CONECTA TUS PASIONES

Bogotá, 01 de marzo de 2021

Cordial saludo

Para ETB es importante mantenerle al tanto de cualquier novedad con respecto de sus servicios. Así, queremos compartir con usted algunos consejos para mejorar la seguridad de sus soluciones de voz corporativa, como un compromiso conjunto entre ETB y nuestros clientes.

Sin conexión digital no hay bienestar y lograr experiencias de conexión valiosas nos permite seguir creciendo no solo como personas, sino también como empresa y ciudad. Por ende, una manera de estar preparados es implementar políticas de seguridad virtual que apoyen a las empresas y entidades a cumplir con este propósito.

En ETB protegemos nuestras redes, plataformas y sistemas de gestión siguiendo las mejores prácticas del mercado. Contamos con esquemas de seguridad perimetral con Firewalls y equipos especializados de voz que permiten ocultar la topología de nuestra red, el control de las llamadas para el manejo de tráfico seguro y confiable; el cifrado y codificación de las comunicaciones y el manejo de políticas de acceso de los servicios, entre otros aspectos. De esta forma, permitimos que sus comunicaciones en los servicios de voz sean seguras, teniendo en cuenta que debe implementar controles de seguridad en sus instalaciones, equipos y procesos dedicados a los sistemas de comunicación de servicios de voz.

Para lograr nuestro objetivo conjunto, compartimos las siguientes técnicas de seguridad:

1. Evalúe periódicamente las condiciones de seguridad física de su PBX-IP y hardware de red.
2. Utilice contraseñas seguras, con caracteres alfanuméricos de mínimo 7 dígitos.
3. No utilice el mismo nombre de usuario y contraseña en sus extensiones.
4. Ubique su PBX-IP detrás de un cortafuego (Firewall).
5. Utilice las opciones de permitir o negar en la configuración SIP.
6. Mantenga separados el enrutamiento entrante y saliente.
7. Limite el registro por extensiones a su red local.
8. Permita solo una o dos llamadas a la vez por entidad SIP.
9. Deshabilite los canales y servicios que no están en uso.
10. Dificulte la tarea para los analizadores de SIP.
11. Limite los planes de llamadas de enrutamiento y número de teléfono.
12. Audite la seguridad de su sistema con regularidad.

Al implementar este esquema de trabajo entre ETB y su organización, construimos modelos de seguridad más eficientes en los servicios de voz corporativa que permitirá mitigar el riesgo de fraude en sus sistemas telefónicos.

Si requiere profundizar acerca de nuestro esquema de seguridad en las soluciones de voz corporativas de ETB, le invitamos a consultar nuestros canales digitales de atención para brindarle la mejor experiencia en este proceso.

Al final de este comunicado encontrará mayor detalle de las recomendaciones de seguridad para su solución PBX-IP con troncal SIP fija o móvil con acceso a internet.

En ETB contamos con soluciones de seguridad complementarias para sus servicios de voz desde el diagnóstico hasta la implementación final de la solución.

En ETB estamos comprometidos con la seguridad de nuestros clientes

CONECTA TUS PASIONES

Conozca más Recomendaciones de Seguridad para su Solución PBX-IP con Troncal SIP fija o móvil con acceso a Internet

1. **Seguridad física de su PBX-IP y hardware de red.**
   Debe asegurar el acceso físico, la ubicación física del lugar debe tener su respectivo mecanismo de seguridad, protegiendo las instalaciones donde se encuentra su hardware de la central telefónica o PBX-IP y el cuarto de equipos y/o gabinetes.
   Limite el acceso a personal técnico con autorización de acceso apropiada; adicionalmente, debe llevar un control de registro de entrada y salida validando que realmente que requieran acceso, así como conocimientos de lo que debe hacer y las actividades a desarrollar.

   Solicite continuamente al proveedor de la planta telefónica las características de nuevas versiones, actualizaciones de software, principalmente lo referente a parches para corregir vulnerabilidades que fortalezcan su sistema telefónico o de VoIP.

   Se sugiere contratar el soporte técnico con empresas legalmente establecidas, que posean la suficiente experiencia y reconocimiento en el campo. Además, acuerde con el proveedor de instalación y mantenimiento de la planta telefónica o PBX-IP, cláusulas de penalización y responsabilidad jurídica y económica por fraudes realizados y atribuidos a la vulnerabilidad sobre la planta telefónica.

