TEMA 3 GESTIÓN ACTIVA DE LA SEGURIDAD

3.1 . LA SEGURIDAD ACTIVA EN LOS SISTEMAS

Una vez que ha sufrido un ataque, lo mejor que le puede suceder a un administrador de seguridad es conocer el objetivo del atacante y el método de ataque que ha perpetrado. Esta información le proporcionará pistas clarificadoras sobre el camino que debe tomar para organizar la defensa. Por tanto, es importante conocer las características que definen tanto al atacante como al ataque.

3.1.1. EL PERFIL DEL ATACANTE Y SU MOTIVACIÓN

En el argot de la seguridad los atacantes suelen clasificarse en función de sus peculiaridades específicas, sus actividades o los motivos que les mueven a perpetrar los ataques. Vamos a describir algunos de estos perfiles.

CLASIFICACIÓN DE ATACANTES POR SU ACTIVIDAD

- HACKER. Es una persona con amplios conocimientos tecnológicos que mantiene actualizados permanentemente. Tiene una gran apetencia por conocer exhaustivamente los sistemas de cifrado y las posibilidades de acceso a cualquier sistema inseguro sin ser descubierto, Ocasionalmente, el hacker puede ser contratado por las empresas para aprovechar sus profundos conocimientos sobre seguridad: se habla de que se ha convertido en un hacker de sombrero blanco (white hat).
- CRACKER. Es un atacante de comportamiento compulsivo obsesionado con asaltar sistemas informáticos y electrónicos o saltarse las claves de protección de aplicaciones de software. El cracker es un gran conocedor de la programación y llega a diseñar software para reventar todo tipo de sistemas.
- LAMMER. Es una persona que desea convertirse en un hacker pero a la que su escaso nivel formativo le supone una gran barrera para conseguirlo. Se dedica a ejecutar programas creados por otros o a descargar indiscriminadamente cualquier aplicación publicada en la web. Frecuentemente, la amenaza del lammer reside en que no controla los efectos del ataque que perpetra. En los primeros estadios de conocimiento, los lammers reciben la denominación de newbies.
- COPYHACKER. Es un falsificador de hardware, fundamentalmente de tarjetas inteligentes. Se relacionan con hackers, copian sus métodos de ruptura de sistemas y después los venden, por lo que su principal motivación no es técnica sino económica.
- BUCANERO. Es el comerciante ilegal de la red. No posee formación técnica significativa pero sí en el área de negocios, lo que frecuentemente aprovecha para cometer fraudes.
- PHREAKER. Posee robustos conocimientos sobre telefonía que aprovecha en su propio beneficio para actividades ilegales.
- KIDDIE. Son simples usuarios de Internet que ponen en ejecución cualquier cosa que puedan descargar sin ningún conocimiento de lo que hace e infectando de virus y malware sus propios equipos, poniendo en riesgo los de otros.

CLASIFICACIÓN DE ATACANTES POR SU RELACIÓN CON EL OBJETO DEL ATAQUE

- SNIFFERS. Son individuos que se dedican a escuchar ilegalmente la red para reconstruir y descifrar los mensajes que circulan por ella.
- SPAMMERS. Gestionan el envío masivo e indiscriminado de millones de mensajes de correo electrónico no solicitado, lo que provoca el colapso tanto de los servidores como de los buzones de los destinatarios.
- PROGRAMADORES DE MALWARE. Son expertos programadores que construyen virus y otros programas maliciosos que buscan notoriedad intentando lograr una propagación desbordante.
- PERSONAL INTERNO A LA ORGANIZACIÓN. Son usuarios incorporados a la organización que por despiste, curiosidad, malicia o ingenuidad pueden causar daño a la organización. ● Antiguos empleados. Son personas que pertenecieron a la organización y que por despecho o venganza actúan contra su antigua empresa aprovechando sus cuentas de usuario aún no canceladas.
- INTRUSOS REMUNERADOS. Son personas expertas en informática contratadas por un tercero para perpetrar ataques relacionados con la fuga de información confidencial o para provocar sabotajes en los sistemas de la organización que atacan.

