

Samsung auto-defensa para redes VoIP



Son las tres de la tarde de un sábado y no hay nadie en la oficina. Las luces de la flamante nueva central IP, parpadean como un árbol de navidad. El sistema ha sido asaltado por un hacker, que ha direccionado todas las llamadas salientes internacionales de un call centre a través del switch.

El hacker ha conseguido acceder a la red para robar las llamadas de la víctima desprevenida. Nadie se ha dado cuenta, nadie lo sabía, hasta que unas semanas más tarde, el departamento financiero recibe una factura de teléfono de 8.000€.

En la misma calle, otra pequeña empresa cae víctima de una red de delincuentes informáticos. Un ex empleado insatisfecho, consigue que un amigo hacker colapse el switch con una gran cantidad de datos, haciendo que el sistema se detenga en la hora de mayor trabajo, en el día de mayor trabajo. La compañía no puede probarlo, pero sabe que ha sido un ex empleado que sabe cómo y cuándo hacer el mayor daño.

Desde finales de los noventa, la industria de las comunicaciones ha ido migrando desde los sistemas de voz tradicionales a los basados en IP, que ponen a su disposición la red de internet para hacer

las llamadas de voz más económicas. Esto hace que, debido a la naturaleza de internet, donde los sistemas deben hacer públicas sus direcciones para poder comunicarse, se produzca un nuevo peligro para las comunicaciones de las empresas. Si un hacker puede ver el sistema, puede atacarlo, con dramáticas consecuencias:

- Puede neutralizar todo el ahorro que supone el uso de la voz sobre IP (VoIP) en tan sólo un fin de semana.
- Un ataque de denegación de servicio, puede paralizar las llamadas entrantes y salientes de la oficina, teniendo que cerrar el negocio.

Los switches de voz que incorporan puertas de enlace VoIP, y que están conectados a internet, tanto directamente como a través de datos, son vulnerables a estos ataques.



La ayuda está aquí.

La última generación de switches de voz de Samsung –Serie OfficeServ 7000- incorpora un grupo de sistemas de seguridad, que protegen de forma efectiva al switch de estos ataques:

1. Túnel VPN y encriptación integrados.
2. Filtro de paquetes y Firewall pre configurados.
3. Detección y protección frente a intrusos.

Debido a que están integrados dentro de un switch de voz convergente, pueden también ser usados para proteger el sistema de voz de posibles ataques.

¿Cómo funciona?

En primer lugar, el Firewall integrado filtra todo el tráfico a través del sistema para detectar aplicaciones sospechosas, que simplemente son bloqueadas antes de que puedan acceder al sistema de voz.

Los sitios remotos pueden ser comunicados a través de túneles VPN con encriptación, de esta forma las direcciones IP son enmascaradas evitando que puedan ser descubiertas por posibles hackers. Las comunicaciones de la compañía son seguras.

El Sistema de Detección de Intrusos (IDS) utiliza un motor de escaneo de paquetes, buscando identificaciones. Si un paquete IP sospechoso es detectado, el sistema entra en acción de inmediato, alertando al administrador del sistema. Asimismo, este dispositivo toma acciones preventivas contra cualquier otra comunicación que provenga de la misma fuente.



	Avaya IP Office	Samsung OfficeServ 7000
Sistema de Voz para empresas.	Sí	Sí
Servicio de Router.	Sí	Sí
Firewall Básico	Sí	Sí
Switch de Datos Layer3	No	Sí
Mobilidad Wi-Fi	No	Sí
Detección/Prevención de Intrusos (IDS/IPS)	No	Sí
Conexión VPN.	No	Sí
Proceso de rastreo de Voz y Datos.	No	Sí
Calidad de Voz con estructuración de paquetes.	No	Sí
Política de Gestión	No	Sí

Los Beneficios.

La ventaja de un sistema que combina seguridad para voz y datos, significa que los ataques con datos para bloquear el sistema pueden ser detectados y prevenidos con antelación a que produzcan algún daño. Las empresas con varias delegaciones pueden conectarse sin tener que mostrar sus direcciones IP. Asimismo, todas las soluciones (Voz, Datos y Seguridad) están unificados en un solo producto.