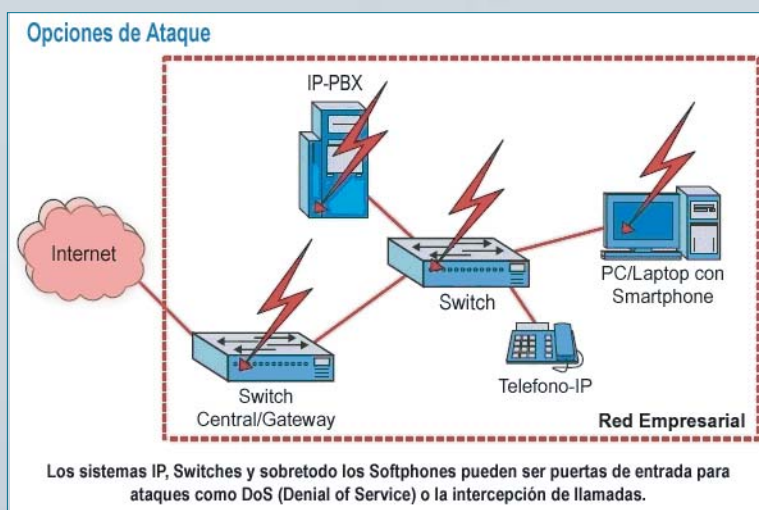


Como hacer aplicaciones VoIP seguras

Este artículo tiene como objetivo mostrar los peligros que corren las aplicaciones VoIP así como las medidas que se pueden tomar para hacer este tipo de tecnología segura sin correr riesgos adquiriendo al mismo tiempo todos sus beneficios.

Imagínese que su buzón de voz está lleno. Desafortunadamente no son llamadas de sus contactos, sino llamadas automáticas que ofrecen por este medio, relojes originales Rolex, medicinas o créditos baratos. Aún es este escenario futurista, pero con la expansión de la telefonía IP podría convertirse el "SPIT" (Spam over Internet




Los mensajes no deseados hacen cada vez más necesario considerar el tema de seguridad en VoIP. Una prueba del interés en este tema es la fundación de la Alianza de Seguridad VoIP (VOIPSA) a principios de este año. Diferentes fabricantes se han unido a este gremio para combatir estos problemas. También los usuarios se preguntan cuales son los puntos de vulnerabilidad en el nuevo mundo de las telecomunicaciones. Existen diferentes puntos en los cuales VoIP da oportunidades de ataque para el abuso o alteración de la comunicación.

Peligros VoIP

Los peligros que se corren con VoIP son de tal manera los siguientes y serán discutidos a continuación:

- ◆ Intercepción de llamadas mediante herramientas del Internet
- ◆ Ataques Denial-of-Service contra el equipo de telecomunicación
- ◆ Uso inautorizado de servicios IP



Junto con el SPIT también se debe mencionar el peligro de que otros individuos escuchen las llamadas. De una forma parecida como en la clásica PSTN, la llamada puede ser escuchada o grabada por personas no deseadas. Para ello sólo se necesita una entrada física al puerto de administración de un switch.

Con alguna de las diversas herramientas que se encuentran sin costo en Internet se pueden grabar paquetes de datos que contengan voz. Mediante un solo clic con el ratón se pueden grabar como archivos de audio. Esto también se podría hacer por medio de un troyano.

Además de esto también existen amenazas de ataques de tipo DoS (Denial-of-Service) que podrían afectar el funcionamiento del Equipo de comunicación IP o la completa red de voz. Esto ocurre al momento que alguien sobrecargue la red mandando enormes cantidades de peticiones o paquetes especiales al equipo. Expertos discuten actualmente sobre el posible peligro que existe al manejar paquetes SIP (Session Initiation Protocol) que no son conformes con la norma. Según algunos comentarios que se encuentran en la lista de correos de la VOIPSA, se recomienda filtrar todo tipo de mensajes que no correspondan con un perfil SIP bien definido para evitar puntos débiles, donde puedan entrar ataques.

Algunos especialistas advierten que terceros dentro de un entorno VoIP pueden entrar a una conversación (Man-in-the-Middle-Attack) para manipularla. También el abuso de los servicios es posible. Esto se hace hackeando el sistema con una identidad falsa, pudiendo así hacer uso de servicios a costos de terceros.

Efectos y Discusiones

Frente a estas opciones de ataque se alarman los proveedores de soluciones de seguridad. Symantec por ejemplo advierte que ataques exitosos pueden paralizar completamente las operaciones de una empresa teniendo como efecto problemas en la cadena de distribución, pérdidas de ganancia o daños de imagen. Uno de sus expertos dice incluso que ningún fabricante se hace cargo de la seguridad en VoIP, si no que más bien están enfocados a que las llamadas se puedan establecer realmente.

