre podemos consultar a personal especializado que puede realizar mediciones de campo sobre los cables e indicarnos si pueden producir algún tipo de alteración sobre nuestros sistemas.

5.16. Cableado de telefonía

Poco más que añadir sobre el cableado de telefonía. Deberemos observar que el cableado tiene la calidad y esta homologado según la normativa del país donde nos encontremos. Deberemos tener también en cuenta lo dicho en el apartado anterior y mantenerlo lejos del cableado eléctrico que transporte mucha potencia. Por lo demás el cableado de telefonía no suele dar ningún tipo de problemas, más que los puramente físicos como seccionamientos del cable, conectores mal montados o defectuosos y cosas así.

Como con el cableado de red deberemos proteger de alguna forma el cableado de telefonía, para preveer la posible actuación de un intruso malintencionado que pueda seccionar el cable y dejarnos sin comunicaciones. Es fundamental poder comprobar el cableado mediante aparatos fabricados a tal efecto de forma sencilla, para detectar roturas o seccionamientos del cable si tenemos el cable protegido por algún tipo de entubado o integrado en la estructura del edificio.

5.17. Cableado de redes

El cableado de redes es más sensible a las perturbaciones electromagnéticas que el cableado de telefonía, por transportar datos a una mayor frecuencia. Asumimos que estamos hablando de cable tipo ethernet del comúnmente instalado hoy en día. Un caso diferente sería el antiguo cableado coaxial, que se recomienda sustituir por el nuevo cableado ethernet o el cableado de fibra óptica, que no sufre perturbaciones electromagnéticas y que tiene como único punto débil a estudiar su fragilidad, que no permite determinadas instalaciones, así como la mayor complejidad de sus conectores.

En el caso del cableado ethernet normal a 10M o 100M que se suele instalar en las redes departamentales o locales deberemos estudiar el cableado, observando que esté protegido mediante entubado o integrado en la estructura del edificio, además de observar que no se encuentre cercano a conducciones de electricidad de alta potencia que puedan crear interferencias electromagnéticas sobre el cableado de red. Se deberán tomar las medidas precisas para evitar el supuesto seccionamiento del cable

por parte de un intruso malintencionado y un método de comprobación mediante dispositivos de comprobación de redes que nos permita encontrar posibles fallos en el cableado.

Es importante que todo el cableado y los conectores estén homologados, cumplan con la normativa aplicable y sean de la máxima calidad, a día de hoy CAT5 o CAT7.

5.18. Sistemas distribuidos dentro del edificio

Cuando tenemos un sistema informático distribuido dentro del edificio debemos tener en cuenta que el factor más importante que debemos estudiar es la conectividad entre los distintos nodos, lo que implicará un estudio de la red pública (dentro del edificio) o privada que usen para comunicarse, así como los dispositivos de red que usen para su comunicación. Es importante también asegurar la conectividad de los sistemas finales que han de usar los servicios proporcionados por el sistema distribuido, pues si no tenemos conectividad no nos servirá de gran cosa tener el sistema distribuido funcionando. Sobre la conectividad no añadiremos nada más pues es un caso de estudio de una red normal, del cableado de esta y de los dispositivos de red que la componen.

Deberemos realizar un estudio de la seguridad física de cada nodo y de como puede afectar la caída de uno de estos nodos al sistema distribuido, observando si la caída de un nodo provoca la caída del sistema, y entonces buscaremos algún tipo de alta disponibilidad o redundancia en los nodos, o si el sistema puede funcionar con algunos nodos caídos, con lo que el mismo sistema distribuido estará proporcionando la redundancia.

5.19. Llaves, cerraduras y armarios

La seguridad física de los armarios y racks es básicamente la de sus cerraduras y llaves, pues aunque podemos estudiar la fortaleza física del armario es poco probable que un supuesto atacante se ponga a reventar un armario o rack para acceder a su interior. Sobre todo cuando tiene otros métodos para hacerlo...

Las llaves y cerraduras dan una falsa seguridad al administrador de sistemas. La gran mayoría de los armarios y racks que se comercializan tienen cerraduras y llaves muy simples que pueden ser abiertas por cualquiera con un poco de habilidad y el material y los conocimientos necesarios. Solo debe estudiar las varias Lock Picking Guides que existen en Internet y que enseñan como abrir todo tipo de cerraduras, incluso las que tienen varios cilindros. El consultor de seguridad física deberá siempre aconsejar el uso de llaves de varios cilindros, similares a las que se encuentran en las puertas blindadas, que son prácticamente imposibles de abrir mediante técnicas de Lock Picking. Todo lo demás es engañarse, porque la persona que quiera acceder a nuestro armario seguramente tendrá los conocimientos y la habilidad para abrirlo si tenemos cerraduras de un cilindro o dos.

No hay nada mejor para darse cuenta de las implicaciones en seguridad física e informática de las técnicas de Lock Picking que bajarse de internet el documento The MIT Lock Picking Guide o

cualquiera de los documentos de Lock Picking que existen en Internet. Aunque al principio la técnica puede ser complicada y difícil de implementar en una cerradura real puede estar seguro que si un intruso ha decidido aplicar estas técnicas sobre su armario o rack tendrá la práctica y los conocimientos necesarios para tener éxito en su empresa.

La única solución es el adquirir armarios y racks con cerraduras seguras, que tengan al menos tres cilindros o que tengan cerraduras similares a las de las puertas blindadas. Solo esto nos asegurará que ningún intruso podrá acceder a nuestros dispositivos.

5.20. Cámaras de seguridad y su monitorización

Las cámaras de seguridad son un elemento imprescindible si tenemos a nuestro cargo sistemas realmente críticos o sistemas especialmente atractivos para los supuestos intrusos o hackers. Esto incluye todos los sistemas que alberguen datos económicos, números de tarjetas de crédito, datos de clientes o proveedores, datos personales de nuestros clientes, etc. Si tenemos centros de datos que almacenan datos de este tipo o cualquier tipo de datos críticos para el funcionamiento de la empresa o secretos deberemos tener personal de vigilancia contratado. Este personal deberá contar con cámaras de seguridad que les permita monitorizar el edificio ante la posibilidad de intrusos o de actuaciones sospechosas del personal. Lo ideal es tener personal de vigilancia presencial en el centro de datos para el control de acceso y luego personal de vigilancia encargado de la monitorización de las cámaras de vigilancia.

Debemos tener en cuenta las cuestiones relativas a la privacidad de nuestro personal cuando instalemos o aconsejemos instalar cámaras de vigilancia. Normalmente deberemos poner en conocimiento de los empleados la existencia de estas cámaras, su localización y su función de vigilancia.

5.21. Control de ventanas y visibilidad desde el exterior

Uno de los errores en seguridad física más comunes que se suelen observar en entornos reales es la visibilidad desde el exterior de los monitores y teclados de los usuarios que están trabajando dentro del edificio. Esto es un fallo de seguridad física muy importante, pues un intruso malintencionado puede observar desde una ventana o desde el exterior del edificio como el personal teclea sus passwords personales o datos secretos o críticos para la empresa. Este es un caso muy común en las oficinas de los bancos, que suelen estar situadas en las primeras plantas de los edificios y tienen normalmente grandes fachadas de cristal que permiten la visibilidad al interior por parte de cualquier intruso.

La solución es muy sencilla. Basta con elegir la localización de los monitores y teclados fuera del alcance de un supuesto observador exterior. No se aconseja en principio la instalación de cortinillas o sistemas similares si no es imprescindible, porque casi siempre con una recolocación de los escritorios de los empleados o de sus sistemas informáticos basta para proporcionar una seguridad física suficiente en este caso.

5.22. Control de desechos y basura

¿A quien puede importarle nuestra basura? Le preguntará seguramente el jefe de administradores cuando le indique que quiere estudiar la colocación de los contenedores de basura de la empresa y los métodos de destrucción de documentación. A cualquier intruso, deberá responderle usted. Y esto es tan cierto como que se producen continuamente fallos de seguridad en las empresas por medio de hacking social que tienen como origen una mala gestión de los desechos y la basura.

Pensemos solo por un momento lo que puede obtener un posible intruso del contenedor de basura de una empresa: Documentación secreta sin destruir, números y claves de empleado, números de la seguridad social, planos de la empresa o de la red, datos técnicos de la red y de los sistemas informáticos de la empresa, datos sobre los empleados y la estructura administrativa de la empresa, números de teléfono internos, datos sobre la jerarquía administrativa de la empresa, y así hasta el infinito. Datos, datos, datos. Un posible intruso puede usar todos estos datos para realizar todo tipo de hacking social sobre sus empleados y departamentos, usándolos para identificarse mediante llamadas a teléfonos internos y solicitar datos que normalmente no se darían si no fuera porque el interlocutor nos está dando datos que no debería saber si no trabajara en la empresa. Este tipo de ataques de hacking social son cada vez más comunes y deben ser una preocupación principal para un consultor de seguridad física.

Hay que ser tajantes con este tema. Todos los documentos internos de la empresa deben de ser destruidos mediante máquinas que existen para esta tarea. Debe elegirse máquinas que destruyan totalmente los documentos, nada de tiras gruesas de papel que pueden volver a unirse con suficiente paciencia, cuanto más destruidos queden los documentos mejor. La incineración de los documentos es por supuesto la opción ideal. Además debe de crearse una política de destrucción de documentación que todos los empleados deberán cumplir, responsabilizándose cada uno de los datos y documentación que desechen.

6. La seguridad física del hardware

La seguridad física del hardware es el último punto a estudiar por un consultor de seguridad física. En nuestro método de ir de lo global a lo específico llegamos ahora a la parte más específica del sistema, al propio hardware. Aquí la seguridad física se torna más ardua, puesto que los sistemas informáticos suelen estar cercanos al usuario final o al mismo administrador, por lo que están expuestos a un mayor peligro de mal uso o uso malintencionado. Puesto que aquí no podemos confiar plenamente en el cumplimiento de políticas o normativas de uso de las máquinas y como estas máquinas están más expuestas a intrusos ajenos al personal de la empresa que hayan superado los controles de acceso de niveles superiores debemos configurar estas máquinas y dispositivos de red de forma que sea lo más complicado posible el realizar manipulaciones sobre ellos, tanto a nivel físico como a nivel informático siempre que sea posible.

6.1. Acceso físico a las máquinas y dispositivos de red

Es inevitable que el personal tenga acceso físico a las máquinas sobre las que deben trabajar, y en

algunos casos incluso a los dispositivos de red. Cuando el usuario debe usar el hardware directamente, como usando disqueteras, CDROMs o similares la máquina que alberga estos dispositivos debe estar cercana al usuario. Lo mismo es aplicable para los servidores y dispositivos de red y los administradores de sistemas, para poder realizar su trabajo tienen que tener normalmente acceso físico a los dispositivos de red.

