Estimado usuario,

Para COMCEL S.A., en adelante COMCEL, la seguridad de los productos y servicios ofrecidos a nuestros clientes es primordial, por tal motivo hemos implementado procesos y herramientas que nos permiten cumplir con los más altos estándares de seguridad de conformidad a las buenas prácticas y términos establecidos por los entes reguladores.

Entendiendo que la seguridad es una responsabilidad conjunta entre los proveedores de servicios y los usuarios finales, adicional a las acciones que adelanta COMCEL se recomienda que por su parte se implementen procedimientos orientados a prevenir o reducir los efectos de ataques informáticos, así como la explotación de posibles vulnerabilidades que puedan tener los equipos a los que conecte los servicios suministrados.

En relación al servicio de telefonía, la creciente oferta de soluciones de bajo costo para implementar centrales telefónicas PBX ha propiciado que por parte de los usuarios finales se descuiden algunos aspectos de seguridad, aumentando el riesgo que estas plantas telefónicas puedan ser vulneradas mediante ataques informáticos externos y que los enlaces conectados a las mismas sean usados para hacer llamadas locales, de larga distancia o a servicios de alto costo sin que esto pueda ser advertido por el cliente.

Por normatividad regulatoria las plantas telefónicas o servidores al que usted conecte los servicios provistos por COMCEL hacen parte de su acometida interna, están bajo su responsabilidad y en consecuencia, conforme a lo establecido en el contrato de Servicios de Telecomunicaciones y/o TIC, el suscriptor o usuario responderá por cualquier anomalía, fraude o adulteración que se encuentre sobre sus equipos de la siguiente manera:

“(;) 14. Es de la absoluta y exclusiva responsabilidad del SUSCRIPTOR o USUARIO, del Poseedor o Propietario correspondiente, garantizar la seguridad de sus instalaciones y acometidas internas. En consecuencia, responderán en forma solidaria y hasta por la culpa leve de cualquier anomalía, fraude o adulteración que se encuentre en las acometidas, así como por las variaciones que sin autorización de LA EMPRESA se hagan en relación con el servicio contratado. (;)”

Las acometidas internas pueden estar expuestas en mayor o menor grado a vulnerabilidades impredecibles producto de acciones fraudulentas, intervenciones y cambios de configuración con o sin autorización del cliente. Por esta razón COMCEL no se hace responsable por los perjuicios derivados de vulnerabilidades de seguridad en este segmento de la red.

Con base en lo anterior, adicional a cualquier medida que como usuario decida

adelantar para fortalecer la seguridad de su red y equipos, sugerimos tener en cuenta e implementar las recomendaciones que se brindan a continuación.

RECOMENDACIONES GENERALES:

- Activar solo los planes de llamadas y discados necesarios. Si en su organización no se hacen llamadas de larga distancia nacional, internacional, a móviles o líneas Premium, entonces no habilitarlas en la planta y preferiblemente solicitar a su proveedor de telefonía deshabilitarlas
- Desactivar todas las facilidades y códigos del sistema que estén configurados de fábrica y que no sean indispensables para la empresa.
- Revisar constantemente la facturación de llamadas de su PBX en especial los servicios de larga distancia y celular, con el fin de identificar consumos fuera de lo normal.
- Supervisar continuamente las troncales tanto de entrada como de salida en horas pico y nocturno, con la finalidad de detectar algún cambio fuera de lo normal.
- Revisar la operación del PBX en el horario no laboral, para evaluar la posibilidad de configurar restricciones que permitan evitar llamadas fuera de este horario.
- Colgar o cortar la comunicación cuando ingresen llamadas no identificadas, tales como: mensajes en idioma extranjero, grabaciones, tonos de datos (modem, fax), etc.
- No conectar o transferir llamadas entrantes desconocidas con una línea externa.
- Reportar al oficial de seguridad si se reciben constantemente llamadas sospechosas o se escuchan tonos de marcación al levantar el auricular del aparato telefónico.
- Contratar el soporte técnico con empresas legalmente establecidas, que posean la suficiente experiencia y reconocimiento en el campo.
- Instalar facilidades y funcionalidades solo si se requieren, asegurarse que ninguna pone en riesgo la seguridad del sistema y que ninguna brinde tono de invitación a marcar después de ser activada. por ejemplo, no activar alguna salida de llamadas al exterior después de que conteste la operadora automática o correo de voz

SEGURIDAD EN ACCESOS:

- Proteger la ubicación física del PBX e instalar algún mecanismo con control de acceso. Al sitio tendrá acceso sólo personal autorizado
- En mantenimientos realizados por terceros, validar los datos del personal técnico con la respectiva empresa antes de ejecutarse la actividad programada
- No permitir el acceso a personal externo sin cita previa
- Revisar las tablas de prefijos y cancelar códigos de larga distancia no utilizados
- Los manuales de configuración y documentación técnica del PBX deben ser confidenciales, con acceso únicamente del personal autorizado