LA MOTIVACIÓN DEL ATACANTE

¿Qué hace que un atacante perpetre un ataque? Las motivaciones son muy variadas y frecuentemente no se dan aisladas. Entre las motivaciones más usuales se encuentran:

- El dinero u otras motivaciones de naturaleza económica.
- La ideología, por ejemplo, en el caso de ataques terroristas o la pertenencia a grupos.
- El compromiso con ciertas personas u organizaciones, a veces bajo presión.
- La autorrealización personal, el reconocimiento social o la mejora del status social, que se da sobre todo en personas con deficiencias relacionales.
- La diversión.

RIESGOS ASOCIADOS CON LAS PERSONAS

La ignorancia es el mayor riesgo que concurre en una persona, pero se combate con una contramedida tan sencilla como la formación de los usuarios del sistema. Sin embargo, no pueden despreciarse otros peligros que exigen tomar contramedidas alternativas que atenúen la valoración del riesgo que comportan.

1. Intrusos o atacantes que utilizan ingeniería social para averiguar o intuir las claves de acceso de las cuentas de usuario legales.
2. Configuración incorrecta de cuentas de usuario, grupos, permisos, derechos, etc. Reticencia a cancelar cuentas, ficheros, derechos de usuarios que ya no existen o no los necesitan.
3. Incumplimiento de las directivas o políticas de seguridad.
4. Errores en la documentación de los sistemas, de sus configuraciones o en la comunicación de esa documentación a técnicos o usuarios. También pueden aparecer problemas cuando se descuida la custodia de esta documentación.
5. Empleados descontentos o deshonestos que abusan de sus derechos de acceso a la información.
6. Equipos erráticos que nadie controla, pero que conservan derechos o funciones heredados.

7. Utilización de contraseñas inseguras, especialmente por administradores o usuarios con acceso a informaciones especialmente sensibles.
8. Usuarios que habilitan puertas traseras en sus equipos a través de las que se pueden ejecutar ataques desde el exterior.
9. Déficit en el tratamiento de medios de almacenamiento desechables.
10. Contraseñas escritas en papel.

3.1.2. EL ATAQUE INFORMÁTICO

El atacante de un sistema, una vez decidido su objetivo, acostumbra a seguir un conjunto ordenado de pasos para llevar a cabo su ataque. Previamente ha tenido que decidir qué sistema de todos los que están a su alcance es el más apropiado para su actividad. A grandes rasgos, las fases de un ataque se resumen en las siguientes actividades:

1. Descubrimiento de los sistemas que componen la red en la que se halla el objetivo.
2. Exploración de las vulnerabilidades de los sistemas de la red.
3. Explotación de las vulnerabilidades detectadas.
4. Compromiso del sistema.
5. Ocultamiento o eliminación de los rastros que prueban el ataque.

Las vulnerabilidades se explotan mediante herramientas específicamente construidas para tal fin que se denominan "exploits", que no es más que un tipo especial de malware.

La corrupción o compromiso del sistema consiste en la modificación del software o los datos residentes en el sistema para inocular puertas traseras o troyanos, creación de cuentas errantes con privilegios, etc., que puedan ser explotadas remotamente por el atacante.

La eliminación de las pruebas del ataque consistirá en borrar los ficheros de log de actividad del sistema o alteración del comportamiento de los procesos que revelan la actividad del sistema como en el caso de los rootkits.

Desde el punto de vista del atacante la oportunidad de ataque viene condicionada por los motivos que tiene para ello (lucro, diversión, venganza), las vulnerabilidades del sistema atacado (falta de actualizaciones, bugs, cortafuegos desactivados) y los conocimientos técnicos que posee (Figura 2. l).

TIPOS DE ATAQUES INFORMÁTICOS COMUNES

Se pueden considerar tantos tipos de ataques como conjunciones posibles de vulnerabilidades, motivaciones de atacante y conocimientos técnicos se posean, por tanto, la lista no es estática sino que crece continuamente, lo que hace que el administrador de seguridad tenga que estar permanentemente actualizado en sus conocimientos y tenga que auditar sus sistemas periódicamente.

