AUDITORIA DE SEGURIDAD INFORMATICA

John Edinson Martínez
Carlos Andrés Giraldo
password s.a.

1. ABSTRAC

Uno de los elementos fundamentales para mejorar la seguridad de la información en una organización es la auditoria de seguridad; Las etapas y metodología de la auditoria deben estar bien definidas y deben ser cumplidas estrictamente.
Un ejemplo de las consideraciones y elementos a considerar en la auditoria de seguridad informática es el análisis de cómo enfrenta la organización uno de los mas grandes males de los últimos años; "el spam".

2. INTRODUCCION

La seguridad informática es hoy día uno de los mayores dolores de cabeza para las grandes organizaciones. Con millones de dólares reportados en pérdidas económicas tan solo en Estados Unidos, según algunas fuentes en Internet, la seguridad informática se convierte cada vez más en una necesidad irremediable y urgente para todos.

Mientras las epidemias de virus informáticos siguen causando estragos en la economía mundial y la persecución contra los responsables es cada vez más persistente, las nuevas tecnologías de la información se siguen difundiendo cada vez mas llegando a millones de personas, muchas de las cuales no saben a que se están enfrentando.

3. AUDITORIA DE SEGURIDAD

La auditoria nace como un órgano de control de algunas instituciones estatales y privadas. Su función inicial es estrictamente económico-financiera y buscaba optimizar los recursos de todo el componente informático de la organización, pero con los nuevos desarrollos tecnológicos se ha ido especializando y profundizando.

La función auditora debe ser absolutamente independiente; no tiene carácter ejecutivo, ni son vinculantes sus conclusiones. Queda a cargo de la empresa tomar las decisiones pertinentes. La auditoria contiene elementos de análisis, de verificación y de exposición de debilidades y disfunciones. Aunque pueden aparecer sugerencias y planes de acción para eliminar las disfunciones y debilidades antedichas; estas sugerencias plasmadas en el Informe final reciben el nombre de recomendaciones.

Es muy importante aclarar el concepto de Auditoria de seguridad informática puesto que se puede llegar a confundir con la clásica auditoria de sistemas y aunque son dos conceptos similares en primera instancia, los objetivos y enfoque de cada uno son diferentes.

AUDITORIA DE SISTEMAS – Definición

La Auditoría de Sistemas es el conjunto de técnicas que permiten detectar deficiencias en las organizaciones de informática y en los sistemas que se desarrollan u operan en ellas, incluyendo los servicios externos de computación, que permitan efectuar acciones preventivas y correctivas para eliminar las fallas y carencias que se detecten.

Se verifica la existencia y aplicación de todas las normas y procedimientos requeridos para minimizar las posibles causas de riesgos tanto en las instalaciones y equipos, como en los programas computacionales y los datos, en todo el ámbito del Sistema: usuarios, instalaciones, equipos.

La auditoria de seguridad informática analiza los procesos relacionados únicamente con la seguridad, ésta puede ser física, lógica y locativa pero siempre orientada a la protección de la información. Es este el punto de mayor diferencia, la seguridad informática se preocupa por la integridad y disponibilidad de la información mientras la auditoria de sistemas incluye otras características más administrativas.

4. CONSIDERACIONES DE LA AUDITORIA

Para un proceso de auditoria de seguridad informática es muy importante ser ordenado y meticuloso y para esto es necesario adoptar una metodología. Existen muchas metodologías, por ejemplo OCTAVE, desarrollada por el instituto Carnegie Mellon – Software Engineering Institute, pero en el entorno local se hace necesario adoptar una metodología estable, bien difundida y libre, es por esto que una buena opción es la utilización de la OSSTMM v2.1. o Manual de la metodología abierta de testeo de seguridad publicado por ISECOM (Institute for segurity and open methodology). Que se considera es amplia y muy acertada para la realidad nacional.

Algunos conceptos importantes para ISECOM considerar un test de seguridad informática como cun verdadero test son los siguientes:

- Cuantificable: Es muy importante no dar conceptos finales de seguridad abstractos o poco precisos, por ejemplo, "mas o menos bien". Los resultados

deben ser cuantificables.

