

¿Por qué es importante el control y la contención de amenazas?

Las amenazas a la seguridad de la red pueden menoscabar significativamente la productividad, interrumpir las actividades comerciales y operaciones, y causar pérdida de información, lo que a su vez puede ocasionar pérdidas económicas y hacer incurrir en el incumplimiento de requisitos legales. Los piratas informáticos continúan desarrollando nuevas técnicas para acceder a la información, a fin de obtener ganancias financieras, y estas técnicas son cada vez más difíciles de detectar. Las empresas necesitan soluciones completas que sean sumamente fáciles de administrar y utilizar para abordar estas amenazas en forma anticipada.

¿Qué problemas deben resolverse?

Las empresas enfrentan una gran variedad de problemas, tales como:

- Productividad de los empleados y TI durante ataques de virus o gusanos
- Seguridad de información confidencial
- Protección de la reputación y marca de la empresa
- Interrupciones en las comunicaciones e impacto
- en las actividades empresariales cotidianas

Ejemplos de amenazas reales que afectan las redes reales

- *Virus Zotob para fraudes con tarjetas de crédito:* el gusano Zotob infectó organizaciones, como por ejemplo, CNN, ABC News, el New York Times, Boeing, y el Departamento de Seguridad Nacional de los Estados Unidos en un esfuerzo por facilitar fraudes con tarjetas de créditos. Los investigadores del FBI creen que al creador de Zotob se le puede haber pagado para crear más de 20 virus adicionales.
- *Caballo de troya "rxbot" para lucro financiero:* el troiano conocido como rxbot infectó a 400.000 computadoras con programas de adware que le permitió obtener a su creador una suma neta superior a los US\$60.000 a través de los creadores de software de publicidad de pago por clic. El presunto infractor fue detenido en noviembre de 2005 bajo la sospecha de infectar a miles de máquinas, incluidas las computadoras de la División de Armamento del Centro Naval de Guerra Aérea de los Estados Unidos y aquéllas

pertenecientes a la Dirección de Sistemas Informáticos del Departamento de Defensa de los Estados Unidos.

- *Troyanos personalizados para la obtención de información empresarial:* se presume que los diseñadores de un troiano personalizado crearon y distribuyeron spyware destinado a la recopilación de información empresarial y que comercializaron el programa con tres firmas de investigaciones privadas. Se cree que estas firmas luego usaron el spyware para robar datos de la competencia de sus clientes. Según la policía, el programa aprovechó las vulnerabilidades del sistema operativo usando métodos estándar de captura de datos, como detección de pulsaciones de teclas, capturas de pantalla y transmisiones de archivos. Según los informes, la policía afirmó que este troiano se introdujo mediante mensajes de correo electrónico o un disco informático promocional supuestamente enviados a determinadas empresas por contactos comerciales conocidos y confiables. Decenas de empresas pueden haber sido infectadas, entre las cuales podrían encontrarse algunas firmas de Estados Unidos y Europa.

Solución de control y contención de amenazas

La Solución de control y contención de amenazas ofrece a los clientes un completo método para controlar y contener amenazas, proporcionando protección exclusiva contra ataques e intrusiones especializados y basados en Internet para organizaciones de todos los tamaños.

- *Visibilidad y protección de 360°:* Proporciona una defensa de red completa y anticipatoria
 - Se proporciona inteligencia contra amenazas para toda la infraestructura en forma económica a través de diversos sistemas y dispositivos
 - La identificación de amenazas de múltiples vectores detecta infracciones a las políticas, explotaciones de vulnerabilidades y conductas anómalas
- *Control simplificado:* Agiliza las políticas y su administración en toda la red
 - Administración estándar de políticas entre múltiples componentes de red
 - Implementación en toda la infraestructura entre diversos sistemas y dispositivos

- Continuidad empresarial: Garantiza las operaciones de la empresa
 - Colaboración y correlación exclusiva entre sistemas, puntos terminales y administración
 - Permite respuestas adaptables a amenazas en tiempo real
 - Elemento central de la estrategia de red de autodefensa de Cisco

Elementos centrales de la solución de control y contención de amenazas

- *Dispositivos de seguridad adaptable de la serie Cisco® ASA 5500:* es una plataforma modular que proporciona servicios de seguridad y VPN de próxima generación para entornos que van desde oficinas pequeñas hasta grandes empresas. <http://www.cisco.com/go/asa>
- *Cisco ASA 5500 edición Anti-X:* combate amenazas de Internet en el gateway, por ejemplo spyware, spam, virus y otras amenazas asociadas con el contenido de Internet. <http://www.cisco.com/go/asa>
- *Cisco Security MARS:* proporciona la interfaz de administración de amenazas de seguridad que traduce los datos sin procesar de red y seguridad en información de inteligencia útil. <http://www.cisco.com/go/mars>
- *Soluciones del sistema de prevención de intrusiones (IPS):* protege los servidores, las aplicaciones y otros activos cruciales contra ataques de red y aplicaciones y gusanos, en los gateways, las sucursales, los centros de datos y a lo largo de toda la red LAN. <http://www.cisco.com/go/ips>
- *Cisco Security Agent:* defiende a los servidores y equipos de escritorio contra ataques especializados, spyware, root kits y ataques de día cero. <http://www.cisco.com/go/csa>
- *Control de admisión a la red de Cisco (NAC):* valida las credenciales de seguridad de usuario y de sistema para proteger la red y la infraestructura contra infecciones. <http://www.cisco.com/go/nac>

El portal Web Cisco Security Center proporciona una guía única e integrada sobre los más recientes eventos de seguridad, además de información aplicada sobre cómo los productos y servicios de Cisco pueden utilizarse para mitigar nuevas amenazas.

