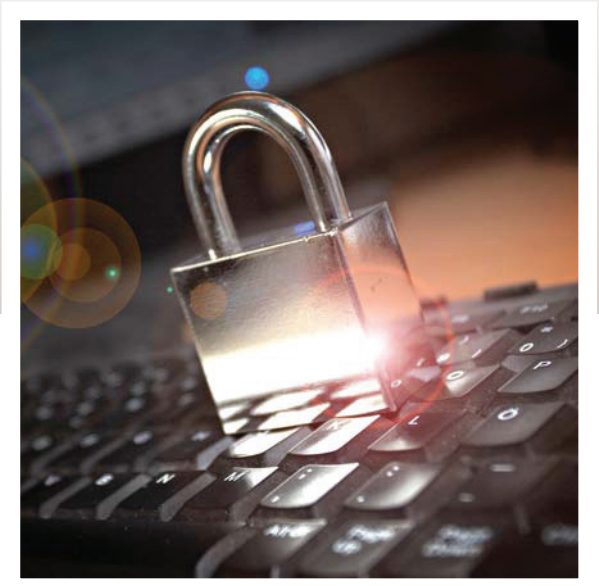
5 tendencias que afectarán su planificación de TI en 2012

Seguridad por niveles



Small Business Computing.com™

Informe ejecutivo

Seguridad por niveles

Muchas de las tendencias de TI que su organización enfrentará en 2012 no son nuevas, pero eso no significa que su personal de TI pueda quedarse quieto mientras la tecnología continúa evolucionando. Este informe ejecutivo es uno de cinco en esta serie en la que se analizarán las tendencias que debe incluir en su planificación de TI para 2012.

A esta altura, casi todos los que interactúan con una PC en forma regular están familiarizados con los conceptos fundamentales de la seguridad de computadoras y redes: instalar software antivirus, elegir contraseñas seguras y protegerlas y descargar e instalar actualizaciones de software. A pesar de estas medidas, las empresas de todos los tamaños continúan sufriendo violaciones de seguridad.

Cuando empresas grandes como Sony y TJX sufren violaciones en los datos, sale en las noticias a nivel internacional. En parte debido a la publicidad y en parte debido al tamaño de los presupuestos y el personal de TI en las grandes empresas, los criminales cibernéticos están volcando su atención a las pequeñas y medianas empresas cada vez más, donde es más probable que la seguridad sea débil, es menos probable que se descubran las violaciones en forma oportuna y donde las recompensas para los criminales pueden ser elevadas. Según el informe de investigaciones de violaciones en los datos de 2011 de Verizon, las pequeñas y medianas empresas se han convertido en los objetivos principales de los piratas informáticos.

Otras encuestas llegan a una conclusión similar:

- Según GFI Software, el 40 por ciento de las pequeñas y medianas empresas ha experimentado una violación de la seguridad debido a que empleados navegaron a un sitio que alojaba malware.
- Según GfK NOP, las pequeñas y medianas empresas perdieron 30 millones de horas hombre para solucionar cuestiones originadas por problemas de seguridad.
- En la misma encuesta, se determinó que las pequeñas y medianas empresas estadounidenses que experimentaron problemas de seguridad gastaron USD 5,6 millones o un promedio de USD 1570 por empresa para reemplazar hardware. También perdieron USD 11,3 millones (un promedio de USD 4800 por empresa) en pérdidas de oportunidades de ingresos o ventas.

Las pequeñas y medianas empresas descuidan la seguridad fácilmente, ya que no aporta directamente a los resultados de la misma forma que los productos o clientes nuevos generan ingresos. En general, el valor verdadero de la seguridad no se determina hasta que algo sale mal y una empresa no ha invertido en ella; en ese aspecto, es similar

a los seguros. Para las pequeñas y medianas empresas, es importante establecer prácticas sólidas de seguridad en sus inicios, ya que esa estrategia de seguridad puede crecer con la empresa —un plan mucho mejor que encontrar una empresa en crecimiento sin una seguridad sólida que está expuesta a toda la variedad de amenazas.