- Consistente y que se pueda repetir: Los test de seguridad no deben surgir de la suerte sino de procesos planeados y bien definidos.
- Valido en el tiempo: Un test de seguridad se debe poder repetir periódicamente sin que esto implique modificaciones considerables.
- No basado en marcas comerciales: La seguridad informática debe ser objetiva y para esto es necesario realizar pruebas que no estén enfocadas a una sola marca de equipos
- Exhaustivo
- Concordante con las leyes nacionales

Una práctica muy común en nuestros días es el hackin ético. Estas prácticas tienen unos costos bastante elevados en el mercado internacional debido a que son análisis mucho mas profundos que buscan penetrar perímetros de defensa y no solamente analizarlos, es decir, exige un nivel de análisis mas profundo que en una auditoria de seguridad informática.

Los Checklist o listas de chequeo

Otro factor que es muy importante considerar es el de las listas de chequeo. En una gran medida la información sobre los problemas de seguridad informática la tienen los propios usuarios y solo se necesita proveer un mecanismo adecuado para que ellos mismos definan sus deficiencias en seguridad informática. El mecanismo mas adecuado en este caso son las listas de chequeo, aunque se debe tener cuidado y proveer las listas correctas al personal adecuado e identificar en que momento las debe desarrollar el auditor mediante observación y no el usuario.

4. LOS PROCESOS DE UNA AUDITORIA DE SEGURIDAD INFORMATICA

La auditoría de seguridad informática consiste en la evaluación, análisis y generación de soluciones para el recurso computacional de la organización. Los procesos cubren cuatro frentes específicos:

1. Auditoría desde Internet, identificando las vulnerabilidades a las que se ve expuesto el recurso computacional y el sitio Web de la organización desde Internet por parte de delincuentes informáticos. Claramente los ataques desde Internet crecen cada día y aunque para muchos usuarios no es muy importante porque consideran que nadie va

a estar interesado en su información estar expuestos a ataques desde cualquier ricon del mundo no debería ser una opción.

2. Auditoría desde la red interna (LAN) de la organización para la identificación de las vulnerabilidades generadas desde el interior de la organización aprovechando los beneficios de la red de área local. Las estadísticas demuestran que un considerable número de ataques informáticos a organizaciones en todas partes del mundo incluyendo Colombia son provenientes del interior de la misma organización. En muchos casos han sido por trabajadores ofendidos o por empleados graciosos pero todos han causado grandes daños. Es por esto que no se debe subestimar la seguridad del interior de la red.
3. Trabajo sobre los equipos, ejecutando herramientas software de identificación de vulnerabilidades, identificación de tipos de archivos contenidos de software espía, virus informáticos y análisis personales del estado físico, lógico y locativo de cada uno de los equipos. Existe un número tan elevado de software potencialmente dañino alcansable por cualquier usuario que es muy importante la evaluación del software de cada equipo.
4. Ejecución de entrevistas sobre el manejo de las políticas de seguridad física, lógica y locativa de los miembros de la organización. Un proceso fundamental en la seguridad de los sistemas es la evaluación del manejo del equipo y este manejo se debe referir no solo al componente lógico sino también al manejo físico y locativo. En este punto es importante hace la diferencia entre seguridad física y locativa. La seguridad locativa se refiere a las instalaciones y la física al manejo del hardware del equipo.

Los procesos o fases de la auditoria se complementan mutuamente y si se llegara a desarrollar solo algunos de estos el aumento de la seguridad de la organización no seria considerable. Es como cerrar la puerta de su casa con varias cerraduras y dejar abierta una gran ventana hacia la calle.

Evaluación del equipo

Cuando se hace la revisión o evaluación de cada equipo sea estación de trabajo o servidor se deben considerar elementos como: Los permisos de los usuarios que pueden iniciar sesión en el equipo o que tienen acceso a él. El rendimiento de la máquina y la cantidad de carga del procesador para limitar aun más ataques de denegación de los servicios. Los procesos presentes en los servicios, estos procesos se deben conocer

como la palma de la mano para poder identificar cuando exista la presencia de procesos no deseados o que tenga algún tipo de bug. Los mas importante y lo que mayores vulnerabilidades introduce a la maquina son los servicios o aplicaciones que ofrece la máquina, por ejemplo un servidor Web o un servidor de Bases de Datos.

