Un Abordaje Radical hacia la Seguridad

Una publicación de IBM® Redbooks® Point-of-View por IBM Academy of Technology

Por **Chung-Sheng Li**, Ph. D., Director IBM Research, **Katsumi Ohnishi**, IBM Executive Architect, y **Josuyla R. Rao**, Director IBM Research

Características más importantes

Adopte un abordaje amplio de seguridad que anticipe y pára a los atacantes antes de que se infiltren a su sistema:

- Cambie su paradigma de seguridad de un perímetro de defensa tradicional a una continuación de seguridad a detalle de micro-perímetro.
- Emplee defensa de micro-perímetro e inteligencia de seguridad, que son claves para abordar las amenazas emergentes en modelos de tendencias de la computación móvil, social y de nube.
- Cambie su solución de productos hacia un abordaje integrado e integral de inteligencia de seguridad.
- Implementar inteligencia de seguridad para mitigar los riesgos de volúmenes crecientes de datos, la proliferación de nubes y usuarios móviles, y las tecnologías web.

Escenario de seguridad actual

El ícono de seguridad en el escritorio de su computadora, que usualmente aparece como un escudo, representa un firewall personal. Protege contra amenazas y ataques y busca en su sistema intrusiones que hayan violado la pared. Aunque esta salvaguarda es un buen ejemplo de seguridad a detalle, las organizaciones no siempre establecen salvaguardas similares dentro de los límites de su empresa. Como resultado, muchos servidores que son críticos para los negocios continúan dependiendo de salvaguardas ordinarias de firewalls corporativos y mecanismos de detección y prevención de intrusiones.

Hoy en día los negocios y los gobiernos deben emprender un abordaje más amplio para dar seguridad a la información y defenderla contra atacantes o infiltradores malintencionados. Esta tarea no es fácil cuando los usuarios demandan acceso rápido y conveniente a la información que esperan sea protegida. Consecuentemente, cada vez más las organizaciones necesitan implementar un abordaje más inteligente que dependa de control a detalle de privilegios de acceso y detección de campo lejano de amenazas potenciales y aparentemente no relacionadas. Dicho abordaje también debe depender de métodos de contención multi-nivel para aislar intrusiones y minimizar el daño.

El dilema para los negocios es que deben permitir acceso a sus sistemas para permitir tareas y servicios, mientras salvaguardan los activos de información. Sin embargo los riesgos continúan creciendo. Por ejemplo, los volúmenes de datos continúan creciendo. Los usuarios de nube, móviles y de teleconmutación acceden a redes de varios dispositivos desde múltiples ubicaciones. Las aplicaciones cada vez más usan Internet para colaborar y comunicarse. Y al usar las tecnologías de Web 2.0, los usuarios de fuera del negocio pueden acceder a datos y controles. Todos estos riesgos ilustran que una violación a la seguridad puede darse en cualquier parte y potencialmente tener un efecto de cascada para generar repercusiones globales.

La respuesta a dichos riesgos fue la de construir grandes firewalls para proteger a toda la empresa. Sin embargo, ahora la tendencia es proteger a cada recurso dentro de la red. Dichos recursos incluyen servidores, middleware, almacenamiento, arquitectura orientada a servicios, aplicaciones e información, y cada uno puede tener diferentes valores estratégicos.

El reaccionar a las violaciones de seguridad no es suficiente para proteger la información, redes, y negocios de una empresa. Usted debe anticipar y protegerse contra ataques malignos antes de que sucedan. Para estar preparados, usted necesita ver a la seguridad como un algo continuo que correlaciona entre eventos físicos y virtuales, entre eventos

© Copyright IBM Corp. 2013

aparentemente inofensivos y sospechosos y entre actividades locales y globales. Usted debe adoptar el conocimiento de seguridad que es usado en las comunidades de inteligencia y de orden público. En estas comunidades, las pistas de eventos inminentes, como un ataque terrorista online antes de que suceda, son recopiladas y analizadas meticulosamente.

Persistencia de amenazas a diferentes niveles

Los negocios están en riesgo de amenazas de seguridad internas y externas como se muestra en Figura 1.

