Guía de prevención de fraudes telefónicos en su empresa

Contenido

1. Definiciones y generalidades sobre fraudes telefónicos

Una buena gestión de su sistema telefónico es la clave para evitar riesgos de fraude telefónico en su empresa

1.1 ¿Qué es un sistema telefónico PBX y para qué sirve?

Los Sistemas Telefónicos Privados o PBX permiten agrupar varias líneas telefónicas bajo un mismo número de fácil recordación o de mayor posicionamiento entre los clientes de las Empresas. El PBX comparte un número determinado de líneas externas y las distribuye en la cantidad de líneas internas que se desee.

Las troncales se agrupan en la central telefónica bajo el número seleccionado por el cliente (piloto), cuando entra o sale una llamada la configuración permite utilizar el canal que se encuentre libre. La capacidad de llamadas simultáneas dependerá del número de líneas agrupadas (troncales).

Ventajas de los PBX:

- El servicio permite agrupar varias líneas telefónicas bajo un mismo número telefónico de fácil recordación (línea piloto). Con el objetivo de posicionar un solo número de la empresa en el mercado, optimizando el tiempo de sus clientes al no tener que marcar varios números telefónicos.
- Mejora la eficiencia del negocio al reducir la pérdida de llamadas.
- Aumenta la capacidad de la empresa para la atención de sus clientes.
- Optimiza el tiempo de los clientes y proveedores al no tener que marcar varios números telefónicos para comunicarse con la empresa.
- Permite la facilidad de marcación abreviada entre las extensiones (troncales) del PBX.
- Las líneas no pierden sus características de línea básica.

Sin embargo, los PBX son constantemente objeto de ataques de personas que, utilizando puntos débiles en la programación y conociendo algunas de sus funcionalidades básicas, buscan acceder remotamente al sistema con el objetivo de realizar, sin autorización, todo tipo de llamadas para beneficio propio. Estos ataques generan altos consumos, que luego son cobrados a su empresa por los operadores móviles o de larga distancia.

Todas las plantas telefónicas pueden ser blanco de estos defraudadores, pero si cuenta con una buena programación de su PBX, la asesoría de un experto y un continuo seguimiento podrá tener un servicio más seguro para su empresa.

1.2 ¿Qué es un sistema telefónico IP PBX y para qué sirve?

Una central IP o IP-PBX es similar que la PBX tradicional, la diferencia está en los servicios de comunicación que funcionan a través de la red de datos. A esta aplicación se le conoce como voz sobre IP (VoIP), donde la IP es la identificación de los dispositivos dentro de la web.

Con los componentes adecuados se puede manejar un número ilimitado de anexos en sitio o remotos vía Internet, añadir vídeo, conectarle troncales digitales o servicios de VoIP para llamadas internacionales a bajo costo. Los aparatos telefónicos que se usan se les llaman teléfonos IP y se conectan a la red de datos (LAN o WAN). La IP-PBX se compone principalmente de un SIP-Server (SIP) o de un Gatekeeper, más un gateway o puerta de enlace que funciona de nexo entre la tecnología IP y los teléfonos analógicos, faxes, teléfonos digitales, teléfonos inalámbricos DECT, líneas urbanas analógicas, tramas E1/T1, líneas GSM, tramas E&M, etc.

2. ¿Cómo se hacen los fraudes a través de un sistema telefónico privado?

Los fraudes a través de un sistema telefónico privado se generan por el desconocimiento de las funciones del sistema y por tener una inadecuada programación de la seguridad del equipo, lo que permite al defraudador aprovecharse y lucrarse a través de la generación de alto tráfico de llamadas locales, móviles y de larga distancia nacional o internacional, dado que la facturación será asumida por la empresa dueña del sistema.

Estas llamadas son realizadas de manera ilegal por los defraudadores para obtener beneficios económicos por medio de reventa de minuos, reoriginamiento y el enrutamiento de tráfico y fuera de Colombia.

3. Funcionalidades más vulnerables de los PBX y fraudes más comunes

Debe tenerse en cuenta que las vulnerabilidades y precauciones a tener dependerán del siste ma telefónico que su empresa utilice, ya sea un PBX tradicional o un IP PBX también conocido como conmutador virtual.

