Las cinco principales amenazas a la seguridad de las PYMEs

RESUMEN

La pequeña y mediana empresa utiliza Internet y las aplicaciones en red para llegar a nuevos clientes y ofrecer mejores servicios a los ya existentes. Por otro lado, las empresas cada vez tienen más dificultades para que sus redes sean seguras y fiables debido a las nuevas amenazas para la seguridad y la estricta legislación. Cisco Systems® proporciona soluciones de seguridad integradas, asequibles y completas, hechas a medida de la pequeña y mediana empresa, que ayudan a garantizar la continuidad de la actividad, mantener la privacidad del cliente y reducir los costes operativos. Las empresas pueden dedicar más tiempo a desarrollar su negocio con tranquilidad, y centrarse menos en los asuntos relacionados con la seguridad de la red.

RETO

Hoy en día, la competencia en el mercado es mundial y las pequeñas y medianas empresas se centran en expandir sus negocios y mejorar la satisfacción del cliente, a la vez que controlan sus gastos. Por suerte, Internet y las aplicaciones en red han conseguido que el panorama competitivo sea más equitativo. Las pequeñas y medianas empresas utilizan sus redes para extender el alcance de sus mercados y comunicarse con clientes y socios de una manera rápida y eficiente. Pero el acceso a Internet, además de hacer posible el comercio electrónico rápido y ágil, también puede abrir la puerta de las empresas a costosas brechas de seguridad. Es más importante que nunca tener una red disponible, segura y de confianza, y es igualmente importante que dicha red sea flexible y escalable para adaptarse tanto a las futuras necesidades de la banda ancha como a los servicios avanzados, tales como las aplicaciones de voz y datos convergentes o inalámbricas.

SEGURIDAD

Según un reciente estudio, la seguridad es el reto más importante al que se enfrentan las pequeñas y medianas empresas. Día a día surgen nuevas amenazas para la seguridad internas o externas a la red de la empresa que pueden afectar gravemente a sus actividades, con el consiguiente perjuicio para sus beneficios y la satisfacción de sus clientes. Además, las pequeñas y medianas empresas tienen que cumplir nuevas leyes y normativas creadas con el fin de proteger la privacidad del cliente y la seguridad de la información electrónica.

Amenaza nº 1: virus y gusanos informáticos

Los gusanos y virus informáticos siguen siendo la amenaza de seguridad más común. El 75 % de las pequeñas y medianas empresas se vieron afectadas por al menos un virus el año pasado.

El efecto de los virus y gusanos sobre la continuidad y rentabilidad de las empresas es devastador. Los brotes más avanzadas y destructivas se extienden a más velocidad que nunca, infectando oficinas enteras en cuestión de segundos. La limpieza de los ordenadores infectados lleva mucho tiempo y el proceso siempre se traduce en pérdida de pedidos, bases de datos corrompidas y clientes enfadados. Mientras las empresas luchan por actualizar sus ordenadores con los últimos parches de los sistemas operativos y software antivirus, nuevos virus amenazan con penetrar en sus defensas en cualquier momento. Paralelamente, los empleados extienden los virus y los programas espía (spyware) sin saberlo cuando acceden a páginas web maliciosas, se descargan material poco fiable o abren ficheros adjuntos de correos electrónicos. Estos ataques son introducidos en la empresa accidentalmente, pero pueden provocar enormes pérdidas económicas. Los sistemas de seguridad deben detectar y repeler gusanos, virus y spyware en todos los puntos de la red.

Amenaza nº 2: robo de información

El robo de información es lucrativo. Los hackers irrumpen en las redes de las empresas para robar números de tarjetas de crédito o de la seguridad social con fines lucrativos. Las pequeñas y medianas empresas son un objetivo fácil en comparación con las grandes empresas. Proteger el perímetro de la red es un buen comienzo, pero no es suficiente, ya que muchos de los robos de información son perpetrados con la ayuda de una persona de dentro, de confianza, como por ejemplo un empleado o un contratista.