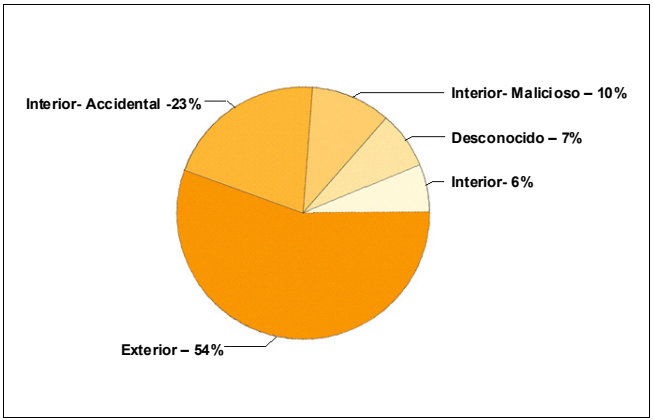

Figura 1 Porcentajes de incidencia de ataques

Las amenazas internas incluyen ataques maliciosos internos y ataques no intencionales con malcode, fuga de datos, o robo de datos valiosos, pasando a través de puntos vulnerables del sistema. Las amenazas externas incluyen denegación de servicio (DoS), vandalismo y propaganda web, botnets (grupos de computadoras en riesgo que ejecutan software de ataque), y alteraciones en equipos. También incluyen ataques a infraestructura crítica, como sistemas de redes eléctricas y combustible, comunicaciones y de transporte.

Las medidas de seguridad para evitar las amenazas incluyen verificaciones de antecedentes de usuarios, acceso restringido, monitoreo físico, monitoreo de integridad de plataforma, controles de escritorio, y elaboración de perfiles y auditoría de interacciones de usuarios. Dichas medidas también incluyen detección y prevención de transferencia de datos delicados hacia un sitio externo no autorizado.

Otras amenazas incluyen inyección SQL, phishing, y amenazas persistentes avanzadas (APT), que han sufrido varias compañías renombradas. Un APT es el ataque más severo en los activos del negocio debido a su progresión en etapas a lo largo del tiempo.

El progreso de un APT avanza de la siguiente manera:

1. Los agresores usan los medios sociales para enviar mensajes de email aparentemente inocentes. Esta técnica es conocida como *phishing*. Los mensajes de email contienen documentos adjuntos o aplicaciones ocultas que pasan a través de la seguridad. Dichas aplicaciones son llamadas *malware*.
2. Malware instala herramientas que permiten al atacante acceso remoto a servidores de control y computadoras por detrás del firewall.
3. El malware extrae las credenciales de usuario. Posteriormente, se mueve hacia los usuarios privilegiados, y finalmente se mueve hacia blancos de alto valor.
4. El malware establece acceso a servidores escalados en puntos claves.
5. El atacante transfiere datos delicados hacia un servidor externo en etapas que está en una máquina externa puesta en riesgo.

Tradicionalmente, los negocios respondían a dichas amenazas fortaleciendo el perímetro de defensa que está a lo largo de las fronteras de la organización. Este abordaje se ha vuelto cada vez menos efectivo debido a la necesidad de llevar a cabo negocios más allá del perímetro. Además, no aborda las violaciones internas.

En el 2008, por primera vez, las violaciones internas sobrepasaron a las externas, desafiando la defensa tradicional basada en perímetro de la cyber seguridad.

El cómo se prepara usted para gestionar los riesgos afecta críticamente sus resultados finales, por ejemplo, en términos de costos, éxito, y efectividad. El escoger la mejor protección para sus activos de datos puede ser confuso considerando la proliferación de abordajes y productos de seguridad.

La necesidad de una solución de mayor alcance

Por décadas, los negocios han confiado en IBM sus redes, datos, y sistemas, esperando calidad, rendimiento, y tecnología de punta. Ahora esperan lo mismo para un recurso de seguridad. Para cumplir con esta demanda de mercado, IBM cambia de un abordaje de producto hacia un abordaje integrado de empresa para inteligencia de seguridad. Este abordaje se basa en elementos fundacionales claves que permiten gestión activa, información en tiempo real, correlación analítica y gestión de amenazas predictiva.

