

CONTROL Y SEGURIDAD DE LOS SISTEMAS

TEMAS SEMANA 6:

- a) Auditorias de la seguridad informática**
- b) Metodologías**
- c) Metodologías de auditoría informática**
- d) Modelos y directrices**

- **¿Por qué es importante una auditoria de la seguridad informática?**

Primero entendamos que es la auditoria a la seguridad informática, esta se refiere a estudios tendientes a comprender y examinar el estado de la seguridad de las tecnologías de la información.



Se trata de un servicio llevado a cabo por profesionales externos a la organización y tiene la finalidad de descubrir posibles vulnerabilidades tras revisiones exhaustivas de software, redes de comunicación, servidores, estaciones de trabajo, dispositivos móviles.

Entendamos a la auditoría de seguridad informática como una evaluación de la infraestructura y los sistemas informáticos cuyo fin es detectar errores y fallas que mediante un informe detallado que se describen:

Equipos instalados, servidores, programas, sistemas operativos...

Procedimientos instalados

Análisis de Seguridad en los equipos y en la red

CONTROL Y SEGURIDAD DE LOS SISTEMAS

Análisis de la eficiencia de los Sistemas y Programas informáticos

Gestión de los sistemas instalados

Verificación del cumplimiento de la Normativa vigentes

Vulnerabilidades que pudieran presentarse en una revisión de las estaciones de trabajo, redes de comunicaciones, servidores.

Entonces entendemos que es necesaria una auditoría a la seguridad porque proporciona información esencial a los administradores y a su personal a partir de la cual se identifican las fortalezas y debilidades de la infraestructura tecnológica, permitiendo que los recursos se apliquen donde sean más necesarios.

El proceso de auditoría también sirve como herramienta para que las organizaciones puedan evaluar sus procesos internos de gestión y determinar si el sistema de gestión de seguridad es adecuado para cumplir los objetivos.

Las organizaciones auditan la gestión de la seguridad por dos razones fundamentales; la primera garantizar la continuidad de la operación de la organización basados en los principios de disponibilidad, confidencialidad e integridad de la información y la segunda están obligadas por ley a ejercer un deber de cuidar la información de sus clientes, proveedores y empleados requiriéndose sistemas y procesos claramente definidos para gestionar los riesgos.

Existen diferentes tipos de auditorías a la seguridad con las que se logra analizar y evaluar diferentes tipos de riesgos a los que están expuestos las organizaciones, por ejemplo existen auditorías de seguridad 360° que son internas, externa, organizacionales o industriales con ellas logramos descubrir de puntos débiles en web, correo, oficinas, oficinas remotas, segregación de roles; revisar de políticas de dominio, actualizaciones, antivirus, etc; revisar privilegios de cuentas de usuarios y

CONTROL Y SEGURIDAD DE LOS SISTEMAS

segregación de tareas y comprobar si los empleados están conscientes de las técnicas de ingeniería social que tanto daño causan a las organizaciones.

Las auditorías a la seguridad informática son importantes ya que son el método de asegurar que todo funcione adecuadamente. Solo así, estarás seguro de que todas las medidas de protección que has instalado en los servidores, redes, páginas web, dispositivos móviles y equipos informáticos son las más recomendadas y funcionan perfectamente.

Y si no es así, permitirán encontrar los puntos donde se debe reforzar la ciberseguridad. Algo que puede hacerse instalando herramientas de seguridad específicas o actualizando las existentes.



- **¿Qué tipos de auditorías a la seguridad existen?**

Existen diferentes tipos de auditorías dentro de la seguridad informática, dependiendo del interés de la organización se podrán llevar a cabo una o varias de ellas.

Auditoría externa o perimetral: Se realiza desde el exterior del perímetro de seguridad de la organización para descubrir vulnerabilidades que pueden ser explotadas remotamente. El auditor asume el rol de un atacante externo a la empresa que, sin el conocimiento de información previa, puede obtener algún beneficio de la organización, o incluso, acceso a información sensible que comprometa la privacidad de la empresa, poniendo a prueba el estado de las barreras de seguridad que dispone la empresa entre internet y su red corporativa.

CONTROL Y SEGURIDAD DE LOS SISTEMAS

Auditoría interna: Se realiza desde dentro de la organización, partiendo de la propia red local o corporativa del cliente para contrastar su nivel de seguridad. El auditor asume el rol de un usuario que dispone de acceso a los sistemas internos de la empresa o desde un sistema conectado a dicha red, bien porque sea el dueño de las credenciales o porque mediante un ataque ha elevado privilegios de forma ilícita.



Auditoría web: Se realiza a un servicio web para detectar cualquier auditoría web: Se realiza a un servicio web para detectar cualquier vulnerabilidad que pueda poseer. Coincide en que también es externa.