3.1 Ataques más comunes al sistema telefónico privado o PBX tradicional

3.1.1 Funcionalidad DISA (Direct Inward System Access) o acceso remoto

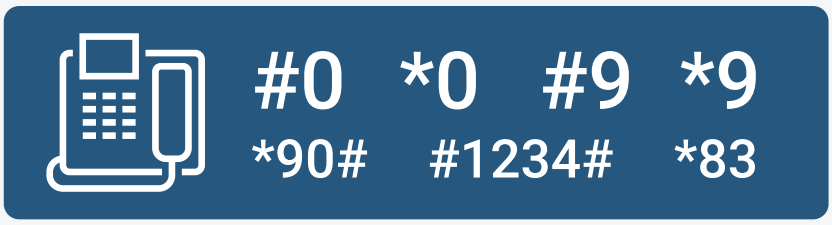
Esta opción se habilita para realizar llamadas desde el PBX, accediendo desde una línea externa de la compañía. La funcionalidad DISA puede abrir la puerta al defraudador, si no se tiene una adecuada programación y políticas de seguridad para su uso.

Por medio de una línea externa y utilizando esta funcionalidad, cualquier persona que conoz- ca el manejo o los códigos de acceso a troncales del PBX puede realizar llamadas que serán cobradas a la empresa.

3.1.2 Servicio de atención automática-activación marcación en dos etapas

Existen algunos sistemas de atención automática en los cuales, a través de ciertas opciones, se accede al tono de marcado y se activa la funcionalidad de marcación en dos etapas. Si el sistema no está configurado de manera apropiada, el servicio de atención automática pasa la llamada de regreso al PBX como una solicitud de tono de marcado y deja al defraudador en posibilidad de realizar llamadas a cualquier lugar y con cargo a la compañía propietaria del PBX.

Algunas de las opciones más utilizadas por los defraudadores son:



Nota: estos varían, de acuerdo con el tipo de PBX o sistema de llamadas y de acuerdo al modo de programación de los mismos.

3.1.3 Redireccionamiento de extensiones de empleados a móviles, larga distancia nacional e internacional

Este fraude, por lo general, se hace con el acompañamiento de personal que tiene acceso a los recursos de la empresa, direccionando su teléfono a un destino de larga distancia nacional, internacional o móvil para la realización de llamadas de terceros a estos destinos.

3.1.4 Buzones de voz

La opción de habilitar casilleros para mensajes de voz ofrece, además de eficiencia en las comunicaciones de una empresa, servicio para sus clientes. Desafortunadamente, los buzones son usualmente atacados por los defraudadores, debido a que esta funcionalidad permite en algunos casos realizar llamadas de regreso (call back) al número telefónico que dejó el mensaje. Estas llamadas pueden ser locales, de larga distancia nacional o internacional o a teléfonos móviles. Además, sin una correcta programación, alguien se podría apoderar de los buzones de voz, cambiándoles las claves de acceso originales.

3.1.5 Transferencia de llamadas a los números de operadoras

Ocurre cuando la recepcionista de la empresa recibe una llamada a través de la cual le solicitan transferirla a las extensiones de operadoras automáticas (ejemplo: 151-159, 171-179 y 191-199), que son en realidad los números del servicio asistido por operadora de las compañías de larga distancia. Al transferirse la llamada, el defraudor accede al servicio de larga distancia nacional o internacional deseado y esa llamada es cobrada a la empresa propietaria del PBX.

3.2 Ataques más comunes al sistema IP PBX

3.2.1 Denegación de servicio

Los ataques de denegación de servicio también llamado ataque DoS, son ataques a un sistema de computadores o red que causa que un servicio o recurso sea inaccesible para el usuario legítimo. Las dos formas más comunes de saturar una maquina son:

a. Generar una serie muy grande de falsos requerimientos de servicio para que la máquina no tenga recursos suficientes para atender los verdaderos requerimientos de servicio.

b. Generar requerimientos mal hechos que generen fallas en el protocolo y este se bloquee o se reinicie para recuperar su funcionalidad.