Teniendo en cuenta este factor debemos intentar mediante el estudio de la red y de las aplicaciones que han de correr los usuarios finales el mantener al menos los servidores y los dispositivos de red lejos del usuario final, en racks, armarios o centros de datos. Los usuarios podrán acceder a sus datos a través de la red local y mantener los datos importantes a salvo, aunque el hardware donde van a trabajar este desprotegido por estar en su puesto de trabajo. Los sistemas NAS y otros sistemas de almacenamiento de datos o servidores de aplicaciones pueden ayudar en esto.

Por tanto la idea es mantener al menos los datos y el trabajo del usuario fuera de la máquina donde el usuario va a trabajar. Deberemos instar al personal de administración para que organice el sistema de forma que los usuarios finales trabajen directamente sobre servidores de ficheros y servidores de aplicaciones, manteniendo así los datos a salvo de errores o manipulaciones del hardware. Bien estudiado este sistema puede suponer un ahorro adicional en hardware en las estaciones de trabajo del usuario final, que podrán ser menos complicadas en su constitución y más sencillas de administrar.

6.2. Racks y armarios

Sobre los racks y armarios ya hemos hablado bastante. Tengamos en cuenta todo lo que hemos comentado sobre su entorno, su localización y las consideraciones que debemos tomar para su adquisición y montaje. Además de todo esto debemos tener en cuenta que estos armarios y racks deben contener máquinas y dispositivos de red, y que esto implica otro nivel de seguridad física que debemos estudiar. En concreto deberemos estudiar que máquinas se incluyen en que racks y lo mismo para los dispositivos de red. Esto evitará que un supuesto intruso o usuario malintencionado que intente reconectar las máquinas o dispositivos del rack para realizar acciones no permitidas lo tenga más difícil. Si mantenemos en un rack los servidores de ficheros, en otro los de aplicaciones y en otro los dispositivos de red tendremos la seguridad de que un supuesto intruso no podrá trucar nuestra red para acceder con los permisos de unas máquinas a otras.

Hay que tener especial cuidado con los racks que contienen dispositivos de red, pues con la actual tendencia a construir VLANs por medio de concentradores que implementan este servicio podemos tener el peligro de que un usuario realice cambios en el cableado de red y tenga acceso a redes a las que no debería tener acceso. Es muy importante también el proteger en los concentradores los puertos donde se pueden conectar sniffers de red, pues proveen a un supuesto intruso de un arma imbatible para obtener datos de nuestra red. Lo mismo es aplicable a las conexiones serie que puedan tener estos dispositivos y que nos permitan la administración remota de los dispositivos, pues la seguridad del control de acceso en estos puertos no suele ser tan fuerte como cuando se accede mediante telnet o interface web.

6.3. Las cajas de las computadoras

Las cajas de las computadoras suelen ser un quebradero de cabeza para todo consultor de seguridad física, porque nos vienen impuestas por el hardware que se ha adquirido y es difícil el convencer a una empresa de que las cambie por otras más seguras.

La caja normal de una computadora no provee ningún tipo de seguridad contra un supuesto acceso a su interior por un intruso, todo lo contrario, cada vez se hacen más fáciles de abrir... Hay varias soluciones que se pueden aplicar para mejorar la seguridad de estos sistemas. La primera y más simple sería el sellado de la caja, que al menos nos alertará si algún intruso ha accedido a su interior. Deberá instruirse al personal de mantenimiento para que ponga y quite los sellos cuando tengan que realizar algún tipo de manipulación dentro de la caja. Otra solución es el taladrar y poner un candado o sistema similar en la caja que impida su apertura, aunque esto es difícil, puesto que lo que suele buscar un supuesto intruso son los datos contenidos en el disco duro, y para eso con abrir parcialmente la caja le basta. Se puede sellar con silicona los tornillos de la caja o todo el borde de la tapa para impedir su apertura, pero esto será un problema si tenemos que realizar cualquier tipo de mantenimiento dentro de la caja. Otra opción más radical todavía (pero no inverosímil) es la soldadura de la tapa de la caja con el armazón, esto asegurará la seguridad de la caja, pero si hay que realizar algún tipo de mantenimiento...

Otra opción es la adquisición de cajas más seguras. Varias compañías venden cajas que tienen cerraduras y sistemas de anclaje de la tapa con el armazón que proporcionan una seguridad considerable contra intrusos. Aquí el único punto débil es la cerradura, que deberá ser segura, como ya indicamos anteriormente. También se puede usar cajas de metacrilato fabricadas a medida para nuestros sistemas. Estas cajas se pueden obtener de varios fabricantes con cualquier tipo de características, sobre todo si encargamos la suficiente cantidad, y pueden estar protegidas mediante llaves contra su apertura. El metacrilato es muy resistente si es lo suficientemente grueso y permite dejar aperturas para el uso de CDROMs, disqueteras y similares. Es una opción engorrosa y difícil de mantener, por lo que se optará siempre que se pueda por cajas seguras antes que por sistemas hechos a medida.

Todas estas opciones son parches para el problema principal, que es el mantener datos importantes en una máquina expuesta al usuario final y a posibles intrusos. La opción correcta es mantener estos datos en lugar seguro (un servidor de archivos dentro de un armario o rack) y que el usuario trabaje de forma remota sobre estos datos, con lo que la seguridad física del ordenador del usuario final será poco importante.

6.4. Seguridad del bios. Password de bios

La seguridad que proporcionan las passwords de bios es una seguridad absolutamente ficticia. Muchos administradores confían ciegamente en la seguridad de los sistemas asegurados mediante passwords de bios, sobre todo cuando se intenta impedir el arranque desde disquetera o desde CDROM. Esto es un grave error. La seguridad que proporciona el password de bios es mínima si no tenemos una seguridad física suficiente sobre el sistema en cuestión. Si un intruso consigue abrir la caja del ordenador puede simplemente activar el puente de borrado de la bios y nuestro password se borrará, o puede simplemente

llevar un bios igual al del ordenador en cuestión y montarlo en el zócalo. Incluso se han dado casos de llegar a desoldar el bios de un ordenador y soldar el nuevo para saltar el password.

Por todas estas técnicas y por muchas otras que existen simplemente no debemos confiar en los password de bios. Si alguien tiene acceso al interior de nuestra máquina podrá hacer lo que quiera con ella. Puede borrar el bios, cambiarlo por otro, instalar una disquetera o un CDROM, una grabadora de CDs, cualquier cosa. La seguridad física de la caja por tanto es fundamental si queremos asegurar que la configuración de la máquina no va a ser cambiada.

No nos cansamos de decirlo. Si tiene datos importantes manténgalos alejados de las máquinas de usuario o de cualquier máquina a la que pueda tener acceso un intruso malintencionado. Es la única forma de mantener sus datos a salvo.

6.5. Equipamiento hardware de las máquinas

Habiendo comentado ya el problema que existe con la poca seguridad que proporciona el bios de los ordenadores el equipamiento hardware que implementemos en la máquina no va a proporcionarnos más seguridad. No vale que no instalemos disquetera ni CDROM ni grabadora de CDs, y que deshabilitemos en el bios la detección de estos. Si alguien tiene acceso físico al interior de la caja del ordenador siempre podrá cambiar el bios y luego instalar su propia disquetera, CDROM o grabadora de CDs, por no hablar del acceso directo al disco duro, que puede sacar, clonar con herramientas como Norton Ghost y luego volver a dejar en su sitio sin que nadie se de cuenta de que se ha replicado la información de la máquina.

Por lo tanto la ausencia de hardware en las máquinas no proporciona una seguridad mayor a las máquinas. Puede proporcionarla contra el intruso sin el tiempo suficiente para realizar cambios en el bios, pero si el intruso tiene suficiente tiempo podrá instalar su propio hardware y hacer lo que desee con nuestra máquina.

6.6. Acceso al interior de los equipos

Hemos tratado ya el acceso al interior de las cajas de los ordenadores, que es un tema complicado. Más complicado aun es el acceso a los equipos de red, sistemas servidores de archivos, sistemas NAS, sistemas servidores de aplicaciones y similares. Estos equipos normalmente no son modificables, y suelen venir con cajas muy poco resistentes y poco preparadas para aguantar el maltrato al que un supuesto intruso podría someterlas. En la mayoría de los casos estos sistemas son de fácil apertura, pues suelen ser ampliables y se busca siempre una fácil ampliación, lo que es bueno para el personal de mantenimiento y administración, pero malo para nosotros como consultores de seguridad física.

La repercusión sobre la seguridad de la apertura de un NAS (Servidor de Almacenamiento) puede ser desastrosa. Todos los datos de trabajo de la empresa pueden quedar a disposición de un intruso. Muchos de estos sistemas tienen discos duros estándar, que pueden ser replicados con un portátil mediante Norton Ghost o similares y devueltos al sistema NAS sin que nadie detecte lo que ha ocurrido. Esta es la

pesadilla de un administrador de seguridad, todos sus datos replicados sin haber dejado ninguna pista. Lo mismo es aplicable para otro tipo de servidores, y algo similar ocurre con los dispositivos de red, que pueden ser alterados una vez abiertos para cambiar la configuración, borrar las claves de acceso y muchas manipulaciones similares.

Insistimos. Lo único que nos salvará de este tipo de ataques de fuerza bruta (nunca mejor dicho) es el mantener este tipo de máquinas críticas protegidas en racks cerrados, en armarios bajo llave o en centros de datos con control de acceso. No hay más magia que esta, no busque soluciones esotéricas a problemas ya solucionados.

6.7. Redundancia de máquinas y sistemas de almacenamiento

Al igual que insistimos en mantener los datos en lugar seguro lejos del usuario final o de un supuesto intruso no podemos dejar de insistir en la necesidad de redundancia o alta disponibilidad en los sistemas críticos y en las máquinas que proporcionen almacenamiento. Es fundamental poder acceder a los datos siempre que sea necesario, y la única forma de asegurar con un porcentaje aceptable de seguridad que nuestros datos estarán disponibles es proveer algún tipo de redundancia para estos datos.