El panorama de amenazas de 2012

El malware ha avanzado mucho desde que el virus ILOVEYOU infectó millones de computadoras en el año 2000 con un simple correo electrónico con un adjunto infectado. Los virus basados en adjuntos todavía existen, pero los usuarios y los productos de seguridad para el correo electrónico se han puesto al día. Los ataques que las pequeñas y medianas empresas enfrentan en 2012 son mucho más específicos y se basan en mecanismos de envío diferentes al correo electrónico. Es mucho más probable que sean obra de una red organizada de criminales que intentan obtener información personal, como números de cuenta y contraseñas. Se pueden utilizar aplicaciones basadas en la Web, desde aplicaciones empresariales internas hasta destinos populares en línea como Facebook, para introducir malware usando tácticas como la inyección SQL.

Las estafas de suplantación de identidad siguen existiendo, pero, en lugar de tender una amplia red en un intento por recoger información confidencial de millones de usuarios, es más probable que usen ingeniería social, a través de lo que parece ser un interés personal, para generar confianza en víctimas potenciales.

Los dispositivos móviles y las conexiones inalámbricas significan que las máquinas y los datos empresariales no están restringidos a la oficina. Antes, mantener una red segura proporcionaba una protección razonable, pero ahora los datos se transmiten a través de redes externas que pueden poner en riesgo a las pequeñas y medianas empresas.

Mientras los criminales sofisticados están detrás de muchos de los ataques actuales, los amateur siguen estando presentes y su trabajo tiene un poderoso potencial. Kits como el que generó el virus de suplantación de identidad Zeus se pueden comprar en línea, lo que permite que cualquier persona se convierta en un criminal cibernético autodidacta.

Qué es lo que necesita protección

En lo que respecta a las PC y los recursos de red de una pequeña o mediana empresa, todo necesita protección. Y, si bien un poco de sentido común puede servir mucho cuando se trata de mantener las laptops fuera de vista cuando están en el automóvil o elegir contraseñas sólidas, otras partes de la infraestructura técnica requieren mayor diligencia.

Aquí se incluye una lista parcial de consejos de seguridad para redes y computadoras del sitio web SmallBusinessComputing.com:

- Mantener los sistemas operativos con las últimas actualizaciones y parches
- Minimizar el uso de cuentas de administrador en las PC
- Usar el cifrado de disco completo para laptops
- Usar WPA2 para proteger las redes inalámbricas

"Mientras los criminales sofisticados están detrás de muchos de los ataques actuales, los amateur siguen estando presentes y su trabajo tiene un poderoso potencial"

- Desactivar las opciones de administración remota
- Limitar el acceso a carpetas compartidas

