Informe de Lippis

Informe técnico

Network Security 2.0

Una estrategia de sistemas para mitigar las amenazas

Versión 1

por

Nicholas John Lippis III

Presidente de Lippis Consulting

Mayo de 2008

Network Security 2.0: Una estrategia de sistemas para mitigar las amenazas

La estrategia generalmente aceptada para mitigar amenazas de TI consiste en crear una “defensa profunda” en capas con tecnología de seguridad como firewalls, IPS, control de acceso a la red, software de clientes anti-x, agregación de alarmas, correlación de eventos, etc. Y si bien esta estrategia de defensa en capas es útil, el panorama de las amenazas ha cambiado, lo que obliga a cambiar de rumbo y adoptar una estrategia de sistemas para proteger los recursos empresariales.

Network Security 2.0: ¿Seguridad en capas o estrategia de sistemas?

Escuche el Podcast

La estrategia tradicional en capas se basó en la implementación de los mejores productos de su clase, que sólo lo eran hasta que aparecían otros productos y los relegaban a la posición de dispositivos autónomos o silos de seguridad mal acoplados, como por ejemplo la combinación de dispositivos de firewall e IPS. Por su parte, la estrategia de sistemas se basa en esta inversión en seguridad de TI al integrarla con administración de sistemas de políticas, reputación e identidad que transcienden la seguridad de puntos terminales, redes, contenidos y aplicaciones. La estrategia de sistemas promete:

Un proveedor de contenidos de Internet protege las redes y servicios de clientes

Descargar el informe técnico

- Aplicar las políticas empresariales y proteger recursos fundamentales
- Disminuir la carga administrativa de seguridad del departamento de TI y reducir el costo total de propiedad (TCO)
- Reducir el riesgo de seguridad de TI y de incumplimientos
- Proteger las empresas contra las nuevas amenazas ubicuas

Un mundo complejo con un nuevo panorama de amenazas

Hoy en día, hacemos negocios en un mundo complejo y conectado como nunca antes. Las nuevas aplicaciones como las comunicaciones unificadas, colaboración y conferencias impulsan niveles más profundos de interacción entre empleados, partners, proveedores y clientes. Los empleados móviles y nómadas se conectan a la red empresarial desde cualquier punto geográfico del planeta. Las aplicaciones Web 2.0 habilitan nuevas combinaciones de contenidos y comunicaciones de variada naturaleza, que en el pasado se proporcionaban por separado, a fin de ofrecer nuevas maneras de comunicarse y conectarse. Todas estas tendencias representan nuevos adelantos de productividad económica extraordinarios pero a la vez crean una nueva serie de amenazas y retos de seguridad.

Un importante hospital psiquiátrico salvaguarda sus datos clínicos clave

Descargar el informe técnico

Network Security 2.0: ¿Cuáles son las nuevas amenazas?

En Network Security 1.0 se infectaban las herramientas de comunicaciones y colaboración dominantes en la época, es decir, el correo electrónico, la MI, la web y la infraestructura con software malicioso, gusanos, virus y otros tipos de explotaciones de puntos vulnerables. Los hackers utilizaban estas herramientas de comunicaciones en sus ataques para provocar daño y en un intento de responder a estos problemas, los líderes de TI crearon una defensa perimetral con tecnología de seguridad de la red de firewalls e IPS. Sin embargo, los hackers lograron eludir la defensa perimetral y para ello se centraron en el comportamiento de los empleados al usar la MI o el correo electrónico, visitar sitios web o utilizar otras aplicaciones que se convirtieron en el blanco perfecto de ataque de los hackers con correo no deseado, software malicioso, etc. En resumidas cuentas, los hackers encontraron nuevas maneras de identificar el comportamiento de los usuarios y pasar por alto las políticas y normas de firewall, con lo que se menoscabó la fortaleza defensiva del perímetro. Así nació Network Security 2.0.

Los hackers han evolucionado y han pasado de la travesura en la búsqueda de emociones al ciberdelito, que constituye la base del nuevo panorama de las amenazas denominado "Network Security 2.0”. Sin duda, las motivaciones de los grupos organizados para el ciberdelito son el lucro y la posibilidad de sacar una tajada con sus explotaciones. Algunos de estos grupos tratan de descubrir distintas maneras para acceder a las bases de datos empresariales que contienen información completa sobre identidad, seguro social o tarjetas de crédito y venden o explotan esa información. Otros grupos cibercriminales tratan de poner en funcionamiento una oficina de servicios al crear un botnet enorme para enviar mensajes no deseados o realizar otras actividades ilícitas.