El modelo de inteligencia de seguridad IBM cubre la gama completa de preocupaciones de seguridad, desde la conformidad hasta la infraestructura. La infraestructura de este modelo ayuda a identificar, predecir, y remediar las amenazas de TI y los riesgos para la empresa, así como a lograr la conformidad. Las posibilidades de seguridad de la infraestructura usan ciclos de planear-hacer-verificar-actuar (PDCA). Estos ciclos se basan en el principio de *defensa a profundidad*, que es un abordaje estructurado y en capas de capacitación, prevención, detección y remediación de seguridad. Esta solución IBM fue construida por miles de investigadores, desarrolladores, consultores, y expertos en la materia de iniciativas de seguridad. Además, IBM ha dado consultoría e implementado miles de proyectos de seguridad, generando habilidades prácticas y mejores prácticas y procesos.

La infraestructura de seguridad

Inteligencia de seguridad, que es el arte y la ciencia de la anticipación, monitoreo, y análisis de riesgos antes de que se presenten, es una tendencia en el mercado actual. La inteligencia de seguridad proporciona visibilidad unificada y análisis en tiempo real de seguridad y dispositivos de red a sistemas operativos de servidores, aplicaciones, puntos finales, y recursos de infraestructura. La inteligencia de seguridad involucra los siguientes aspectos claves, y cada uno involucra desde un nivel básico hasta un nivel óptimo, o de una instancia reactiva a una proactiva:

- *Las personas*, que se trasladan de un directorio centralizado hacia suministro de usuario con una robusta autenticación, a análisis basados en papeles, gobernanza de identidad, y controles de usuario privilegiados.
- *Los datos*, que evolucionan desde cifrado, controles de acceso, monitoreo de acceso, y prevención de pérdida de datos hacia análisis de flujo de datos y gobernanza de datos. El cómputo social es cada vez más importante para interceptar tanto fugas de datos como ataques agudos de phishing .
- *Las aplicaciones*, que se trasladan desde exploración de aplicaciones, firewall, y exploración de código de origen hacia procesos de ingeniería de aplicaciones seguras y detección de fraudes .
- *La infraestructura*, que evoluciona desde defensa de perímetro de antivirus ordinaria hacia gestión de activos y gestión de seguridad de red y punto final (detección y prevención de intrusiones e inspección profunda de paquete) hacia moni toreo de red avanzado, técnicas forenses, y minería de datos.

Puntos de solución claves para inteligencia de seguridad

IBM se enfoca en cuatro áreas claves para entregar inteligencia de seguridad: amenazas avanzadas, computación en nube, computación móvil, y regulación y conformidad.

Las amenazas avanzadas, o APTs, son ataques sofisticados y dirigidos que están diseñados para obtener acceso continuo a información crítica. Estas amenazas están creciendo y se vuelven más severas y más frecuentes. La solución es una capa de red robusta que integra seguridad, análisis, e inteligencia en amenazas, en adición a los factores humanos y sociales debido a que las amenazas usualmente se inician como ataques de phishing.

Al consolidar datos masivos, las soluciones de inteligencia de seguridad proporcionan conocimiento más profundo para la defensa contra diversas amenazas, incluyendo APT. La solución IBM security information and event management (SIEM) le ayuda a distinguir amenazas reales de “noise.” También ayuda a reducir alertas de falsos positivos al usar datos contextuales y análisis más inteligentes.

La mayoría de los negocios se ha dado cuenta de que necesitan tomar ventaja de la computación en nube pero están preocupados con los riesgos potenciales. Tanto como un proveedor de servicios, así como un proveedor de seguridad, IBM está bien posicionada para proporcionar una infraestructura segura en la nube y en plataformas para aislar la información en centro de datos y nubes con seguridad.

De acuerdo a Gartner, Inc., 90% de los negocios darán soporte a aplicaciones corporativas en dispositivos móviles para el 2014.[1] Para ir al ritmo de este entorno de trabajo ampliado, una preocupación prioritaria para la mayoría de los CIOs es proporcionar a los empleados un amplio acceso mientras al mismo tiempo dan seguridad a sus dispositivos móviles. IBM se enfoca en acceso seguro a datos corporativos mientras da soporte a privacidad y ofrece amplias posibilidades de seguridad a lo largo de puntos finales, puertas de enlace, y desarrollo de aplicaciones. IBM también ofrece productos para integrar y entregar gestión de dispositivos móviles y proporciona control de acceso e identidad federada para aplicaciones y sistemas de usuarios'.

