ASEGURAMIENTO DE INFRAESTRUCTURAS DE RED Y DE SERVIDORES

Montoya, Jorge.
jorge.montoya08@hotmail.com
Universidad Piloto de Colombia

Resumen— El desarrollo de una metodología para el aseguramiento de infraestructuras de red y de servidores enfocado a las diversas organizaciones y negocios que hay actualmente en el mercado, se basa en el desarrollo de metodologías que deben incluir una serie de guías, procedimientos y de buenas prácticas de seguridad. La metodología debe estar definida dentro de un marco de buenas prácticas de aseguramiento de infraestructuras tecnológicas, teniendo en cuenta también el entorno físico y ambiental, donde está incluida la infraestructura de red y la plataforma de servidores, dentro de esta metodología se deben tener cuenta las directrices definidas en diferentes estándares y normas internacionales tales como: ISO 27001:2005, ISO 27002, SOX, PCI, HIPA, etc.

Índice de Términos— SOX (Ley Sarbanes-Oxley), PCI (Payment Card Industry), HIPA (Health Information Protection Act), ISO (International Organization for Standardization).

I. INTRODUCCIÓN

El aseguramiento de toda una infraestructura tecnológica para una compañía puede resultar bastante complejo, ya que demanda mucho tiempo, costos, conocimientos específicos, y sobre todo experiencia.

Muchas compañías de diversos sectores de negocio invierten mucho dinero en recursos tecnológicos para el óptimo funcionamiento de su negocio, como lo es por ejemplo la adquisición de equipos de red robustos (Switchs, Routers. Firewalls etc), canales dedicados, redes VPN, dispositivos móviles, software de aplicaciones, inteligencia de negocios, e infraestructura de servidores de última generación, que son máquinas con tecnología redundante, que vienen con múltiples procesadores muy rápidos, con memoria RAM de gran capacidad, y un almacenamiento de gran volumen.

A pesar de contar con toda esta infraestructura de red y servidores de última generación, se presenta la problemática que en muchas de estas organizaciones, y en especial las áreas de TI, no tienen en cuenta el aseguramiento y buenas prácticas que deben de tener este tipo de infraestructura a nivel de hardware y software.

Y además no se tiene en cuenta que los sistemas Microsoft Windows son, en la actualidad, el sistema operativo más utilizado por las organizaciones y, de su masividad, surge el interés o la casualidad de que sea víctima del embate de los atacantes en todo el mundo.

II. PORQUE ASEGURAR LA RED Y LOS SERVIDORES

Es muy importante identificar las vulnerabilidades a las que están expuestos todos los días la infraestructura de red (LAN, WAN, VPN) de una organización y la plataforma de servidores de diferentes sistemas operativos (Microsoft Windows Server, Sistemas Linux y Unix, etc.) y que se tengan en cuenta los diferentes riesgos que se pueden presentar en la infraestructura tecnológica si estas vulnerabilidades no son contrarrestadas, y no se adopten las mejores prácticas de aseguramiento para los diferentes tecnologías que pueda tener una compañía.

Se hace necesario y muy importante tener metodologías para el aseguramiento de una infraestructura de red y las diferentes plataformas de servidores que existen actualmente, en base al desarrollo de metodologías que incluyan una serie de guías, procedimientos y de buenas prácticas de seguridad que permitan contrarrestar las

múltiples vulnerabilidades que existen en la actualidad para este tipo de infraestructuras y que muchas áreas de TI de diversas organizaciones no tienen en cuenta, de tal manera que se puedan disminuir los principales riesgos de seguridad, y ser más eficientes en la administración y funcionamiento de toda una infraestructura tecnológica.

Es importante destacar que si la problemática que se plantea no se trata debidamente, el impacto que se puede presentar en una organización puede ser muy negativo ya que puede verse comprometida seriamente la seguridad de toda la infraestructura tecnológica, por medio de ataques ya sea de denegación de servicio, que incluyen las Bases de datos y las aplicaciones del negocio, los diferentes servicios de red, y darse también la fuga y perdida de información crítica de una organización.