Lo más aconsejable para este tipo de sistemas es la instalación de sistemas de alta disponibilidad, donde varias máquinas proporcionan la misma funcionalidad y se sincronizan permaneciendo siempre todas en el mismo estado. Si la máquina que está proporcionando el servicio falla otra de las máquinas del clúster ocupa su lugar y el sistema puede seguir funcionando. Normalmente el sistema avisa a los administradores de este tipo de eventos para que solucione el fallo en la primera máquina. Con un cluster de dos o tres máquinas proporcionando la misma funcionalidad podemos obtener tasas de fiabilidad muy altas, sobre todo cuando hablamos de integridad de datos. La replicación de los datos de un servidor de archivos principal en otros servidores de archivos secundarios (preferentemente alojados en otro edificio) es otra opción recomendable para proporcionar seguridad física en los sistemas de almacenamiento o en servidores de aplicaciones. La diferencia con los sistemas de alta disponibilidad es que estos sistemas no se sustituyen unos a otros automáticamente, solo mantienen una copia de los datos a buen recaudo en otro servidor por si es necesario acceder a ellas. Si puede instale un sistema de alta disponibilidad. Pero si su presupuesto no se lo permite programe copias de seguridad en servidores localizados lejos del servidor principal a través de la red para no perder nunca datos.

Siempre existe la posibilidad de que un intruso se apodere de uno de los sistemas y obtenga los datos de esa máquina, por lo que la seguridad física e informática de este tipo de máquinas es crítica.

6.8. Sistemas de backup

Los sistemas de backup son una necesidad inexcusable hoy en día en cualquier empresa que maneje una cantidad de datos medianamente grande. Teniendo esto en cuenta y suponiendo que disponemos de un sistema de backup fiable debemos tener en cuenta otra serie de consideraciones.

La primera es la seguridad física de los backups, de la que ya hemos hablado, y para la que optábamos como mejor solución la que aconsejaba mantener los backups lejos de los sistemas que contienen los datos de los que hemos hecho backup.

La segunda es la seguridad física de las máquinas de backup, para las que deberemos tener las mismas medidas que para los servidores de archivos: Mantener más de una máquina de backups, sistema centralizado de backups alojado en un rack o armario seguro, monitorización de las máquinas de backup, etc.

Una cuestión a tener en cuenta con los sistemas de backup es la seguridad física de los medios donde se realizan los backups. Las cintas de backup pueden ser afectadas por los campos magnéticos fuertes, los discos ZIP también, los discos duros fallan y soportan mal los golpes y los movimientos bruscos y los CDs tienen una vida corta y son más bien delicados. Deberán tomarse las medidas necesarias para proteger físicamente los medios donde se realizan los backups, teniendo en cuenta las consideraciones propias para cada medio. Tradicionalmente los medios más seguros para hacer backups han sido las cintas de backup y cintas DAT, pero esto siempre puede cambiar.

De nada sirve hacer backups si cuando los necesitamos no funcionan. Debemos comprobar que los backups que hemos realizado pueden ser restaurados correctamente, o estaremos confiando en un sistema que no podemos asegurar que funciona correctamente.

6.9. Sistemas UPS

Los sistemas UPS son imprescindibles en la seguridad física de un sistema informático. La mayoría de los sistemas operativos responden mal a las caídas repentinas y puede producirse perdida de datos importantes si no se usan sistemas de archivos con Journaling como Ext3, Reiserfs, XFS, JFS o similares.

Es complicado decir que es más conveniente, si mantener un gran UPS que alimente un grupo de máquinas, por ejemplo un rack o un armario con muchos dispositivos o si tener varios UPS que proporcionen alimentación a menos máquinas. El UPS puede convertirse en un punto del fallo del sistema, pues si falla todo el sistema se vendrá abajo. Los grandes UPS suelen ser más seguros, proporcionan mayor autonomía y protección, pero en el hipotético caso de que fallen nos dejan con todo el sistema caído. Los UPS más pequeños no tienen tantas características pero cumplen bien su cometido. El presupuesto también será un punto a tener en cuenta para la elección de una u otra opción, pues un gran UPS es bastante más caro que varios UPS pequeños.

Es importante ubicar los UPS dentro de los racks o armarios, donde no puedan ser desactivados por un supuesto intruso o por un fallo de un usuario o administrador.

6.10. Redundancia a nivel de hardware

Igual que aconsejamos la redundancia a nivel de máquinas para todo el sistema en general debemos aconsejar también la redundancia a nivel interno de hardware. Hoy existen ordenadores que incorporan dos fuentes de alimentación, varios discos duros montados en RAID, e incluso dos placas base. Los dispositivos de red también incorporan redundancia en una forma similar. Todo este tipo de funcionalidad es muy beneficiosa para la seguridad física del sistema en general, pues permite que parte del hardware falle sin que el sistema caiga. Debemos tener en cuenta que este tipo de sistemas son caros, y que a veces los sistemas de alta disponibilidad construidos con varias máquinas pueden ser igual de eficientes y más económicos que los sistemas redundantes a nivel de hardware.

El caso del RAID es diferente. Hoy por hoy cualquier servidor corporativo debería incorporar algún tipo de RAID, ya sea RAID 0, RAID 1 o RAID 5, sobre hardware o sobre software. Con el precio continuamente decreciente de los discos duros podemos permitirnos un sistema de RAID basado en software sobre un sistema IDE por un precio realmente bajo, y esto nos proporcionará redundancia en el hardware sin aumentar excesivamente el presupuesto.

6.11. Redundancia a nivel de red y conectividad

La redundancia a nivel de red, incluida la conectividad a redes públicas como Internet o a redes corporativas privadas entre empresas debe ser hoy en día una de las mayores preocupaciones de un consultor de seguridad física. La mayoría de los tiempos muertos que se producen en el trabajo diario en la mayoría de las empresas se deben a fallos en la red o en la conectividad a Internet. Esto es especialmente crítico cuando hablamos de terminales de usuario final que permiten el trabajo remoto sobre servidores empresariales, como es el caso de los nuevos terminales implantados en bancos, sistemas de pago o facturación e incluso aplicaciones remotas tipo Citrix y similares.

Deberemos estudiar en primer lugar la conexión global a las redes públicas como Internet o en su caso si esta existe la conexión privada que entre distintos edificios o departamentos de la empresa existan. Para garantizar la conexión a Internet o una conexión privada sobre redes públicas no hay mejor consejo que la utilización de diferentes medios de conexión a la red mediante diferentes proveedores. El número de conexiones redundantes y el número de proveedores que deberemos contratar dependen enormemente del tiempo que podamos permitirnos tener la red sin conexión. Para asegurar una conexión normal en una empresa suele bastar la contratación de dos lineas independientes con dos proveedores diferentes, mediante ADSL/DSL, cable o lineas dedicadas. Deberemos estudiar al contratar el servicio la seguridad que nos ofrece la compañía en cuestión sobre la disponibilidad del servicio. En las lineas ADSL normales el contrato que se suscribe suele especificar que la compañía puede mantener sus lineas caídas durante un cierto espacio de tiempo sin que por ello tenga que indemnizar al usuario final por ello. Deberemos huir de este tipo de contratos, buscando contratos que aunque sean más caros nos aseguren una cierta disponibilidad de la conexión, o al menos que incluya indemnizaciones por cortes de conexión, lo que redundará en una mayor implicación del proveedor de conexión en asegurar la conectividad.

Es importante comprobar que las redes físicas sobre las que contratamos los proveedores sean diferentes,

pues es bastante común que los proveedores de conectividad a Internet usen el mismo cableado de una compañía, sea esta pública o privada. En este caso tendremos un punto de fallo importante a tener en cuenta, pues si hay un problema en el cableado las dos lineas contratadas quedaran inutilizadas. En casos muy críticos puede ser incluso necesario la contratación de lineas privadas o enlaces propios de la empresa, como conexiones entre edificios mediante microondas. Los enlaces de microondas son una forma segura de comunicación entre edificios corporativos y son cada vez más usadas por las empresas, aunque debemos tener en cuenta que son caras, que necesitamos tener visibilidad entre las sedes que queremos comunicar y que necesitaremos gran cantidad de permisos para obtener la licencia de emisión. Una vez funcionando los enlaces de microondas pueden ser controlados por la misma empresa o por una empresa contratada y son fiables y resistentes a condiciones climáticas adversas o situaciones similares.

La idea general para proporcionar la conectividad a redes públicas o privadas dentro del edificio es mantener más de una opción de conectividad, de forma que si una falla tengamos otra u otras disponibles para mantener las conexiones. Siempre es posible mantener lineas privadas que suelen ser caras y complementar estas con lineas públicas como el ADSL/DSL/Cable para soportar el tráfico que pueda producirse si la linea principal cae. Existen sistemas de enrutadores que pueden utilizar todas las conexiones que tengamos disponibles al mismo tiempo, proporcionando un gran ancho de banda, pero que pueden seguir funcionando si alguna de las conexiones cae.

Para las redes departamentales y locales deberemos buscar también una cierta redundancia en la conexión con la red troncal de la empresa y por tanto con los enrutadores que proporcionan la conectividad con el exterior. Puede ser interesante mantener varias conexiones con varios concentradores en cada planta con la red troncal que permitan el fallo de uno de estos y mantengan las conexiones.

Es importante que la red local pueda funcionar siempre que sea posible independientemente de la conexión a la red troncal. Es difícil encontrar el punto medio donde los sistemas estén centralizados y comunicados por la red troncal y a la vez mantener una serie de servicios indispensables en la red local que puedan funcionar al menos durante espacios cortos de tiempo sin conexión con la red troncal. Esto tiene como hemos visto más arriba implicaciones en la seguridad física, pues cuanto más cerca del usuario final se encuentren los servidores de archivos o de aplicaciones más posibilidades existen de que estos sean manipulados o de que puedan fallar.

El sistema ideal por tanto permitiría el funcionamiento de las redes departamentales durante un periodo de tiempo razonable que permita fallos en la conectividad con la red troncal y con las redes exteriores y que a la vez tenga una seguridad física e informática importante. Puede ser necesario aconsejar la instalación de sistemas de almacenamiento de datos y servidores de aplicaciones que puedan funcionar en modo autónomo dentro de los departamentos y que luego repliquen esta información siempre que la red esté disponible con los servidores principales de la empresa. Lo mismo es aplicable a los sistemas de backups, que pueden realizarse a pequeña escala dentro de los departamentos y luego realizarse globalmente dentro de la empresa usando la red troncal. Los sistemas de archivos que pueden funcionar en modo desconectado, como Coda, Intermezzo o similares son muy útiles en estos casos, pues permitirán trabajar cuando la red está desconectada y replicarán automáticamente los datos cuando exista conexión con los servidores principales.