Servicios de seguridad basados en el ciclo de vida útil para las soluciones de control y contención de amenazas

- El portal Cisco Security Center proporciona una guía única e integrada sobre los más recientes eventos de seguridad, además de información sobre cómo los productos y servicios de Cisco pueden utilizarse para mitigar amenazas.
- Los clientes suscritos a firmas de Cisco IPS tienen acceso a la base de datos de Cisco Security IntelliShield Alert Manager, que proporciona una completa información sobre eventos IPS y puede correlacionar firmas IPS con alertas de IntelliShield para acelerar la solución a posibles ataques.
- Los servicios de asesoría de implementación de Cisco IPS, Cisco Security MARS, Cisco NAC y Cisco Security Agent simplifican la instalación de nuevas soluciones por medio de especialistas de Cisco que usan sólidos principios de diseño y cuentan con gran experiencia en la integración de redes.

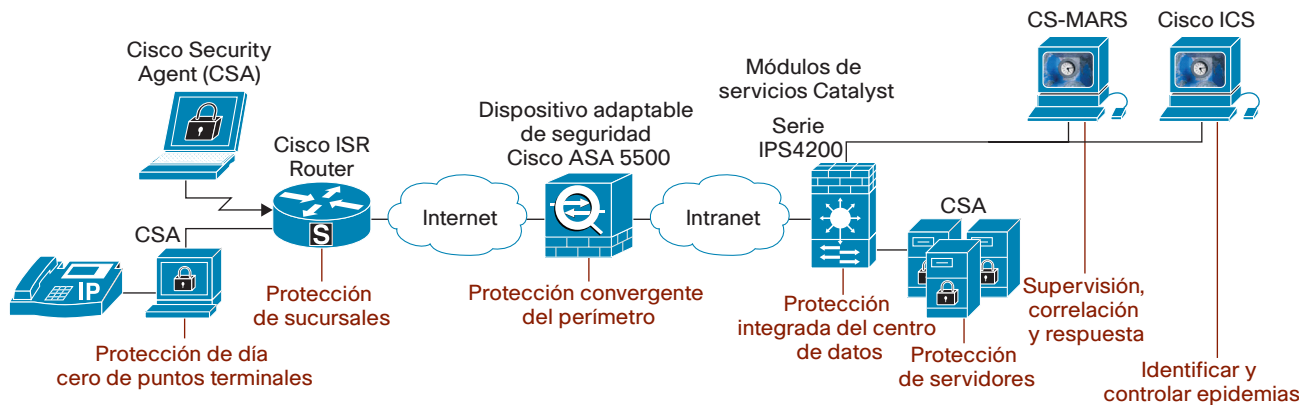
- El Servicio de actualización y afinación remotas Cisco IPS simplifica las operaciones cotidianas de dispositivos IPS mediante la implementación y afinación de actualizaciones de firmas en la medida en que estén disponibles.

¿Dónde comienzo?

La mayoría de las organizaciones cuentan con herramientas que pueden utilizarse como punto de partida para lograr una sólida y completa arquitectura de prevención de amenazas. La tecnología puede introducirse por fases a medida que se actualice la estrategia de seguridad de la empresa. Los procesos de seguridad deben revisarse periódicamente para asegurar que la organización esté adoptando las mejores prácticas. Una estrategia de seguridad completa y anticipatoria es un proceso en constante evolución; identificar los puntos cruciales es un primer paso muy importante. Solicite a su **representante de cuentas** de Cisco el informe técnico sobre control y contención de amenazas de Cisco para obtener información más detallada sobre cómo puede comenzar su siguiente fase de la solución de seguridad.

¿Por qué Cisco?

Cisco es la empresa líder mundial en soluciones de seguridad para redes. Cisco ofrece la mayor capacidad para combatir amenazas en toda la infraestructura de TI, desde los puntos terminales hasta la red y la capa de administración. La solución de seguridad de Cisco adaptable, integrada y de colaboración aborda ampliamente las amenazas que deben enfrentar las organizaciones en la actualidad, ayudando a asegurar la productividad de la TI y los empleados, y la protección de los activos de información más cruciales de las organizaciones. Desde amenazas provenientes de Internet hasta ataques e intrusiones especializados, las soluciones de Cisco ofrecen a los administradores de TI y seguridad las herramientas que necesitan para defender sus organizaciones en una era en que las amenazas contra la seguridad de la información son cada vez más complejas y difíciles de combatir.



1 Fuente: <http://www.securityfocus.com/news/11297>

2 Fuente: <http://www.techweb.com/wire/security/177103378>

3 Fuente: TechWeb <http://www.techweb.com/article/showArticle.jhtml;jsessionid=U45GMNUB4Y4VOQSNLPSKH0CJUNN2JVN?articleId=181501294&pgno=2>