Abordar las vulnerabilidades de seguridad de su empresa o de sus sistemas de misión crítica

Rational. software

Soluciones de seguridad cibernética de IBM: evaluación y defensa contra las vulnerabilidades de la seguridad.

Aspectos destacados

- ***Ayudan a defenderse contra las amenazas a la red basadas en Internet.***
- ***Les permiten a las organizaciones buscar y examinar las vulnerabilidades comunes de las aplicaciones de la Web.***
- ***Contribuyen a simplificar, proteger y acelerar el despliegue de los servicios de la Web y XML.***
- ***Ofrecen una solución integral, que brinda soporte para la seguridad, la conformidad y la evolución cibernéticas.***

Creación de la seguridad cibernética en el ciclo de vida

En la primera mitad del año 2008, los miembros del equipo de investigación y desarrollo de IBM Internet Security Systems ™ (ISS) X-Force®, analizaron y documentaron 3.534 vulnerabilidades informáticas, exposiciones a riesgos o parámetros de configuración que podían comprometer la confidencialidad, la integridad o la posibilidad de acceso de un sistema. Dicha exposición a potenciales riesgos es hasta un 5% mayor que la registrada durante la primera mitad del año 2007.[1]

Las redes gubernamentales son vulnerables a estas amenazas crecientes. En el año 2007, la Government Accountability Office (GAO-Oficina de Responsabilidad Gubernamental) de Estados Unidos de Norteamérica detectó que “ciertas debilidades significativas continuaban amenazando la confidencialidad, la integridad, y la posibilidad de acceso a la información y a los sistemas de información vitales”.[2]

Estos puntos débiles no provenían de una falta de normas, sino más bien de la ausencia de conformidad con las mismas. IBM se percató, gracias a sus negocios globales, de que sólo una propuesta integral podría proteger a las empresas o a sus sistemas de misión crítica de los ataques cibernéticos.

Detección, protección y administración de las vulnerabilidades dentro de la infraestructura

Cuando la mayoría de los funcionarios del gobierno de Estados Unidos de Norteamérica analizan la forma de hacer frente a las vulnerabilidades en sus empresas o sistemas esenciales, siempre comienzan evaluando aquéllas que se encuentran dentro de su entorno operativo. Sin embargo, en el mundo actual, tan centrado en Internet, existen numerosas vulnerabilidades, tanto en la infraestructura como en las aplicaciones de una organización, que individuos, empresas y naciones extranjeras intentan aprovechar, con la esperanza de ingresar a, o alterar, los sistemas vitales en los que confía el gobierno de Estados Unidos de Norteamérica.

Un programa sólido de IT consta de políticas, procesos y tecnologías que permiten descubrir, de manera continua, nuevos recursos y otros ya existentes (posibles conexiones ficticias, sistemas autorizados pero que no cumplen con las normas, y otros recursos que intentan conectarse a su red). Dicho programa debería evaluar y remediar (detectar, proteger y administrar) las vulnerabilidades, y proporcionar seguridad basada en los hosts y en la red. Por último, debería ofrecer también instrucciones y controles centralizados que incluyan actualizaciones, alertas, informes y acceso basado en roles.

La primera línea de defensa consiste en detectar, proteger y administrar, de manera eficaz, las vulnerabilidades que existen dentro de la infraestructura (servidores, routers, interruptores, etc.) de los sistemas operativos. Los productos y servicios ISS de IMB buscan, detectan, protegen y administran las vulnerabilidades dentro de su infraestructura operativa.

El equipo de X-Force, una organización de investigación y desarrollo de seguridad cibernética de vanguardia, lleva a cabo, de manera ininterrumpida, estudios y análisis de prácticamente todos los aspectos y componentes de los sistemas operativos. Este grupo detecta vulnerabilidades en forma continua y puede brindar protección contra las mismas, en tanto que los proveedores del sector crean e implementan parches para hacerles frente.

Además, el dispositivo unified threat management (UMT) de la solución IBM Proventia® Network Multi-Function Security (MFS) e IBM Proventia Network Enterprise Scanner brindan protección a nivel de enlaces y redes para defenderse de las amenazas basadas en Internet, sin poner en peligro el ancho de banda o la disponibilidad de la red.

