Recomendaciones de seguridad en plantas IP

COLOMBIANET y SEPCOM COMUNICACIONES S.A.S en adelante COLOMBIANET es el prestador de los servicios de Internet.

Para COLOMBIANET la seguridad informática de nuestros clientes es primordial, por tal motivo se han implementado herramientas de software y hardware que nos permiten cumplir con los más altos estándares de seguridad en nuestra red y con los términos establecidos por la regulación.

Con el propósito de prevenir que los servidores o plantas IP que están conectados al servicio de Internet suministrados por COLOMBIANET sean objeto de ataques fraudulentos, es indispensable contar con las medidas de seguridad necesarias para evitar posibles ataques de hackers, virus o cualquier otro acto de intervención de terceros. Por esta razón, a continuación, le entregamos algunas recomendaciones y obligaciones que nuestros suscriptores deben cumplir para apoyar las acciones que realizamos y fortalecer su seguridad.

Implementar y actualizar permanentemente las plantas telefónicas o servidores que almacenan la información con las versiones de seguridad recomendadas por el respectivo fabricante.

Implementar y actualizar permanentemente las versiones de software que permitan blindar las plantas telefónicas o servidores de ataques externos, en donde las líneas conectadas a las plantas telefónicas de nuestros clientes se pueden alcanzar por medio de la red de datos, para gestionar llamadas internas, entrantes y salientes.

Dado que las plantas telefónicas o servidores que el suscriptor conecte a los equipos de COLOMBIANET hacen parte de la acometida interna del usuario, es importante destacar que estos elementos son absoluta y exclusiva responsabilidad del usuario del servicio. En consecuencia, conforme a lo establecido para sus obligaciones en la Cláusula Cuarta del contrato de Servicios de Telecomunicaciones, el suscriptor o usuario responderá por cualquier anomalía, fraude o adulteración que se encuentre sobre sus equipos de la siguiente manera:

"(...) 14. Es de la absoluta y exclusiva responsabilidad del **SUSCRIPTOR o USUARIO**, del Poseedor o Propietario correspondiente, garantizar la seguridad de sus instalaciones y acometidas internas. En consecuencia, responderán en forma solidaria y hasta por la culpa leve de cualquier anomalía, fraude o adulteración que se encuentre en las acometidas, así como por las variaciones que sin autorización de **LA EMPRESA** se hagan en relación con el servicio contratado. (...)"
Teniendo en cuenta que la red está expuesta a situaciones de vulnerabilidad impredecibles y/o irresistibles en caso de prácticas fraudulentas, configuraciones, intervenciones efectuadas por el cliente, por terceros o de tipo técnico que se puedan

presentar en las plantas telefónicas o servidores, COLOMBIANET no se hace responsable por las fallas de seguridad en dichas plantas y perjuicios ocasionados. Para mantener la seguridad de la red es requerido el esfuerzo decidido de Suscriptores o Usuarios.

Reiteramos la importancia de tener presentes y llevar a la práctica las siguientes recomendaciones en cuestión de seguridad VoIP, las cuales resguardan los equipos de ataques y vulnerabilidades en la red.

Estas recomendaciones están enfocadas sobre sistemas basados en Asterisk y se recomienda que sean implementadas por una empresa con experiencia en el tema.

Seguridad externa (acceso al sistema)

- Tener una política adecuada de acceso físico al servidor.
- Usar redes privadas virtuales (VPN).
- Restringir acceso desde el exterior si no se necesita. Esto aplica a los puertos UDP 5060 y 4569 (SIP e IAX2) y TCP 22, 443 (los más comunes). Bloquear los puertos que deban ser usados.
- Desactivar los servicios que no usen, especialmente servicio WEB. Para verificar los servicios use el comando chkconfig list.
- Si se necesita contar con administración remota del equipo lo ideal es usar un túnel SSH o VPN.
- Bloquear los puertos del Asterisk Manager Interface. Usar "permit=" y "deny=" en manager.conf para limitar las conexiones entrantes sólo a hosts conocidos. Se recomienda el uso de claves seguras, 12 caracteres como mínimo en una combinación alfanumérica y caracteres especiales.
- Evitar utilizar puertos estándares.
- No utilizar el puerto por defecto para las conexiones SSH al servidor donde está instalada la planta. Esta configuración se realiza en /etc/ssh/sshd_config.
- Usar Firewall (cortafuegos) para filtrar solicitudes entrantes con el fin de proteger el sistema operativo y el servidor de comunicaciones Asterisk; es necesario aceptar sólo las conexiones que sean necesarias y rechazar las demás.
- COLOMBIANET no se hace responsable de la instalación de software, sugerimos el uso de los siguientes programas de detección de intrusos por ejemplo fail2ban y portsentry para evitar escaneos y ataques de DoS (denegación de servicio).
- No aceptar usuarios no autenticados, esto se hace estableciendo "allowguest=no" en la parte [general] de sip.conf.
- Establecer el valor de la entrada "alwaysauthreject=yes" en el archivo sip.conf., esta opción está disponible desde la versión 1.2 de Asterisk, por defecto su valor es "no", lo que puede ser potencialmente inseguro. Estableciendo este valor en "yes" se rechazarán los pedidos de autenticación fallidos utilizando

nombres de extensiones válidas con la misma información de un rechazo de usuario inexistente. De esta forma no se facilita la tarea al atacante para detectar nombres de extensiones existentes utilizando técnicas de "fuerza bruta".

