RECOMENDACIONES DE SEGURIDAD PARA SU CONMUTADOR TELEFONICO
(PBX ó Telefonía IP)

ESTIMADO CLIENTE:

Hacemos de su conocimiento que hemos detectado casos poco frecuentes y aislados de anomalías al hacer uso de las facilidades técnicas que ofrecen los conmutadores y equipos de telefonía IP, mismas que permiten el acceso a través de sus líneas telefónicas, independientemente del proveedor de las mismas, para hacer llamadas de LD nacionales y/o mundiales no autorizadas.

Debido a lo anterior, se le hacen las siguientes recomendaciones de seguridad.

RECOMENDACIONES GENERALES:

- Desactivar todas las facilidades y códigos del sistema que estén configurados de fábrica y habilitar aquellos que 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.
- Contratar el soporte técnico con empresas legalmente establecidas, que posean la suficiente experiencia y reconocimiento en el campo.
- Instalar algunas facilidades, si se requieren como la operadora automática ó correo de voz y asegurar que éstas no pongan en riesgo la seguridad del sistema. Particularmente, ratificar que no se obtenga tono de marcar después de cada activación (por ejemplo, activar alguna salida al exterior después de accionar algún mensaje automático).

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 los password 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/ó bloquear la clave o el teléfono.
- Si cuenta con routers para acceso remoto al PBX vía internet, asegurarse de contar con las medidas de seguridad que eviten que IP's ajenas a la empresa puedan accesarlos 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 los passwords definidos 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 post it, enviar por email, compartirlo con compañeros, etc).
- Si el 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.
- Cualquier llamada de larga distancia ó a celular no debe ser permitida a menos que se use una clave con los permisos correspondientes.

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 ó 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.

Los fabricantes de equipo han desarrollado algunos dispositivos de seguridad, pero depende de las organizaciones asegurar que se obtenga provecho de ellos.

Por último, si el conmutador tiene estas facilidades operando, le recomendamos que sean restringidas o eliminadas definitivamente, ya que **TELEFONOS DE MEXICO, S.A.B. DE C.V. no se hace responsable por lo cargos generados como resultado del uso indebido o fraudulento de dichas facilidades mismos que en su caso deberán ser pagados sin excepción.**

Sin más por el momento, le reiteramos que nuestro compromiso es servirle, quedando a sus órdenes para cualquier duda o aclaración.

TELMEX agradece su preferencia.

RECOMENDACIONES ESPECÍFICAS CLIENTE ASTERISK (CONMUTADOR VIRTUAL IP):

Existen ciertas reglas de aplicación inmediata que eliminan problemas de seguridad, protegiendo al servidor Asterisk de los barridos masivos y los ataques posteriores. Estos métodos y herramientas de protección ya existen, simplemente hay que aplicarlos.

1) No aceptar pedidos de autenticación SIP desde cualquier dirección IP. Utilizar las líneas "permit=" y "deny=" de sip.conf para sólo permitir un subconjunto razonable de direcciones IP alcanzar cada usuario/extensión listado en el archivo sip.conf. Aún aceptando llamadas entrantes desde "anywhere" (via [default]) no se debe permitir a esos usuarios alcanzar elementos autenticados.

2) 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 por defecto su valor es "no", lo que puede ser potencialmente inseguro. Estableciendo este valor en "yes" se rechazarán los pedidos de autenticación fallidos utilizando nombres de extensiones válidas con la misma información de un rechazo de usuario inexistente. De esta forma no facilitamos la tarea al atacante para detectar nombres de extensiones existentes utilizando técnicas de "fuerza bruta".

3) Utilizar claves SEGURAS para las entidades SIP. Este es probablemente la más importante medida de seguridad. Si alguna vez viste programas que generan y prueban claves por fuerza bruta sabrás que se necesita algo más que palabras y números para una clave segura. Usar símbolos, números, una mezcla de letras minúsculas y mayúsculas y al menos 12 caracteres de largo.

4) Bloquear los puertos del Asterisk Manager Interface. Usar "permit=" y "deny=" en manager.conf para limitar las conexiones entrantes sólo a hosts conocidos. Una vez más utilizar claves seguras aquí también, 12 caracteres al menos en una combinación de números, letras y símbolos.

5) Permitir sólo una o dos llamadas por vez por entidades SIP cuando sea posible. Limitar el uso no autorizado de las líneas voip es una sabia decisión, esto también es util para el caso que usuarios legítimos hagan pública su clave y pierdan control de su uso.

6) Los nombres de usuarios SIP deben ser diferentes que sus extensiones. A pesar de ser conveniente tener una extensión "1234" que mapee a una entrada SIP "1234" la cual es también el usuario SIP "1234", esto también facilita a los atacantes para descubrir nombres de autenticación SIP. En su ligar usar las direciones MAC del dispositivo, o alguna

combinación de frases comunes + extensión MD5 hash (por ejemplo: desde el shell prompt, hacer "md5 -s ThePassword5000")

7) Asegurarse que el contexto [default] sea seguro. No permitir que llamadores no autenticados alcancen contestos que les permitan llamar. Permitr sólo una cantidad limitada de llamadas activas pasen por el contexto default (utilizar la función "GROUP" como contador). Prohibir totalmente las llamadas no autenticadas (si es que así lo queremos) estableciendo "allowguest=no" en la parte [general] de sip.conf.