Auditoría de red inalámbrica: Se realiza a una red inalámbrica, tanto dentro como fuera de la organización del cliente. En el proceso de auditar las comunicaciones Wireless se llevan a cabo distintas pruebas con el fin de determinar el nivel de seguridad y confidencialidad que proporcionan la configuración de dichas redes.

Auditoría de código fuente: Se realiza sobre una aplicación, herramienta o programa, mediante el uso de la ingeniería inversa para detectar la existencia de posibles errores, bugs de seguridad, puertas traseras, etcétera.

CONTROL Y SEGURIDAD DE LOS SISTEMAS

Auditoría de dispositivos móviles: Se realiza a un dispositivo o una red de dispositivos móviles de una organización. Sobre todo, está enfocada en los móviles de empresa.

Ejercicio de Red Team: En este tipo de ejercicio será nuestro equipo de auditores los que simularan el rol de un adversario cuyo objetivo será realizar una intrusión con la que lograr comprometer los principales activos de la organización.

También existe la auditoria denominada hacking ético. El hacking ético es en sí una auditoría efectuada por profesionales de seguridad de la información, quienes reciben el nombre de “pentester”. A la actividad que realizan se le conoce como “hacking ético” o “pruebas de penetración”

Las pruebas de penetración surgieron como respuesta a la presencia y realización de los primeros ataques informáticos a las organizaciones, los cuales trajeron graves consecuencias, como pérdidas monetarias y de reputación. Es aquí donde interviene el trabajo de un “hacker ético”, ya que su labor es buscar vulnerabilidades en los sistemas de la organización para, posteriormente, poder mitigarlos y evitar fugas de información sensible.

Durante los últimos años, nuevas técnicas de intrusión que atentan contra la seguridad de la información se han sofisticado, por lo que organizaciones y empresas han implementado al hacking ético, aunque combatir la idea de que esta actividad es dañina, no ha sido tarea fácil.

El hacking ético, también es conocido como prueba de intrusión o pentest, se define esencialmente como el “arte” de comprobar la existencia de vulnerabilidades de seguridad en una organización, para posteriormente a través de un informe, revelar aquellos fallos de seguridad encontrados, mitigarlos a la brevedad posible y evitar fugas de información y ataques informáticos.

Pese a su mala fama, no todos los hackers son delincuentes cibernéticos, algunos ayudan a las organizaciones a reforzar su seguridad. Por ello, para tratar de diferenciar a un grupo de otro, se introdujeron los términos crackers y hackers éticos.

CONTROL Y SEGURIDAD DE LOS SISTEMAS

Los primeros identifican a aquéllos que realizan técnicas de intrusión con fines maliciosos y lucrativos; mientras que los segundos se refieren a quienes lo hacen con fines éticos y por el bien de la organización que lo solicite.

Otra conceptualización que reciben es la de “sombrero negro o Black Hat” y “sombrero blanco o White Hat”.

Los hacker de sombrero negro, mejor conocidos como “Black Hat”, tienen la cualidad de explotar vulnerabilidades en los sistemas con la finalidad de demostrarse que lo pudieron hacer burlando la seguridad del mismo. Ejemplo de ello lo tenemos en el Control y seguridad de los sistemas caso acontecido en febrero del 2008, cuando la página web oficial de la Presidencia de la República fue afectada por un atacante que se hacía llamar “H4t3 M3”; logró dejar como recordatorio una imagen de lo más elocuente gracias a que esa página web tenía una vulnerabilidad.

La información fue revelada en el foro de la Comunidad Underground Latinoamericana, en dónde el joven hacker advirtió que podía modificar desde la agenda presidencial hasta las noticias, pero que no lo haría.

Por su parte, los hackers de sombrero blanco o “White Hat”, también conocidos como hackers éticos, pentesters y expertos en seguridad; tienen la finalidad de realizar pruebas de intrusión en organizaciones que así lo pidan, para posteriormente rendirles un informe, en el que se detallan todos aquellos puntos vulnerables encontrados para que, posteriormente, la empresa los mitigue a la brevedad posible.

CONTROL Y SEGURIDAD DE LOS SISTEMAS

A continuación, se describe dicha clasificación en la siguiente ilustración:



- ¿Qué se evalúa en una auditoria de tipo hacking ético?

Los servicios que con mayor frecuencia ofrecen los hackers blancos (hackers éticos) a las empresas son las pruebas de penetración, con la intención de analizar si la compañía está preparada para soportar un ataque sofisticado perpetrado desde fuera, es decir por un hacker externo o por un atacante interno con conexión a la red.

Durante las pruebas de penetración, según enumera Victor Chapela, se analizan tanto la red interna, como Internet, aplicaciones expuestas, servidores, puertos y avenidas de acceso, además se hacen pruebas de contraseñas. Al mismo tiempo, se analiza la red inalámbrica, de ésta se revisa la configuración, se hace sniffing[1] de tráfico y contraseñas, intentando penetrar y romper el cifrado.