Sin pretender ser una lista exhaustiva, los principales ataques a un sistema informático se ll organizan en torno a las siguientes actividades:

- Acciones de reconocimiento y descubrimiento de dispositivos y sistemas.
- Detección de vulnerabilidades.
- Robo de información mediante la interceptación de tráfico.
- Modificación de contenidos en los mensajes intercambiados por la red.
- Alteración de los números de secuencia en los mensajes transmitidos.
- Análisis de tráfico de red.
- Suplantación de la identidad de los agentes de procesos.
- Alteración de las tablas de enrutamiento, tablas de direcciones fisicas, etc.
- Conexión no autorizada a los sistemas de la red, lo que da paso a la introducción de malware, fraudes, extorsiones, ataques criptográficos, etc.

- Denegaciones de servicio, tanto simples (DOS, Denial of Service) como distribuidos (DDoS, Distributed Denial of Service).
- Propagación de malware.
- Alteración o destrucción de información.

Algunos de estos ataques serán estudiados más adelante. En cualquier caso, el gestor de la seguridad tiene que estar prevenido contra estos y otros posibles ataques. La mayor parte de las suites de seguridad para la gestión de malware proporcionan métodos de detección heurísticos que vigilan comportamientos de usuarios y aplicaciones sospechosas por alejarse del comportamiento habitual del sistema.

Por ejemplo, si un antivirus observa que un fichero ejecutable ha crecido de tamaño evaluará el evento como una posible infección en ese fichero, aunque realmente no haya averiguado de qué infección se trata. Este sistema de alertas heurísticos genera la mayor parte de los falsos positivos en antivirus.

Detección de malware en un sistema Windows y Linux

HERRAMIENTAS UTILIZADAS EN UN ATAQUE

Para ejecutar el ataque, el atacante utiliza herramientas apropiadas para el tipo de ataque que desea perpetrar y de los objetivos que pretende conseguir con él. Estas herramientas tienen un alto grado de sofisticación ya que se adecuan al ataque concreto. También hay que considerar que un ataque suele requerir varias de estas herramientas, ejecutadas en una secuencia determinada, para conseguir objetivos intermedios desde los que escalar mayores privilegios, crackear contraseñas, introducir malware, etc. Entre las herramientas más comunes están las que se describen seguidamente:

- **Escáneres de puertos**. Permiten detectar los servicios instalados en el sistema en que se ejecutan (escáner local) o en otro sistema remoto (escáner de puertos remoto). ● Sniffers o escuchadores de red. Son dispositivos o aplicaciones que escuchan la red para capturar los paquetes de datos qu circulan por ella.
- **Exploits.** Son herramientas que buscan y explotan vulnerabilidades conocidas de los sistemas sobre los que se ejecuta el ataque o bien sistemas desde los que se pretende llevar a cabo el ataque.

- **Backdoors o puertas traseras**. Son aplicaciones que permiten abrir agujeros de seguridad en los sistemas, habitualmente dejando puertos abiertos que admiten diálogos con aplicaciones externas dirigidas por el atacante.
- **Rootkits.** Son utilizados por los atacantes para ocultar malware, frecuentemente puertas traseras, por lo que despistan al sistema de vigilancia del propio sistema o de las suites de seguridad.
- **Auto-rooters.** Son herramientas capaces de automatizar un ataque realizando la secuencia de actividades encaminada a obtener el acceso al sistema o explotar una vulnerabilidad.
- **Password-crackers**. Son utilidades que permiten averiguar las contraseñas de los usuarios mediante técnicas de diccionario, fuerza bruta o ingeniería social.
- **Generadores de malware**. Son aplicaciones especialmente diseñadas para la generación de virus u otro tipo de malware.

Además de estas utilidades específicas, los atacantes suelen tener elevados conocimientos sobre técnicas de ocultación y suplantación, así como de criptografia.

Figura 3.3. Descripción de los exploits remotos descargables desde una página web para su uso en un ataque que explota una vulnerabilidad.

3.2. LA DEFENSA EN PROFUNDIDAD EN SISTEMAS PERSONALES

El concepto de defensa en profundidad deriva del ámbito militar y se orienta a que el atacante pierda su empuje inicial haciendo que tenga que superar múltiples barreras para alcanzar su objetivo en vez de un único obstáculo. Cada barrera supondrá una contramedida de seguridad. Con un sistema de defensa en

profundidad puede que el atacante consiga derribar alguna barrera, pero desde ese primer objetivo se encontrará con otra, y después con otra...