3.2.2 Llamadas no solicitadas

Ocurre cuando el protocolo SIP puede aceptar llamadas en los endpoints sin autenticación y fácil acceso. Con solo conocer su IP el defraudador logra que se hagan barridos de direcciones buscando los puertos de SIP o h323 abiertos para enviar tráfico sin tener ninguna identifica ción del origen, ya que, a diferencia de la voz convencional, no se tiene que ser usuarios de la misma red o de una central interconectada para enviar tráfico; en IP se puede hacer sin dejar rastro y utilizar audio grabado para que un servidor como una ametralladora envíe tráfico sin dejar rastro.

3.2.3 Autenticación de usuarios no autorizados

Se da por una inadecuada definición de políticas de contraseñas sobre las plataformas (longi- tud corta, sin complejidad, etc.) porque no hay un control ni obligación del sistema para hacer cambio de claves cada determinado tiempo de uso de cuentas y claves genéricas.

3.2.4 Otros Riesgos

- No bloquear el usuario después de un número de intentos fallidos.
- Sesiones abiertas simultáneamente para un mismo usuario (esto no se debe permitir).
- Mal uso del acceso remoto.
- Falta de políticas y procesos sólidos de seguridad dentro de la empresa.
- Configuración por defecto de los equipos utilizados, tal como los entrega el fabricante de la solución.

4. Recomendaciones para evitar fraudes telefónicos en su empresa

- No active funciones del PBX que no vaya a utilizar, por ejemplo, la DISA, buzones de voz, desvío de llamadas y acceso a servicio de operadoras. Compruebe periódicamente (a diario) si la funcionalidad DISA ha sido activada. Si no se puede deshabilitar DISA por razones comerciales, se debe solicitar a los usuarios que ingresen un código de autorización personal además del código requerido para obtener una línea externa. El proveedor de PBX debe estar disponible para brindar soporte en las diversas funciones que se habilitarán, deshabilitarán o restringirán.
- Habilite las reglas de marcación dinámica si es posible, hora del día y / o las políticas de destino de enrutamiento, tenga en cuenta que estas llamadas irregulares suelen realizarse en las noches y fines de semana y se pueden evitar configurando correctamente el PBX para que bloquee las llamadas en horarios no laborales.
- Use contraseñas seguras con una combinación de mayúsculas y minúsculas, números y símbolos. Implemente políticas de caducidad de contraseñas y configure políticas de notificación adecuadas para cuentas bloqueadas.
- Cambie las contraseñas predeterminadas para todos sus dispositivos, especialmente las cuentas con privilegios administrativos.
- No continúe con las contraseñas por defecto suministradas por el proveedor para la administración de la planta telefónica, evite contraseñas débiles (ejemplo: 0000 o 1234) para los accesos a los servicios y buzones de voz.
- Configure su sistema para no permitir acceder a tono de discado en ninguna circunstancia (marcación en 2 etapas).
- Solo permita el acceso desde direcciones IP específicas, si necesita acceso público. Considere implementar una arquitectura de servidor de salto como Citrix.
- Mantenga seguros los buzones de correo de voz, para ello debe cambiar periódicamente las contraseñas y eliminar o bloquearlos buzones de correo no utilizados. Proteja con PIN, si es posible, se recomienda al menos un PIN de 6 o más dígitos; (fuerce a los usuarios a cambiar las contraseñas en su primer inicio de sesión a su buzón de correo o añadir un prefijo. No permita disponer de las contraseñas que estén relacionadas con su número de extensión y debe desactivarse después de una cantidad específica de intentos fallidos)