5. EJEMPLO DE ANALISIS

Uno de los procesos más importantes de la auditoria de seguridad informática es el análisis de los servicios, para esto se ha dispuesto el siguiente ejemplo sobre uno de los problemas que mas afecta en la actualidad los servicios y las tecnologías de internet, el "SPAM".

SPAM, ENTENDAMOS EL PROBLEMA

El tema que ocupa este apartado es un problema de cifras alarmantes en todas las perspectivas desde las que se podría analizar, "El Spam". Se analizaremos las técnicas empleadas por los spammers y algunos datos resultados de estudios realizados en todo el mundo.

Es muy común ver como los delincuentes informáticos aprovechan las vulnerabilidades de los sistemas que en la mayoría de casos son producto de una mala administración. Los costos, los recursos consumidos y los problemas relacionados con el envío, en la mayoría de casos, de miles o millones de mensajes son asumidos por servidores vulnerables.

Sin embargo existen muchas aplicaciones que contribuyen a la prevención y control del spam, tanto para servidores como para usuarios finales, algunas de las cuales son muy efectivas y con las cuales podemos determinar la cantidad de mensajes basura y lo que implica cada uno. De esta forma se pueden hacer estudios y generar datos estadísticos de este flagelo de la nueva era.

Un estudio norteamericano reciente dice que el receptor de un mensaje spam pierde una media de 4,4 segundos por ese suceso totalmente inadecuado. Multiplicando por el número de mensajes y receptores, llegan a la conclusión de que eso equivale a cuatro mil millones de dólares en pérdidas de productividad anuales. Y teniendo en cuenta otro tipo de detalles, las empresas se ven obligadas a perder cifras que superan los cinco mil millones.

Un poco de historia

Originalmente 'Spam' se llamo al jamón con especias (Spiced Ham) producido por *Hormel Foods Corporation* en 1926 como el primer producto de carne enlatada que no requería refrigeración. Esta

característica hacia que estuviera en todas partes, incluyendo en los ejércitos americanos y rusos de la segunda guerra mundial. Tal vez por esto se ha utilizado el termino para calificar el correo electrónico no solicitado, y se ha convertido en una de las mayores molestias para las personas en la red.

Las siglas proceden de Shoulder Pork and hAM o SPiced hAM. La sigla se empezó a asociar con el correo indeseado gracias a los autores del show Monty Python's Flying Circus.
Es posible que la palabra spam se haya empleado por primera vez en los chats Bitnet Relay, que eran los precursores de IRC.
Por el primer caso de spam en el correo se considera una carta enviada en 1978 por Digital Equipment Corporation. Dicha empresa mandó un anuncio sobre el nuevo ordenador DEC-20 a todos los usuarios de Arpanet de la costa occidental de los E.E.U.U. Sin embargo, la palabra spam no se adoptó antes de 1994, cuando en Usenet apareció un anuncio del despacho de los abogados Lawrence Cantera y Martha Siegiel. Informaban en él de su servicio de rellenar formularios de la lotería para visado americano. El anuncio fue enviado mediante un script a todos los grupos de discusión de entonces.
Actualmente, con la noción spam se determina correo electrónico enviado a propósito, en grandes cantidades, a personas que no desean recibir tales mensajes. Pueden (pero no tienen que) ser ofertas comerciales, propaganda política, etc.

Eventos en el año 2003

En enero 2003 la empresa encargada de registrar los dominios británicos de Internet, Nominet UK, suspendio durante 8 horas su servicio *Whois*, que permite identificar a los propietarios de los dominios dados de alta. La razón: los spammers atacaron a los servidores, para intentar apoderarse de su base de datos. El comunicado que ofreció la empresa afirmaba: "Alguien muy persistente ha intentado conseguir una copia detallada del registro .uk. El ataque consiste en hacer preguntas sistemáticamente al servidor Whois, desde cientos de servidores".