El robo de información puede suponer un alto coste para las pequeñas y medianas empresas, ya que dependen de la satisfacción del cliente y la buena reputación para el crecimiento de su negocio. Las empresas que no protegen su información adecuadamente podrían verse afectadas por una publicidad negativa, sanciones gubernamentales o incluso demandas judiciales. Por ejemplo, las nuevas leyes de consumo promulgadas en California obligan a cualquier empresa que sospeche que cierta información de un cliente ha podido ser vista por personas no autorizadas a notificarlo a todos sus clientes. Toda estrategia de seguridad debe evitar el robo de información electrónica confidencial tanto desde dentro como desde fuera de la empresa.

1 Maritz Research, 2005

Amenaza nº 3: disponibilidad de la empresa

Los gusanos y virus informáticos no son los únicos que ponen en peligro la disponibilidad de la empresa. Los ataques de negación de servicio (DoS) pueden bloquear páginas web y operaciones de comercio electrónico, enviando un gran volumen de tráfico hacia un elemento crítico de la red, haciendo que falle o que sea incapaz de procesar el tráfico legítimo. Una vez más, el resultado es desastroso: se pierden datos y pedidos y no se responde a las peticiones del cliente. Si estos ataques se hacen de dominio público, la credibilidad de la empresa se ve perjudicada. Si bien la mayor parte de la publicidad en torno a los ataques de DoS se han centrado en los grandes bancos y en las 500 empresas más importantes, las pequeñas y medianas empresas no son inmunes, ya que son consideradas más fáciles de atacar que una gran empresa.

Existen otros ataques mucho menos dramáticos pero mucho más habituales que amenazan también a la disponibilidad de la empresa. Por ejemplo, un ataque de robo de recursos se introduce en las redes y ordenadores, utilizándolos para el uso compartido ilegal de archivos de música, películas o software. A menudo, las empresas no son conscientes de que se está produciendo una brecha en la seguridad, pero mientras tanto, sus redes y ordenadores tardan más en responder a sus clientes y su participación inadvertida en el uso compartido ilegal de archivos les hace vulnerables a demandas judiciales.

Amenaza nº 4: lo desconocido

Cada avance de la informática y las comunicaciones viene acompañado de una nueva forma de explotar las tecnologías para beneficio propio o para hacer daño. Las nuevas versiones de hardware o software ofrecen este tipo de oportunidades. Cuando la conexión de redes peer-to-peer y la mensajería instantánea eran aplicaciones relativamente nuevas, sus usuarios se veían atacados, por ejemplo, por códigos maliciosos escritos especialmente para ellas. Ahora los teléfonos móviles son un objetivo habitual de los virus.
Como no podemos predecir lo que está por venir, la mejor defensa es aquella que pueda adaptarse a las amenazas futuras y que sea asequible.

Amenaza nº 5: legislación sobre seguridad

Aparte de estas amenazas a la seguridad, las nuevas leyes y normativas exigen que las pequeñas y medianas empresas protejan la privacidad y la integridad de la información que se les ha confiado. En la Unión Europea, por ejemplo, la Ley de Protección de Datos de la UE, se ocupa de la protección de los datos personales depositados en las empresas. Casi todas las industrias deben cumplir una legislación que regula sus negocios y requiere medidas de seguridad adicionales. En Estados Unidos, la Ley de Responsabilidad y Transferibilidad de Seguros Médicos (HIPAA) exige que las empresas de sanidad, incluidas las consultas privadas de los médicos, dispongan de medidas en el lugar para garantizar la privacidad de la información sobre el estado de salud y evitar accesos no autorizados.

Es responsabilidad de las empresas cumplir la legislación y normativa de aplicación en sus empresas y mercados. Los clientes quieren asegurarse de que su información sea privada. Todas las empresas tienen que tomar medidas para que sus infraestructuras de negocio sean seguras, pero sus presupuestos son limitados, especialmente los de las pequeñas y medianas empresas, que requieren soluciones proporcionadas y asequibles.

SMART BUSINESS ROADMAP DE CISCO: LA HOJA DE RUTA PARA LAS EMPRESAS INTELIGENTES

Cisco® Smart Business Roadmap permite a las PYMEs compaginar su plan tecnológico con sus prioridades comerciales. Proporciona una evolución estructurada para ayudar a las empresas a adaptarse al cambio de manera previsora. Además otorga a los responsables de tomar decisiones comerciales y técnicas la seguridad de que sus inversiones inmediatas en tecnología serán un apoyo para sus objetivos a largo plazo.