3.2.1. DEFENSA EN PROFUNDIDAD

La seguridad física consiste en la aplicación de contramedidas tales como barreras físicas o procedimientos de control que prevengan amenazas contra los recursos que se pretenden proteger, disminuyendo los riesgos.

La seguridad de los sistemas debe organizarse según las propuestas de una defensa en profundidad, es decir, debe proveer múltiples barreras con seguridad integrada en cada una de ellas.

La definición formal que proporciona el Centro Criptológico Nacional Español es que:

Definición

"La defensa en profundidad es una estrategia consistente en introducir múltiples capas de seguridad que permitan reducir la probabilidad de compromiso en caso de que una de las capas falle y en el peor de los casos minimizar el impacto (Guía STIC 400 2006)".

Esta organización en niveles permite dividir el problema global de la seguridad en otros más pequeños y manejables con soluciones altamente especializadas, contribuyendo de este modo a mejorar la calidad de la implantación del plan de seguridad. Si establecemos un modelo de capas con las soluciones tecnológicas de seguridad que se proponen para cada nivel.

APLICACIÓN	RED INTERNA	SEGURIDAD FISICA	DATOS	HOST	PERÍMETRO	SEGURIDAD FISICA
Técnicas desarrollo seguro	VLANs	Control de acceso físico	Cifrado	Gestión de contraseñas	Firewall	Política de seguridad
Gestión de contraseñas	Auditoría de seguridad	Monitorización (CTV(	Data Leak Prevention (DLP)	Parches de seguridad	Pruebas de penetración	Roles y responsable de seguridad
Control de acceso	IDS / IPS	Vigilancia y alarmas	Sanitización de datos	Prevención de intrusiones de host	web App Fitewall (WAF)	Procedimientos y estándares
Web App Firewall (WAF)	802.1X, MAC	Seguridad perimetral	Digital Rights Management (DRM)	Antimalware	IDS / IPS	Educación sobre seguridad
Evaluación de la seguridad	SSL / TLS, SSH, Kerberos	Controles ambientales		Gestión de logs	VPN, NAC	
				Gestión de vulnerabilidades		

Tabla3.4. Niveles de una defensa en profundidad.

En función del momento en que se activa la contramedida o medida de seguridad, esta puede ser reactiva (tipo pasivo) o proactiva (activa o preventiva), según si se activa como reacción a un incidente o bien antes de que se produzca como medio de prevención. Sin embargo, si atendemos al tipo de recurso protegido, las contramedidas pueden ser físicas o lógicas como ya se ha estudiado en la unidad anterior.

MEDIDAS DE DEFENSA

Describimos ahora, a modo de ejemplo, algunas de las características más importantes de las medidas de defensa que se utilizan en los sistemas asegurados con defensa en profundidad.