Como ya se ha mencionado si no son adoptadas buenas prácticas de seguridad que permitan contrarrestar las diferentes vulnerabilidades a las que día a día se encuentran expuestas las infraestructuras de tecnologia, puede verse comprometida seriamente la seguridad de toda una plataforma tecnológica, y el impacto puede ser muy negativo para el buen nombre y reputación de una organización en particular.

III. PROBLEMATICA

Cada día surgen nuevas amenazas que atentan contra la seguridad de una red, y por ende todos los datos y las aplicaciones que se encuentran instaladas y almacenadas en los diferentes servidores.

Estas amenazas utilizan las redes de comunicaciones e Internet para propagarse, por lo tanto estos sistemas son vulnerables y están expuestos ante cualquier ataque. En particular son muy frecuentes los ataques coordinados en los cuales un atacante remoto utiliza un grupo de computadores bajo su control (maquinas zombies) para colapsar los computadores de una entidad legítima y así de esta forma poder cometer cualquier tipo de ilícito.

Con el objeto de reclutar maquinas zombies, los atacantes realizan de forma automática exploraciones buscando sistemas con diversas vulnerabilidades y entre ellas la más frecuente consiste en buscar servidores de diferentes sistemas operativos (Windows Server, Sistemas Linux y Unix) en los que por citar un ejemplo las contraseñas de los usuarios dados de alta sean sencillas o fáciles de adivinar.

Así mismo las áreas de TI de las organizaciones se encuentran en los puntos extremos tratando de mantener la infraestructura de red y de servidores a salvo de la avalancha de nuevas vulnerabilidades y amenazas que afectan una red y los diferentes sistemas operativos. Debido a que los sistemas se vuelven más complejos, se hace más difícil mantener los controles adecuados de acceso a la red y mitigar las vulnerabilidades nuevas. Se puede afirmar que las mejores prácticas para el aseguramiento de una red y los servidores en tres áreas básicas consisten en: Parchado del servidor, la higiene del servidor, y el control de acceso a la red. Y aunque pueda parecer obvio, muy pocas áreas de TI logran implementar la mayor parte de estas mejores prácticas de una manera consistente y efectiva.

Varios fabricantes de sistemas operativos para servidores, han planteado unas pautas de seguridad muy básicas que no abarcan toda la complejidad que requiere el aseguramiento y las buenas prácticas para una plataforma de servidores, y específicamente si pertenecen a diversos sectores de negocio donde se deben de cumplir con varias directrices y normas ya establecidas por autoridades nacionales e internacionales.

IV. CARACTERISTICAS BASICAS DE LA SEGURIDAD

La seguridad es una palabra con una definición demasiado amplia, y aún es complejo llegar a un acuerdo acerca de qué significa.

En el ámbito informático, la seguridad equivale principalmente a garantizar al usuario:

- Consistencia: Comportarse como se espera que se comporte y mantener su comportamiento sin cambios inesperados.
- Servicio: El sistema debe prestar todos los servicios que ofrece de manera confiable, constante

y consistente.

• Protección: Si un programa tiene errores y sufre una caída, no debe afectar a la ejecución de otros procesos. Un programa diseñado expresamente para hacer daño debe tener un impacto mínimo en el sistema.

Los segmentos de memoria de un proceso deben ser invisibles e inmodificables para cualquier otro proceso.

• Control de Acceso: Los datos generados por un usuario no deben ser accesibles a otro usuario a menos que así sea específicamente solicitado por su dueño. Soportar diferentes modos de acceso a un archivo, de modo que el sistema pueda exigir que un archivo pueda ser leído pero no ejecutado o abierto para escritura.

Los mecanismos de control de acceso deben ser tan granulares como sea posible.

• Autenticación: El sistema debe poseer los mecanismos necesarios para asegurarse que un usuario es quien dice ser y tiene suficientes privilegios para llevar a cabo todas las operaciones que desee realizar. Debe ser capaz de notificar al administrador acerca de cualquier anomalía.