6.12. Alojamiento físico de las máquinas

Hemos hablado ya bastante sobre el alojamiento físico de las máquinas principales que proporcionan los servicios críticos de la empresa, incluidos los servidores de archivos, los servidores de aplicaciones, los sistemas de backup y todas las máquinas que proporcionan seguridad informática a la empresa, como firewalls, detectores de intrusos y similares. Ahora vamos a ir un poco más allá hablando sobre las máquinas que están más cerca del usuario final, como los equipos de escritorio y los concentradores departamentales.

La regla a aplicar en este caso es la misma que hemos aplicado para los demás sistemas. Cuanto menos acceso tenga el usuario final a las máquinas sobre las que tiene que trabajar y que contienen los datos sobre los que trabaja y su propio trabajo, así como los dispositivos de red local como concentradores y similares, mejor para la seguridad física. Idealmente se alojarán todas las máquinas a las que no deba acceder físicamente el usuario final en racks y armarios, o se implantarán sistemas de trabajo remoto sobre servidores de aplicaciones como Citrix y similares. Esta última opción es la ideal, porque permite al usuario trabajar en su estación de trabajo que no debe tener una seguridad física estricta y mantener los datos sobre los que trabaja y su propio trabajo en los servidores principales de la empresa, que estarán correctamente protegidos en el apartado de seguridad física. Este tipo de sistemas permite además mantener hardware menos potente en los escritorios de los usuarios y mejora la administración y la gestión de datos y backups para los administradores. Estos sistemas actúan básicamente como los antiguos terminales X o terminales de texto, y son cada vez más usados en todo tipo de empresas, sobre todo en bancos o sistemas financieros donde la seguridad de los datos que se maneja es crítica y el usuario final debe tener el mínimo de acceso a los datos que maneja. Es muy común hoy en día el uso de aplicaciones que corren sobre navegadores web y que usan servidores de aplicaciones y bases de datos para acceder a los datos necesarios para realizar el trabajo. Cualquiera de estas soluciones es buena y debe ser aconsejada siempre que sea económicamente y administrativamente posible.

Para los dispositivos de red lo mejor es alojar estos dispositivos como ya hemos comentado en armarios o racks. Deberemos estudiar el cableado de forma que no exista la posibilidad de que este sea seccionado o desconectado. Por lo demás no tendremos mayores consideraciones con los dispositivos de red, únicamente si estos deben obligatoriamente estar alojados cerca del usuario final (personal que debe realizar pruebas con la red o realizar cambios en el cableado) protegeremos los dispositivos contra manipulaciones remotas limitando el acceso por medio de claves suficientemente seguras. También es posible en algunos dispositivos el activar o desactivar parte de su funcionalidad para limitar el acceso que el usuario final tiene a estos dispositivos.

6.13. Control de calidad de las máquinas y dispositivos de red

El control de calidad de las máquinas y los dispositivos de red debe estar basado en dos premisas. La primera es la adquisición de equipos certificados y donde el fabricante nos asegure que se han realizado las pruebas de estress suficientes sobre ellos para garantizar su calidad. La segunda es la monitorización de estos equipos y la estimación de la vida útil y el tiempo medio de fallos en los mismos.

La adquisición de los servidores, los equipos de usuario final y los dispositivos de red dentro de una

empresa debe estar regida en primer lugar por la calidad de estos. A medio y largo plazo lo barato sale caro cuando estamos hablando de hardware. Para ordenadores elegiremos máquinas de fabricantes que entreguen equipos completos preconfigurados y probados en la cadena de montaje, esto es fundamental, porque los equipos montados adhoc usando piezas de varios fabricantes es más posible que fallen por la interacción entre los distintos componentes que no ha sido probada por la variedad de hardware existente. Estos equipos son más caros que un equipo montado (usualmente llamados clónicos) pero nos aseguran una certificación de que el hardware que contienen trabaja correctamente en conjunto y han sido sometidos a una serie de pruebas de funcionamiento para comprobarlo. Es importante estudiar el hardware que se va adquirir cuidadosamente, incluyendo la posibilidad de adquirir equipos con una cierta seguridad física implementada, como dobles fuentes de alimentación, controladoras RAID o cajas con una cierta seguridad física. Es aconsejable realizar una inversión un poco mayor al adquirir este hardware porque a medio y largo plazo esta inversión se verá recompensada en un mayor tiempo entre fallos y una mayor fiabilidad de los equipos.

Las máquinas servidoras que se han de montar en rack suelen venir con certificación de su funcionamiento, así que sólo deberemos preocuparnos de las características de estas y de elegir un fabricante que distribuya los equipos preconfigurados y probados en la cadena de montaje. En estas máquinas debemos realizar toda la inversión económica que nos sea posible, porque estos equipos son críticos para el funcionamiento del sistema y una mayor inversión en estas máquinas redundará en mayor tiempo entre fallos y por tanto en un mejor aprovechamiento del trabajo. Un servidor que se viene abajo puede dejar a un grupo de usuarios sin posibilidad de trabajar, lo que supone una cantidad considerable de dinero perdido para la empresa, así que lo que invirtamos en el hardware de los servidores lo recuperaremos a medio y largo plazo en forma de menores tiempos de paro del sistema y en una menor inversión en mantenimiento. Es importante que estas máquinas tengan todos los sistemas de redundancia y seguridad que nos podamos permitir, incluyendo si lo encontramos más conveniente la instalación de sistemas de clusters de alta disponibilidad que proporcionen los servicios aunque algunas de las máquinas caiga. Debemos tener en cuenta que el hardware falla, es algo que ocurrirá tarde o temprano, y por tanto toda la redundancia que tengamos en los dispositivos críticos será dinero bien invertido.

Los dispositivos de red deben ser elegidos entre los principales fabricantes de estos dispositivos. Es posible encontrar dispositivos más baratos de pequeños fabricantes o de fabricantes de dispositivos de gama baja, pero a medio y largo plazo la inversión que realicemos redundará en un menor tiempo de fallos y un mantenimiento menor. Elegir los dispositivos entre los grandes fabricantes nos asegurará que estos dispositivos han sido probados tanto en la fábrica como en miles de instalaciones reales hasta la saciedad, y nos permitirá solucionar los problemas que podamos tener con ellos fácilmente, pues existe una comunidad muy amplia de usuarios que pueden ayudarnos a través de las news o las listas de correo y permitirá al personal de mantenimiento mantener los equipos más fácilmente. Es aconsejable incorporar cuantos más equipos del mismo fabricante podamos mejor, pues el mantenimiento será mas sencillo y las facilidades de soporte y asistencia técnica estarán a cargo de una única empresa, a la que podremos acudir cuando tengamos algún problema. En cambio si tenemos dispositivos de muchos fabricantes mezclados en nuestra red tendremos que recurrir a varias empresas para su mantenimiento y servicio técnico, lo que supone más tiempo de administración y por lo tanto más dinero gastado.

En general podemos concluir que la calidad de las máquinas y dispositivos de red son directamente proporcionales a su precio. No podemos llevarnos a engaño, podemos encontrar gangas de dispositivos muy fiables por precios asequibles, pero si tenemos un sistema crítico sobre el que debemos realizar

consultoría de seguridad aconsejaremos la instalación de los mejores equipos que podamos permitirnos, con la mayor redundancia, las mejores certificaciones y el mejor servicio técnico posibles. Siempre suele ser posible encontrar un punto medio entre el presupuesto que se quiere dedicar a instalar hardware y la calidad del hardware que vamos a aconsejar, es trabajo del consultor el distribuir estos recursos de forma que los dispositivos más críticos sean los de mayor calidad, compensando con una calidad algo menor en los dispositivos menos críticos. Para elegir que dispositivos corresponden a cada grupo deberemos estudiar el sistema en su conjunto, el uso que se va a realizar de él, los puntos de fallo y la repercusión que un supuesto fallo en el hardware tendrá en la productividad de la empresa, que es al final lo que debemos proteger.

Otro aspecto donde el consultor debe ser inflexible es en la monitorización del hardware, sobre todo de los servidores y de los dispositivos de red. Se recomendará la adquisición de software de monitorización de redes y de hardware que permita esta monitorización. Para el hardware el sistema más común de monitorización es el SNMP, que permite mediante software como Netview de HP la monitorización del estado del hardware, de como está funcionando y de los parámetros que puedan afectar al tiempo medio entre fallos de este hardware. La monitorización del hardware es un punto que se suele olvidar en la seguridad física y que es fundamental, porque nos permite predecir fallos antes de que estos se produzcan o detectarlos inmediatamente cuando estos se producen, porque no podemos engañarnos, tarde o temprano cualquier hardware fallará, y es fundamental que estemos preparados para este fallo. Para el caso de que el fallo se produzca lo único eficaz es contar con una política creada para la sustitución o mantenimiento del hardware de la forma más rápida y eficaz, política que debemos crear antes de que se produzca el fallo, puesto que cuando el fallo se produce el descontrol que se produce puede llevarnos a un mayor tiempo de caída del sistema si no tenemos muy claro los pasos a seguir para sustituir o mantener un determinado sistema hardware.

6.14. Control y seguridad de portátiles

Para el consultor de seguridad física los portátiles no suelen ser un gran problema, al menos no mayor que cualquier otra máquina del sistema, pero para la seguridad informática los portátiles son un verdadero quebradero de cabeza.

Comenzamos con la seguridad física. Debemos tener en cuenta la portabilidad de estos dispositivos, lo que los hace susceptibles de ser robados con facilidad, sobre todo cuando se encuentran fuera de la empresa. Debe crearse una política de uso y responsabilidad para las personas que utilizan ordenadores portátiles de la empresa y sobre todo para las personas que tienen que llevarse estos dispositivos fuera de la empresa. Lo más importante, aparte del valor económico de los portátiles, son los datos que pueden contener, datos que en muchos casos pueden ser importantes e incluso vitales para la empresa. Por eso debe responsabilizarse seriamente a los usuarios de los portátiles que sacan de la empresa, manteniendo un control de entradasalida de estos dispositivos y de la integridad física de los mismos. En caso de robo el usuario debe comunicar con absoluta inmediatez a la empresa el evento que se ha producido, para que esta pueda minimizar los riesgos que implica el robo de los datos que ese portátil pueda contener. Como regla general los portátiles que deban abandonar la empresa no deberían contener ningún tipo de dato importante o comprometido para la empresa, en caso de que el usuario necesite acceso a estos datos pongamos desde su domicilio particular puede ser más conveniente la instalación de una linea ADSL/DSL/Cable y que conecten de forma segura a los servidores de la empresa y trabajen de forma

remota. Si el usuario debe de usar estos dispositivos en otras empresas o en trabajos de campo deberán protegerse de todas las formas posibles los datos críticos que puedan contener, encriptándolos con sistemas seguros y permitiendo sólo el acceso al trabajador por medio de claves intransferibles de las que este deberá ser responsable.