Un banco comunitario protege los datos y simplifica el cumplimiento de la normativa vigente

Descargar el informe técnico

Desde el punto de vista de la empresa, la principal preocupación de seguridad de TI es la pérdida y el robo de datos ya que este siniestro perjudica la marca de la organización y socava las relaciones comerciales con clientes, partners y proveedores, sin mencionar sus consecuencias legales. Para los líderes empresariales, la pérdida y el robo de datos es una situación totalmente negativa debido a que los ejecutivos están obligados a comunicar públicamente toda violación de seguridad a clientes y funcionarios gubernamentales aunque sólo crean o supongan que se ha producido una pérdida de datos. Y aun cuando la pérdida de datos no se utilice con fines maliciosos, el directorio tiene la obligación de comunicarla a través de los medios masivos de comunicación, lo que genera el mismo riesgo que el uso malicioso de los datos perdidos. A veces el hecho de que los datos no se usen con fines maliciosos puede ser más grave para las empresas ya que genera incertidumbre y los clientes se preguntan cuándo se robarán su identidad a causa de la violación de la seguridad.

Por el nuevo tipo de entorno de amenazas contra la marca y el prestigio que se relaciona con Network Security 2.0, la seguridad de la red representa hoy un problema empresarial de alto nivel. Los líderes comerciales y de TI respondieron con administración del riesgo y en especial con posiciones de administración del riesgo de TI, que se centran en la administración de seguridad, defensa y cumplimiento, que se financian con los presupuestos departamentales y de cumplimiento asignados a nivel de directorio. En particular los proyectos de la industria de tarjetas de pago (PCI), lo que nos remite al Consejo de normas de seguridad de la industria de tarjetas de pago, son proyectos del directorio que establecen requisitos específicos de seguridad de la red, a fin de proteger la información de tarjetas de débito, tarjetas de crédito, cajeros automáticos, puntos de venta, información confidencial, etc.

Cómo crear una administración pública estatal más segura e inteligente

Descargar el informe técnico

La mayoría de los directorios de todo el mundo están preocupados por el cumplimiento, en especial el cumplimiento de PCI, la pérdida y el robo de datos, y preguntan a sus líderes comerciales y de TI qué medidas se están adoptando para brindar protección contra las explotaciones y cumplir con la normativa vigente. Preguntan cuáles son las políticas, las tecnologías implementadas o que deben adquirirse para crear las defensas contra el software malicioso, el spyware, los botnets o cualquier otra cosa que en el seno de la empresa pudiera contribuir a la fuga de datos o al incumplimiento.

La característica distintiva del panorama Network Security 2.0 es la ineficacia de las defensas de la era 2K. A principios de 2000 si una empresa se infectaba con un virus de Internet que se propagaba por toda su red, el departamento de TI compraba un IPS con una buena cobertura de firmas, lo instalaba y así bloqueaba el gusano y resolvía el problema. Hoy, existen varias amenazas Network Security 2.0 con una política integrada para pasar por alto las defensas puntuales como firewalls, filtros de correo no deseado, dispositivos IPS, etc. Para defenderse contra las “amenazas inteligentes”, es preciso que todos los dispositivos de seguridad de la red funcionen en conjunto. Para defenderse contra las explotaciones o amenazas inteligentes, se necesita una estrategia de sistemas de la seguridad que se base en las inversiones ya realizadas en la seguridad en capas. En síntesis, se necesita una función de organización que aproveche la inteligencia de defensa que ya existe en la red con el objeto de mitigar esta nueva categoría de amenazas.

La sucursal inteligente, surge un nuevo modelo de creación de valor agregado

Descargar el informe técnico

Estrategia de sistemas de la seguridad de TI

La seguridad de puntos terminales, la red, contenidos y aplicaciones son los cuatro componentes arquitectónicos de la estrategia de sistemas de la seguridad de la red. Cada uno de estos componentes forma parte de una defensa de seguridad en capas. Los puntos terminales se protegen mediante software anti-x. Las redes se protegen mediante firewalls, IPS, NBAD, NAC y tecnología de seguridad NAP. La red debe contar con protección al nivel de protocolo para analizar en profundidad los flujos, detectar posibles comportamientos anómalos y actuar en consecuencia.

La seguridad de contenidos es un enfoque nuevo y emergente de defensa contra amenazas, que protege a los usuarios contra el contenido de mensajes de correo electrónico, sitios web, MI, etc. ya que el propio flujo de contenidos puede constituir una amenaza que deba mitigarse. Los nuevos servidores de correo electrónico entran en línea y desaparecen con gran rapidez, al igual que los servidores web que alojan software malicioso.

