5 Puntos Para Mejorar La Seguridad De Su Red

Basándose en una DMZ para proteger la red y los datos, es como poner el dinero en un banco que depende de un guardia y una sola puerta para asegurar tu preciado dinero. Ahora imagine lo tentador que es para quienes tienen acceso, tener a disposicion ese dinero. Pero los bancos no mantienen el dinero en efectivo en las mesas del vestíbulo, ellos las esconden en cajas de seguridad en el interior de las bóvedas, a puertas cerradas, en el interior de un edificio patrullado por un guardia y asegurado por una puerta. Del mismo modo, la ***segmentación de red*** ofrece una seguridad similar para los datos sensibles de una organización.

La necesidad de la **segmentación de la red** ha sido ampliamente discutido por años, pero sigue siendo uno de los métodos de seguridad que son implementados con menos frecuencia, y rara vez se emplea como medio de defensa estratégica. Si aún no sabes que pasos a seguir para mejorar

La segmentación de la red eficaz es un gran trabajo, pero se reduce a tan sólo **cinco pasos básicos**:

Comprender el negocio y los objetivos de la organización

Para saber lo que se debe proteger, es necesario entender los datos y componentes del negocio, como las terminales de punto de venta y los componentes de back-end y front-end, el soporte de las funciones básicas de la empresa. Luego, identificar qué

activos, datos y personal son esenciales para asegurar la continuidad del negocio.

Crear un plan

Debes **clasificar, aislar y proteger** los componentes más importantes de la red. Aquí es importante conocer el grupo de elementos relacionados entre sí, por ejemplo, todos los servidores Windows, en una LAN virtual (VLAN). Otros grupos de activos podrían incluir infraestructura (routers, switches, VPN y VoIP) en una VLAN y los activos de seguridad (IDS, cortafuegos, filtros web y escáneres) en otro.

Los servidores de recursos financieros o humanos típicamente necesitan su **propia VLAN** debido a la naturaleza confidencial de la información que procesan y almacenan. Sin duda la segmentación de departamentos en diferentes redes virtuales, dan la seguridad de mantener los datos sensibles dentro del grupo de personas que necesitan dicha información.

Determinar quién puede acceder a ciertos datos

Esto se reduce a la necesidad de determinados grupos internos de la empresa al momento de manejar determinados datos. En otras palabras, supongamos que en la empresa existe un grupo de soporte y otro de ventas, ambos grupos pueden compartir información común como el estado de pago, nombre, id de cliente. Pero puede que el grupo de ventas maneje alguna otra información como los métodos y datos del método de pago, sin duda es una información sensible que no todos los usuarios deben conocer.

En otro aspecto, la empresa puede contar con diversas sedes en

la ciudad. Ahora se debe analizar el acceso que puede o no tener determinada sede a otra. Pero si tiene acceso, determinar que grupos deben tener acceso a la otra red.

Poner en práctica la segmentación

En una organización grande, la segmentación de la red es un importante proyecto a largo plazo, pero cada paso del camino sirve para **mejorar la seguridad de la red**. Con la segmentación es posible identificar todo el tráfico, y así determinar lo que es normal y necesaria para la toma de medidas necesarias. Una vez que sepa lo que es necesario, inicie el bloqueo del acceso a la VLAN de cualquier otro lugar, con el objetivo final de denegación predeterminada.

Mantenimiento

La segmentación de la red no es que realices y luego creas que se puede mantener solo. La política de acceso a la red, que se define en los firewalls, routers y dispositivos relacionados, cambia constantemente para atender a los nuevos requerimientos del negocio. Asegurar que los nuevos cambios no violan su estrategia de segmentación requiere un buen grado de visibilidad y automatización. El potencial de sobrecarga de administración necesario para mantener una buena segmentación es una de las razones organizaciones rehuir de ella. Pero, la segmentación adecuada es fundamental.

Finalmente

La segmentación de red es un componente efectivo, en una estrategia para la defensa de los datos sensibles en una empresa. Las organizaciones que la implementan deben estar preparados para manejar decenas de firewalls, switches y routers, cada uno con cientos de reglas, todos los cuales se verán afectados por el proceso de segmentación de la red y potencialmente por las actualizaciones y cambios, incluso después de que todo este trabajando perfectamente. Un enfoque riguroso es esencial, y también se requiere una importante inversión de tiempo y personal.