Como el equipo está en manos del usuario y además alejado de la empresa y por tanto de los administradores y encargados de seguridad el hardware tiene muchas posibilidades de ser manipulado. El usuario puede conectar todo tipo de dispositivos a él, puede sacar el disco duro y replicarlo o cambiarlo por otro, puede modificar el hardware por medio de tarjetas PCMCIA (PCCARD) y mil cosas más. La única solución es la responsabilización de forma seria del usuario de la integridad física de la máquina, teniendo una política muy clara de lo que el usuario puede hacer o no hacer con el ordenador.

Otro punto a tener en cuenta y que no es el tema de este documento es la seguridad informática. Aquí los administradores de sistemas tienen un verdadero problema, puesto que los portátiles que salen de la empresa suelen volver a ella repletos de virus, software no deseado, errores cometidos por el usuario o simplemente con programas y datos borrados. Para protegerse de este tipo de eventos hay dos soluciones, una de ellas es el adquirir software antivirus, firewalls personales, software de control de acceso al portátil que impida la instalación de software y medidas similares; la otra opción es el control a la salida del portátil de su contenido por medio de un backup, que se volverá a comprobar cuando el portátil vuelva a la empresa para comprobar la integridad de los datos. Estos métodos proporcionarán una mínima seguridad, aunque siempre estaremos expuestos a todo tipo de manipulaciones del software.

6.15. Keycatchers y otros sistemas de captación de datos

Aunque este tipo de dispositivos son poco usados hoy en día por su fácil detección debemos hacer un estudio al menos básico de que no existan ningún tipo de aparatos de este tipo ni en las máquinas de usuario ni en la red.

Los keycatchers son dongles que se interponen entre el teclado y el ordenador para captar las pulsaciones del usuario, grabando los datos que se introducen, buscando sobre todo la adquisición de claves que el usuario pueda teclear. Son dispositivos aparatosos y fáciles de detectar, aunque también son fáciles de instalar y volver a quitar. Un dispositivo de estos simplemente instalado diez minutos en la máquina de trabajo del personal de un banco puede proporcionar al hacker las claves para acceder al sistema interno de la empresa, números de tarjetas de crédito, números de cuenta y otro tipo de datos secretos. Esto es desastroso para la empresa, así que deberá estudiarse las conexiones entre teclado y ordenador para detectar estos dispositivos, aunque como hemos dicho cada vez son menos comunes y poco útiles para un supuesto intruso.

Hay muchos otros sistemas de captación de datos. Desde dispositivos que se intercalan en el cable de red y graban los datos en bruto que luego se pueden decodificar y estudiar (estamos hablando de hacking casi a nivel militar, no se asusten) hasta simplemente un intruso conectando un portátil a un puerto de un switch que replique todo el tráfico y un sniffer para obtener los datos y passwords que circulen a través de la red. Este tipo de dispositivos pueden ocultarse en la empresa y permanecer inadvertidos mandando datos al hacker que los ha instalado durante cierto tiempo, por lo que deberán ser una preocupación. Otro

tipo de dispositivos temibles son los que captan datos de redes wireless, que pueden decodificar el sistema de encriptación WEP y hacer sniffing de la red obteniendo datos y passwords. A nivel militar existen dispositivos de captación de datos mucho más sofisticados, que pueden incluso captar las comunicaciones de un cable sin tener conexión física con este, simplemente con el campo magnético que genera y cosas así, pero no son dispositivos de los que debamos preocuparnos a no ser que seamos una agencia gubernamental o la sede de una multinacional.

6.16. Concentradores, bocas de red y conectividad

Los concentradores y las bocas de red suponen un peligro inmediato de seguridad física, pues cualquier intruso con un portátil o un aparato de mano con una tarjeta compactflash de red puede conectar a cualquiera de ellas y probablemente obtendrá una dirección IP y conexión a la red interna de la empresa. Debemos estudiar por tanto las bocas de red que no estén ocupadas (y las que estén ocupadas y puedan ser desconectadas y usadas) y los concentradores que tengan conexiones libres. Para el caso de los concentradores el mantra es el mismo de siempre, deben estar en armarios o racks cerrados donde solo los administradores de red tengan acceso a ellos. Para las bocas de red es más complicado. Si tenemos una red fija y no tenemos perspectivas de tener que instalar nuevas máquinas a menudo lo más aconsejable es desconectar todas las bocas de red que no estén siendo usadas para que nadie pueda conectar a ellas. Si tenemos que instalar una nueva máquina o necesitamos otra boca de red vamos al rack y conectamos el cable que da conectividad a la boca de red en cuestión. Tener todas las bocas de red conectadas es tener accesos libres a la red repartidos por toda la empresa que cualquiera puede usar, incluido un supuesto intruso.

Para las bocas de red que están siendo usadas por los usuarios deberemos monitorizar e identificar de alguna forma las máquinas que deben estar en cada red, o asignarlas las direcciones IPs y la conectividad por medio de las direcciones MAC de las tarjetas, esto nos avisará o prevendrá el que un supuesto intruso desconecte una máquina y conecte un portátil o un dispositivo de mano y acceda a la red. Es trabajoso mantener en el servidor DHCP o en los concentradores todas las direcciones MAC de las tarjetas de red en las maquinas de usuario, pero esto nos asegurará que sólo las máquinas que nosotros deseamos tendrán acceso a nuestra red.

6.17. Sistemas de alta disponibilidad

En todo el manual hemos explicado que para asegurar el hardware no hay nada más eficaz que la redundancia de sistemas. Una de las formas más comunes hoy en día de redundancia de sistemas son los clusters de máquinas de alta disponibilidad. Estos sistemas se componen de dos o más máquinas que cumplen exactamente la misma función y que comparten los datos sobre los que trabajan por medio de un bus compartido SCSI o un canal de fibra conectados a un sistema de almacenamiento que permite el acceso compartido por varias máquinas. La idea es que uno de los sistemas cumple la función encomendada al sistema, sea como servidor de aplicaciones, de bases de datos, servidor web o cualquier otro cometido. Si este sistema falla el otro detecta el fallo por medio de un enlace mantenido por medio de una red y/o un enlace nullmodem por puerto serie denominado heartbeat, al detectar el fallo el segundo sistema toma la dirección IP del primero y lo sustituye en la tarea que este estuviera realizando.

Es un sistema ideal para asegurar la disponibilidad de un servicio determinado, y suele ser más barato mantener un cluster de dos máquinas que tener una máquina con todos sus subsistemas redundantes.

Los sistemas de alta disponibilidad son cada vez más populares, en parte por su gran fiabilidad y relativamente bajo costo y también por la disponibilidad de software libre que permite el montaje de estos sistemas por un precio asequible a la mayoría de empresas. Estos sistemas deben complementarse siempre con la redundancia que podamos permitirnos a nivel de cada máquina, como UPSs, dobles fuentes de alimentación o discos montados en RAID.

Aunque los sistemas de alta disponibilidad no son la panacea para la seguridad física (nada lo es) podemos asegurar que son uno de los métodos más eficaces para proveer de una redundancia en el hardware de forma eficaz y relativamente económica. Además son fáciles de montar y administrar e incluso existen empresas dedicadas al montaje de software preconfigurado para funcionar en sistemas de alta disponibilidad, como firewalls, bases de datos o sistemas similares.

6.18. Seguridad física del cableado

La seguridad física del cableado es bastante sencilla aunque difícil de asegurar. La principal preocupación para un consultor de seguridad física es que el cableado pueda fallar o que pueda ser seccionado por un intruso malintencionado. En principio tendremos también en cuenta lo comentado para las bocas de red y los conectores, que son también parte del cableado.

Para comprobar la red existen aparatos diseñados para esta tarea, que nos permitirán comprobar los cables para ver si tienen algún tipo de problema. También deberemos comprobar que el cableado cumple las normativas necesarias y que tiene la calidad necesaria, normalmente CAT5 o CAT7. Para el cableado coaxial grueso o fino deberemos usar otro tipo de aparatos para comprobarlos y deberemos comprobar sus características eléctricas y las de los terminadores y dispositivos "T" que conectan las máquinas. Como cada vez son menos comunes no hablaremos mucho de ellos. Para evitar el posible seccionamiento del cableado de red lo mejor es entubarlo o integrarlo en la estructura del edificio. Muchos edificios tienen paneles desmontables dentro de los cuales se puede alojar el cableado de red, pero deberá asegurarse que no son fácilmente desmontables o cualquiera podría abrirlos y seccionar el cable. Para los cables de fibra óptica deberemos estudiar la posibilidad del seccionamiento del cable, las características ópticas de este (para esto necesitamos instrumental al efecto, puede ser necesario contratar a un especialista) y vigilar que este tipo de cables que suelen ser frágiles no estén acodados o doblados excesivamente.

6.19. Dispositivos Tap para captura de datos

Los dispositivos Tap son un caso similar al que comentábamos para los keycatchers y máquinas conectadas a las bocas de red. Tienen un problema añadido, y es que estos dispositivos permiten leer el tráfico de una red sin tener que emitir ningún tipo de dato en la red, por lo que son en principio indetectables a nivel de seguridad informática. Se suelen usar para instalar dispositivos IDS stealth (Detectores de intrusos no detectables como máquinas de la red) y para hacer sniffing de la red sin ser

detectados. Son muy útiles para el administrador de sistemas, pero pueden volverse contra nosotros si un supuesto intruso malintencionado lo instala en nuestra red. Estos dispositivos pueden funcionar incluso sin una dirección IP asignada, y con todo pueden estudiar los datos que pasan por la red a la que están conectados, sobre todo si se conectan al puerto que replica los demás puertos de un concentrador. Para evitar esto solo tenemos dos opciones, una de ellas es limitar de alguna forma las direcciones MAC a las que se envían los datos, ya sea por medio de los concentradores o por medio de la VLAN, la otra es la vigilancia intensiva de que este tipo de dispositivos no se inserten en las bocas de red desocupadas y sobre todo en los concentradores. De todas formas si hemos tomado las medidas aconsejadas más arriba para los concentradores es poco probable que un intruso pueda introducir un Tap y un portátil para obtener datos de nuestra red.