Este fenómeno exige una estrategia de defensa basada en la reputación frente a una basada en firmas y la capacidad para responder a una gran cantidad de variantes ya que los ataques suelen tener objetivos muy específicos aunque cambian con rapidez según los entornos. En consecuencia, es preciso contar con la capacidad para responder a muchos ataques singulares diferentes, dado que cada ataque es diferente. Ya pasaron los días en los que los ataques generalizados presentaban un único patrón como NIMDA. En cambio, hoy, los ataques son de la más variada naturaleza y las políticas les permiten cambiar para anular las defensas. Los ataques a las aplicaciones de colaboración proceden de aplicaciones de correo electrónico, web, MI u otras aplicaciones de comunicaciones emergentes. Como hoy en día el atacante se basa en el hecho de que los propios usuarios propagarán los ataques frente a aquéllos de autopropagación, la seguridad de contenidos tiene como misión principal inspeccionar el contenido para evitar que los usuarios lleven a cabo acciones que den rienda suelta a un ataque exitoso.
Se anticipa que las aplicaciones y los datos a los que acceden serán el siguiente blanco al que apuntarán los atacantes. Ante el constante aumento de servicios Web 2.0 y SOA/Web habilitados en las organizaciones, se anticipa que estas aplicaciones serán el blanco perfecto de ataque, debido a que en ellas residen datos empresariales, información sobre clientes y propiedad intelectual.

La estrategia de sistemas tiene como eje principal organizar las tecnologías de defensa contra amenazas existentes para que funcionen en conjunto como un sistema, en gran medida como lo hace Tivoli en el caso de la TI. Para lograr este objetivo, las capacidades de administración de sistemas vinculan los cuatros componentes mediante políticas, reputación, servicios e identidad. La administración de sistemas puede aplicar políticas comunes en los cuatro componentes. Los productos como el sistema MARS 6.0 de Cisco agregan información de alarmas, que crea eventos correlacionados y propone medidas correctivas automáticas o de acción de las operaciones de la red. Estos productos de seguridad de agregación de alarmas y correlación de eventos cargan la información de alarmas de cada uno de los cuatro componentes y correlacionan los datos que proporcionan los escenarios de posibles amenazas en la red y abordan una política o responden de manera proactiva a la amenaza.

La estrategia de sistemas se basa en el aprovechamiento de los mejores productos de seguridad de su clase que ya están implementados en una empresa y en su gestión a través de administración de sistemas. Esta estrategia aplica las políticas de la empresa en los cuatro componentes y protege los recursos de TI fundamentales, además de reducir la carga operativa de TI y los costos. En consecuencia, se reduce el riesgo de TI desde el punto de vista de la seguridad y el cumplimiento de la normativa vigente. Además, esta estrategia libera a los compradores de soluciones de seguridad del dilema entre tener que adquirir los mejores productos de su clase o crear una estrategia de sistemas de defensa de TI.

Las compañías start-up no pueden seguir el ritmo

Toda nueva ola de amenazas a la seguridad ha creado un mercado para que las start-ups desarrollen el mejor producto de su clase con el fin de mitigar la amenaza en cuestión. Estas empresas suelen ser muy buenas a la hora de diseñar técnicamente una defensa contra una determinada amenaza; sin embargo, no cuentan con los recursos necesarios para responder a la siguiente ola de amenazas. En síntesis, estas empresas compiten con los atacantes y

como éstos han evolucionado y se han convertido en cibercriminales dotados de enormes recursos económicos que superan con creces los magros recursos de las empresas, los cibercriminales siempre ganan. El resultado de este ciclo es que los mejores productos de su clase no tienen mucho porvenir. Se convierten en dispositivos autónomos como firewall, NBAD, IPS, dispositivo NAC, etc. o se trata de ampliar su gama de mitigación de amenazas en una cantidad reducida de áreas a través del desarrollo interno o un partner y crear un silo de seguridad laxamente acoplado. Por ejemplo, la alianza entre 3Com! con su producto IPS Tipping Point y Lancope con su producto StealthWatch ha dado como resultado un silo de seguridad laxamente acoplado de productos de mitigación de amenazas IPS y NBAD.

¿Mitigar amenazas emergentes o ubicuas?

No se quiere decir que los mejores productos de su clase sean malos, sino que, cuando se los implementa como parte de una estrategia de sistemas holística, se prolonga su vida útil y se mejora la posición de seguridad de la empresa. Por ejemplo, tomemos el caso de Cisco. Cisco ofrece un dispositivo NAC, que es el mejor producto de su clase, pero para aprovecharlo al máximo conviene integrarlo en la estrategia de sistemas, que permite al dispositivo NAC funcionar junto con otros productos de seguridad como TrustSec de Cisco. En una estrategia de sistemas, el dispositivo NAC toca todo lo que la red conecta, con lo cual amplía su alcance y utilidad. En el caso de Cisco, su estrategia de seguridad consiste en ofrecer los mejores productos de su clase que pueden funcionar y migrar con el paso del tiempo a una estrategia de sistemas que brinda más valor agregado a los clientes. Por ejemplo, un cliente de Cisco puede implementar IronPort de Cisco, que puede no formar parte del marco de administración común, o que Cisco Segurity Manager no puede administrar desde el primer día; no obstante, es el mejor producto de seguridad de su clase para correo electrónico, el que con el tiempo pasará a integrar la estrategia de sistemas. En síntesis, Cisco desarrolló una visión y estrategia para una plataforma de seguridad de red que coloca a los clientes en un viaje.