Para guiar a las empresas en crecimiento en cada etapa de desarrollo: fundación, crecimiento y optimización, el Smart Business Roadmap de Cisco ofrece un doble enfoque:

- Red de Autodefensa de Cisco (Cisco Self-Defending Network)
- Solución Secure Network Foundation de Cisco

Red de Autodefensa de Cisco (The Cisco Self-Defending Network)

La Red de Autodefensa de Cisco es una estrategia a largo plazo para asegurar los procesos de las empresas identificando, evitando y adaptándose tanto a las amenazas internas como a las externas. La Red de Autodefensa de Cisco protege a las empresas hoy y se adapta a las necesidades futuras. Con Cisco, las empresas pueden proteger no sólo sus redes sino también sus inversiones en las mismas. Los resultados son la mejora de los procesos de la empresa y un ahorro considerable.

La Red de Autodefensa de Cisco posee tres características diferenciadoras: integración, colaboración y adaptabilidad. En primer lugar, integra la seguridad en todos los elementos de la red, asegurando que cada punto de la red sea capaz de protegerse ante amenazas internas y externas. En segundo lugar, estos elementos de la red trabajan conjuntamente para intercambiar información y proporcionar una protección adicional. En tercer lugar, la red utiliza un sistema de reconocimiento de comportamiento innovador para adaptarse a las nuevas amenazas conforme éstas van surgiendo. La Red de Autodefensa de Cisco es una solución de seguridad sencilla pero completa y rentable para pequeñas y medianas empresas que crea redes de autodefensa protegidas y de confianza.

Solución Secure Network Foundation de Cisco

La solución Secure Network Foundation de Cisco se basa en el marco de las redes de autodefensa. Permite a las pequeñas y medianas empresas centrarse en la rentabilidad más que en las redes. Proporciona servicios seguros y estables a todos los usuarios, tanto por conexión tradicional como inalámbrica. Los servicios de seguridad están integrados en los routers, conmutadores (switches) y dispositivos de seguridad de Cisco, ayudando a las pequeñas y medianas empresas a hacer más eficientes sus operaciones y reducir sus costes. La solución Secure Network Foundation de Cisco incorpora la tecnología de Red de Autodefensa de Cisco, que protege a las empresas hoy y se adapta a las necesidades futuras. Las empresas pueden continuar con sus operaciones, incluso cuando se ven amenazadas, y pueden cumplir los requisitos de seguridad y privacidad de los datos exigidos tanto por el cliente como por las leyes.

Permanece abierto y en funcionamiento, incluso cuando estás siendo atacado.

Ante el acecho de nuevos ataques, las empresas y clientes necesitan garantías de estar protegidos contra las interrupciones y los bloqueos de servicios causados por la

corrupción de datos. La Red de Autodefensa de Cisco proporciona un enfoque múltiple y comprobado, que protege a las empresas de los devastadores efectos de los ataques de gusanos, virus, ciberterroristas y otros.

Los virus, gusanos y programas espías entran en la empresa normalmente por el correo electrónico o a través de aplicaciones de mensajería instantánea, descarga de páginas web, o transferencia de archivos, a pesar de que otros ataques más sofisticados pueden entrar a través de servicios inalámbricos móviles o servicios de sistemas operativos. El Sistema de Prevención de Intrusiones (IPS) de Cisco, líder en la industria y disponible en los dispositivos de seguridad, routers, y conmutadores de Cisco, explora e inspecciona todo el tráfico entrante en tiempo real, en busca de irregularidades que puedan ser síntoma de un ataque. Si se detecta alguna anomalía, el IPS calcula la gravedad del riesgo y se comunica con otros componentes responsables de la seguridad de la red para detener la amenaza desde su raíz y evitar que se extienda por toda la red.

La seguridad integrada en la empresa detiene ataques conocidos y desconocidos en tiempo real, y la comunicación entre los diferentes componentes de la red permite que se adapten a las cambiantes condiciones de seguridad. Las capas de seguridad permiten a las pequeñas y medianas empresas responder ante sus clientes y permanecer abiertas y en funcionamiento incluso cuando están siendo atacadas.

Protege la privacidad del cliente.

La solución Secure Network Foundation de Cisco utiliza múltiples herramientas para proteger la información del cliente contra usuarios no autorizados de dentro o fuera de la empresa.