6.20. Monitorización de equipos y dispositivos de red

Hablaremos aquí sobre la monitorización física de los equipos y dispositivos de red. Es aconsejable de vez en cuando realizar una inspección física de todo el hardware instalado en la empresa, buscando todos los puntos de fallo y errores que comentamos en este documento y cualquier otro que podamos encontrar o que se nos ocurra. Es una tarea que no lleva demasiado tiempo y que puede suponer la diferencia entre tener una red y un hardware seguros o no tenerlos. Si tenemos personal de vigilancia con la capacidad técnica para realizar esta tarea se les puede encargar a ellos, en caso contrario uno de los administradores o encargados de la seguridad deberá realizar una ronda de vigilancia de los equipos cada cierto tiempo para comprobar que todo está como debe estar. No es necesario la contratación de personal de consultoría para realizar este tipo de estudios o vigilancias rutinarias del hardware, basta con detectar los fallos más evidentes y tener el sistema actualizado y en un estado conocido.

Es aconsejable la implantación de una política de seguridad física del hardware que debe cumplirse, pero tan importante como imponer esta política es la monitorización de que esta política se cumple y que el hardware cumple las medidas de seguridad física que hayamos decidido.

6.21. Monitorización del hardware. SMART y sistemas SNMP

Tan importante como el aseguramiento del hardware es su monitorización, es algo en lo que ya hemos insistido. Existen varios sistemas de monitorización del hardware, algunos de ellos estándar como el SNMP o el SMART y otros específicos del hardware que tengamos instalado. Buscaremos siempre sistemas de monitorización que puedan funcionar a través de la red y sobre una única consola que nos permita tener todo el hardware controlado, existe software de este tipo que nos permitirá ir añadiendo las características del hardware que vayamos instalando.

Sobre el SNMP debemos decir que es el sistema estándar de monitorización de hardware. Casi cualquier máquina o dispositivo de red medianamente complicado proveerá de servicios SNMP para permitir la monitorización de todos sus parámetros. Además de los parámetros estándar que el protocolo prevee para todos los sistemas cada fabricante puede incorporar una serie de extensiones a este sistema y proporcionar los datos necesarios para que el sistema gestor SNMP pueda monitorizar estos sistemas. Incluso pueden proveer las llamadas traps, que son avisos que el hardware manda al sistema de

monitorización para avisar de algún cambio en el hardware o error en el sistema, pasando así de un sistema principalmente pasivo como es el SNMP a un sistema activo que permite recibir avisos cuando es necesario.

Deberemos elegir hardware que soporte SNMP y que incorpore el máximo número de extensiones que permitan monitorizar el hardware en todos los parámetros posibles. En el caso de los dispositivos de red estos suelen contar con una lista incontable de parámetros a monitorizar, a veces tantos que pueden marear un poco al administrador poco avezado en estas lides. Un buen software de gestión de red resolverá el problema de tratar con montones de dispositivos de red con montones de parámetros a monitorizar, y un sistema de estos bien instalado y funcionando correctamente es una herramienta impagable para el administrador de sistemas. Entre los parámetros que se pueden monitorizar de estos dispositivos se encuentran todos los parámetros software como tráfico en los interfaces, estadísticas de tráfico, tipos de tráfico y cientos de parámetros más; luego tenemos los parámetros hardware, como velocidad de giro de los ventiladores, temperatura de la caja y de los dispositivos internos, tasas de fallo debidas al cableado o al mismo hardware y muchos parámetros más.

En los ordenadores es menos común encontrar SNMP, pero existen varios fabricantes que proporcionan agentes SNMP que permiten la monitorización de todos los parámetros del sistema. En cualquier caso siempre podemos optar por agentes software SNMP libres como los incluidos en los sistemas de software libre como Linux o FreeBSD, estos sistemas proporcionan monitorización de parámetros como el tráfico en los interfaces, estadísticas de uso del sistema y muchos más, además de ser programables y permitir la monitorización de prácticamente cualquier parámetro ya sea sobre el hardware o del funcionamiento del software del sistema. Es interesante contar con SNMP en las máquinas, sobre todo en los servidores y en las máquinas más críticas, pues estos nos permitirá el tener un sistema estandarizado para todo el conjunto del hardware y nos ahorrará tiempo de administración.

Respecto al software gestor de red que usa los datos SNMP para ofrecernos una vista completa de nuestro hardware debemos decir que suele ser caro y difícil de usar, pero que una vez instalado y controlado su funcionamiento su funcionalidad es impagable, pues permite monitorizar todos los parámetros de redes inmensas y a la vez nos permite reconfigurar dispositivos o realizar cambios en la misma estructura de la red. Un sistema de este tipo es OpenView de HP, que provee todas estas funcionalidades. Como software libre citaremos a OpenNMS que intenta ser una alternativa libre a los sistemas de gestión de red comerciales y que tiene a día de hoy una funcionalidad ya muy importante.

Otro tipo de sistemas de monitorización son los basados en tomar muestras, como por ejemplo Nagios, Big Brother y similares. Este tipo de sistemas puede usar también SNMP para monitorizar dispositivos de red y luego pruebas de otro tipo para monitorizar máquinas y servicios, comprobando la salud de estos y ofreciéndonos un vistazo rápido de nuestra red, de nuestros servidores y de los servicios que estamos proveyendo a nuestros usuarios o clientes. Es muy aconsejable la instalación de un sistema de este tipo, porque además de permitirnos estudiar nuestro sistema para ver fallos o máquinas caídas nos envía avisos mediante correo electrónico o pagers si alguno de estos sistemas o servicios falla.

Por último comentaremos los sistemas SMART, que son un sistema implementado en casi todos los discos duros modernos que nos ofrecen una cantidad ingente de datos sobre el funcionamiento de estos y sobre su vida útil. Los discos duros son los sistemas que probablemente más fallan en un ordenador, por

contener partes mecánicas que están constantemente en movimiento. El sistema SMART está implementado en el hardware y puede ser leído por medio de software al efecto, informándonos de todos los parámetros de funcionamiento del disco duro y de parámetros como el tiempo estimado entre fallos o el tiempo estimado de vida del disco. Es aconsejable utilizar las utilidades al efecto para aprovechar la funcionalidad SMART de los discos duros, y poder así preveer fallos antes de que estos se produzcan. El poder saber que un disco duro va a fallar muy probablemente en un espacio corto de tiempo puede ser vital para replicarlo y sustituirlo por otro nuevo, evitando una gran cantidad de problemas de administración y posible perdida de datos.

6.22. Control remoto de hardware

El control remoto del hardware podemos verlo desde dos puntos de vista. El punto de vista hardware puro, donde estaríamos hablando de los sistemas SNMP que hemos comentado en el punto anterior o el punto de vista del software, que abarca una gran cantidad de servicios como TELNET, SSH, FTP/SCP/SFTP, Webmin y similares, etc.

En el caso de la seguridad física solo nos interesa la posibilidad de que alguien controle de forma remota nuestro hardware. Esto es cada vez menos común y no debe ser una gran preocupación para el consultor. Uno de los puntos a tener en cuenta es si existen modems conectados a las máquinas que puedan ser accedidos desde el exterior, y por supuesto la conectividad de red desde el exterior, pero estos son puntos más adecuados para el tratamiento por parte del personal de seguridad informática que por el personal de seguridad física.

Nuestra mayor preocupación será por tanto la ocultación dentro de la empresa por un intruso malintencionado de dispositivos como portátiles, pequeños ordenadores tipo Capuccino o similares conectados a nuestra red interna y que puedan servir a un atacante exterior para controlar nuestra red y por tanto nuestro hardware, aunque esta posibilidad es pequeña y casi poco plausible. Los sistemas de seguridad informática deberían detectar este tipo de dispositivos fácilmente y trazarlos hasta ser eliminados.

Se puede hablar también de control remoto del hardware cuando hablamos de virus, troyanos, gusanos o rootkits instalados dentro de la empresa, ya sea a través de la red pública o por usuarios mal formados o malintencionados. Estos sistemas proporcionan a un supuesto atacante exterior control sobre nuestro software y hardware, pero deberían ser fácilmente detectables por el personal de seguridad informática.

6.23. Acceso a datos técnicos de la red y del hardware

Aquí tenemos un punto verdaderamente importante dentro de la seguridad física. Hay que ser muy claros en este punto: Nadie que no sea parte del personal de administración de la red y del hardware debe tener acceso a los datos técnicos de la red y del hardware. Si alguien necesita acceso puntual a algún dato se investigará si realmente necesita ese acceso y se concederá el acceso en base a cada petición y con todas las reservas posibles.

Conocer los datos técnicos de la red y del hardware de un sistema proporciona a un supuesto atacante dos facilidades muy apreciadas por estos: La primera es la facilidad que el conocimiento del hardware y la estructura de la red proporciona para realizar ataques informáticos de todo tipo. La segunda es la posibilidad de usar estos datos para usarlos en ataques de Hacking Social, que son tan peligrosos como los ataques informáticos.

Para protegernos de este tipo de ataques debemos mantener la estructura de la red y del hardware (incluido marcas, software instalado, direcciones IP, MACs, etc) secretas o al menos bajo un control de acceso estricto. Uno de los primeros pasos que realiza siempre un hacker antes de atacar un sistema es estudiar la estructura de la red y de las máquinas que la componen. Si ya tiene estos datos tiene la mitad del trabajo hecho, y nosotros la mitad del sistema hackeado... Deberemos por tanto mantener los datos técnicos en armarios a tal efecto, y deberá pedirse permiso al personal de administración de red para acceder a ellos, proporcionando únicamente los datos imprescindibles y apuntando siempre quien ha solicitado los datos y para que. Un buen control de estos datos redundará en una mayor seguridad de todo el sistema. Por parte de los encargados de la seguridad informática deberán considerar cualquier intento de análisis remoto de la estructura de la red o de las máquinas como un intento de intrusión (no hablamos aquí de un simple escaneo de puertos, por supuesto, sino de ataques más sofisticados de recopilación de datos) y por tanto deberán comunicarlo a quien consideren necesario.

Otro peligro son los ataques de hacking social. Un intruso que ha obtenido datos técnicos muy concretos sobre la red de la empresa y sobre el hardware y los ordenadores de la empresa puede hacerse pasar por una persona del servicio técnico de cualquiera de las marcas con las que trabajamos o por personal de otro departamento, proporcionando estos datos a una persona del personal de administración o al usuario final puede convencerlo para que le proporcione otros datos, como claves de acceso o datos que puedan llevarle a conseguir un acceso remoto a nuestros sistemas. El hacking social debe ser considerado como una de las mayores amenazas para la seguridad de los sistemas hoy en día y el mejor arma que tiene un hacker social son los datos, sobre todo si se trata de datos técnicos que se suponen secretos o únicamente conocidos por el personal de la empresa.