Se necesita un abordaje amplio que anticipe, monitoree y analice los riesgos antes de que ocurran.

Los negocios invierten grandes esfuerzos para estar en conformidad con los requerimientos regulatorios gubernamentales y de la industria, usualmente con costos que se incrementan. Con ayuda de IBM, los negocios pueden correlacionar regulaciones a su infraestructura de TI y de negocios, lo que puede reducir costos, hacer más eficiente la complejidad de los sistemas, automatizar la configuración, y simplificar el monitoreo, la auditoría y los informes. IBM ofrece productos que pueden proporcionar registro y correlación confiables y que puedan realizar funciones de orquestación, análisis y panel de instrumentos.

Más acerca de inteligencia de seguridad

El simplemente construir sus defensas de perímetro no da seguridad a su negocio. El usar los productos y servicios de la infraestructura de seguridad de IBM, ilustrada en Figura 2, IBM puede ayudarle a predecir, identificar, y remediar amenazas y lograr la conformidad. Para cumplir estas metas, IBM ofrece productos y servicios para los dominios de infraestructura de IT de personas, datos, aplicaciones, e infraestructura, en adición a servicios de conformidad y seguridad.

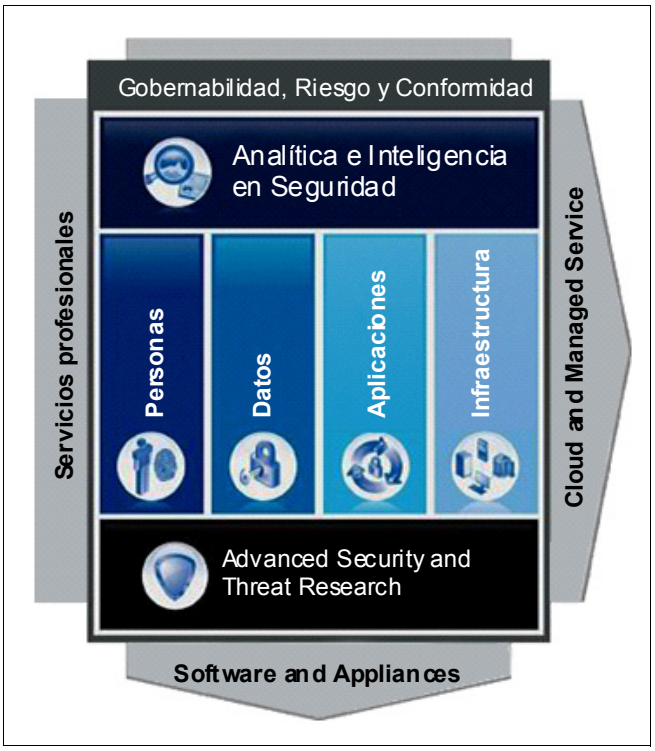

Figura 2 Infraestructura de seguridad IBM

IBM ofrece inteligencia de seguridad de principio a fin con un espectro completo de servicios y productos para los principales dominios de negocios:

- Personas. IBM proporciona servicios para evaluación de identidad, análisis basados en papel, controles de usuarios, despliegue, y hospedaje al usar los siguientes productos:
  - IBM Tivoli Identity and Access
  - IBM Tivoli Federated ID
  - IBM Tivoli Single Sign-on
- Datos. IBM proporciona servicios para evaluación, cifrado, desarrollo de prevención de pérdida de datos (DLP), análisis de flujo y gobernanza al usar los siguientes productos:
  - IBM InfoSphere® Guardium®
  - IBM InfoSphere Optim™ Data Masking
  - Cifrado de cinta y disco
  - IBM Tivoli® Key Manager
- Aplicaciones. IBM proporciona servicios para evaluación, procesos de ingeniería seguros, y detección de fraudes usando los siguientes productos:
  - IBM Rational® AppScan® Source Edition
  - IBM Rational AppScan Standard Edition
  - IBM Tivoli Security Policy Manager