2. **Utilice contraseñas seguras.**
   Internet presenta oportunidades y retos; por lo tanto, **Nunca utilice las contraseñas predeterminadas en su PBX-IP,** suministradas por su proveedor para la administración de la planta telefónica y equipos de Voz sobre IP.

   Cree contraseñas seguras, es fácil y en muchos casos es la mejor manera de detener el 99% de todos los ataques que es la forma que comúnmente en que los piratas informáticos ingresan a los sistemas PBX-IP.

   Como primera recomendación, en cuanto a claves y usuarios, debe ser reemplazar el nombre de usuario y las contraseñas de todas las cuentas con acceso de administrador, y cambie las contraseñas periódicamente.

   En segundo lugar, al crear las nuevas cuentas de usuario, asegúrese de **no usar o permitir** contraseñas fáciles de adivinar como "1234", "contraseña", "nombre de compañía1", el número de la extensión, etc., use una contraseña fuerte, aleatoria y única. Combinación mínima de 12 caracteres incluyendo mayúsculas, minúsculas, números y símbolos.

   Los detectores de contraseñas pueden descubrir mucho con solo un poco de información e ingeniería social.

   Algunas recomendaciones para crear contraseñas seguras:
   https://www.pandasecurity.com/spain/mediacenter/seguridad/10-trucos-para-crear-contrasenas-seguras/

3. **No utilice Nunca el mismo nombre de usuario y contraseña en sus extensiones.**

   Usar la contraseña 101 para la extensión 101 es una invitación a para ser afectado. Utilice claves con Combinación mínima de 12 caracteres incluyendo mayúsculas, minúsculas, números y símbolos. Usted registra la extensión por una única vez, no debe digitarla todo el tiempo. Realice un inventario de las extensiones lógicas creadas en su planta y contrástelas frente a las físicas.

4. **Coloque su PBX-IP detrás de un cortafuego. (Firewall)**

   Proteja la interfaz de administración remota, si piensa utilizarla. Utilice conexiones VPN temporales, son una buena manera de limitar el acceso y habilitar la administración remota de su PBX-IP. No use la dirección IP pública para acceder remotamente a la planta telefónica, preferiblemente utilice NAT y conexiones seguras a través de VPN (red privada virtual).

   Colocar su PBX-IP detrás de un firewall y restringir el acceso remoto a su PBX-IP a una única dirección IP específica desalentará mucho a cualquiera que desee ingresar. Asegúrese de activar únicamente los puertos que son absolutamente esenciales para ejecutar su PBX-IP. Bloquee en el firewall los puertos TCP/IP de acceso remoto que no utilice en su sistema de PBX-I y las solicitudes WAN anónimas (PING). Recuerde que, si pueden encontrarlo pueden atacarlo.

   Los firewalls, serán tan buenos como las reglas definidas en ellos.

   Cuando sea posible, coloque su PBX-IP en una LAN con traducción de direcciones de red (NAT). Esta opción NAT le da a su PBX-IP una dirección IP privada y hace que sea mucho más difícil acceder desde Internet. Tómese el tiempo para configurarlo correctamente y no tener problemas con el audio.

   Utilice un sistema de detección de intrusos (IDS) y herramientas de protección de forma automatizada de sus llamadas.

   La opción del SBC (Session Border Controller) es un nuevo componente que dispone de funcionalidades que harán que su red de telefonía IP o VoIP sea mucho más segura y se integre mejor con el equipamiento SIP de diferentes fabricantes y proveedores de servicios.

5. **Use las opciones de permitir o negar en la configuración SIP.**

   Use configuraciones para permitir solo un pequeño rango de acceso de direcciones IP a la extensión/usuario en su archivo de configuración SIP. Si decide permitir llamadas entrantes desde “cualquier lugar” (predeterminado), no permitirá que esos usuarios lleguen a algún elemento autenticado. Si su sistema telefónico se encuentra soportado en un servidor de Voz sobre IP, configure que el acceso únicamente sea de direcciones IP conocidas y no permita autenticación del protocolo SIP desde cualquier dirección IP, para esto se sugiere utilizar listas de acceso y/o IPtables. Adicionalmente, restringir el uso de su PBX-IP en función de la ubicación geográfica de una dirección IP de origen le permite restringir el acceso por continente / país / región / ciudad.