- **Defensa en políticas,** procedimientos y concienciación. Establecen el tono de seguridad en toda la organización en relación a la protección de activos informáticos, definen los objetivos y actividades de control y proveen un criterio para la realización de auditorías. Para mejorar su efectividad, las políticas deben ser comunicadas a todo el personal de la empresa ya que la concienciación es un elemento clave. Debe exigirse a todo el personal un compromiso serio con la seguridad.
- **Defensa en cortafuegos.** La primera línea de defensa de la red es el cortafuegos (firewall), que analiza las conexiones entre las redes interna y externa de una organización y restringe el acceso de acuerdo con una política de seguridad. Actualmente al cortafuegos se le han añadido otras funciones de seguridad que antiguamente estaban dispersas, pero sigue siendo el principal activo de seguridad en la red, siempre que sea correctamente gestionado: uno de los mayores peligros es pensar que se tiene el cortafuegos correctamente configurado cuando en realidad no sea así porque no esté actualizado, porque las reglas que componen la política de acceso no estén bien configuradas o porque no se auditen correctamente los eventos.
- **Defensa en el sistema de detección de intrusos.** Un sistema de detección de infrusos (IDS, Intrusion Detection System) es un sistema que monitoriza el tráfico de la red y alerta o previene de cualquier actividad sospechosa en tiempo real. Son sistemas que generan una gran cantidad de falsos positivos, es decir, detectan algunas actividades legítimas como si fueran maliciosas, lo que hay que vigilar constantemente para minimizarlos y que ello no interrumpa la actividad de producción de la red. Algunos IDS también pueden implantar procesos específicos de intervención para atajar los problemas de seguridad detectados.
- **Defensa en el control de acceso a la red.** El control de acceso a la red (NAC, Network Access Control) también debe ser estrechamente vigilado. Un buen control de acceso permite inspeccionar los sistemas que se conectan a la red para dilucidar si cumplen o no las políticas de seguridad requeridas por el administrador de la red. Por ejemplo, podría determinarse que cualquier ordenador que se conecte a una red debe tener su antivirus actualizado y su cortafuegos personal activado. Si el sistema no cumpliera con los requisitos exigidos, se le puede denegar el acceso o permitirle una conexión solo a ciertos segmentos de la red.
- **Defensa contra malware**. Las tecnologías antimalware, que protegen de amenazas como virus, troyanos, botnets, spyware y otras formas de código malicioso, continúan avanzando para presentarse a los usuarios como auténticas suites de seguridad altamente sofisticadas. Sin embargo, para que sean eficaces deben ser correctamente gestionadas.
- **Defensa mediante cifrado.** El cifrado de datos protege de muchos ataques, especialmente los de confidencialidad, integridad y autenticidad como ya se había estudiado en la unidad anterior. De este modo, aunque el resto de los controles hayan sido violados aún quedará una barrera

importante. Debemos recordar que la seguridad del cifrado depende de la custodia de una clave o contraseña por lo que habrá que protegerla con sumo cuidado.

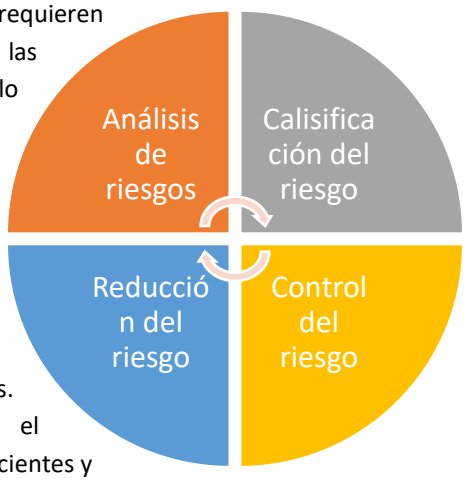
- **Defensa de los equipamientos físicos.** Aunque se tenga un buen sistema de defensa lógica, de nada servirá si no se cuida la seguridad física. Por tanto, es imprescindible mantener controles de seguridad física como cámaras, alarmas, vigilancia, etc. Siempre es importante, pero cobra especial relieve en lugares como el centro de proceso de datos.

AUDITORÍA DE SEGURIDAD

Para hacer una valoración correcta de la seguridad, lo que se concretará en una auditoría, debe analizarse el riesgo que comportan las vulnerabilidades y la capacidad de ataque de los atacantes.

Para analizar los riesgos, hay que ver qué supone una amenaza y valorar la probabilidad de que ocurra, así como la magnitud del daño que podría causar en caso de que ocurriera.

En su forma general, la gestión del riesgo (risk management) se compone de cuatro fases diferenciadas:



1. **Análisis.** Determina los componentes de un sistema que requieren protección (y que luego habrá que auditar), las vulnerabilidades que los debilitan y las amenazas que lo ponen en peligro.
2. **Clasificación**. Determina si los riesgos encontrados son asumibles o hay que actuar contra ellos para atenuarlos o eliminarlos completamente, es decir, debe definirse el modo de gestión del riesgo.
3. **Reducción.** Define e implementa las medidas de protección (contramedidas). Además, sensibiliza y capacita a los usuarios para que cumplan con estas medidas.
4. **Control**. Analiza el funcionamiento, la efectividad y el cumplimiento de las medidas para ajustar las medidas deficientes y sancionar su incumplimiento. Esta es la parte más específica de la auditoría.

