Guía de prevención de fraudes telefónicos en su empresa

tigo une

Contenido

1. Definiciones y generalidades sobre fraudes telefónicos 3

1.1 ¿Qué es un sistema telefónico PBX y para qué sirve? 3

1.2 ¿Qué es un sistema telefónico IP PBX y para qué sirve? 4

1.3 ¿Qué es un sistema Asterisk y para qué sirve? 4

2. ¿Cómo se hacen los fraudes a través de un sistema telefónico privado? 5

3. Funcionalidades más vulnerables de los PBX y fraudes más comunes 5

3.1 Ataques más comunes al sistema telefónico privado o PBX tradicional 5

3.1.1 Funcionalidad DISA (Direct Inward Systey fram Access) o acceso remoto 5

3.1.2 Servicio de atención automática-activación marcación en dos etapas 6

3.1.3 Redireccionamiento de extensiones de empleados a móviles, larga distancia nacional e internacional 6

3.1.4 Buzones de voz 6

3.1.5 Transferencia de llamadas a los números de operadoras 6

3.2 Ataques más comunes al sistema IP PBX 7

3.2.1 Negación de servicio 7

3.2.2 Llamadas no solicitadas 7

3.2.3 Autenticación de usuarios no autorizados 7

3.2.4 Otros Riesgos 7

4. Recomendaciones para evitar fraudes telefónicos en su empresa 8

5. Recomendaciones para prevenir ataques en sistemas Asterisk, IP PBX, Free PBX, conmutadores virtuales, etc. 9

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 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 (piloto). Con el objetivo de posicionar un solo número de la PYME 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 atención de los clientes
- Optimiza el tiempo de los clientes y proveedores al no tener que marcar varios números telefónicos.
- 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 fraudulentos de personas que, utilizando puntos débiles en la programación y conociendo algunas de sus funcionalidades básicas, acceden remotamente al sistema y realizan todo tipo de llamadas para beneficio propio sin ninguna autorización. 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 usted 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 un equipo de comunicaciones diseñado para ofrecer servicios de comunicación a través de las redes de datos. A esta aplicación se le conoce como voz sobre IP (VoIP), donde IP es la identificación de los dispositivos dentro de la web.

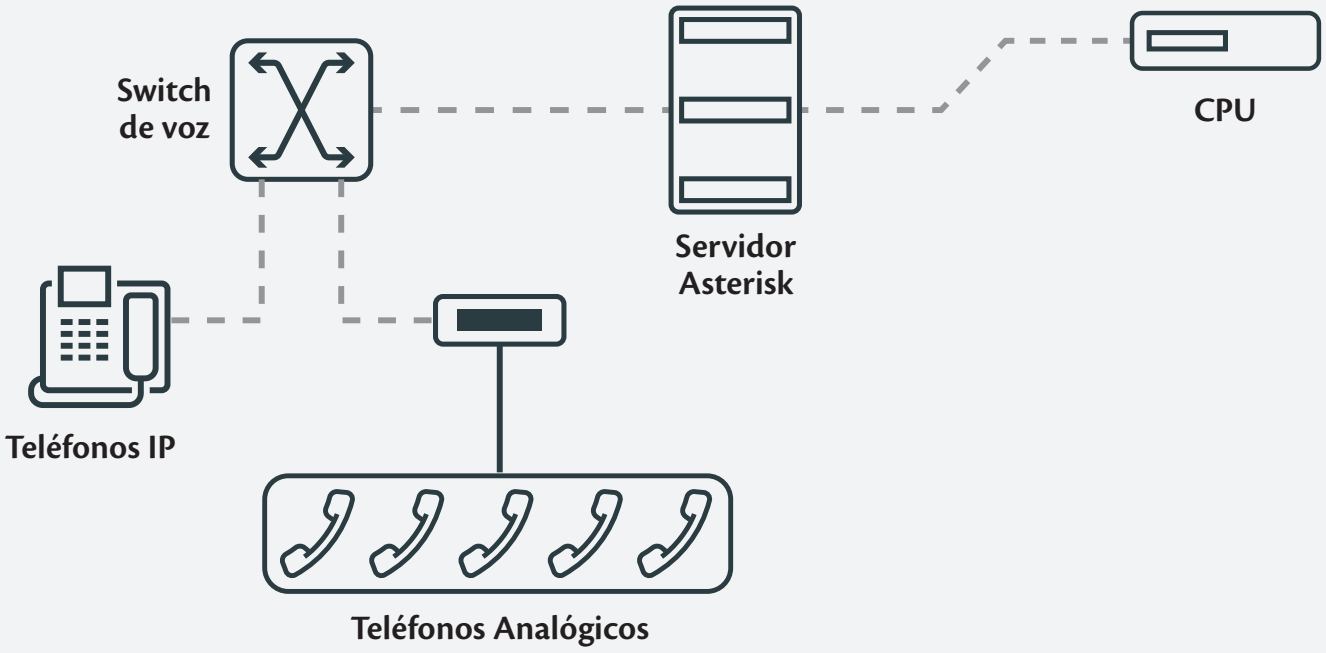
Con los componentes adecuados se puede manejar un número ilimitado de anexos en sitio o remotos vía Internet, añadir vídeo, conectarle troncales digitales o servicios de VoIP para llamadas internacionales a bajo costo. Los aparatos telefónicos que se usan se les llaman teléfonos IP y se conectan a la 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.

