Conceptos básicos de seguridad de red para pymes

¿Qué es la seguridad de red?

La seguridad de la red es cualquier actividad diseñada para proteger la usabilidad e integridad de su red y de sus datos. Incluye las tecnologías de hardware y software. La seguridad efectiva de la red administra el acceso a la red. Va dirigida a distintas amenazas y evita que entren o que se propaguen en la red.

¿Cómo funciona la seguridad de la red?

La seguridad de la red combina varios niveles de defensas en el perímetro y en la red. Cada nivel de seguridad de la red implementa políticas y controles. Los usuarios autorizados obtienen acceso a los recursos de la red, pero impide que los agentes maliciosos lleven a cabo explotaciones y amenazas.

¿Cómo me beneficio de la seguridad de la red?

La digitalización ha transformado nuestro mundo. Cómo vivimos, trabajamos, jugamos y aprendemos: todo ha cambiado. Cada organización que desee ofrecer los servicios que los clientes y empleados exigen debe proteger su red. La seguridad de la red también le ayuda a proteger la información confidencial de los ataques. En última instancia, protege su reputación.

6 medidas que puede adoptar para proteger su red

1. Supervise el tráfico entrante y saliente de su firewall y lea los informes cuidadosamente. No dependa de alertas para identificar una actividad peligrosa. Asegúrese de que alguien de su equipo comprende los datos y está preparado para tomar las medidas necesarias.
2. Esté atento a las nuevas amenazas a medida que se detectan y se publican en línea. Por ejemplo, la página TrendWatch de Trend Micro realiza un seguimiento de la actividad actual de las amenazas.
3. Habilite las actualizaciones periódicas para su software del firewall y del antivirus.
4. Forme a los empleados de manera continua para que comprendan cualquier cambio en su política de uso aceptable. Además, fomente un enfoque de “vigilancia vecinal” de la seguridad. Si un empleado nota algo sospechoso, como que no puede iniciar sesión en una cuenta de correo electrónico de inmediato, debe notificárselo a la persona adecuada inmediatamente.
5. Instale una solución de protección de datos. Este tipo de dispositivo puede proteger a su empresa contra la pérdida de datos si se vulnera la seguridad de su red.
6. Tenga en cuenta soluciones de seguridad adicionales que protegerán aún más su red y ampliarán las capacidades de su empresa.

Opción B

Conceptos básicos de seguridad de red para pymes

Tipos de seguridad de red

Control de acceso

No todos los usuarios deben tener acceso a su red. Para mantener alejados a los posibles atacantes, necesita reconocer a cada usuario y a cada dispositivo. A continuación, puede aplicar sus políticas de seguridad. Puede bloquear los dispositivos de terminales no conformes o darles un acceso limitado. Este proceso es el control de acceso a la red (NAC).

Software antivirus y antimalware

El " malware" , la abreviatura en inglés de " software malicioso" , incluye los virus, los gusanos, los troyanos, el ransomware y el spyware. A veces, el malware infecta una red pero permanece inactivo durante días o incluso semanas. Los mejores programas antimalware no solo buscan malware en el momento de la entrada, sino que también realizan un seguimiento continuo de los archivos después para detectar anomalías, eliminar el malware y reparar los daños.

Seguridad de la aplicación

Cualquier software que utilice para llevar su negocio necesita estar protegido, ya sea que su personal de TI lo construya o lo compre. Por desgracia, cualquier aplicación puede contener agujeros o vulnerabilidades que los atacantes pueden utilizar para infiltrarse en su red. La seguridad de las aplicaciones abarca el hardware, el software y los procesos que utiliza para cerrar esos huecos.

Análisis de comportamiento

Para detectar el comportamiento anormal de la red, debe saber lo que es un comportamiento normal. Las herramientas de análisis del comportamiento diferencian automáticamente las actividades que se desvían de la norma. Su equipo de seguridad puede entonces identificar mejor los indicadores de compromiso que plantean un problema potencial y remediar rápidamente las amenazas.