SEGURIDAD EN EL SISTEMA:

- Tener bitácora de actividades de mantenimiento, programaciones o cambios al sistema

- Asegurar la calidad y protección de los reportes que genera el sistema (Call Detail Record). Esta información puede ser utilizada para efectos de control, seguimiento e investigación, si se requiere
- Recomendable tener un software tarificador que permita llevar un registro detallado de todas las llamadas generadas desde el PBX
- No activar funciones especiales del PBX que no se vayan a utilizar como la programación de extensiones, buzones de voz, desvío de llamadas, administración remota por MODEM, servicio DISA, etc.
- Deshabilitar el acceso a números con tarifa Premium (número 900)
- Para mantenimiento remoto al PBX se debe establecer con el proveedor fechas y horas específicas para esta actividad; de esta forma confirmar que el módem o equipo utilizado para el acceso remoto sea apagado o bloqueado al momento de finalizar el trabajo
- Configurar el sistema para no permitir que llamadas externas accedan a tono de marcado bajo ninguna circunstancia, ya que esto podría permitir el realizar llamadas no autorizadas
- Bloquear los buzones de voz y servicios que no están en funcionamiento
- Tener todas las salidas hacia larga distancia controladas (troncales analógicas, digitales ya sea que estén conectadas al PBX o fuera de él)
- En caso de activar puertos de acceso DISA (sistema de acceso directo de entrada), asegurarse de que el código de autorización sea de una longitud mayor a 7 dígitos, cambiándolo continuamente, además de tener un control personalizado de los accesos a dicha función DISA
- En ningún momento se deberá activar la función DISA sin códigos de acceso
- El administrador es el único que deberá tener acceso a las contraseñas del PBX
- Corroborar al menos cada 15 días la conexión del tarificador hacia el PBX
- Programar en el software tarificador un monto límite para larga distancia y cuando se sobrepase deberá avisar y/o bloquear la clave o el teléfono
- Si cuenta con enrutadores (Routers) para acceso remoto al PBX vía internet, asegurarse de contar con las medidas de seguridad que eviten que IP ajenas a la empresa puedan accederlos y tomar el control de las llamadas del conmutador

SEGURIDAD EN USUARIOS Y CONTRASEÑAS:

- Definir políticas para la creación y administración de usuarios y contraseñas de acceso al PBX, en especial con las contraseñas definidas para el acceso remoto (en caso de requerirse). Periódicamente realizar una depuración de usuarios, niveles de acceso y extensiones en servicio
- Definir categorías, perfiles y niveles de acceso para cada usuario, con el fin de controlar la administración del equipo y el consumo en servicios como larga distancia y celular. Realizar una revisión periódica de los mismos

- Recomendar a los empleados cambiar periódicamente su clave de larga distancia y de acceso a su buzón de voz, así como la protección de los mismos (no escribirlos en Postit, enviar por correo electrónico, compartirlo con compañeros, etc.)

- Si el PBX permite 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
- Cualquier llamada de larga distancia o a servicios móviles no debe ser permitida a menos que se use una clave con los permisos correspondientes

SEGURIDAD EN SISTEMAS BASADOS EN ASTERISK:

- Contratar la instalación, mantenimiento y actualización del sistema con compañías de tecnología reconocidas y certificadas
- Tener una política adecuada de acceso físico al servidor
- Usar redes privadas virtuales VPN
- No dar acceso desde el exterior si no se necesita. Esto aplica a los puertos UDP 5060 y 4569 (SIP e IAX) y TCP 22, 443 (los más comunes)
- Bloquear los puertos que no vayan a ser usados
- Desactivar los servicios que no use, especialmente servicio WEB. Para verificar los servicios use el comando chkconfig –list
- Si se necesita contar con administración remota del equipo lo ideal es usar un túnel SSH o mejor aún una conexión por VPN
- Para las ocasiones que no se pueda cerrar el protocolo HTTPS para las redes de confianza, agregar seguridad adicional al mismo
- Bloquear los puertos del Asterisk Manager Interface. Usar “permit=” y “deny=” en manager.conf para limitar las conexiones entrantes sólo a hosts conocidos. Aun aceptando llamadas entrantes desde “anywhere” (vía [default]) no se debe permitir a esos usuarios alcanzar elementos autenticados
- Tener listas de Acceso (ACL) para el registro de las extensiones. No aceptar pedidos de autenticación SIP desde cualquier dirección IP
- Evitar utilizar puertos estándares
- No utilizar el puerto por defecto para las conexiones SSH al servidor donde tiene instalada su planta. Esta configuración se realiza en /etc/ssh/sshd_config
- Usar cortafuegos (Firewalls) para filtrar solicitudes entrantes: para proteger el sistema operativo y el servidor de comunicaciones Asterisk, es necesario aceptar sólo las conexiones que sean necesarias y rechazar las demás
- Instalar programas de detección de intrusos. Por ejemplo fail2ban y portsentry para evitar escaneos y ataques de DoS (denegación de servicio)
- Asegurarse que el contexto [default] sea seguro. No permitir que llamadores no autenticados alcancen contestos que les permitan llamar. Permitir sólo una cantidad limitada de llamadas activas pasen por el contexto default (utilizar la función “GROUP” como contador)
- No aceptar usuarios no autenticados: esto se hace estableciendo