[1] Gartner Newsroom
http://www.gartner.com/it/page.jsp?id=1480514

- Infraestructura. IBM proporciona servicios para seguridad de red (detección y prevención de intrusiones, e inspección profunda de paquete), tácticas forenses, minería de datos, pruebas de penetración, firewall, sistemas de prevención de intrusión, servicios de gestión de vulnerabilidad, y protección móvil gestionada, al usar los siguientes productos:
  - IBM Tivoli Network Intrusion Prevention
  - IBM WebSphere® DataPower® XML Gateway
  - IBM Tivoli Endpoint Manager (antivirus al usar Trend Micro)
  - IBM Security zSecure™ mainframe security

Qué sigue: cómo IBM puede ayudar

Para ayudarle a implementar inteligencia de seguridad, IBM ofrece los servicios del equipo IBM X-Force® Research and Development, que es uno de los equipos de investigación y desarrollo de seguridad comercial más renombrados en el mundo. Este equipo estudia y monitorea las últimas tendencias de amenazas incluyendo vulnerabilidades, explotaciones y ataques activos, virus y otro malware, spam, phishing, y contenido web malicioso. Además de asesorar a los clientes y al público en general cómo responder a amenazas emergentes y críticas, el equipo X-Force también entrega contenido de seguridad para proteger a los clientes de IBM de estas amenazas.

El equipo X-Force publica semestralmente el IBM X-Force Trend and Risk Report, que ayuda a los clientes, investigadores, y público para comprender los últimos riesgos de seguridad e ir al frente de las amenazas emergentes. El informe explora a conciencia los desafíos más significativos que enfrentan los profesionales de la seguridad hoy en día. Para los IBM X-Force Trend and Risk Reports vaya a:

http://www.ibm.com/security/xforce/downloads.html

Además del equipo IBM X-Force, los servicios y productos de IBM ofrecen una solución de espectro completo que puede ayudar a defender sus datos, aplicaciones, e infraestructura de ataques; proteger sus activos de información; y permitir acceso seguro para sus usuarios.

Recursos para obtener más información

Para obtener más información acerca de los conceptos destacados en este documento, consulte los siguientes recursos:

- Publicaciones IBM Redbooks acerca de seguridad

  http://www.redbooks.ibm.com/Redbooks.nsf/portals/Security?Open&count=20
- IBM X-Force Trend and Risk Reports

  http://www.ibm.com/security/xforce/downloads.html
- IBM Institute for Advanced Security

  http://instituteforadvancedsecurity.com/default.aspx
- *Security in Development: The IBM Secure Engineering Framework*, REDP-4641

  http://www.redbooks.ibm.com/redpapers/pdfs/redp4641.pdf

Avisos

Esta información fue desarrollada para los productos y servicios ofrecidos en los Estados Unidos.

IBM puede no ofrecer los productos, servicios o dispositivos tratados en el presente documento en otros países. Consulte a su representante IBM local, para información adicional sobre los productos y servicios disponibles en su área. Cualquier referencia a un producto, servicio o programa IBM, no pretende declarar ni implica que solo puedan utilizarse productos, servicios o programas de IBM. En su lugar, puede utilizarse cualquier producto, servicio o programa funcionalmente equivalente que no infrinja cualquier derecho de propiedad intelectual de IBM. No obstante, es del usuario's la responsabilidad de evaluar y verificar el funcionamiento de cualquier producto, programa o servicio no IBM.

IBM puede tener patentes o solicitudes de patentes pendientes de aplicaciones que tratan los asuntos descritos en el presente documento. La entrega del presente documento no le otorga ninguna licencia sobre dichas patentes. Puede enviar consultas sobre licencias, por escrito, a:
IBM Director of Licensing, IBM Corporation, North Castle Drive, Armonk, NY 10504-1785 U.S.A.

El siguiente párrafo no se aplica al Reino Unido u otros países donde dichas disposiciones sean incompatibles con la legislación local:
INTERNATIONAL BUSINESS MACHINES CORPORATION SUMINISTRA LA PRESENTE PUBLICACIÓN "COMO ESTÁ" SIN GARANTÍA DE NINGUNA CLASE, EXPRESA O IMPLÍCITA, INCLUYENDO, PERO SIN LIMITACIÓN, LAS GARANTÍAS IMPLÍCITAS DE NO VULNERACIÓN, COMERCIALIZACIÓN Y ADECUACIÓN PARA UN PROPÓSITO PARTICULAR. Algunos Estados no permiten la exclusión de garantías expresas o implícitas en ciertas transacciones, por lo tanto, esta declaración puede no aplicarse a su caso.