Las redes privadas virtuales (VPN): Seguridad IP (IPsec) y Capa de Seguridad de Enchufe (Secure Socket Layer, SSL), permiten la comunicación entre pequeñas oficinas y trabajadores remotos, manteniendo la oficina principal bajo una privacidad absoluta, incluso cuando se utiliza el servicio público de Internet en los medios de transporte. Los más altos estándares de autentificación de usuarios garantizan que sólo los usuarios válidos pueden acceder a la VPN. Unas estrictas tecnologías de encriptación hacen que los datos sean ilegibles para cualquier persona que intente interceptar las comunicaciones VPN en una red pública. El sistema de seguridad de puntos finales Secure Desktop de Cisco tiene como objetivo minimizar el riesgo de que datos como cookies, historial del navegador, archivos temporales y contenidos de descargas permanezcan en el equipo una vez terminada la sesión SSL VPN.

La existencia de cortafuegos (firewalls) e IPS (Sistemas de Prevención de Intrusos) en todos los puntos de entrada de una red ayuda a detener gusanos, spyware o hackers que intenten penetrar en la red de la empresa para robar información. Los cortafuegos también son de utilidad para evitar que los usuarios de dentro de la empresa accedan a información confidencial. Por ejemplo, las normas internas de firewall pueden evitar que personal no autorizado acceda a los ordenadores del departamento de finanzas, recursos humanos o contabilidad, o que pueda ver su tráfico de datos. Las redes de área local virtuales (VLAN) permiten a las empresas segmentar aún más la comunicación interna dentro de la organización. La información confidencial o financiera de los clientes puede ser almacenada en su propia VLAN, separada lógicamente de la LAN de los empleados.

La solución Secure Network Foundation de Cisco ayuda a las empresas a cumplir los requisitos legales de seguridad y privacidad de la información del cliente, protegiendo la red de brechas de seguridad o accesos no autorizados desde dentro o desde fuera de la red.

Control de costes

La solución Secure Network Foundation de Cisco ayuda a las pymes a controlar los costes de dos maneras: primero, evitando costes innecesarios asociados con brechas de seguridad, y segundo, utilizando componentes de seguridad integrados, asequibles y multifuncionales que crezcan con el negocio a medida que van cambiando sus necesidades. Una seguridad integrada simplifica la gestión y el mantenimiento de las redes, reduciendo así sus costes totales de propiedad de una red.

Las brechas de seguridad en las redes acarrean, además de los costes obvios, otros costes ocultos. Por ejemplo, muchas amenazas de seguridad, como virus relativamente inocuos, causan pocos daños, y los costes obvios que se les asocian son el tiempo y los recursos gastados para limpiar los sistemas de la empresa infectados. Los costes aumentan con el número de sistemas infectados, por lo que una buena protección y una rápida detección permiten ahorrar dinero. Otros costes menos obvios son el tiempo que se pierde mientras que se limpian los ordenadores de los empleados. Algunos ejemplos de costes ocultos serían la pérdida de oportunidades y clientes, la disminución de la reputación de la empresa o los costes legales relacionados con las brechas de seguridad. Estos costes, a pesar de ser menos comunes, pueden ser elevados. En 2005, los delitos en la red supusieron un coste de 2.400 millones de libras a las empresas británicas. La solución Secure Network Foundation de Cisco ayuda a las empresas a evitar tanto los costes obvios asociados a las brechas de seguridad, como los ocultos, reduciendo así el riesgo de la empresa y aumentando su credibilidad y la confianza del cliente.

Las pequeñas y medianas empresas no disponen de los recursos humanos ni de suficiente capital disponible para comprar y mantener complejas soluciones de seguridad. La solución Secure Network Foundation de Cisco es segura, fiable y reduce el coste total de propiedad de la red. De este modo, las empresas pueden centrarse en sus negocios y no en sus redes. La solución Secure Network Foundation de Cisco se adapta con facilidad a las necesidades de la empresa y a las condiciones de seguridad, asegurando así que los gastos se vean compensados por el crecimiento del negocio.