Resolución de la problemática de seguridad y vulnerabilidad de las aplicaciones como segunda línea de defensa

Además de asegurar su infraestructura, su organización necesita resolver la problemática de la seguridad y la vulnerabilidad de las aplicaciones de la Web (cross-site scripting, SQL injection, desbordamiento de buffer, etc.) dentro del entorno operativo. Esto es fundamental a la hora de elaborar una estrategia integral de defensa profunda. Las soluciones IBM Rational AppScan® automatizan las evaluaciones de la vulnerabilidad para el más diverso grupo de tecnologías, incluyendo Asynchronous JavaScript y XML (AJAX), Adobe® Flash y servicios de la Web. Ofrecen adaptabilidad y extensibilidad a toda la comunidad de código abierto, recomendaciones sobre las reparaciones de avanzada, y la estructura de Psycan para comprobadores de penetración, así como también más de 40 informes de conformidad con las normas vigentes, incluyendo: FISMA (Federal Information Security Management Act), NIST (National Institute of Standards and Technology) 800-53A, DCID (Director of Central Intelligence Directive)6/3, PCI DSS (Payment Card Industry Data Security Standard), Health Insurance Portability, HIPAA (Accountability Act) y muchas otras.

Después de proteger sus aplicaciones contra los accesos no autorizados a sus sistemas de misión crítica, su empresa puede implementar el software IBM Rational Policy Tester ™ con el fin de controlar y administrar la calidad, la privacidad, y la posibilidad de acceso de los contenidos y la conformidad de su sitio Web. Este producto puede ayudarlo a asegurarse de que sus datos operativos o de marcas registradas no terminen en su sitio Web quedando a disposición del público en general. Puede utilizarse para evaluar la conformidad de su sitio Web con las normas de OPSEC.

Despliegue de las aplicaciones de SOA para mantenerse al día con las nuevas tecnologías

El surgimiento de service-oriented arhitecture (SOA) abre la puerta a nuevos e interesantes métodos para el desarrollo e integración de los sistemas, en los que la funcionalidad puede construirse en torno a los negocios, y presentarse como un paquete de servicios. No obstante, una solución de seguridad cibernética integral necesita proteger a SOA como nueva frontera, tanto de oportunidades como de vulnerabilidades.

El software IBM WebSphere® DataPower®SOA Appliances, diseñado por algunos de los principales expertos del mundo en seguridad de servicios de

la Web y XML, ofrece protección total y configurable, funciones de puesta en vigor de normas, desde la seguridad de los servicios de la Web hasta el control de acceso XML..

Unificación de lo antes mencionado

Ninguna de las soluciones arriba detalladas pueden hacer frente, por sí solas, al problema de la seguridad cibernética e IBM es consciente de esta situación. Durante años, hemos enviado a nuestras tecnologías de protección y detección a batallar, día a día, en las trincheras cibernéticas. Si bien hemos aprendido que resulta relativamente sencillo proteger las redes, aún nos queda pendiente el tema de la seguridad en los correos electrónicos. Los usuarios deben preservar su capacidad de compartir datos a través de la Web, y las empresas, de integrar sus sistemas de back-office a los sistemas de otras organizaciones.

La necesidad de compartir información abre la puerta al aprovechamiento de todas las aplicaciones de la Web y del tráfico de los servicios XML de la Web. No obstante, las herramientas aquí descritas trabajan en forma conjunta para realizar transmisiones totalmente seguras de información gubernamental vital, incluyendo los datos confidenciales de inteligencia a combatientes, y pueden limitar la capacidad de los delincuentes cibernéticos y otros adversarios, de comprometer el flujo de los recursos a la primera línea.

Conciencia operativa

El software IBM Tivoli® Security Information and Event Manager proporciona una solución de administración centralizada de seguridad y conformidad que otorga la visibilidad del estado de protección de la empresa. Esta herramienta recoge los informes y sucesos provenientes de todas las otras piezas que integran la solución cibernética, y provee valiosas datos de seguridad que le permitirán obrar en consecuencia.

Tivoli Security Information and Event Manager facilita la conformidad mediante el uso de un dashboard centralizado y funciones de creación de informes. Ayuda a proteger su propiedad intelectual y privacidad auditando el comportamiento de todos los usuarios, privilegiados o no. Además, administra eficaz y eficientemente las operaciones de seguridad, dado que correlaciona los sucesos, los investiga, establece prioridades, y elabora respuestas, todo de manera centralizada.