Este punto de vista no refleja la realidad. Diferentes fabricantes ya han desarrollado conceptos que consideran el aspecto de seguridad en la telefonía IP. El fuerte interés en estas soluciones es subrayado por la VOIPSA que afirma que diferentes fabricantes ya tienen controlada la seguridad dentro de las redes corporativas.

El instituto de tecnología IDG hizo pruebas el año pasado con diferentes marcas de equipos VoIP. Las pruebas consistían en armar maquetas combinando diferentes equipos para proveer seguridad. Durante tres días se dedicó un grupo de hackers a tratar de interferir con la operación del equipo. Los resultados fueron aceptables. Esto mostró que dependiendo de la configuración del sistema usado, se pueden evitar en la mayoría de los casos intervenciones en la telefonía IP.

Los analistas de Gartner tampoco ven problemas con la seguridad de la telefonía IP. Incluso llegan a considerar que el tema de seguridad en VoIP es uno de los cinco temas de seguridad TI más sobrevalorados del momento. Estos especialistas justificaron su punto de vista con el hecho de que los ataques a los sistemas IP son poco frecuentes y además que los métodos de protección de los dispositivos de telefonía IP se parecen mucho a los disponibles para la telefonía clásica. Uno de los principales analistas de Gartner garantiza que las ventajas de la telefonía IP son mucho mayores que los riesgos de seguridad.

Esta evaluación del riesgo es respaldada por expertos de empresas líderes en seguridad de información que han registrado cada año aproximadamente 4000 nuevas debilidades dentro de Software empresarial, mientras que sólo se han registrado 35 debilidades de seguridad en VoIP desde el 2002. Para discutir sobre la seguridad de la nueva tecnología hay que considerar adicionalmente que los sistemas de telefonía tradicionales también tienen puntos débiles, que pueden ser atacados por terceros. Incluso, hay que considerar que la tecnología de los dispositivos es altamente propietaria, de forma que los sistemas pueden ser muy complicados de manejar y solo poca gente tiene los conocimientos suficientes para ello. Por estas razones, diversos expertos están completamente convencidos que la tecnología VoIP puede ser aún más segura que la telefonía común.

Medidas de Seguridad

Generalmente, los usuarios que quieran implementar VoIP en su empresa deben de considerar algunas recomendaciones. Desde el inicio de la implementación se debe desarrollar un concepto para la seguridad de la telefonía. Para ello hay que dividir el tráfico de datos del de voz por lo menos de forma lógica. Esto se puede hacer por medio de LANs virtuales (VLANs). Esta es una condición para garantizar la requerida calidad de servicio así como la disponibilidad. Adicionalmente se deben de incluir diferentes áreas con mecanismos de defensa contra ataques DoS para evitar la sobrecarga de contenidos dañinos en los segmentos de red.

Para protegerse adicionalmente de oyentes no deseados se eleva la seguridad mediante el uso de VPNs IPsec. Además se recomienda instalar una eficiente solución de acceso y autenticación para el sistema VoIP. De esta manera se pueden evitar los accesos ilícitos. El acceso con fines de administración o mantenimiento debería de ser por IPsec o Secure Shell (SSH). El National Institute of Standards and Technology (NIST) recomienda en su reporte con el título "Security Considerations for Voice over IP Systems" tratar de evitar el mantenimiento remoto y usar solamente interfases físicas al sistema VoIP.

Para garantizar un buen nivel de seguridad en su sistema VoIP se requiere considerar los siguientes puntos:

- ◆ Dividir Datos y Voz por lo menos de forma lógica.
- ◆ Encriptar transmisiones sensibles.
- ◆ Instalar sistemas de acceso y autenticación.
- ◆ Implementar soluciones para evitar ataques de tipo flooding como DoS.
- ◆ Proteger sistema de telefonía IP del abuso de la función de administrador.
- ◆ Cambiar todas las contraseñas estándar de los sistemas VoIP.
- ◆ Evitar el uso de Softphones
- ◆ Mantener el Firmware de los equipos actualizados.

Si uno toma estas medidas de seguridad, entonces ya no hay impedimentos para el uso seguro de telefonía IP en su empresa. Los expertos dicen que todas las empresas que quieren implementar VoIP, no se deben de dejar intimidar por la problemática de seguridad, ya que sobretodo en el entorno empresarial se puede controlar este tema de una forma profesional.

Resultado

Existen problemas de seguridad con la tecnología VoIP de una forma parecida que en el mundo clásico de telecomunicaciones. También aquí se podían interceptar llamadas, efectuar ataques al equipo de telecomunicación y abusar de los servicios de telefonía. Las empresas deben de tomar en cuenta esto y tomar medidas de seguridad para este entorno sin dudar de la implementación de VoIP.

Jalercom S.A. de C.V.



Av. Sor Juana Inés de la Cruz 344 1er Piso
Col. Centro C.P 54000
Tlalnepantla, Estado de México
Tel (55) 55.65.60.55
Fax(55) 55.65.60.55 ext 112
mail: sales@jalercom.com
http://www.jalercom.com