CONSTRUYENDO LAS BASES PARA UNA RED SEGURA

La solución Secure Network Foundation de Cisco está integrada en diversos productos Cisco:

- Routers de servicios integrados de Cisco
- Dispositivos de seguridad adaptables ASA 5500 Series de Cisco
- Switches Catalyst® de Cisco (Catalyst® Switches)
- Puntos de acceso Aironet® de Cisco

Estos productos constituyen las piedras angulares de la Red de Autodefensa de Cisco para la pequeña y mediana empresa.

Routers de servicios integrados de Cisco

Los routers de servicios integrados de Cisco combinan varias funciones en una única plataforma router fiable y económica. Los routers de servicios integrados de Cisco combinan las capacidades de un cable DSL o un router de acceso a banda ancha con un enlace redundante integrado, un conmutador de red de área local, un cortafuegos, un IPS o VPN, un punto de acceso inalámbrico, y un conmutador de red de área local inalámbrico: todo en un único dispositivo. Muchas de estas capacidades pueden ir

añadiéndose a los routers de servicios integrados de Cisco dependiendo de las necesidades, y por tanto las empresas pueden ir incorporándolas a medida que su negocio crezca. Son apropiados para oficinas donde trabaja desde una sola persona hasta oficinas pequeñas o medianas, puesto que proporcionan una base inteligente para las futuras necesidades del negocio. Las empresas pueden añadir servicios de voz y datos, seguridad, o tecnología inalámbrica cuando los necesiten, sin tener que hacer un excesivo desembolso adicional.

2 National High-Tech Crime Unit/ Unidad Nacional de Crímenes de Alta Tecnología

Dispositivo de Seguridad Adaptable ASA 5500 Series Business Edition de Cisco

La serie de dispositivos de Seguridad Adaptable ASA 5500 Series Business Edition de alto rendimiento de Cisco se basa en una tecnología de seguridad comprobada por Cisco que reacciona y se adapta para ofrecer protección contra amenazas conocidas y desconocidas. El Dispositivo de Seguridad Adaptable ASA 5500 Series de Cisco combina el mejor cortafuegos de su categoría, IPS, protección anti-X contra virus, spam y spyware, y servicios VPN de acceso remoto y site-to-site. El Dispositivo de Seguridad Adaptable ASA 5500 Series de Cisco proporciona la más alta protección contra el acceso de usuarios no autorizados, gusanos, virus, spyware y aplicaciones poco seguras o maliciosas. Este dispositivo está diseñado para las redes de las pequeñas y medianas empresas de hoy. Es rentable, de fácil uso y gestión, y puede ser actualizado. A medida que emergen nuevas amenazas a la seguridad, las actualizaciones y extensiones de seguridad instaladas por el usuario permitirán que los productos ASA de Cisco se adapten para poder continuar protegiendo su negocio. El Dispositivo de Seguridad Adaptable ASA 5500 Series de Cisco es la perfecta elección para una oficina principal o cualquier filial que necesite una solución de seguridad completa.

Switches Catalyst® de Cisco (Catalyst® Switches)

Los Conmutadores Catalyst de Cisco tienen todas las funcionalidades necesarias para obtener unas redes inteligentes, sencillas y seguras. Están diseñados para cumplir todos los requisitos de seguridad, rendimiento y fiabilidad necesarios. Al permitir la convergencia de diversas aplicaciones en una red, los Conmutadores Catalyst de Cisco aumentan la capacidad de respuesta de los empleados a los clientes, al tiempo que mejoran la eficacia operativa. Todos los Conmutadores Catalyst de Cisco poseen funcionalidades de seguridad capaces de detener las irregularidades de tráfico y evitar que éstas sobrecarguen el conmutador o se extiendan a otros puntos de la red.

El Asistente de Red de Cisco (Cisco Network Assistant) es una herramienta de gestión para ciertos conmutadores Catalyst, gratuita y fácil de usar, que permite gestionar la instalación y configuración de red de manera sencilla y localizar y resolver problemas. Smartports Advisor es otra herramienta de configuración que detecta automáticamente todos los dispositivos Cisco que se encuentren conectados y recomienda configuraciones preprogramadas para el puerto conmutador al que se conecta el dispositivo. Simplifica la implantación de redes, evitando a las empresas tener que concentrarse en la utilización de tecnologías avanzadas. El Asistente para Resolución de Problemas (Troubleshooting Advisor tool) identifica automáticamente todos los problemas potencialmente relacionados con la red, como el cableado y los errores de configuración, y los registra en la tabla correspondiente. Además, proporciona la descripción del problema y permite al usuario corregirlo con un simple clic.