- Crear cuentas de tipo dirección MAC ej: [7EFFAA678821], en lo posible evitar las típicas cuentas sip (extensiones) [102], [105], [109], etc. Esto se hace en el archivo sip.conf. Para facilitar el marcado se pueden usar alias en el archivo extensions.conf en la parte de [global].
- Tener listas de Acceso (ACL) para el registro de las extensiones. No aceptar pedidos de autenticación SIP desde cualquier dirección IP. Utilizar las líneas "permit=" y "deny=" de sip.conf para que sólo permita que un subconjunto razonable de direcciones IP alcance cada usuario/extensión listado en el archivo sip.conf.
- Utilizar claves seguras para las entidades SIP. Usar símbolos, números, una mezcla de letras minúsculas, mayúsculas, números y caracteres especiales y al menos 12 caracteres de longitud. La clave se configura en cada cuenta SIP, en el parámetro "secret=". Cambiar por una clave segura.
- Los nombres de usuarios SIP deben ser diferentes que sus extensiones. A pesar de ser conveniente tener una extensión "1234" que mapee a una entrada SIP "1234" la cual es también el usuario SIP "1234", esto también facilita a los atacantes para descubrir nombres de autenticación SIP. En su lugar usar las direciones MAC del dispositivo, o alguna combinación de frases comunes + extensión MD5 hash (por ejemplo: desde el shell prompt, hacer "md5 -s ThePassword5000").
- Cambiar usuarios y claves por defecto en las diferentes distribuciones de Asterisk.
- Cambiar claves periódicamente.
- Utilizar claves seguras para cualquier ingreso de administración de la planta, SSH, HTTP, etc.

Seguridad de operación

- De acuerdo a las necesidades de comunicación de su compañía limitar el número máximo de llamadas simultáneas por extensión a 2. Esto se hace agregando o modificando el parámetro call-limit=2 en cada cuenta creada del archivo sip.conf.
- Verificar los archivos de logs (bitácoras) del sistema, ubicados generalmente en /var/log/secure y /var/log/messages.
- Activar solo el plan de llamadas necesario.
- Es altamente recomendable que, si no se hacen llamadas internacionales, a móviles y/o a líneas premium entonces no se habiliten tanto en la planta como con el proveedor de telefonía.
- Poner limitantes no al teléfono sino a la persona, obligando a quien marca a proporcionar un código que le autorice a marcar a ese destino. Esto se hace

con el parámetro "Authenticate()".

- Estar al día con las actualizaciones, vulnerabilidades y soluciones. Actualizar las distribuciones a la versión más reciente y estable.
- Llevar un control exhaustivo del sistema.
- Asegurar que los buzones no activados tengan una vigencia y sean desactivados después de cumplirla.
- Los componentes críticos de hardware deben ser bloqueados con dispositivos anti- manipulación.
- Contar con un contacto directo con personal del proveedor de PBX para realizar consultas sobre cuestiones de seguridad.
- Utilizar un procedimiento para conocer las funciones específicas del personal que no hace parte de la empresa a fin de dar de baja claves y accesos cuando esto ocurra. Cambie las contraseñas de administrador cuando los administradores cambien.
- El correo de voz debe ser protegido con PIN, si es posible, un PIN de 6 dígitos o más, el PIN se debe cambiar el número predeterminado (contraseñas de los buzones de correo de voz no deben ser los últimos cuatro dígitos del número de teléfono) y debe desactivarse después de un número especificado de intentos fallidos.
- Asegurarse que el contexto [default] sea seguro. No permitir que llamadores no autenticados alcancen contextos que les permitan llamar. Permitir sólo una cantidad limitada de llamadas activas pasen por el contexto default (utilizar la función "GROUP" como contador). Prohibir totalmente las llamadas no autenticadas (si es que así lo queremos) estableciendo "allowguest=no" en la parte [general] de sip.conf.
- Uso de honeypots: En la terminología informática, un honeypot es una trampa para contrarrestar los intentos de uso no autorizado de los sistemas de información. Un honeypot IP -PBX puede ser establecida por un operador para atraer a los atacantes al aparecer para ofrecer un blanco legítimo y atractivo, cuando en realidad el IP-PBX honeypot es realmente aislado y controlado, y registrará la fuente de direcciones IP de los atacantes para su posterior bloqueo proactivo. El bloqueo de rangos de direcciones IP también se puede considerar, para prohibir las conexiones de los proveedores de servicios de Internet que son conocidos por albergar comunidades de hackers.

En COLOMBIANET seguiremos ofreciéndoles a nuestros usuarios, el mejor servicio y los máximos niveles de calidad para soportar sus necesidades de comunicación y crecimiento.

Cordial saludo,

Prevención Fraude COLOMBIANET.