"allowguest=no" en la parte [general] de sip.conf

- Establecer el valor de la entrada "alwaysauthreject=yes" en el archivo sip.conf. Esta opción está disponible desde la versión 1.2 de Asterisk, pero su valor por defecto es "no", lo que puede ser potencialmente inseguro. Estableciendo este valor en "yes" se rechazarán los pedidos de autenticación fallidos utilizando extensiones válidas.

De esta forma se dificulta la tarea al atacante para detectar nombres de extensiones existentes utilizando técnicas de "fuerza bruta"

- Crear cuentas de tipo dirección MAC ej: [00FFAA998877], en lo posible evitar las típicas cuentas SIP (extensiones) [100], [200] etc. Esto se hace en el archivo sip.conf. Para facilitar el marcado se pueden usar alias en el archivo extensions.conf en la parte de [global]
- Tener listas de Acceso (ACL) para el registro de las extensiones. No aceptar pedidos de autenticación SIP desde cualquier dirección IP
- Utilizar claves seguras para las entidades SIP. Usar símbolos, números, una mezcla de letras minúsculas, mayúsculas, números y caracteres especiales y al menos 12 caracteres de longitud. La clave se configura en cada cuenta SIP, en el parámetro “secret=”. Cambiar por una clave segura
- Los nombres de usuarios SIP deben ser diferentes que sus extensiones pues esto facilitaría a los atacantes para descubrir nombres de autenticación SIP. Usar mejor las direcciones MAC del dispositivo, o alguna combinación de frases comunes + extensión MD5 Hash (por ejemplo: desde el shell prompt, hacer “md5 -s ThePassword5000″)
- No dejar los usuarios y claves por defecto en las diferentes distribuciones de Asterisk
- Rotar claves periódicamente
- Utilizar claves seguras para cualquier ingreso de administración de la planta, SSH, HTTP, etc.
- De acuerdo a las necesidades de comunicación de su compañía limitar el número máximo de llamadas simultáneas por extensión a 2. Esto se hace agregando o modificando el parámetro call-limit=2 en cada cuenta creada del archivo sip.conf
- Verificar los archivos de logs (bitácoras) del sistema, ubicados generalmente en /var/log/secure y /var/log/messages.
- Poner limitantes no al teléfono sino a la persona que hace uso del mismo, obligando a proporcionar un código que le autorice a marcar a ese destino. Esto se hace con el parámetro “Authenticate()”
- Mantenerse informado sobre vulnerabilidades emergentes, actualizaciones, recomendaciones de seguridad y soluciones propuestas
- Actualizar las distribuciones a la versión más reciente y estable
- Llevar un control exhaustivo del sistema

FACTOR HUMANO:

- Tener política de uso y seguridad del servicio telefónico y difundirla al personal
- Especificar al personal que el teléfono es propiedad de la empresa y que debe ser usado solo para cuestiones de trabajo, no personales
- Los empleados, operadoras o recepcionistas deben saber que nunca deben transferir una llamada fuera de la empresa o institución, también

deben saber que no deben intentar transferir la llamada a una extensión 900 (por ejemplo)

- Nunca aceptar llamadas por cobrar o con costo a terceros sin identificar plenamente al solicitante

En su calidad de usuario y/o suscriptor del servicio y como responsable de la acometida interna y equipos que ésta cobije, le recomendamos seguir las recomendaciones aquí brindadas ya que COMCEL no se hace responsable de los cargos generados por omisión o desconocimiento en la aplicación de controles y buenas prácticas de seguridad, sin que estas se limiten a las que aquí le hemos sugerido.

Finalmente, reiteramos que nuestro compromiso es servirle y en COMCEL seguiremos ofreciéndole el mejor servicio para soportar sus necesidades de comunicación con los más altos niveles de calidad

Atentamente,

Gerencia de Protección Tecnológica – COMCEL S.A.