Puntos de acceso Aironet de Cisco

Los puntos de acceso Aironet de Cisco proporcionan acceso inalámbrico a una red de área local para las pequeñas y medianas empresas. Los productos inalámbricos de Cisco tienen el mismo nivel de seguridad, escalabilidad y gestión que una red de área local tradicional. Los puntos de acceso Aironet de Cisco soportan una movilidad segura y rápida, si se utilizan con dispositivos de Cisco u otros dispositivos compatibles, permitiendo a los usuarios autentificados moverse con seguridad de un punto a otro.

Funcionamiento fiable y sin problemas

El disponer de un servicio y apoyo excelente e integral es un factor decisivo para el éxito a largo plazo de cualquier solución de red. El asistente de soporte Cisco SMB Support Assistant ha sido diseñado para satisfacer las necesidades de las pequeñas y medianas empresas. Se trata de un programa de soporte rentable y fácil de usar que resuelve los problemas típicos de las pequeñas y medianas empresas, permitiendo que la red esté disponible y sea segura en todo momento. Las empresas pueden obtener un diagnóstico temporal y consejos para la resolución de problemas y la sustitución de componentes. El asistente de soporte Cisco SMB Support Assistant es un conjunto de herramientas seguras en línea que permite a los clientes recuperar contraseñas, acceder a la documentación de soporte, realizar inspecciones de seguridad de la red, descargar parches de seguridad y abrir casos de soporte técnico cuando sea necesario.

POR QUÉ CISCO

La solución Secure Network Foundation de Cisco para pequeñas y medianas empresas mantiene activos los procesos de negocio, garantiza la privacidad de la información del cliente, controla los costes asociados con el mantenimiento de una Red de Autodefensa protegida, segura y disponible. En resumen, todo esto aumenta la confianza del cliente, mantiene o incrementa la eficiencia de los trabajadores, ayuda a las empresas a cumplir los requisitos legales y reduce los costes totales de propiedad de una red.

La solución Secure Network Foundation de Cisco es sólo una de las múltiples soluciones de Cisco Smart Business Roadmap, diseñadas para mejorar la eficiencia de los trabajadores, apoyar los servicios innovadores, aumentar la satisfacción del cliente y reducir los costes operativos. Con unas capacidades mejoradas en las áreas de voz, seguridad, movilidad y protección de las inversiones, las soluciones Smart Business Roadmap de Cisco pueden satisfacer las necesidades de las empresas ahora y en el futuro.

Cisco y sus socios de comunicación se esfuerzan por ofrecer a las pequeñas y medianas empresas el mejor trato posible, basándose en su amplia experiencia. Gracias a las opciones de financiación, el servicio premiado de atención y apoyo al cliente y la formación personalizada, Cisco consigue que las empresas puedan sacarle el máximo partido posible a su Solución Smart Business Roadmap.

Cisco es la empresa líder en el mercado de routing, switching y seguridad, que proporciona soluciones flexibles a las empresas para satisfacer sus necesidades actuales y futuras, y permitirles crecer y mejorar. La estrategia de seguridad de la compañía se basa en la Red de Autodefensa de Cisco, que integra la seguridad en todos los puntos de la infraestructura, colabora para proporcionar una protección adicional y se adapta a las condiciones de la red y a las nuevas amenazas de seguridad. Cisco ofrece una amplia gama de productos además de la Solución Smart Business Roadmap de Cisco para ayudar a las pequeñas y medianas empresas a seguir un camino evolutivo, inteligente y estructurado, para sacar el máximo provecho a sus inversiones tecnológicas.

ANEXO

Para más información acerca de la solución Secure Network Foundation de Cisco, contacte con una empresa asociada de Cisco o visite: http://www.cisco.com/en/US/netsol/ns644/networking_solutions_packages_list.html

Para más información acerca de Cisco Smart Business Roadmap, contacte con una empresa asociada de Cisco o visite: http://www.cisco.com/go/sbr

Para encontrar un socio de comunicaciones de Cisco, visite: http://www.cisco.com/go/partnerlocator

Para más información acerca de los métodos de financiación de la solución Secure Network Foundation de Cisco, visite: http://www.cisco.com/go/ciscocapital