¿Qué cubre la seguridad de la red?

Los ciberataques son cada vez más numerosos y sofisticados en todo el mundo. Se espera que esta tendencia se acentúe. Según IDC, se prevé que para 2025, 41.000 millones de dispositivos en todo el mundo estarán conectados al Internet of Things (IoT), lo que aumentará el número de dispositivos utilizados en la vida cotidiana para proporcionar datos que podrían ser objeto de ciberataques.

La seguridad de la red implica políticas y prácticas destinadas a combatir el cibercrimen. Entre sus objetivos, destaca la prevención y monitorización de accesos no autorizados, mal uso, modificación o interrupción de una red informática y de los recursos accesibles a través de ella. Garantizar la seguridad de la red es esencial para proteger tanto los datos empresariales como los personales, actuando como una línea de defensa crucial contra la pérdida de información y la interrupción del servicio.

Beneficios de la seguridad de la red

- Protección de datos sensibles: evita el acceso no autorizado a información confidencial.
- Continuidad del negocio: minimiza el riesgo de interrupciones operativas causadas por ciberataques.
- Reputación empresarial: protege la imagen de la empresa ante clientes y partners.
- Cumplimiento normativo: garantiza que la empresa cumpla con las normas y reglamentos de seguridad.

Principales amenazas

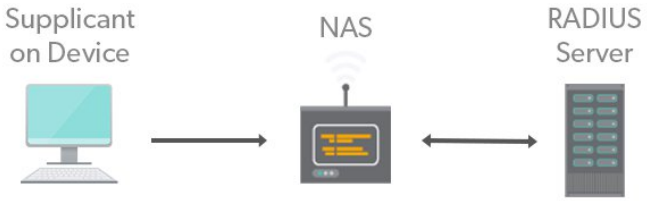
- Malware: software malicioso que puede dañar, inutilizar sistemas y/o robar datos.
- Phishing: intenta obtener datos sensibles haciéndose pasar por entidades de confianza.
- Ransomware: un tipo de malware que encripta los datos y exige un rescate para liberarlos.

Impacto de las amenazas cibernéticas

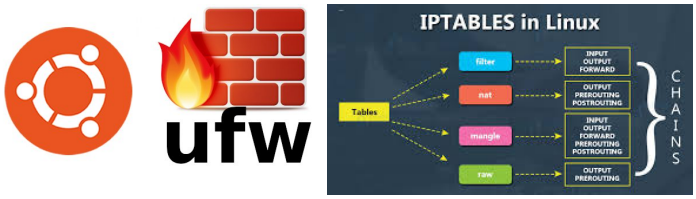
- Pérdida de datos: la información importante puede ser destruida o robada.
- Interrupción del servicio: los ataques pueden paralizar operaciones críticas.
- Costos altos: los gastos de recuperación y rescate pueden ser altos.
- Daño reputacional: daño o pérdida de confianza de clientes y socios.

Estrategias de seguridad de red

- Autenticación segura: utilice sistemas para garantizar que solo las personas autorizadas puedan acceder a la red.



- Firewalls y sistemas de detección de intrusos: crean barreras y monitorean la red para identificar y neutralizar actividades sospechosas.



- Cifrado de datos: protege los datos confidenciales durante la transmisión y el almacenamiento, haciéndolos inaccesibles sin la clave correcta.

- Políticas de seguridad y formación: garantizar que los empleados sean conscientes de los riesgos y adopten prácticas seguras.