Carrera 7 No 20 – 99 Piso 1 Oficina de Correspondencia ETB
Código Postal: Bogotá 110311
Conmutador: 242 2000

Bogotá D.C.

Comunicación Preventiva Fraude

Apreciado Cliente:

En ETB nos complace ser su aliado en la prestación de servicios de comunicaciones y contribuir así a la obtención de los logros fijados por su empresa.

Es nuestro compromiso mantenerlo siempre informado y más aún cuando de seguridad se trata. ETB como su operador de telecomunicaciones tiene el deber de suministrarle la información sobre los riesgos relativos a la seguridad en la red y del servicio contratado que complementan los mecanismos implementados por la compañía para evitar su ocurrencia y a los que puede recurrir el usuario para preservar la seguridad de la red y las comunicaciones[1].

El uso de código malicioso para lograr acceso abusivo a los sistemas es una de las tendencias que afectan el entorno de las telecomunicaciones, principalmente las centrales telefónicas privadas (PBX) donde se busca control o acceso a la configuración del servidor para comprometerlo con el fin de vender o realizar llamadas sin consentimiento del propietario.

Por lo tanto, le recomendamos conocer y mantener estrictos cuidados con la seguridad, mantenimiento y programación de estos equipos, asegurando que la configuración de los mismos no sea manipulada por terceros no autorizados. **Recuerde que estos equipos son de su propiedad y entera responsabilidad.**

Si en su organización están instalados enlaces E1's, RDSI, troncales y/o canales SIP, Servicios Voz sobre IP, líneas telefónicas fijas o móviles interconectadas a su planta telefónica conformando un PBX; los defraudadores informáticos pueden vulnerar y acceder a su sistema y utilizar la planta telefónica para beneficio propio, esto puede reflejarse en la generación indiscriminada de llamadas que son enrutadas a través de su sistema de comunicaciones y que le pueden generar cobros elevados en su factura.

Como mecanismos de prevención, lo invitamos a tener en cuenta:

- ✓ No mantenga las contraseñas por defecto suministradas por su proveedor para la administración de la planta telefónica y equipos de Voz sobre IP.
- ✓ Utilice contraseñas aleatorias y como mínimo utilice 12 caracteres alfanuméricos combinados y con caracteres especiales; no utilice como contraseña el número de la extensión.
- ✓ Proteja la interfaz de administración remota. Utilice conexiones VPN temporales.
- ✓ Bloquee en el firewall los puertos TCP/IP de acceso remoto que no utilice en su sistema de PBX.
- ✓ Mantenga seguro los buzones de correo y elimine los que no utiliza.
- ✓ Bloquee la marcación en dos etapas desde su sistema de IVR y/o correo de voz.
- ✓ Mantenga registros de las llamadas por un período prudencial.
- ✓ Solicite continuamente al proveedor de la planta telefónica las características de nuevas versiones, actualizaciones de software, principalmente lo que se refiere a parches para corregir vulnerabilidades que permitan fortalecer su sistema telefónico.
- ✓ Utilice un sistema de detección de intrusos (IDS) y herramientas de protección de forma automatizada de sus llamadas.
- ✓ 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.

[1] Numeral 2.1.1.2.4 del Artículo 2.1.1.2; Articulo 2.1.10.7 - Resolución 5111 de 2017 - CRC: "Por la cual se establece el Régimen Integral de Protección de los Derechos de los Usuarios de los Servicios de Comunicaciones," se modifica el capítulo 1 del Título II de la Resolución 5050 de 2016 – CRC

- ✓ Se sugiere contratar el soporte técnico con empresas legalmente establecidas, que posean la suficiente experiencia y reconocimiento en el campo.
- ✓ Realice un inventario de las extensiones lógicas creadas en su planta y contrástelas frente a las físicas.
- ✓ Realice un monitoreo permanente de los destinos tanto entrantes como salientes, hacia y desde su planta telefónica, para detectar tráfico irregular.
- ✓ 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.
- ✓ Permita máximo dos llamadas activas a la vez por troncal y/o canal SIP.
- ✓ Acuerde con el proveedor de instalación y mantenimiento de la planta telefónica, cláusulas de penalización y responsabilidad jurídica y económica por fraudes realizados y atribuidos a la vulnerabilidad sobre la planta telefónica.
- ✓ Establezca políticas claras sobre la seguridad del sistema telefónico y en la planta PBX:

    - Establezca un plan de marcación llamadas y defina responsables del tráfico
    - Restrinja llamadas desde las extensiones que no requieren comunicación LDI o LDN o Móviles.
    - No permita configuración de extensiones sin uso o responsable.

- ✓ 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.
- ✓ 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).
- ✓ Si la central telefónica - PBX posee opciones de restricción, no permitir más de tres (3) intentos de ingreso de PIN o claves de acceso erróneos, antes de bloquear la cuenta, buzón de voz o extensión.
- ✓ 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.
- ✓ Proteja la ubicación física de la central telefónica o PBX y el cuarto de equipos y/o gabinetes. El lugar en donde se encuentran instalados estos equipos, debe tener su respectivo mecanismo de seguridad. A este sitio únicamente debe acceder personal autorizado y se debe llevar un control de registro de entrada y salida. **Recuerde que es su responsabilidad garantizar la seguridad de sus instalaciones o acometidas internas.**
- ✓ 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.

- ➢ Para estos temas existen recomendaciones concernientes a la administración y configuración de una PBX, con el fin que nuestros clientes puedan prevenir este tipo de situaciones. Estas recomendaciones ETB las tiene publicadas en la página web http://www.etb.com.co/guiadeconsulta/normatividad.html

- ➢ Si requiere mayor información al respecto comuníquese al teléfono (**1)2422652** o al email control_fraude@etb.com.co

Esperamos con esta información dar una pequeña reseña frente al entendimiento, el manejo y la importancia de propender por la seguridad en la red, con el fin de seguir adelante con el mejor servicio y sin afectaciones de ningún tipo.

En ETB continuamos trabajando para darle a su empresa, acceso al más amplio portafolio de soluciones integrales, de forma eficiente y competitiva. Y le manifestamos nuestro interés de seguir prestándole el mejor servicio.

Cordialmente,

Dirección de Aseguramiento de Ingresos y Control Fraude
Vicepresidencia Financiera