Parte de la auditoría incluye también revisar módems, VPN, página web, incluso se hace ingeniería social, es decir se trabaja con el personal o con los asociados de la empresa para ver si se dejarían engañar para proporcionar contraseñas o acceso a la red.

CONTROL Y SEGURIDAD DE LOS SISTEMAS

De igual forma, se mide el nivel de respuesta a incidentes internos, también se busca emular si un empleado de bajos privilegios podría tener acceso a los estados financieros o a la nómina de la compañía. Se consideran además los valores de los activos, la criticidad de la vulnerabilidad y la probabilidad del ataque, su impacto, la forma de corregirlo y el esfuerzo requerido para esto.

Para evitar cualquier contratiempo o daño a la infraestructura, o continuidad de negocio del cliente, las pruebas siguen una metodología y manejan estándares, como el Manual de la Metodología Abierta de Comprobación de la Seguridad (OSSTMM, por sus siglas en inglés) o el Proyecto Abierto de Seguridad de Aplicaciones Web (OWASP).

Según el Mapa de Seguridad propuesto por el OSSTMM[2], las secciones a las cuales se aplican el hacking ético son las siguientes:

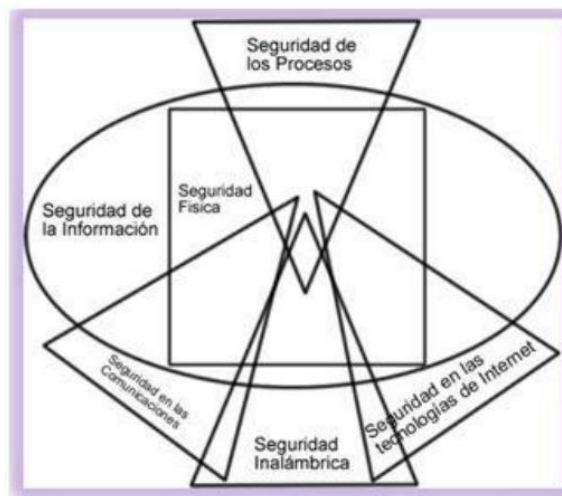


Fig. 2 mapa de seguridad

Fuente: tomado del manual de la metodología abierta de testeo de seguridad osstmm 2.1 de isecom

A continuación, se describen brevemente dichas secciones.

CONTROL Y SEGURIDAD DE LOS SISTEMAS

a. Seguridad física

Alude a las pruebas de seguridad realizadas a un medio físico y no electrónico en la naturaleza. Comprende el elemento tangible de la seguridad donde la interacción requiere un esfuerzo físico o una transmisión de energía para que sea manipulado.

A considerar:

Revisión del perímetro

Revisión de monitoreo

Evaluación de controles de acceso

Revisión de respuestas de alarmas

Revisión de ubicación y

Revisión de entorno.

b. Seguridad en las comunicaciones

Comprende dos fases: Telecomunicaciones y las redes de datos. La primera fase alude a todas las redes de telecomunicación, sean digitales o analógicas, la otra, se refiere a todos los sistemas electrónicos y redes de datos donde la interacción se realiza a través de cables establecidos y cables de líneas de red.

c. Seguridad inalámbrica

Refiere a todas las comunicaciones electrónicas, señales y emanaciones que se producen del conocido espectro EM – Electromagnetic. Esto incluye ELSEC como comunicaciones electrónicas, SIGSEC como señales, y EMSEC que son emanaciones sin ataduras por los cables. Los módulos de verificación requeridos en el hacking ético para dicho rubro son:

Verificación de radiación electromagnética (EMR)

Verificación de redes inalámbricas 802.11, Verificación de redes bluetooth

Verificación de dispositivos de entrada inalámbricos

Verificación de dispositivos móviles inalámbricos

Verificación de comunicaciones sin cable

CONTROL Y SEGURIDAD DE LOS SISTEMAS

Verificación de dispositivos de vigilancia inalámbricos

Verificación de dispositivos de transacción inalámbricos

Verificación de RFID y

Verificación de sistemas Infrarrojos.

d. Seguridad en las tecnologías de Internet

Se refiere a las pruebas de intrusión efectuadas a las aplicaciones web, tales pruebas son esencialmente el "arte" de comprobar una aplicación en ejecución remota o local, sin saber el funcionamiento interno de la aplicación, para encontrar vulnerabilidades de seguridad[3]. Los módulos de verificación requeridos en el hacking ético para dicho rubro son:

Logística de Controles

Sondeo de Red,

Identificación de los servicios de sistemas,

Búsqueda de información competitiva,

Revisión de privacidad,

Obtención de Documentos,

Búsqueda y verificación de vulnerabilidades,

Testeo de aplicaciones de internet,

Enrutamiento, Testeo de sistemas confiados,

Testeo de control de acceso,

Testeo de Sistema de Detección de Intruso IDS,

Testeo de Medidas de Contingencia,

Descifrado de contraseñas,

Testeo de Negación de servicios y

Evaluación de políticas de Seguridad.

