CloudPBX - Seguridad de la plataforma en la nube

Hoy en día la práctica de "hacking" a diversos sistemas se vuelve más común y es por ello que cada día debemos adoptar nuevas estrategias de seguridad para evitar ser víctimas; así en este documento enlistaremos las recomendaciones o buenas prácticas aplicables las instancias Cloud PBX.

Recomendaciones importantes:

- Establecer y mantener la contraseña de la GUI o administración Web de la PBX con un formato seguro: 14 caracteres o más, que incluyan: **mayúsculas, símbolos, números y caracteres especiales**. La administración de la PBX permite conocer **contraseñas de todos los dispositivos**, troncales y configuraciones globales.
- **NO almacenar contraseñas** del usuario de administración Web de la PBX en las opciones del navegador que utilizamos (chrome, edge, firefox). **NO almacenar** información de extensiones o de usuario en **navegadores, archivos planos** (notas, word, etc); si se manejan estos archivos que sea solo de manera temporal y eliminarlos cuanto antes sea posible.
- Establecer y mantener las contraseñas de las extensiones (contraseña SIP) con al menos 12 caracteres, que incluyan: **mayúsculas, minúsculas, simbolos, números y un caracter especial. NO incluír** por ninguna razón el nombre de la empresa, nombre del puesto o persona y números o letras contínuas. Ejemplo incorrecto: Extensión 123, clave: abc123.
- Establecer en los dispositivos o teléfonos físicos (Grandstream, fanvil u otros) una contraseña de administración Web robusta (admin) para que mediante el intento de hacking de los mismos dispositivos no se tenga acceso a la PBX o extensiones.
- Si se utilizan softphones en computadoras o dispositivos, las computadora deben contar con un **antivirus y debe estar debidamente actualizado** ya que en la computadora o dispositivo se almacena el programa y en él se almacenan las credenciales de la cuenta/extensión SIP.
- Mantener actualizados los firmwares de los dispositivos telefónicos (grandstream, fanvil, u otros) con el último firmware disponible de parte del fabricante; así como los firmwares de todos los smartphones que utilicen una extensión de la PBX. En el caso de los softphones en computadora o PC es requerido que la PC cuente con actualizaciones del sistema operativo al día (parches).

Seguridad nativa de plataforma:

La plataforma Cloud PBX incluye algunos métodos preventivos o de seguridad, los cuales NO deben ser modificados para garantizar la seguridad e integridad de la misma. Los elementos importantes son:

- Mantener activa la función de **detector de intrusos.**
- **No modificar valores** en el detector de intrusos.
- Habilitar de ser posible las **notificaciones por correo** del detector de intrusos.
- **Mantener activo el firewall** o cortafuegos de la plataforma para evitar acceso a puertos no necesarios.

Advertencias:

- Los servicios Cloud PBX se entregan mediante una IP pública, lo que implica estar disponible en todo el mundo y ser buscados por hackers; normalmente las PBX representan una “mina de oro” para ellos pues una plataforma PBX "hackeada" les permitirá negociar tráfico de llamadas internacionales sin costo alguno. Por lo anterior se han implementado métodos y recursos de seguridad para asegurar la plataforma y protegerla pero es responsabilidad del cliente mantener seguras todas las áreas y no realizar modificaciones en aspectos de red, seguridad y usuarios las cuales pueden alterar los métodos y recursos de seguridad.
- Existen robots que operan 24x7 los cuales escanean IP’s constantemente para indagar que IPs atienden servicios SIP/VoIP y luego de detectar la disponibilidad se dedican a generar listas para que otros robots lancen ataques SIP para hackear cuentas (extensiones) vulnerables (claves débiles) y así poder realizar llamadas internacionales mediante la extensión hackeada. Es importante mantener las contraseñas de extensiones con una política de seguridad robusta.
- Es responsabilidad del cliente propietario de la PBX el cumplir con los lineamientos mínimos recomendados en seguridad de la Cloud PBX, por ello se provee de un usuario administrador que contiene los privilegios necesarios para dicha actividad.
- Es responsabilidad del cliente cualquier vulnerabilidad que haya sido explotada mediante hackings a su plataforma Cloud PBX por causas que pudieron haber sido mitigadas mediante las prácticas de seguridad aquí descritas.

Antes sospechas que debo hacer?

Si tiene dudas o sospechas de que su plataforma CloudPBX ha sido vulnerada por algún procedimiento mal realizado o por la explotación de una computadora con acceso a la PBX, remita un caso inmediatamente a soporte técnico mediante el correo electrónico

soporte@voxdatacomm.com o al PBX 2278-8181.

> Vox Datacomm, S.A.: NO se hace responsable por servicios vulnerados por terceras personas, tampoco se hace responsable del pago de facturas o servicios de telefonía del cliente final que ha tenido vulnerabilidades en su PBX a causa de no seguir las prácticas de seguridad descritas previamente en este documento. La información aquí expuesta y compartida NO supone un compromiso o garantía de que la Cloud PBX es infalible ante

ataques/vulnerabilidades. El cliente es el único responsable por la gestión y administración de la PBX y de garantizar su seguridad mediante la revisión periódica y mantenimiento de los protocolos de seguridad.

Revision #10
Created 27 January 2022 15:08:10 by Eduardo Mejia
Updated 9 July 2024 20:39:54 by Eduardo Mejia