   Opciones como fail2ban están disponibles para sistemas basados en asterisk http://www.fail2ban.org/wiki/index.php/Main_Page

6. **Mantenga el enrutamiento entrante y saliente separados.**
   Mantenga el enrutamiento de sus llamadas entrantes en un contexto diferente al de su enrutamiento saliente, así si un intruso logra ingresar a su sistema, no podrá realizar llamadas.
   Establezca políticas claras sobre la seguridad del sistema telefónico y en la planta PBX-IP:
   - Establezca un plan de marcación llamadas y defina responsables del tráfico
   - Restrinja las llamadas desde las extensiones que no requieren comunicación LDI o LDN o Móviles. (En caso de estar habilitadas estas opciones)
   - No permita configuración de extensiones sin uso o responsable.

7. **Limite el registro por extensiones a su red local.**
   Restringir las direcciones IP que sus extensiones pueden registrar en la red local. Las PBX-IP pueden usar las ACL (listas de control de acceso), en la configuración SIP para bloquear las direcciones IP, para permitir o rechazar registros. Esto puede defender de los intentos de registro a fuerza bruta.
   Recuerde realizar un inventario de las extensiones lógicas creadas en su planta y contrástelas frente a las físicas. Si la central telefónica o el PBX-IP posee opciones de restricción, no permita más de tres (3) intentos de ingreso de PIN o claves de acceso erróneos, antes de bloquear la cuenta, buzón de voz o extensión.

   Compruebe en el log de la planta telefónica los intentos fallidos de autenticación y en el caso de varios intentos, añadir de forma automática en el IPtables la dirección IP de nuestro ‘supuesto’ intruso. Utilice aplicaciones para la prevención de intrusos en su sistema que actúa penalizando o bloqueando las conexiones remotas que intentan accesos por fuerza bruta.

   Opciones como fail2ban están disponibles para sistemas basados en asterisk http://www.fail2ban.org/wiki/index.php/Main_Page

8. **Permitir sólo una o dos llamadas a la vez por entidad SIP**
   Donde sea posible limite la exposición si los poseedores legítimos de las contraseñas en tu sistema olvidan sus “pistas” para ingresar dichas contraseñas. Como medida de control permita máximo dos llamadas activas a la vez por troncal y/o canal SIP.

9. **Deshabilite los canales y servicios que no están en uso.**
   Deshabilite los canales que no esté usando como skinny y MGCP. Para su PBX-IP si sólo utiliza SIP es lo que debe habilitar. Mantenga seguro los buzones de correo y elimine los que no utiliza.

10. **Dificulte la tarea para los analizadores de SIP.**
    Esto hace que la PBX-IP no informe a un escáner SIP que extensiones son válidas, rechazando las solicitudes de autenticación en nombres de usuario existentes con los mismos detalles de nombres de usuario inexistentes. Otra forma de dificultar la labor de

los escáneres SIP es instalar un firewall de puerto SIP bloqueando el "escaneo" del puerto 5060 y 5061 y puede deshabilitar el punto final de intento por un tiempo específico cuando detecte una violación.

Si no pueden encontrarlo no pueden atacarlo.

11. **Limite y restrinja los planes de llamadas de enrutamiento y número de teléfono.**
Restringir las llamadas a destinos no deseadas o de alto costo y no permita llamadas a números 0800, números Premium, adicionalmente, utilice un prefijo de marcación acordado con su proveedor.

Otra opción es configurar en su PBX-IP limitación de consumos por fechas y horas y permitir el control de realización de llamadas. Bloquee la marcación en dos etapas desde su sistema de IVR y/o correo de voz.

Haga uso de los servicios gratuitos que ETB pone a su disposición (Código Secreto y Local exclusivo, Cambios de categorías LD), los cuales le permiten la restricción de llamadas no permitidas.

12. **Audite la seguridad de su sistema con regularidad.**
Realice auditorías de seguridad a su sistema PBX-IP y los registros de llamadas (CDR) para validar fechas, horas y destinos de llamadas. Revisar sus registros y CDR diariamente porque incluso un día de llamadas ilegítimas puede sumar una gran cantidad de dinero rápidamente.

Desarrolle un plan de acción dentro de la política de la compañía para conocer qué acciones deben ser adoptadas y que procedimientos se deben ejecutar en el momento de posibles problemas de seguridad en su sistema telefónico.

- Mantenga registros de las llamadas por un período prudencial.
- Realice un monitoreo permanente de los destinos tanto entrantes como salientes, hacia y desde su planta telefónica, para detectar tráfico irregular.
- Revise periódicamente la facturación de llamadas de su Central o PBX, en especial los servicios de larga distancia y celular, con el fin de identificar consumos fuera de lo normal.