1.3 ¿Qué es un sistema Asterisk y para qué sirve?

Asterisk es un software que puede convertir un computador normal en un servidor para comunicaciones sobre VoIP, usando soluciones OPEN SOURCE (código abierto).

Es utilizado para la generación de un sistema PBX en las empresas, así como sistemas integrales para call-centers, salas de conferencias, buzones de voz.

Tiene la ventaja de utilizar medios de comunicación IP: Troncales SIP, líneas TOIP, como sistemas análogos RDSI primarios o básicos y líneas PSTN.



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

El fraude telefónico se refiere al uso no autorizado de un sistema de comunicación por atacantes externos y cada vez más usado por hackers debido al poco refuerzo que se hace en la seguridad de los sistemas de comunicaciones. El hackeo de PBX (conmutador) es un gran negocio para los delincuentes.

Sin embargo, la mayoría de los fraudes a través de un sistema telefónico privado se generan por el desconocimiento de las funciones del sistema y por no tener una correcta programación de la seguridad del equipo, 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 recibida por la empresa dueña del sistema.

Estas llamadas son realizadas por los defraudadores a través del sistema telefónico privado para obtener beneficios económicos por medio de reventa de minutos, reoriginamiento y el enrutamiento de tráfico dentro y fuera de Colombia, de manera ilegal.

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

Debe tenerse en cuenta que las vulnerabilidades y precauciones a tener, dependerán del sistema 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 Systey fram Access) o acceso remoto

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

Por medio de una línea externa y utilizando esta funcionalidad, cualquier persona que conozca 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 apropiadamente configurado, 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 al 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 herramienta 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 Negación de servicio

Los ataques de negación de servicio son los que se basan en saturar de alguna manera la máquina que está prestando un servicio, para que esta no pueda seguirlo prestando. 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

Que el protocolo SIP pueda aceptar llamadas en los endpoints sin autenticación y el fácil acceso solo conociendo su IP proporciona que se hagan barridos de direcciones buscando los puertos de SIP o h323 abiertos para enviar tráfico sin tener ninguna identificación del origen, ya que a diferencia de la voz convencional, no tenemos 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 password sobre las plataformas (longitud corta, si 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 del 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 de conciencia en seguridad dentro de la empresa.
- Configuración por defecto de los equipos 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.
- 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.
- 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 bajo ninguna circunstancia (marcación en 2 etapas).
- Elimine o bloquee los buzones de voz que no estén en funcionamiento.
- Mantenga seguro los buzones de correo, para ello, es necesario cambiar periódicamente las contraseñas y eliminar los buzones de correo no utilizados (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).
- Cuelgue cuando reciba llamadas con anuncios en una lengua extranjera.
- 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).
- 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.
- Pregunte a su proveedor por el modo nocturno de su planta para evitar llamadas fuera del horario laboral.
- 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. Si se detecta algún tráfico irregular o sospecha del mismo, comuníquese inmediatamente con el operador de telecomunicaciones.
- Audite periódicamente el sistema PBX para comprobar la seguridad, puntos débiles y la forma en que la programación se ajuste a las necesidades de la empresa.

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:

- Esté al día en actualizaciones, 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 el 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
- desde estas.
- Evite utilizar puertos estándares (5060, 4569, 80, 22, etc.).
- Haga un mantenimiento continuo de la aplicación.

- 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, como: un firewall y el PortSentry para evitar escaneos y ataques DoS.
- Denegar 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.
- Realice una correcta configuración del dialplan: si el extensions.conf No lo ha configurado con estrictas medidas de seguridad, los usuarios maliciosos se autentifican y registran en su sistema para hacerse pasar por una extensión con permisos y poder hacer llamadas como un usuario normal. Ante esto debe configurar contraseñas robustas difíciles de identificar.

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 estos defraudadores y que el manejo y mantenimiento de estos equipos son de su entera responsabilidad, conforme a lo establecido en la cláusula séptima del contrato único de condiciones uniformes, sin embargo, 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 mayor 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