Aproveche al máximo su dinero: Cinco consejos de seguridad

La seguridad de buena calidad no debería ser un punto negativo del presupuesto.

¿Cómo puede su empresa proteger sus recursos, incluidos los datos de los clientes, a un bajo costo de propiedad? Las experiencias de los clientes de Cisco responden la pregunta.

1. Reúna las tecnologías: Intégrelas

La combinación de las distintas tecnologías de seguridad en un solo sistema es beneficioso para su empresa. La seguridad integrada reduce los costos, fortalece la protección y aumenta la productividad. Un cliente de Cisco que tiene alrededor de 45 empleados obtuvo todos estos resultados con la solución de seguridad de red inalámbrica de punta a punta.

¿Qué debe combinarse? La seguridad de red multicapa, la seguridad digital de una sola función y la seguridad física son algunos de los tipos que debe tomar en consideración.

- Un sistema muy básico puede combinar una red privada virtual (VPN), antivirus y antispam, firewall y herramientas de videovigilancia.
- Los sistemas más avanzados incorporan herramientas de cifrado y prevención de intrusiones.

Todas las herramientas de seguridad necesitan software de administración para su instalación, control y actualización. Con un solo sistema integrado que puede administrarse a distancia por la web, usted aumenta el control, simplifica y agiliza las tareas de los usuarios, y reduce los costos de personal técnico.

Un sistema integrado también protege su inversión a medida que su empresa cambia o crece. Un cliente señaló: “Con nuestro sistema anterior, era muy difícil saber si podíamos agregar un nuevo proyecto o sistema a la red. Con nuestro sistema actual, sabemos con seguridad que podemos agregar todo lo que necesitamos, cuando lo necesitamos, y es muy fácil”.

2. Simplifique los procesos para los empleados

La seguridad de buena calidad es algo más que productos. También aborda las vulnerabilidades de ingeniería social. La manera en que usted o su departamento de TI comunican las políticas de seguridad a los empleados, configuran y usan las herramientas de seguridad, y controlan su cumplimiento determina el nivel de seguridad que su empresa puede lograr. La clave del éxito: que sea fácil.

- **Automatizar.** Los 17 empleados de una compañía usan ahora la tecnología integrada de “túnel” VPN de Cisco® para garantizar que los archivos que se envían y reciben de los clientes siempre estén protegidos. Esto limita el acceso a los archivos únicamente a los empleados autorizados para verlos y les permite tener acceso a ellos en cualquier momento en que los necesiten y en cualquier lugar en que se encuentren.

- **Simplificar la instalación y el uso de las herramientas.** Una compañía con tres empleados eligió las cámaras de videovigilancia de Cisco que admiten Power over Ethernet. El propietario de la empresa sólo tuvo que conectar las cámaras con el cable de la computadora. Ahora los empleados supervisan con facilidad lo captado por las cámaras desde cualquier computadora de la oficina. Les basta con dar una mirada a la pantalla de la computadora para saber si alguien está en la recepción, y quién entra o sale de las oficinas.

3. Vigile las 24 horas del día, los 7 días de la semana

El delito cibernético es implacable. No permita que su sistema de seguridad se quede dormido. Asegúrese de que haga todo lo posible para proteger a su empresa.

- **Instale las actualizaciones de software de seguridad más recientes.** Esta es una de las formas más rápidas de fortalecer la protección. Establezca un sistema, preferentemente automatizado por un servicio o software de administración de revisiones, que garantice la inmediata descarga e instalación de las actualizaciones en sus equipos portátiles, computadoras de escritorio y teléfonos IP, así como también en los equipos y servidores de red.

- **Use el sistema para supervisar y registrar eventos.** El software de administración le permite ver y grabar actividades. También puede enviar alarmas.

- **Pruebe su seguridad.** Si realiza auditorías internas, y lo hace de manera periódica, sabrá en qué lugar su empresa está protegida y dónde no lo está. Un explorador de vulnerabilidades le permitirá descubrir puntos débiles de la red y de las aplicaciones web.

4. Considere el valor de la confiabilidad

La inversión en soluciones de seguridad supone ponderar los atributos del producto frente a su costo. Un atributo que algunos compradores suelen ignorar es la confiabilidad; sin embargo, después, deben afrontar los costos de las fallas del sistema.

El director de finanzas de una pequeña en crecimiento que utiliza la seguridad de red de Cisco para operaciones con tarjetas de crédito, informes de datos y videovigilancia descubrió que la confiabilidad del sistema:

- Aumentó la productividad y el buen ánimo de los empleados.
- Mejoró la atención al cliente
- Redujo los gastos

¿Cuánto le cuesta a su empresa una solución de seguridad que falla? ¿Tiene el personal técnico con los conocimientos y el tiempo necesarios para restablecer el servicio? ¿El proveedor le brinda asistencia técnica telefónica en línea y en persona para solucionar su problema? ¿Qué dice el contrato de servicio técnico? ¿En qué consiste la garantía del producto?

5. Administre el flujo de efectivo con opciones de financiamiento

Cuando averigüe entre varios proveedores cuánto cuesta una solución de seguridad, fíjese qué financiamiento ofrecen. Algunos proveedores le permitirán usar sus fondos para proteger su flujo de efectivo al tiempo que optimiza su seguridad.

Pasos a seguir
Obtenga más información sobre las soluciones de seguridad de Cisco que pueden proteger a su empresa. Busque un reseller de Cisco local con experiencia que se ocupará de satisfacer sus necesidades específicas.