El 20 de febrero 2003 ante el creciente aumento del 'correo basura' - este año se recibirán en Estados Unidos unos 320.000 millones de correos electrónicos no solicitados, según estimaciones de la firma de investigación Jupiter Research [Fuente: *CNN*].

El 22 de abril 2003 Ian Ralsky, el rey del spam, recibió un autentico ataque distribuido de denegación de servicio que consiste en inundar su correo postal.

El 9 mayo de 2003 la empresa Microsoft, propietaria de *Hotmail*, dice que sus sistemas de control

del spam bloquean 2400 millones de mensajes de correo basura.

En mayo de 2003 Estados Unidos celebra una audiencia de la comisión de comercio celebrada en torno al problema del spam. En ella, el vicepresidente de AOL (America Online), Ted Leonsis, afirmó que es necesaria una ley nacional para tratar a combatir el problema del spam. El presidente de la comisión de comercio, John McCain, aventuró como fecha probable de envío del proyecto de ley anti-spam al pleno del Senado, para el mes de agosto. [Fuente: Reuters]

En junio de 2003 MessageLabs, un importante proveedor de sistemas de seguridad informática, publica en su estudio mensual que, de los mensajes controlados por ellos (133.9 millones), el análisis indica que el spam ya representa el 55.1%.

De donde proviene el spam?

En un estudio reciente, correspondiente al primer semestre del 2004, se aprecia claramente, que son tan solo 5 países los responsables de alojar el 99,68% de los sitios que son referenciados a través de correos no deseados.
Según Commtouch, empresa desarrolladora de tecnología anti-spam, en un análisis asegura que los correos masivos, han elegido a China (73, 58%), Corea del Sur (10, 91%), Estados Unidos (9,47%) y Rusia (3,5%) para instalar sus sitios web. En este ranking figuran tambien dos paises latinoamericanos entre los primeros lugares, Brasil con el 2,23% y Argentina con el 0.09%.
Sin embargo, Estados Unidos con un 55.69% sigue liderando la lista de países desde los cuales se siguen enviando los correos basura, seguido por Corea del Sur (10.23%) y China (6,60%). Más abajo se encuentran Brasil, Canadá y Hong Kong.
El estudio también muestra el crecimiento del spam, que en vez de disminuir, creció de 350.000 correos por día en el inicio del semestre, a cerca de 500.000 en junio. El idioma más utilizado en los mensajes fue el inglés, ya que sólo el 5,77% de los correos no solicitados fue escrito en otro idioma.
En cuanto a las temáticas del spam, el tema recurrente pareció ser la oferta de todo tipo de drogas y medicamentos, con un 29,53%. En el primer semestre de 2004, la palabra Viagra apareció en el 14,1 % de todos los mensajes enviados.
En segundo lugar, se enviaron masivamente ofertas de hipotecas y refinanciación de deudas (9,68% del total). El tercer puesto fue para los ofrecimientos de alargar el órgano sexual masculino (7.05%). Los correos vendiendo pornografía y acceso a casinos virtuales, bajaron un 3,1% y 0,45% respectivamente.
Menos del 10% de los correos analizados cumplían con las

regulaciones CAN-SPAM de Estados Unidos, que indican que el mensaje debe tener una casilla activa a la cual responder, debe incluir una dirección postal, y una forma real de desuscripción. Según estas reglas, también se debe aclarar que el mensaje enviado es una oferta o publicidad que pudo no ser solicitada por el destinatario.
Otra de las conclusiones del informe es que los spammers están sofisticando cada día mas la forma de burlar de los filtros antispam. Alguna de sus tácticas incluyen la inserción de caracteres al azar y palabras combinadas sin sentido, para desafiar al software bloqueador. Todo esto indica que la solución a la problemática del spam todavía está muy lejana.
Pero para entender mas el problema es necesario conocer mas a fondo como es el proceso normal de envió de un correo electrónico, como se desarrolla la comunicación entre servidores y cuales pueden ser los motivos por los cuales un servidor es candidato a ser usado para el envió masivo de correo electrónico basura o spam.