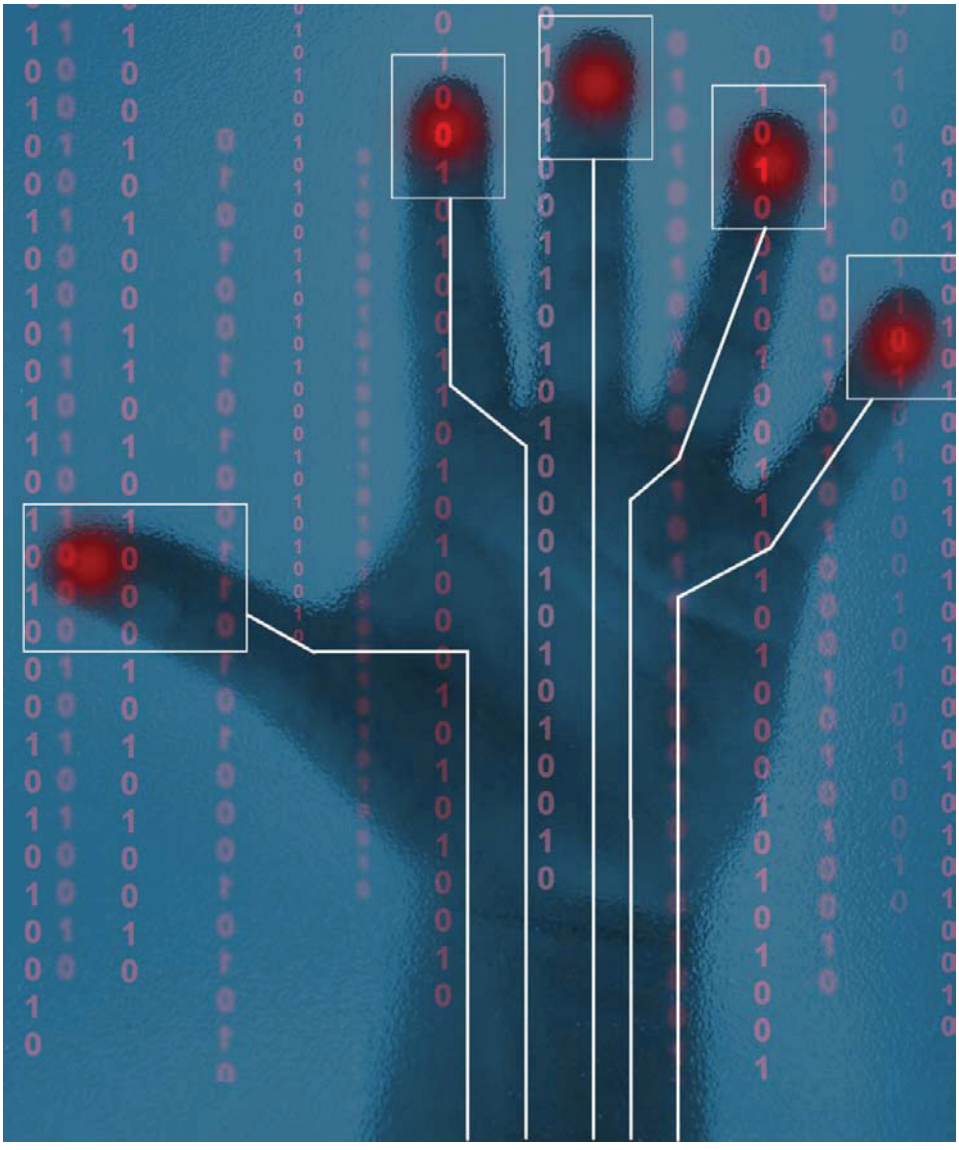
Es necesario proteger a extremos y redes por igual, lo que significa que un software antivirus y contraseñas seguras son solo el comienzo. Debe proteger las diferentes capas de la infraestructura que existen en hasta las empresas más pequeñas. Los firewalls y lo que algunos proveedores de tecnología llaman gestión unificada de amenazas (UTM) ayudan a proteger las redes de las pequeñas empresas frente a ataques externos. Las herramientas de seguridad de extremos como las VPN y la protección de antivirus ayudan a proteger frente a ataques internos. La protección de acceso y el cifrado permiten proteger los datos. Las pequeñas y medianas empresas que operan en ciertas industrias como el gobierno podrán requerir sistemas de administración de información de seguridad (SIM) para cumplir con las regulaciones de la industria.

Este enfoque, conocido como seguridad por niveles, es esencial para proteger tanto la infraestructura como la información en 2012. Dado el daño que el malware puede ocasionar, la seguridad por niveles debe considerarse fundamental para proteger la empresa.

Cómo implementar la seguridad por niveles

No se equivoque; un enfoque integral para la seguridad requiere una inversión en términos de tiempo y dinero. El primer paso en un enfoque holístico para la seguridad es convertir la seguridad en una prioridad en la empresa.

En muchas pequeñas y medianas empresas, la seguridad y otras cuestiones de TI están a cargo de la persona con mayor experiencia trabajando con computadoras o de un generalista de TI. Este enfoque puede funcionar en las empresas más pequeñas, pero es poco probable que pueda ampliarse correctamente a medida que la empresa crezca. Otro enfoque popular es subcontratar la totalidad o parte de las responsabilidades de TI a un integrador de sistemas o una empresa de servicios de TI que sea un socio de canal para los principales proveedores de TI. Las pequeñas y medianas empresas tienen más probabilidades de conseguir personas



experimentadas y con certificación en seguridad de TI cuando trabajan con uno de estos socios.

Luego de encontrar a las personas correctas para administrar la seguridad, se deben encontrar los productos correctos. Tal como se mencionó antes, la seguridad por niveles requiere todo: desde software de cifrado para el control de acceso hasta software antivirus, sistemas de protección contra intrusiones, seguridad móvil y firewalls. Las pequeñas y medianas empresas pueden combinar sus defensas de seguridad de una variedad de proveedores sobre la base de precios y características y, luego, pueden integrarlas en una solución de seguridad por niveles. Pero, como con cualquier proyecto de integración de TI, no existe garantía de que todo salga a la perfección. Una manera eficaz de desarrollar seguridad por niveles sin contratiempos es buscar productos de un solo proveedor que estén diseñados para funcionar juntos, o un integrador con un paquete comprobado de soluciones que funcionen juntas.