6.24. Grabación de datos. Grabadoras de CD, disqueteras, etc

No nos extenderemos excesivamente en este punto. Si su empresa necesita que los usuarios no se lleven datos de su empresa no los mantenga en la máquina del usuario. Así de simple. El consejo que un consultor en seguridad puede darle no es otro más que el que mantenga los datos en los servidores y que los usuarios trabajen sobre los datos de forma remota. Todos los demás sistemas son útiles pero no eficaces. Usted puede quitar de las máquinas de usuario las grabadoras de CDs, las disqueteras, incluso puede inventar un método para que no usen dongles USB o similares, pero puede estar seguro que un usuario decidido a sacar los datos de su máquina, ya sea por desconocimiento, para facilitar su trabajo o por simple malicia conseguirá hacerlo. Por eso lo mejor que puede hacer es no fiarse de ninguno de estos sistemas, simplemente mantenga los datos alejados del usuario final y así evitará que este pueda replicarlos.

6.25. Dongles USB y Sistemas de Almacenamiento USB. Sistemas

serie o paralelo

Los dongles USB son como un dolor de muelas para los administradores de sistemas y los encargados de las seguridad del sistema. Para empezar tenemos lo que puede venir en ellos: virus, software pirateado, todo tipo de software o datos poco recomendables para un lugar de trabajo, juegos, etc. Luego tenemos todo lo que se puede llevar en ellos: datos de la empresa, software cuya licencia ha sido adquirido por la empresa, software bajado de internet, etc.

Si lo que más nos preocupa (tenemos antivirus, firewall, control de software, etc) es que el usuario pueda replicar datos y sacarlos de al empresa solo podemos hacer dos cosas, la primera y la que siempre recomendamos es mantener los datos lejos del usuario, la segunda es inhabilitar los puertos USB y los sistemas serie o paralelo, ya sea mediante métodos software o hardware.

Los puertos serie y paralelo no suponen un gran peligro, puesto que los dispositivos de almacenamiento que normalmente se conectan a ellos suelen necesitar en el sistema operativo Windows de drivers especiales, que podemos controlar que no se puedan instalar de diversas formas, sobre todo mediante software de control de instalación de software. Los dispositivos USB son un problema mayor, como ahora veremos.

Si estamos hablando de Software Libre como Linux o FreeBSD no hay mucho problema. El soporte USB de almacenamiento viene como módulos del kernel que pueden quitarse del sistema con lo que no se podrá usar dongles USB ni dispositivos de almacenamiento USB. Lo mismo para los dispositivos serie y paralelo. Este sistema es muy simple y es ideal para evitar este tipo de comportamientos.

Pero si hablamos de Windows el caso es diferente. Aquí es más complicado quitar los drivers de almacenamiento externo USB, sobre todo en Windows XP que incorpora de serie drivers para todo este tipo de dispositivos. Si es posible se quitarán del sistema los drivers para este tipo de dispositivos o se inhabilitará mediante software la instalación de nuevo hardware en el sistema (lo cual es un problema si tenemos impresoras o ratones y teclados USB que deben autodetectarse).

La solución más radical (y no por ello la más recomendable) es quitar el cableado de los puertos USB frontales que conectan a la placa base y ya puestos a cacharrear podemos incluso sellar o desoldar los puertos USB integrados en la placa base. Si no queremos realizar semejante chapuza podemos intentar desactivar estos puertos mediante switches o puentes en la placa base, pero esto no es siempre posible. Si queremos aislar de verdad el sistema siempre podemos comprar cajas de metacrilato cerradas que solo permiten la ventilación del sistema y no el acceso a este, pero estamos hablando ya de soluciones realmente radicales para un simple dongle USB...

6.26. Sistemas de radiofrecuencia. Tecnología Wireless y Bluetooth

Si me pregunta como consultor de seguridad física que puede hacer para mejorar su sistema de red mediante radiofrecuencia, sea este Wireless o Bluetooth mi primera respuesta sera: ¡Quítelo ya!

Puede ser un poco radical, pero tener un sistema que permite el acceso a los datos en bruto a cualquiera desde el exterior de la empresa y para el cual día a día aparecen más y más bugs y formas de saltarse la encriptación y la seguridad lo mejor es no usarlo. Si realmente necesita usarlo entonces mi consejo es que utilice las últimas tarjetas y puntos de acceso con la última tecnología disponible, tanto en Wireless como en Bluetooth, pues en ambos sistemas se han encontrado errores que permiten al menos el hacer sniffing de las redes desde el exterior de las empresas. De ahí el Warchalking del que hablábamos antes. Si ya tiene un sistema instalado y este es vulnerable asegúrese de que todas las conexiones que realice a través de la red inalámbrica sean seguras, usando SSH, SSL y similares, sino su sistema podrá ser comprometido.

Con los últimos sistemas lanzados y el nuevo WEP la seguridad ha mejorado, pero hace nada han salido varios bugs que permiten engañar a los sistemas Bluetooth y pueden estar seguros de que aparecerán otros bugs y formas de saltarse la seguridad de estos sistemas. Son sistemas demasiado golosos para los hackers como para que estos no estudien mil y una formas de romperlos. Es muy cómodo ponerse con un coche y un portátil al lado de una empresa y conectarse a la red de esta y realizar cualquier cosa como usar su ancho de banda para realizar ataques de denegación de servicio o Dios sabe qué. Mi consejo: Evítelas si puede.

6.27. Dispositivos de mano. Palms y PocketPCs

Para los dispositivos de mano solo debemos decir que deben tomarse exactamente las mismas medidas que para los portátiles, aunque teniendo en cuenta que normalmente no contienen datos tan críticos para la empresa como los portátiles, aunque son mucho más fáciles de robar. Es bastante común este caso, el robo de un dispositivo de mano con todos los datos de un empleado, que luego pueden ser usados para realizar hacking social, pues suelen contener números de teléfono internos de la empresa, datos sobre la empresa y en los casos mas aterradores incluso passwords de acceso a los sistemas.

Lo mejor que se puede hacer es aconsejar a los empleados el no mantener nunca datos importantes en este tipo de dispositivos, sobre todo passwords de acceso, y el aconsejar también que si uno de estos dispositivos es robado o perdido se realice un informe para el empresa donde se indique al personal de seguridad que datos susceptibles de ser usados para hacking social o informático pudiera contener el dispositivo.

6.28. Control del acceso del personal externo contratado al hardware

El caso es el siguiente: Contratamos a un consultor externo o a personal de mantenimiento para realizar una serie de acciones sobre nuestro hardware. ¿Como nos aseguramos que únicamente va a realizar las manipulaciones para las que le hemos contratado y no otras? Es sencillo, lo único que debemos hacer es tener un formulario que el personal externo deberá firmar y donde se especificará la fecha de la manipulación, la manipulación exacta que se le permite hacer y si es necesario también lo que no se le permite hacer. De esta forma aseguramos que la persona que trabaje sobre nuestros sistemas no va a realizar más manipulación que la contratada.

Siempre es conveniente que una persona del personal de administración esté presente cuando se realice cualquier mantenimiento o consultoría sobre sistemas críticos de la empresa, pues así podrá vigilar que las acciones realizadas son las correctas e incluso podrá asesorar al consultor o personal de mantenimiento si este tiene algún tipo de duda sobre el sistema.

A. FDL

GNU Free Documentation License Version 1.2, November 2002

0. PREAMBLE

The purpose of this License is to make a manual, textbook, or other functional and useful document "free" in the sense of freedom: to assure everyone the effective freedom to copy and redistribute it, with or without modifying it, either commercially or noncommercially. Secondarily, this License preserves for the author and publisher a way to get credit for their work, while not being considered responsible for modifications made by others.

This License is a kind of "copyleft", which means that derivative works of the document must themselves be free in the same sense. It complements the GNU General Public License, which is a copyleft license designed for free software.

We have designed this License in order to use it for manuals for free software, because free software needs free documentation: a free program should come with manuals providing the same freedoms that the software does. But this License is not limited to software manuals; it can be used for any textual work, regardless of subject matter or whether it is published as a printed book. We recommend this License principally for works whose purpose is instruction or reference.

APPLICABILITY AND DEFINITIONS

This License applies to any manual or other work, in any medium, that contains a notice placed by the copyright holder saying it can be distributed under the terms of this License. Such a notice grants a worldwide, royaltyfree license, unlimited in duration, to use that work under the conditions stated herein. The "Document", below, refers to any such manual or work. Any member of the public is a licensee, and is addressed as "you". You accept the license if you copy, modify or distribute the work in a way requiring permission under copyright law.

A "Modified Version" of the Document means any work containing the Document or a portion of it, either copied verbatim, or with modifications and/or translated into another language.

A "Secondary Section" is a named appendix or a frontmatter section of the Document that deals exclusively with the relationship of the publishers or authors of the Document to the Document's overall subject (or to related matters) and contains nothing that could fall directly within that overall subject. (Thus, if the Document is in part a textbook of mathematics, a Secondary Section may not explain any mathematics.) The relationship could be a matter of historical connection with the subject or with related matters, or of legal, commercial, philosophical, ethical or political position regarding them.

The "Invariant Sections" are certain Secondary Sections whose titles are designated, as being those of Invariant Sections, in the notice that says that the Document is released under this License. If a section does not fit the above definition of Secondary then it is not allowed to be designated as Invariant. The Document may contain zero Invariant Sections. If the Document does not identify any Invariant Sections then there are none.

The "Cover Texts" are certain short passages of text that are listed, as FrontCover Texts or BackCover Texts, in the notice that says that the Document is released under this License. A FrontCover Text may be at most 5 words, and a BackCover Text may be at most 25 words.

A "Transparent" copy of the Document means a machinereadable copy, represented in a format whose specification is available to the general public, that is suitable for revising the document straightforwardly with generic text editors or (for images composed of pixels) generic paint programs or (for drawings) some widely available drawing editor, and that is suitable for input to text formatters or for automatic translation to a variety of formats suitable for input to text formatters. A copy made in an otherwise Transparent file format whose markup, or absence of markup, has been arranged to thwart or discourage subsequent modification by readers is not Transparent. An image format is not Transparent if used for any substantial amount of text. A copy that is not "Transparent" is called "Opaque".

Examples of suitable formats for Transparent copies include plain ASCII without markup, Texinfo input format, LaTeX input format, SGML or XML using a publicly available DTD, and standardconforming simple HTML, PostScript or PDF designed for human modification. Examples of transparent image formats include PNG, XCF and JPG. Opaque formats include proprietary formats that can be read and edited only by proprietary word processors, SGML or XML for which the DTD and/or processing tools are not generally available, and the machinegenerated HTML, PostScript or PDF produced by some word processors for output purposes only.