Programas que intervienen en el envío de un correo

En el envío del correo participan varios programas:
• El programa usado por el usuario final, que sirve no sólo para recibir y enviar, sino también para leer y escribir coreos electrónicos, es conocido como MUA - Mail User Agent. Ejemplos: Mozilla Thunderbird, Outlook Express, Incredimail, PINE, Mutt;
• La parte del servidor responsable de la comunicación con los usuarios (recepción del correo) y del envío y recepción del correo de otros servidores es conocida como MTA - Mail Transfer Agent. Los más conocidos son: sendmail, qmail, Postfix, Exim;
• La parte del servidor responsable de la entrega del correo al usuario local se llama MDA - Mail Delivery Agent. Ejemplos de MDA autónomos: Maildrop, Procmail. La mayoría de los MTA poseen mecanismos propios de entrega del correo local a los usuarios, por tanto no siempre es necesario emplear MDA adicionales.

Servidores open relay

Cuando fue creado el protocolo SMTP, no existía el problema del spam y cada usuario tenía la capacidad de utilizar cualquier servidor para enviar sus mensajes al mundo. Ahora, cuando los spammers buscan la oportunidad de aprovecharse de algún servidor y enviar miles de mensajes, este método no es aconsejable. Los servidores que permiten el envío de correo al mundo sin autorización son conocidos como open relay.
Cada servidor que permite a usuarios no autorizados el envío de correo, tarde o temprano cae en manos de los spammers, lo que puede acarrear consecuencias muy serias. Primero: porque puede provocar una reducción de eficacia

del servidor, el cual en vez de recibir y entregar mensajes a usuarios autorizados, enviará spam. Segundo: el proveedor de internet puede anular el contrato con motivo del uso del servidor para fines ilegales o inmorales. Tercero: la dirección IP del servidor terminara en las listas negras y muchos servidores dejarán de recibir sus mensajes (la eliminación de la IP de muchas listas negras es muy difícil, incluso a veces imposible).

Servidores *open proxy*

Otro tipo de servidores mal configurados que pueden ser empleados
por los spammers son los *open proxy*, o sea, los servidores proxy a los que pueden conectar usuarios no autorizados. Los servidores *open proxy* pueden funcionar en base a una gama extensa de programación y protocolos. El protocolo más frecuente es HTTP-CONNECT, pero hay algunos *open proxy* que permiten la conexión a través de los protocolos HTTP-POST, SOCKS4, SOCKS5 y otros.
Un *open proxy* puede ser usado por el spammer de manera idéntica que *open relay* para enviar correspondencia no autorizada. Además, muchos *open proxy* permiten ocultar su dirección IP. Un proxy de esta índole es un bocado exquisito para los spammers.

Zombie

Zombie es un método nuevo y a la vez el más invasor, empleado por los spammers para traspasar los costos y las responsabilidades a terceros. Esta técnica está basada en la unión de un virus (worm) con un troyano. El objetivo es crear un *open proxy* en el ordenador infectado por el virus. De esta manera se crea una red enorme de *open proxy* anónimos, de los que se aprovechan los spammers de todo el mundo. El ejemplo más conocido de zombie son los virus de la serie *Sobig*. He aquí como funciona el virus:

- El primer elemento, después de infectar el ordenador del usuario (al abrir el adjunto de un email), se envía a todas las direcciones encontradas en los archivos .txt y .html del disco duro.
- Entre las 19:00 y las 23:00, hora UTC, se conecta con una de las 22 direcciones IP que contiene el código del virus) en el puerto 8998 UDP para obtener la dirección URL de la que podrá tomar el segundo elemento.
- Tras haber tomado el segundo elemento (el troyano) se instala y se ejecuta; la dirección IP del ordenador infectado es enviada al autor del zombie. A continuación, se toma el tercer elemento.
- El tercer elemento es el programa *Wingate* modificado, que después de su instalación automática pone en marcha el *open proxy* en el ordenador del usuario.


password