CONTROL Y SEGURIDAD DE LOS SISTEMAS

e. Seguridad del resguardo de información

Aborda los medios empleados para el almacenamiento adecuado de la información, va ligado con los controles empleados para su seguridad.

f. Seguridad de los proceso

Representa un método para lograr acceso privilegiado a una organización y sus activos mediante la ayuda involuntaria del personal de la organización, en especial con la ayuda de aquellos que resguardan los puntos de accesos principales. Esto se hace por medios de comunicación tales como el teléfono, e-mail, chat, tableros de anuncios, etcétera, y se realiza de una manera fraudulenta con la finalidad de obtener una posición "privilegiada

En este rubro la aplicación del hacking ético se emplea por medio de la práctica de la ingeniería social, la cual es una técnica especializada o empírica del uso de acciones estudiadas o habilidosas que permiten manipular a las personas para que voluntariamente realicen actos que normalmente no harían[4].

En conclusión, el hacking ético es una técnica aplicada a distintos escenarios, por lo que es importante hacerlo del conocimiento de la gente en beneficio de las organizaciones; así la relación entre detección y explotación de vulnerabilidades existentes podrá controlarse de la mejor manera posible.

- **¿Qué se debe tener en cuenta para auditar la seguridad informática?**

Cuando se trata de implementar modelos para gestionar la seguridad de la información el aspecto más importante para garantizar la mejora del sistema **son las revisiones**, y una de sus principales herramientas son las auditorías de seguridad. Realizar una auditoría de seguridad suele ser una tarea complicada **pero que sirve para entregar mucha información acerca del estado de la seguridad**.

CONTROL Y SEGURIDAD DE LOS SISTEMAS



Realizar una auditoría de seguridad suele ser una tarea complicada pero que sirve para entregar mucha información acerca del estado actual de la protección de la información en una empresa. Además, brinda la posibilidad de comparar los sistemas de gestión con respecto a normativas y requerimientos legales que deben cumplir las organizaciones.

Con todas las implicaciones que tiene una auditoría de seguridad de la información es necesario tener claro cuáles son los puntos por los cuales se quiere empezar. Para esto es recomendable analizar que en la política de seguridad se tenga en cuenta la clasificación de los activos de información al igual que las medidas de protección respectivas. Para conocer un poco más sobre las políticas de seguridad pueden leer nuestro post **¿Qué se debe tener en cuenta en la política de seguridad de la información?**

Con una auditoría se debe llegar a validar que los niveles de riesgo a los cuales está expuesta una organización realmente cumplen con sus políticas, garantizando que esta, a su vez, cumple con las regulaciones externas y los estándares que apliquen según la industria. Este análisis debe ser transversal a la organización, revisando todos sus procesos.

Cuando se trata de auditoría de un sistema de gestión de la seguridad, se pueden considerar dos opciones. La primera es realizar una auditoría interna es decir, utilizando un equipo de trabajo de la empresa. La gran ventaja de este tipo de auditorías es que las realizan personas que conocen los procesos y cómo funciona la empresa, por lo cual puede llegar a ser más rápida y realizarse con una mayor periodicidad.

CONTROL Y SEGURIDAD DE LOS SISTEMAS

La otra opción es hacer una auditoría externa, en la cual participa un experto ajeno a la empresa y se hace más independiente. La principal ventaja que tiene hacer este tipo de auditorías es que al no conocer mucho de la empresa no hay prejuicios que puedan hacer que se omitan algún tipo de revisiones, que de otra forma parecerían obvias. Dentro de este tipo de auditorías es común que se realice algún Penetration Test para buscar las vulnerabilidades que puedan dar lugar a un incidente de seguridad.

Independiente del tipo de auditoría seleccionado siempre se debe velar porque además de tener especialistas técnicos, se incluyan también especialistas en gestión de procesos para trabajar no solamente sobre la tecnología sino también sobre la forma en que fluye la información a lo largo de la empresa.

En cualquier caso debe ser clara la necesidad de la revisión periódica de los riesgos en las empresas, lo cual se puede lograr a través de auditorías constantes, siguiendo un proceso juicioso y que esté incorporado como parte de la gestión de la seguridad. Finalmente para que una auditoría genere realmente valor debe estar ligada a los objetivos estratégicos de tal forma que su cumplimiento no sea ajeno a garantizar la seguridad de la información.