The "Title Page" means, for a printed book, the title page itself, plus such following pages as are needed to hold, legibly, the material this License requires to appear in the title page. For works in formats which do not have any title page as such, "Title Page" means the text near the most prominent appearance of the work's title, preceding the beginning of the body of the text.

A section "Entitled XYZ" means a named subunit of the Document whose title either is precisely XYZ or contains XYZ in parentheses following text that translates XYZ in another language. (Here XYZ

stands for a specific section name mentioned below, such as "Acknowledgements", "Dedications", "Endorsements", or "History".) To "Preserve the Title" of such a section when you modify the Document means that it remains a section "Entitled XYZ" according to this definition.

The Document may include Warranty Disclaimers next to the notice which states that this License applies to the Document. These Warranty Disclaimers are considered to be included by reference in this License, but only as regards disclaiming warranties: any other implication that these Warranty Disclaimers may have is void and has no effect on the meaning of this License.

2. VERBATIM COPYING

You may copy and distribute the Document in any medium, either commercially or noncommercially, provided that this License, the copyright notices, and the license notice saying this License applies to the Document are reproduced in all copies, and that you add no other conditions whatsoever to those of this License. You may not use technical measures to obstruct or control the reading or further copying of the copies you make or distribute. However, you may accept compensation in exchange for copies. If you distribute a large enough number of copies you must also follow the conditions in section 3.

You may also lend copies, under the same conditions stated above, and you may publicly display copies.

3. COPYING IN QUANTITY

If you publish printed copies (or copies in media that commonly have printed covers) of the Document, numbering more than 100, and the Document’s license notice requires Cover Texts, you must enclose the copies in covers that carry, clearly and legibly, all these Cover Texts: FrontCover Texts on the front cover, and BackCover Texts on the back cover. Both covers must also clearly and legibly identify you as the publisher of these copies. The front cover must present the full title with all words of the title equally prominent and visible. You may add other material on the covers in addition. Copying with changes limited to the covers, as long as they preserve the title of the Document and satisfy these conditions, can be treated as verbatim copying in other respects.

If the required texts for either cover are too voluminous to fit legibly, you should put the first ones listed (as many as fit reasonably) on the actual cover, and continue the rest onto adjacent pages.

If you publish or distribute Opaque copies of the Document numbering more than 100, you must either include a machinereadable Transparent copy along with each Opaque copy, or state in or with each Opaque copy a computernetwork location from which the general networkusing public has access to download using publicstandard network protocols a complete Transparent copy of the Document, free of added material. If you use the latter option, you must take reasonably prudent steps, when you begin distribution of Opaque copies in quantity, to ensure that this Transparent copy will remain thus accessible at the stated location until at least one year after the last time you distribute an Opaque copy (directly or through your agents or retailers) of that edition to the public.

It is requested, but not required, that you contact the authors of the Document well before redistributing any large number of copies, to give them a chance to provide you with an updated version of the Document.

4. MODIFICATIONS

You may copy and distribute a Modified Version of the Document under the conditions of sections 2 and 3 above, provided that you release the Modified Version under precisely this License, with the Modified Version filling the role of the Document, thus licensing distribution and modification of the Modified Version to whoever possesses a copy of it. In addition, you must do these things in the Modified Version:

1. Use in the Title Page (and on the covers, if any) a title distinct from that of the Document, and from those of previous versions (which should, if there were any, be listed in the History section of the Document). You may use the same title as a previous version if the original publisher of that version gives permission.
2. List on the Title Page, as authors, one or more persons or entities responsible for authorship of the modifications in the Modified Version, together with at least five of the principal authors of the Document (all of its principal authors, if it has fewer than five), unless they release you from this requirement.
3. State on the Title page the name of the publisher of the Modified Version, as the publisher.
4. Preserve all the copyright notices of the Document.
5. Add an appropriate copyright notice for your modifications adjacent to the other copyright notices.
6. Include, immediately after the copyright notices, a license notice giving the public permission to use the Modified Version under the terms of this License, in the form shown in the Addendum below.
7. Preserve in that license notice the full lists of Invariant Sections and required Cover Texts given in the Document’s license notice.
8. Include an unaltered copy of this License.
9. Preserve the section Entitled "History", Preserve its Title, and add to it an item stating at least the title, year, new authors, and publisher of the Modified Version as given on the Title Page. If there is no section Entitled "History" in the Document, create one stating the title, year, authors, and publisher of the Document as given on its Title Page, then add an item describing the Modified Version as stated in the previous sentence.
10. Preserve the network location, if any, given in the Document for public access to a Transparent copy of the Document, and likewise the network locations given in the Document for previous versions it was based on. These may be placed in the "History" section. You may omit a network location for a work that was published at least four years before the Document itself, or if the original publisher of the version it refers to gives permission.
11. For any section Entitled "Acknowledgements" or "Dedications", Preserve the Title of the section, and preserve in the section all the substance and tone of each of the contributor acknowledgements and/or dedications given therein.
12. Preserve all the Invariant Sections of the Document, unaltered in their text and in their titles. Section numbers or the equivalent are not considered part of the section titles.

13. Delete any section Entitled "Endorsements". Such a section may not be included in the Modified Version.
14. Do not retitle any existing section to be Entitled "Endorsements" or to conflict in title with any Invariant Section.
15. Preserve any Warranty Disclaimers.

If the Modified Version includes new frontmatter sections or appendices that qualify as Secondary Sections and contain no material copied from the Document, you may at your option designate some or all of these sections as invariant. To do this, add their titles to the list of Invariant Sections in the Modified Version’s license notice. These titles must be distinct from any other section titles.

You may add a section Entitled "Endorsements", provided it contains nothing but endorsements of your Modified Version by various partiesfor example, statements of peer review or that the text has been approved by an organization as the authoritative definition of a standard.

You may add a passage of up to five words as a FrontCover Text, and a passage of up to 25 words as a BackCover Text, to the end of the list of Cover Texts in the Modified Version. Only one passage of FrontCover Text and one of BackCover Text may be added by (or through arrangements made by) any one entity. If the Document already includes a cover text for the same cover, previously added by you or by arrangement made by the same entity you are acting on behalf of, you may not add another; but you may replace the old one, on explicit permission from the previous publisher that added the old one.

The author(s) and publisher(s) of the Document do not by this License give permission to use their names for publicity for or to assert or imply endorsement of any Modified Version.

5. COMBINING DOCUMENTS

You may combine the Document with other documents released under this License, under the terms defined in section 4 above for modified versions, provided that you include in the combination all of the Invariant Sections of all of the original documents, unmodified, and list them all as Invariant Sections of your combined work in its license notice, and that you preserve all their Warranty Disclaimers.

The combined work need only contain one copy of this License, and multiple identical Invariant Sections may be replaced with a single copy. If there are multiple Invariant Sections with the same name but different contents, make the title of each such section unique by adding at the end of it, in parentheses, the name of the original author or publisher of that section if known, or else a unique number. Make the same adjustment to the section titles in the list of Invariant Sections in the license notice of the combined work.

In the combination, you must combine any sections Entitled "History" in the various original documents, forming one section Entitled "History"; likewise combine any sections Entitled "Acknowledgements", and any sections Entitled "Dedications". You must delete all sections Entitled "Endorsements".

6. COLLECTIONS OF DOCUMENTS

You may make a collection consisting of the Document and other documents released under this License, and replace the individual copies of this License in the various documents with a single copy that is included in the collection, provided that you follow the rules of this License for verbatim copying of each of the documents in all other respects.

You may extract a single document from such a collection, and distribute it individually under this License, provided you insert a copy of this License into the extracted document, and follow this License in all other respects regarding verbatim copying of that document.

7. AGGREGATION WITH INDEPENDENT WORKS

A compilation of the Document or its derivatives with other separate and independent documents or works, in or on a volume of a storage or distribution medium, is called an "aggregate" if the copyright resulting from the compilation is not used to limit the legal rights of the compilation’s users beyond what the individual works permit. When the Document is included in an aggregate, this License does not apply to the other works in the aggregate which are not themselves derivative works of the Document.

If the Cover Text requirement of section 3 is applicable to these copies of the Document, then if the Document is less than one half of the entire aggregate, the Document’s Cover Texts may be placed on covers that bracket the Document within the aggregate, or the electronic equivalent of covers if the Document is in electronic form. Otherwise they must appear on printed covers that bracket the whole aggregate.

8. TRANSLATION

Translation is considered a kind of modification, so you may distribute translations of the Document under the terms of section 4. Replacing Invariant Sections with translations requires special permission from their copyright holders, but you may include translations of some or all Invariant Sections in addition to the original versions of these Invariant Sections. You may include a translation of this License, and all the license notices in the Document, and any Warranty Disclaimers, provided that you also include the original English version of this License and the original versions of those notices and disclaimers. In case of a disagreement between the translation and the original version of this License or a notice or disclaimer, the original version will prevail.

If a section in the Document is Entitled "Acknowledgements", "Dedications", or "History", the requirement (section 4) to Preserve its Title (section 1) will typically require changing the actual title.

9. TERMINATION

You may not copy, modify, sublicense, or distribute the Document except as expressly provided for

under this License. Any other attempt to copy, modify, sublicense or distribute the Document is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

10. FUTURE REVISIONS OF THIS LICENSE

The Free Software Foundation may publish new, revised versions of the GNU Free Documentation License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. See http://www.gnu.org/copyleft/.

Each version of the License is given a distinguishing version number. If the Document specifies that a particular numbered version of this License "or any later version" applies to it, you have the option of following the terms and conditions either of that specified version or of any later version that has been published (not as a draft) by the Free Software Foundation. If the Document does not specify a version number of this License, you may choose any version ever published (not as a draft) by the Free Software Foundation.

ADDENDUM: How to use this License for your documents

To use this License in a document you have written, include a copy of the License in the document and put the following copyright and license notices just after the title page:

Copyright (c) YEAR YOUR NAME. Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.2 or any later version published by the Free Software Foundation; with no Invariant Sections, no FrontCover Texts, and no BackCover Texts. A copy of the license is included in the section entitled "GNU Free Documentation License".

If you have Invariant Sections, FrontCover Texts and BackCover Texts, replace the "with...Texts." line with this:

with the Invariant Sections being LIST THEIR TITLES, with the FrontCover Texts being LIST, and with the BackCover Texts being LIST.

If you have Invariant Sections without Cover Texts, or some other combination of the three, merge those two alternatives to suit the situation.

If your document contains nontrivial examples of program code, we recommend releasing these examples in parallel under your choice of free software license, such as the GNU General Public License, to permit their use in free software.