- Tenga precaución con cualquier sistema de recepción automática de llamadas incluyendo aquellas que han estado integradas a su red de datos (consola automática, IVR, IVM, correo de voz con mensajería unificada).
- Elimine la posibilidad de acceder a una línea externa marcando por medio de la operadora automática o en los servicios de mensajería de voz; no debe contar con ningún método que permita acceder al tono de marcado desde su PBX a menos que se use una red privada virtual (VPN). No conecte llamadas entrantes que soliciten las extensiones 151-159, 171-179 y 191-199.
- Defina categorías, políticas internas y niveles de acceso para cierto tipo de llamadas (LDN, LDI, móviles).
- Antes de aceptar asesoría y soporte para probar o configurar su sistema telefónico por parte de personas que dicen pertenecer a las compañías telefónicas, solicite una identificación, indague por el número de la orden de servicio o valide con la compañía telefónica respectiva.
- Fuera del horario diurno de oficina, un sistema PBX debe configurarse en modo de servicio nocturno. Esto ofrece un servicio restringido y reduce la vulnerabilidad a los piratas informáticos por la noche y los fines de semana. Esto puede no ser factible para las empresas con actividad internacional que requieren el uso global de la PBX las 24 horas del día.
- Maneje los manuales de configuración del PBX como documentos a los que solo debe tener acceso personal autorizado.
- Establezca con su proveedor fecha y horas específicas para el mantenimiento remoto de su sistema y confirme que el módem utilizado para el mantenimiento a distancia o remoto sea apagado o bloqueado en el momento de finalizar el trabajo.
- Incluya en los contratos de instalación y mantenimiento del sistema con terceros, cláusulas de responsabilidad por cambios no acordados.
- Vigile y compruebe el trabajo de los técnicos durante y después de los trabajos de mantenimiento.
- Realice control y seguimiento de los mantenimientos, reprogramaciones o cambios al sistema, llevando fecha, hora y detalle de las modificaciones.
- Revise la facturación periódicamente, apoyándose en los reportes internos del sistema y comparándolos con la facturación de las empresas telefónicas.
- Realice un monitoreo permanente de los destinos tanto entrantes como salientes, hacia y desde la planta telefónica, para detectar tráfico irregular. En caso de sospechar del mismo, comuníquese inmediatamente con el operador de telecomunicaciones.

- Audite periódicamente el sistema PBX para comprobar la seguridad y los puntos débiles, verifique que se estén operando los controles designados y supervise la forma en que la programación se ajusta a las necesidades de la empresa.
- Habilite controles de admisión de llamadas, sesiones máximas, políticas de registro, etc.
- Restrinja el reenvío de llamadas, limite ese servicio a 6 dígitos para que solo puedan reenviar a otros números internos. Tenga en cuenta que esto no es muy útil en el caso de que la empresa tenga más de un PBX (un PBX por filial) debido a que el pirata marcará en la primera PBX y de allí llamará a la segunda PBX, la segunda PBX verá que la llamada recibida proviene de su colega PBX (llamada interna) y permitirá que se establezca una llamada internacional arriba. Este escenario explica el término "fraude a través de marcado" para ese tipo de pirateo de PBX.
- Especifique las características / instalaciones mínimas requeridas por un usuario estándar y solo brinde estos servicios. Las instalaciones adicionales deben solicitarse por escrito y ser aprobadas por un gerente alguien autorizado para tal fin.

5. Recomendaciones para prevenir ataques en sistemas Asterisk, IP PBX, Free PBX, conmutadores virtuales, etc.

Además de las recomendaciones anteriores debes tener en cuenta que:

- Debe estar al día en actualizaciones (estables), vulnerabilidades y soluciones sobre esta aplicación de software libre
- Lleve un control exhaustivo del sistema: versiones de paquetes, nuevas actualizaciones
- Compruebe en el log del Asterisk los intentos fallidos de autenticación y, en caso de varios intentos, añada de forma automática en el IPTables la dirección IP del 'supuesto' atacante
- Las direcciones IP de atacantes se deben añadir al firewall para denegar el acceso a la red
- Evite utilizar puertos estándares (5060, 4569, 80, 22, etc.)
- Deshabilite rangos de puertos no esenciales
- Bloquee todos los puertos TCP 'inferiores' (<1024) a direcciones IP públicas
- Utilice puertos no estándar para interfaces accesibles desde la web, si deben ser accesibles desde direcciones IP públicas
- Escanee su red desde una IP pública para descubrir puertos abiertos y protegerlos
- Durante la instalación, programe y configure el sistema adecuadamente, si es necesario, consulte con un experto en el tema para cerrar vulnerabilidades y prevenir ataques desde la red.
- Implemente herramientas que le den seguridad y protejan a su red, tales como firewall, IDS y el PortSentry para evitar escaneos y ataques DoS.
- Deniegue peticiones al 5060/4569 UDP desde el exterior siempre que no tengamos usuarios SIP/IAX externos.
- Deshabilite el "allowguest=yes" que lo traen algunas interfaces habilitado por defecto
- Configure el "realm", el "defaultuser" y el parámetro "secret" siempre, se recomienda cambiar configuración por fefecto.
- Realice una correcta configuración del Dialplan. Si el extensions.conf no se ha configurado con estrictas medidas de seguridad, los usuarios maliciosos se podrían autenticar y registrar en su sistema para hacerse pasar por una extensión con permisos y realizar llamadas como un usuario normal. Ante esto debe configurar contraseñas robustas difíciles de identificar