Prevención de la pérdida de datos

Las organizaciones deben asegurarse de que su personal no envía información confidencial fuera de la red. Las tecnologías de prevención de pérdida de datos, o DLP, pueden impedir que las personas carguen, reenvíen o incluso impriman información importante de forma insegura.

Seguridad para el correo electrónico

Los gateways de correo electrónico son el vector de amenaza número uno para una violación de la seguridad. Los atacantes utilizan información personal y tácticas de ingeniería social para crear sofisticadas campañas de suplantación de identidad para engañar a los destinatarios y enviarlos a sitios que ofrecen malware. Una aplicación de seguridad para el correo electrónico bloquea los ataques entrantes y controla los mensajes salientes para evitar la pérdida de datos confidenciales.

Firewalls

Los firewalls levantan una barrera entre la red interna fiable y las redes externas no fiables, como Internet. Usan un conjunto de reglas definidas para permitir o bloquear el tráfico. Un firewall puede ser hardware, software o ambos. Cisco ofrece dispositivos de Unified Threat Management (UTM) y firewalls de última generación centrados en las amenazas.

Sistemas de prevención de intrusiones

Un sistema de prevención de intrusiones (IPS) escanea el tráfico de red para bloquear los ataques de forma activa. Los appliances de IPS de última generación de Cisco hacen esto correlacionando grandes cantidades de inteligencia sobre amenazas globales, no solo para bloquear las actividades maliciosas, sino para rastrear el progreso de archivos sospechosos y malware en la red y así evitar que se extiendan brotes o que se produzcan infecciones de nuevo.

Conceptos básicos de seguridad de red para pymes

Seguridad de dispositivos móviles

Los ciberdelincuentes se centran cada vez más en las aplicaciones y los dispositivos móviles. Dentro de 3 años, puede que el 90 % de las organizaciones de TI apoyen las aplicaciones empresariales en los dispositivos móviles personales. Es evidente que necesita controlar qué dispositivos pueden acceder a su red. También tendrá que configurar sus conexiones para que el tráfico de red sea privado.

Segmentación de red

La segmentación definida por software clasifica el tráfico de red en diferentes categorías y hace que sea más fácil hacer cumplir las políticas de seguridad. De forma ideal, la clasificación está basada en la identidad del terminal, no simplemente en las direcciones IP. Puede asignar derechos de acceso basados en el rol, y la ubicación, entre otros, para hacer que el nivel correcto de acceso se conceda a la gente correcta y para que los dispositivos sospechosos se contengan y se reparen.

VPN

Una red privada virtual cifra la conexión de un terminal a una red, a menudo a través de Internet. Normalmente, una VPN de acceso remoto usa IPsec o capa de conexión segura para autentificar la comunicación entre el dispositivo y la red.

Seguridad web

Una solución de seguridad web controlará el uso que el personal hace de la web, bloqueará las amenazas basadas en la web y negará el acceso a los sitios web maliciosos. Protegerá el gateway web del sitio o de la nube. " Seguridad web" también se refiere a los pasos que adopta para proteger su propio sitio web.

Seguridad inalámbrica

Las redes inalámbricas no son tan seguras como las redes por cable. Sin medidas de seguridad rigurosas, instalar una LAN inalámbrica puede ser como poner puertos Ethernet en todas partes, incluso en el aparcamiento. Para evitar que la gente se aproveche de la red, necesita productos diseñados específicamente para proteger la red inalámbrica.

Sede central en América
Cisco Systems, Inc.
San José, CA

Sede central en Asia-Pacífico
Cisco Systems (EE. UU.) Pte. Ltd.
Singapur

Sede central en Europa
Cisco Systems International BV Amsterdam,
Países Bajos

Cisco tiene más de 200 oficinas en todo el mundo. Las direcciones y los números de teléfono y fax se encuentran en la Web de Cisco en **www.cisco.com/go/offices.**