Las pequeñas y medianas empresas que carecen de los recursos para dedicar personas a la seguridad y que no cuentan con la experiencia para crear un sistema de seguridad por niveles por su cuenta también tienen la opción de subcontratar la seguridad a un proveedor de servicios de seguridad administrados (MSSP).

Los MSSP pueden ofrecer toda la funcionalidad de seguridad que una pequeña y mediana empresa necesita para implementar la seguridad por niveles, incluida la seguridad para tecnologías emergentes como la informática en la nube y las plataformas móviles, cuyos problemas de seguridad pueden ser desconocidos para muchas pequeñas y medianas empresas. Los MSSP también pueden prestar servicios como respuesta de emergencia ante un incidente de seguridad o capacitación sobre seguridad para empleados.

Como en cualquier tipo de subcontratación, al recurrir a un MSSP, se entrega una parte específica del negocio de una pequeña y mediana empresa a expertos que están capacitados en esa área. Esto permite que los empleados de la pequeña y mediana empresa se enfoquen en el negocio en sí, es decir, desarrollar productos nuevos e incrementar los ingresos. Los MSSP ofrecen protección integral simple a las pequeñas y medianas empresas que carecen del tiempo, los recursos y la experiencia para administrar la seguridad por niveles que necesitarán en 2012.

De qué manera puede ayudar Dell

Dell y sus socios ofrecen las soluciones de seguridad que las pequeñas y medianas empresas pueden usar para proteger sus máquinas y datos en 2012. Dell trabaja con algunas de las marcas más conocidas en seguridad para crear una protección integral simplificada frente a los ataques que cada vez son más recurrentes y sofisticados.

En la capa de seguridad de datos, la protección de datos de Dell proporciona control de acceso mediante el cifrado de datos para mantener los datos seguros. En cuanto a la seguridad de extremos, Dell se asocia con Trend Micro Worry Free para mantener a las máquinas y sus datos seguros. La seguridad de red se proporciona a través de la asociación de Dell con SonicWALL, así como las puertas de enlace de servicios Dell PowerConnect J-SRX.

Las laptops y workstations de Dell con la tecnología de Windows 7 Professional ofrecen lo último en seguridad para el sistema operativo y, en combinación con Windows Server, ayudan a crear una red segura para las empresas de cualquier tamaño.

Dell SecureWorks presta servicios de seguridad administrados a empresas de todos los tamaños. SecureWorks proporciona los controles clave para regulaciones importantes como PCI, SOX, HIPAA y otras. Además, ofrece seguridad para el correo electrónico, la nube, dispositivos móviles y la Web, escaneo de aplicaciones web, prevención y detección de intrusiones y más. Los clientes que optan por Dell SecureWorks pueden elegir la plataforma y las opciones de servicio que son adecuadas para ellos, de modo que la protección sea acorde a sus necesidades y presupuesto.

Conclusión

Las pequeñas y medianas empresas se encuentran firmemente en la mira de los ataques malintencionados en línea. Para combatir estos ataques, las empresas interesadas en proteger a sus empleados, su infraestructura y sus datos recurrirán a la seguridad por niveles cada vez más. Un enfoque de seguridad por niveles defiende todos los niveles de la infraestructura frente a ataques y ofrece a las pequeñas y medianas empresas el enfoque más eficaz para una seguridad integral.

En 2012, muchas de las pequeñas y medianas empresas que no tengan experiencia ni recursos de seguridad recurrirán a proveedores de servicios de seguridad administrados para que las ayuden a implementar la seguridad por niveles. Los MSSP permiten que las pequeñas y medianas empresas se centren en el negocio en sí y colocan a expertos en seguridad, que de otra manera no estarían disponibles para una pequeña empresa, a cargo de la infraestructura de seguridad. Con el incremento de los ataques malintencionados tanto en frecuencia como en volumen, el año 2012 es el momento para investigar sobre la seguridad por niveles.

Dell y sus socios de seguridad están equipados para ayudar a las pequeñas y medianas empresas a proteger sus máquinas y datos en este año. Mediante su enfoque de seguridad por niveles, Dell ayuda a mantener los datos seguros en toda la infraestructura de TI, y su servicio de seguridad administrado SecureWorks puede ofrecer seguridad de nivel empresarial a clientes que desean concentrarse en su negocio y dejar que los profesionales se encarguen de la seguridad de TI.