• Siempre habrá agujeros (fallas en la lógica de los programas) desconocidos para el responsable del sistema.

• La seguridad es inversamente proporcional a la usabilidad.

V. HERRAMIENTAS DE SEGURIDAD

Una herramienta de seguridad es una serie de programas diseñados para ayudar al administrador, sea alertándolo o realizando por sí mismo las acciones necesarias a mantener un sistema seguro.

Pueden ser:

• Orientadas a host: Trabajan exclusivamente con la información disponible dentro del host (configuración, bitácoras, etc.).

• Orientadas a red: Trabajan exclusivamente con la información proveniente de la red (barridos de puertos, conexiones no autorizadas, etc.).

Se debe tener en cuenta que toda herramienta de seguridad útil para el administrador es también útil para un atacante, y toda herramienta de seguridad disponible para un administrador se debe asumir que está también disponible para un atacante.

A la hora de proteger los recursos del sistema es primordial identificar las vulnerabilidades y amenazas que ciernen contra ellos. Una vulnerabilidad es cualquier situación que pueda desembocar en un problema de seguridad, y una amenaza es la acción específica que aprovecha una vulnerabilidad para crear un problema de seguridad; entre ambas existe una estrecha relación: sin vulnerabilidades no hay amenazas, y sin amenazas no hay vulnerabilidades.

Se suelen dividir las amenazas que existen sobre los sistemas informáticos en tres grandes grupos, en función del ámbito o la forma en que se pueden producir:

• Desastres del entorno: Dentro de este grupo se incluyen todos los posibles problemas relacionados con la ubicación del entorno de trabajo informático o de la propia organización, así como con las personas que de una u otra forma están relacionadas con el mismo. Por ejemplo, se han de tener en cuenta desastres naturales (terremotos, inundaciones, etc.), desastres producidos por elementos cercanos, como los cortes de fluido eléctrico, y peligros relacionados con operadores, programadores o usuarios del sistema.

• Amenazas en el sistema: Bajo esta denominación se contemplan todas las vulnerabilidades de los equipos y su software que pueden acarrear amenazas a la seguridad, como fallos en el sistema operativo, medidas de protección que éste ofrece, fallos en los programas, copias de seguridad.

• Amenazas en la red: Cada día es menos común que una máquina trabaje aislada de todas las demás; se tiende a comunicar equipos mediante redes locales, redes WAN, conexiones VPN, Intranets o la propia Internet, y esta interconexión acarrea nuevas y peligrosas amenazas a la seguridad de los equipos, peligros que hasta el momento de la conexión no se suelen tener en cuenta. Por ejemplo, es necesario analizar aspectos relativos al cifrado de los datos en tránsito por la red, a proteger una red local del resto de Internet, o a instalar sistemas de autenticación de usuarios remotos que necesitan acceder a ciertos recursos internos a la organización (como un investigador que se conecta desde su casa a través de una VPN).

Algo importante a la hora de analizar las amenazas a las que se enfrentan nuestros sistemas es analizar los potenciales tipos de atacantes que pueden intentar violar la seguridad. Es algo normal que a la hora de hablar de atacantes todo el mundo piense en piratas informáticos llamados "hackers". No obstante, esto no es más que el fruto de la repercusión que en todos los medios tienen estos individuos y sus acciones; en realidad, la inmensa mayoría de problemas de seguridad vienen dados por atacantes internos a la organización afectada.

No siempre se debe de contemplar a las amenazas como actos intencionados contra un sistema informático: muchos de los problemas pueden ser ocasionados por accidentes, desde un operador que derrama una taza de café sobre una estación hasta un usuario que tropieza con el cable de alimentación de un servidor y lo desconecta de la línea eléctrica, pasando por temas como el borrado accidental de datos o los errores de programación. Por supuesto, tampoco es correcto pensar solo en los accesos no autorizados al sistema: un usuario de una máquina puede intentar conseguir privilegios que no le correspondan, una persona externa a la organización puede lanzar un ataque de negación de servicio contra la misma sin necesidad de conocer ni siquiera un login y una contraseña.