Esta información puede incluir imprecisiones técnicas o errores tipográficos. Periódicamente se hacen cambios a la presente información; dichos cambios se incorporarán en nuevas ediciones de la publicación. IBM puede realizar mejorías y/o cambios a los producto(s) y/o a los programa(s) descritos en esta publicación en cualquier momento, sin aviso previo.

Cualquier referencia en esta información a sitios web no IBM se proporcionan únicamente para su comodidad y de ninguna manera constituyen un aval de dichos sitios web. Los materiales en esos websites no forman parte de los materiales para este producto de IBM y la utilización de dichos websites son de su responsabilidad.

IBM puede utilizar o distribuir cualquier información que usted suministre de cualquier modo que crea apropiado sin incurrir en cualquier obligación para usted.

Información concerniente a productos no IBM que se obtuvo a partir de proveedores de esos productos, sus anuncios publicados u otras fuentes de uso público. IBM no ha probado dichos productos y no puede confirmar la exactitud de rendimiento, compatibilidad u otras afirmaciones relacionadas a productos no IBM. Preguntas sobre las capacidades de los productos no IBM deben dirigirse a los proveedores de dichos productos.

La presente información contiene ejemplos de datos e informes utilizados en las operaciones de negocio diarias. Para ilustrarlos de la manera más completa posible, los ejemplos incluyen nombres de personas, empresas, marcas y productos. Dichos nombres son ficticios y cualquier semejanza con los nombres y las direcciones utilizadas por una empresa real es pura coincidencia.

Los datos de rendimiento contenidos aquí se han determinado en un entorno controlado. Por lo tanto, los resultados obtenidos en entornos operativos diferentes pueden variar significativamente. Algunas mediciones pueden haberse realizado en sistemas en desarrollo y no existe ninguna garantía de que dichas mediciones serán las mismas en sistemas generalmente disponibles. Además, algunas medidas se pueden estimar mediante extrapolación. Los resultados actuales pueden variar. Los usuarios del presente documento deben verificar los datos aplicables a sus entornos particulares.

LICENCIA DE COPYRIGHT:

La presente información contiene programas de aplicación de muestra en el idioma de origen, que ilustran las técnicas de programación en diferentes plataformas operativas. Los programas de ejemplo se pueden copiar, modificar y distribuir en cualquier forma sin ningún pago a IBM, para fines de desarrollo, utilización, marketing o distribución de programas de aplicación compatibles con la interfaz de programación de aplicaciones de la plataforma operativa para la cual los programas de ejemplo están escritos. Estos ejemplos no han sido completamente probados bajo todas las condiciones. Por lo tanto, IBM no puede garantizar ni hacer cualquier afirmación sobre la confiabilidad, capacidad de servicio o función de dichos programas.

Este documento, REDP-4944-00, se creó o actualizó en December 2, 2013.

Marcas registradas

IBM, el logotipo IBM e ibm.com son marcas o marcas registradas de International Business Machines Corporation en los Estados Unidos, otros países o ambos. Estos y otros términos con marca registrada de IBM están identificados en su primera ocurrencia en esta información con el símbolo apropiado (o), indicando que son marcas registradas o de derecho consuetudinario en EE.UU., propiedad de IBM, en el momento en que esta información sea publicada. Tales marcas también pueden ser registradas o de derecho común en otros países. Una lista actualizada de marcas registradas de IBM se encuentra disponible en la Web en http://www.ibm.com/legal/copytrade.shtml

Los siguientes términos son marcas registradas de International Business Machines Corporation en los Estados Unidos, otros países o ambos:

AppScan®
DataPower®
Guardium®
IBM®
InfoSphere®
Optim™
Rational®
Redbooks®
Redbooks (logo)
Tivoli®
WebSphere®
X-Force®
zSecure™

Los siguientes términos son marcas registradas de otras compañías:

Los nombres de otras empresas, productos o servicios pueden ser marcas registradas de terceros.

© Copyright IBM Corp. 2013