- Interconéctese sobre una interfaz de confianza cuando sea posible, TLS o Ipsec
- Limite el acceso y el procesamiento de llamadas a direcciones IP conocidas
- Asegure su perímetro con un SBC local, o a través de un proveedor de servicios
- Establezca políticas de bloqueo de cuentas para combatir la fuerza bruta y los ataques basados en diccionarios
- Bloquee las respuestas de ICMP para dispositivos de misión crítica y solo permita selectivamente respuestas de ICMP a IP de confianza
- Utilice la autenticación de challenge-response para encriptar la comunicación a cualquier portal basado en web a través de IP pública
- Conozca el dispositivo que está ejecutando. Por ejemplo, algunos SBC permiten el registro de punto final sin un nombre de usuario o contraseña, siempre que se configure una extensión
- Permita solo IP confiables para enviar al puerto VoIP predeterminado
- Envíe llamadas VoIP a su propia red para probar su vulnerabilidad
- Ignore o bloquee por completo los mensajes de direcciones IP desconocidas. Algunos dispositivos enviarán 100 llamadas a una IP no autorizada, solo para rechazar la llamada en un mensaje posterior. Esto solo sirve para informar a un intruso que un dispositivo VoIP está disponible y escuchando
- Los sistemas de administración deben estar protegidos con contraseña y la sesión debe bloquearse después de una cantidad específica de intentos fallidos. El sistema debería expirar después de un período de inactividad especificado. Implemente una fuerte protección con contraseña, SIP permite utilizar contraseñas complejas en IP-PBX. Reemplace de inmediato las contraseñas predeterminadas de fábrica (por ejemplo, administrador, usuario, etc.) con otras contraseñas seguras
- Desconecte extensiones no asignadas o líneas directas (no autorizadas)
- Configure un canal seguro en el SIP para que la información viaje cifrada utilizando SSL (prevención)
- Valide que el método “INVITE” del protocolo SIP esté configurado sólo para teléfonos válidos en la troncal.
- Asegúrese de que los teléfonos VoIP tengan un filtro en el protocolo SIP para el número de invitaciones que se puedan recibir.
- Configure adecuadamente el enrutador. Un enrutador bien configurado generará una alerta desde el firewall interno o el Sistema de detección de intrusos (IDS) en caso de un ataque a una IP-PBX. Se debe recomienda guardar los registros del cortafuego como evidencia de un ataque en caso de una queja oficial.

IMPORTANTE

Si su empresa cuenta con servicios de telecomunicaciones como E1s, RDSI, Troncal SIP o líneas telefónicas análogas e IP conectadas a su planta telefónica conformando un sistema de telefonía privado, será su obligación conocer y aplicar estos estrictos controles de seguridad, mantenimiento y manejo de los equipos, cuya configuración y uso son de su entera responsabilidad.

Recuerde que todos los sistemas telefónicos pueden ser blanco de los defraudadores y que el manejo y mantenimiento de estos equipos son de su entera responsabilidad, conforme a lo establecido en el contrato no debe cometer ni ser partícipe de actividades de fraude.

Si su empresa cuenta con una buena programación, con estrictos cuidados con la seguridad y un continuo seguimiento, podrá prevenir este riesgo.

En TigoUne queremos informarle sobre este riesgo para ayudarle a prevenir posibles fraudes telefónicos que le pueden costar mucho más que una llamada de atención. Conozca cómo se hacen estos fraudes y siga estas recomendaciones para evitarlos. Para una adecuada programación de su sistema telefónico, le recomendamos asesorarse con el proveedor de su planta telefónica.

Si desea más información sobre los tipos de fraude y funcionalidades más vulnerables de los sistemas telefónicos, comuníquese con su ejecutivo TigoUne o llame a nuestra

Línea nacional de servicio al cliente de Empresas

01 8000 513 287

www.tigoune.com.co/empresas


tigo
une