VI. METODOLOGIA PARA EL ASEGURAMIENTO

A. Fase de Identificación

Se basa en la identificación y descripción de la infraestructura tecnológica de una organización; la cual consiste en obtener toda la información y diagnósticos referidos acerca de esta infraestructura.

Consiste en el análisis de las posibles relaciones de los riesgos físicos, los riesgos lógicos y los índices de vulnerabilidades asociados a las amenazas sobre la infraestructura de red y de servidores.

B. Fase de Diseño

Se basa en la generación y diseño de propuestas de guías, procedimientos y buenas prácticas de aseguramiento para la infraestructura de red y servidores.

La generación de alternativas de guías y buenas prácticas se debe realizar con el estudio de las evaluaciones realizadas sobre la infraestructura de red y de servidores, tomando en cuenta las medidas y procedimientos que se desarrollen.

C. Fase de Implementación

Se basa en la implementación de las estrategias y procedimientos que permitan minimizar el impacto de los riesgos a los que están expuestos una infraestructura de red y de servidores.

D. Fase de Evaluación

Una vez ya identificados los riesgos y las posibles amenazas presentes en la infraestructura de red y de servidores, se deben evaluar las estrategias definidas para minimizar el impacto de los riesgos que se encuentran en los niveles más desfavorables.

VII. CONCLUSIONES

Debido a que actualmente existen muchos riesgos y que se puede presentar una gran cantidad de amenazas para atacar las vulnerabilidades de seguridad en una infraestructura de tecnología se debe tener en cuenta que para contrarrestar estas amenazas, es necesario conocer en primera medida, como se efectúan estos ataques, para instalar los mecanismos de seguridad necesarios a nivel de guías, procedimientos, y buenas prácticas de seguridad, basados en estándares y normativas internacionales y que permitan contrarrestar estas amenazas.

En cualquier sistema informático y en este caso una infraestructura de tecnología se deben tener en cuenta factores como aplicaciones y desarrollos de software confiable, protocolos de red adecuados, controles de acceso a la red, las bases de datos y las aplicaciones, un hardware adecuado y actualizado, y muy importante tener unas políticas de seguridad bien definidas que deben ser conocidas por todo los usuarios de los sistemas.

REFERENCIAS

José F. Torres. Practicas básicas de seguridad en Windows. 2da. Escuela Venezolana de Seguridad de Cómputo. Agosto 2006.

Universidad Autónoma de Madrid. Guía básica de seguridad para Windows. Disponible en http://www.uam.es/servicios/ti/servicios/ss/rec/winnt.html

Stearns William. Essential security checks for Linux Systems. 2003. Disponible en

http://labmice.techtarget.com/articles/securingwin2000.htm

McClure, Stuart. Scambray, Joel. Kurtz, George. “Parte 2 Hackeo del Sistema”. En Hackers 6: Secretos y soluciones de seguridad en redes. Traducido por Eloy Pineda Rojas. México. McGraw Hill Editores, S.A de C.V, 2010. p 157-308.

Vieites Gómez, Álvaro. “Enciclopedia de la Seguridad Informática”. 2da Edición. Madrid. RA-MA S.A. Editorial y Publicaciones, 2011.

A. S. Tanenbaum. “Sistemas Operativos Distribuidos”. Prentice Hall Hispanoamericana S.A., México, 1996.

Tori, Carlos. “Cap 7. Servidores Windows, Cap 8 Servidores Unix”. En Hacking Ético. Rosario, Argentina. Editado por Carlos Tori, 2008. p 190-284.

Autor

Jorge Ivan Montoya M. Ingeniero de Sistemas egresado de la Universidad Autónoma de Colombia especialista en proyectos de infraestructura de TI y Datacenters. Certificado en tecnologías de Servidores Microsoft Windows, Linux y Unix, Redes Cisco. Certificación en ITIL V3. Implementación de estándares, políticas y directrices de seguridad Informática y seguridad de la información, aseguramiento de infraestructuras tecnológicas alineadas a los objetivos de una organización.