Cisco promete que la posición de seguridad de esta empresa mejorará a medida que avance en el viaje. Por ejemplo, para prevenir la pérdida de datos, un cliente puede aprovechar la mejor solución de seguridad de su clase para correo electrónico, IronPort, con funciones de CSA (Cisco Security Agent), además de cifrado de medios de almacenamiento y reunir estas soluciones como si fueran un sistema para ofrecer una solución de prevención de pérdida de datos eficaz. Ésta es una estrategia de sistemas basada en los mejores productos de su clase y aumenta el valor de las mejores soluciones de su clase, que se destacan a la hora de mitigar las amenazas existentes y emergentes en el mediano plazo a una defensa contra las amenazas ubicuas como la prevención de pérdida de datos.
No centre sus expectativas en un organismo de normalización para definir las interfaces o la arquitectura de seguridad estándar. La industria no cuenta con este tipo de organización. Es necesario que los líderes comerciales y de TI centren su atención en los grandes proveedores de TI como Cisco, EMC, IBM, HP, Microsoft, etc. para obtener la visión, la plataforma y los partners que les ayudarán a responder a estas amenazas inteligentes. Los grandes proveedores de TI reconocen que la seguridad es un común denominador en toda la TI y debe formar parte de una estrategia global de sistemas. Esto es positivo porque para defenderse contra las explotaciones Network Security 2.0, se necesita una estrategia de sistemas. No piense en la estrategia de sistemas como en algo para proporcionar una respuesta automática contra amenazas al cerrar los puertos, direcciones IP, subredes o cambiar las ACL. Piense en términos de un sistema autónomo para comprender que el nuevo rumbo es la defensa contra amenazas a nivel de sistemas.

Seguridad de la red autónoma

La visión de la industria es pensar en términos de un efecto autónomo que aumenta con el paso de tiempo a medida que se van integrando cada vez los cuatro componentes en el enfoque de sistemas. A medida que los cuatro componentes comienzan a trabajar en conjunto bajo la administración de sistemas, el efecto autónomo aumentará. Como el sistema nervioso humano que responde automáticamente a los sensores, el cerebro no tiene que pensar antes de que se adopte una medida. Por ejemplo, una persona pone la mano en un calefactor caliente, el sistema nervioso responde automáticamente indicándole que saque la mano de allí. No se necesita ningún pensamiento. Tampoco se necesita ningún pensamiento para que el sistema inmunológico combata un virus o una infección, para

Cómo comenzar a crear una estrategia de sistemas de la seguridad de la red

El atractivo de la estrategia de sistemas es que aprovecha la infraestructura de defensa existente y no exige el retiro prematuro de las inversiones ya realizadas en seguridad. Cisco es la empresa líder en esta estrategia y ha realizado inversiones en su sistema de supervisión, análisis y respuesta. MARS, y productos CSA. Los usuarios de estos productos pueden comenzar la implementación sin necesidad de adquirir nuevos productos. Otros proveedores importantes de soluciones de seguridad y TI como IBM, Microsoft, HP y CA responderán con ofertas y un ecosistema propio. Los puntos fuertes específicos de cada empresa serán los que diferencien estas soluciones. La solución Microsoft se basará en un equipo de escritorio y en servidor, mientras que IBM y HP posiblemente se enfoquen en el centro de datos; CA podría basarse en aplicaciones. Cisco es la única empresa que se basa en la red y como todos los recursos de TI se conectan a través de la red, es una posición sólida para brindar protección contra amenazas.

Es preciso que los líderes comerciales y de TI seleccionen un proveedor de administración de sistemas. La solución MARS de Cisco se mencionó antes, pero también existe Q1 Labs QRader que es un sistema de administración y correlación de eventos de seguridad que podría evolucionar a un sistema de administración de sistemas. Nortel y Juniper trabajan en conjunto con Q1, mientras que Enterasys fabrica su sistema para ofrecer su Dragon Security Command Console. Al margen de un conjunto de funciones para proporcionar políticas, reputación e identidad, Nortel, Juniper y Enterasys carecen de la visón, la plataforma, el ecosistema y la solución completa para brindar una auténtica estrategia de sistemas de la seguridad de la red.