Evolución de la seguridad cibernética para mantenerse al día con el desarrollo de las aplicaciones

Una vez que los sistemas operativos reciben la certificación de information assurance (IA), algunas personas suponen que ya han conseguido la protección total de su empresa. En realidad, sólo han cubierto la versión en curso del sistema operativo. A medida que estos sistemas evolucionan, la introducción de nuevas prestaciones, funciones y tecnologías- tanto de hardware como de software- presenta nuevas vulnerabilidades. Cada vez que se realiza una modificación importante, se debe repetir todo el proceso de seguridad informática con el fin proteger con solidez la última versión del sistema operativo.

Con el propósito de lograr la protección integral de su empresa, la seguridad cibernética debe formar parte de todo el ciclo de vida del sistema, comenzado por el desarrollo. La integración entre los productos de seguridad de IBM, la solución Rational Change y el conjunto de soluciones para la administración de los riesgos da soporte a la cobertura absoluta del antedicho ciclo.

En la fase de desarrollo, hay distintos momentos en los que se deben tener presentes IA y las medidas de seguridad, a saber:

- Definición de los requisitos.
- Configuración y diseño del sistema.
- Creación de los códigos.
- Etapas de prueba.

Tal como ocurre en el caso de las fallas o de los errores funcionales, la detección de las vulnerabilidades, durante las primeras etapas del proceso, facilita su resolución. Al utilizar IBM Rational Unified Process® (IBM RUP®), se puede identificar y hacer frente a los defectos durante las primeras fases del desarrollo, lo que permite evitar los altos costos y tiempos relacionados con su reparación una vez que ya se ha desplegado un sistema en el entorno operativo. Esto significa que un sistema operativo recién desplegado puede presentar mayor seguridad al comienzo, permitiendo así que obtenga la certificación de IA con mayor rapidez y a un costo total menor.

Extensión de IA y de la seguridad cibernética más allá del desarrollo tradicional

Cuando usted extiende IA y las medidas de seguridad más allá de las fases tradicionales del desarrollo del ciclo de vida y se los incorpora dentro de los procedimientos de búsqueda de defectos y flujo de trabajo, entonces se obtiene un proceso fácil de localizar y repetir que permite identificar, evaluar y hacer frente a las fallas de seguridad en su sistema operativo.

Las vulnerabilidades identificadas mediante los productos que IBM ofrece pueden informarse como fallas directamente en el proceso de desarrollo. Y, una vez que las modificaciones al sistema llegan a la etapa de prueba, las soluciones de IBM pueden ayudarlo comprobar la solución en su entorno, y a corroborar que dichas fallas hayan sido efectivamente abordadas. Por último, los ofrecimientos de IBM en materia de seguridad le permiten comprobar una versión de prueba del sistema antes de ponerlo en funcionamiento. Esta propuesta no sólo posibilita que se optimice el software development lifecycle (SDLC), sino que es un requisito previo para la obtención de toda certificación y norma de acreditación.

¿Por qué IBM?

IBM ofrece las estrategias, los servicios y las tecnologías necesarios para hacer frente a los grandes desafíos cibernéticos. Nuestra propuesta integral permite administrar y proteger con éxito la tecnología de los sistemas cibernéticos, del capital humano y de los niveles de control y administración de los riesgos.

Tan sólo en el año 2008 invertimos más de un billón y medio de dólares en tecnología de seguridad, incluyendo tres soluciones centrales que comprenden las siguientes soluciones de seguridad cibernética de IBM:

- **IBM Rational AppScan**- un conjunto de soluciones de vanguardia de seguridad para las aplicaciones de la Web que puede buscar y comprobar las vulnerabilidades comunes de dichas aplicaciones, incluyendo la seguridad de IBM Rational Policy Tester for OPSEC.
- **IBM Proventia Network MFS**- una solución diseñada para defenderse de las amenazas a la red basadas en Internet.
- **IBM WebSphere DataPower SOA Appliances**- una solución que ayuda a proteger la información en tránsito entre el servicio y el cliente, para las transacciones de los servicios ricos en cuanto a seguridad de XML y de la Web.

Para obtener más información

Para conocer más sobre las soluciones de seguridad cibernética de IBM, póngase en contacto con su representante de IBM o asociado de negocios IBM, o visite:

ibm.com/federal/security

IBM Corporation
Software Group
Rute 100
Somers, NY, 10589
U.S.A.

Producido en Estados Unidos de Norteamérica
Enero de 2009

---

1. IBM, IBM Internet Security Systems X-Force™ 2008 Mid-Year Trend Statistics, Julio 2008

2. U.S.Government Accountability Office, information Security: Progress Reported., but Weaknesses at Federal Agencies Persist, Gregory C. Wilhusen. Marzo 12, 2008

RAS14013-USEN-00