Toda organización debería gestionar sus riegos de seguridad de acuerdo con una auditoría de seguridad, que no es más que un examen de cada aspecto de la red que pudiera ser hipotéticamente comprometido. Es costumbre exigir una auditoría de seguridad anualmente, aunque se recomienda hacerla con mayor frecuencia.

La auditoría puede hacerse desde dentro de la organización (auditoría interna) si ésta posee personal suficientemente formado o se puede contratar externamente a un consultor especializado mediante outsourcing (externalización).

En función del tipo de elemento auditado, las auditorias de seguridad pueden clasificarse del siguiente modo:

- **Auditoría de la red interna.** Examina la LAN de la organización, así como los sistemas que se conectan a ella.

- **Auditoría de la red perimetral.** Se encarga de analizar las redes y servicios que se publican a Internet, aunque este concepto será desarrollado más adelante.
- **Auditoría de test de intrusión.** Evalúa el riesgo de ataque comprobando su resistencia a posibles ataques. La realización de este test comporta un riesgo para el sistema evaluado ya que si el test da resultado positivo puede quedar comprometido el sistema evaluado, por ello, hay que realizarlos cuidando especialmente las condiciones en que se realiza, siempre bajo un estricto control.
- **Auditoría de vulnerabilidades.** Se trata de hacer un examen exhaustivo del software. A veces se considera al test de intrusión un caso particular del análisis de vulnerabilidades en el que se aprovecha una vulnerabilidad mediante un exploit para romper el sistema de acceso al sistema evaluado.
- **Auditoría forense.** Es un análisis forense posterior a un ataque con objeto de averiguar cómo se produjo para evitarlo en el futuro.

EL CONTROL DE ACCESO AL SISTEMA

La primera medida de protección de un sistema consiste en impedir el acceso físico al mismo. En los equipos de escritorio, esto es imposible puesto que los usuarios trabajan delante de los equipos físicos, por lo que en estos casos hay que habilitar medidas alternativas equivalentes.

En lo servidores, la protección se hace más fácil (basta con que estén bajo llave o en un lugar reservado), pero también más necesaria por el grado de compromiso que se pone en entredicho en caso de ataque. En este caso, el acceso a las salas de servidores debe estar monitorizado y controlado mediante tarjetas de acceso o sistemas biométricos.

Para diseñar un buen sistema de acceso seguro a las instalaciones se puede reflexionar sobre las siguientes cuestiones o tecnologías:

- ¿Qué salas contienen sistemas críticos y deben ser protegidas?
- ¿Qué formas de acceso podrían utilizar los intrusos?
- Definición de los horarios de acceso permitidos para cada usuario.
- Instrucción de los empleados sobre el sistema de acceso.
- Métodos de autenticación permitidos en la organización.
- Chequeos periódicos del sistema de seguridad (auditoría).
- Cambio frecuente de contraseñas como parte de la política de seguridad.
- Creación de un plan de seguridad y de respuesta frente a brechas.

A partir de aquí debe diseñarse la seguridad lógica. La parte más importante de esta seguridad es una buena política de gestión de contraseñas. Parece mentira, pero este es uno de los puntos más débiles en la mayor parte de las organizaciones. Una buena política de contraseñas incrementa notablemente la seguridad de los sistemas.

Para crear una buena política de contraseñas podríamos considerar algunos o todos los factores siguientes en función de nuestras exigencias de seguridad:

- Longitud mínima de las contraseñas de las cuentas de usuario, especialmente si se trata de usuarios administradores o con ciertos privilegios.
- Caducidad de las contraseñas. Toda contraseña de usuario debe tener una fecha de caducidad de modo que, si la pierde o se la roban sin su advertencia, el acceso estará comprometido solo durante el tiempo en que esa contraseña sea válida.
- No permitir que la renovación de una contraseña coincida con una anterior del mismo usuario.
- Exigir contraseñas complejas. Por ejemplo, que contenga caracteres alfabéticos en mayúsculas y minúsculas, símbolos y números.
- Combinar el uso de contraseñas (algo que el usuario sabe) con tarjetas de seguridad (algo que el usuario tiene).
- Auditar todos los accesos de usuario en el sistema, así como los cambios de contraseñas o las alteraciones de privilegios de las cuentas.