



VoIPstudio White Paper

Garantiza la seguridad de tu servicio VoIP.
Por qué importa y cómo conseguirlo.

Garantiza la seguridad de tu servicio VoIP

Introducción	3
Beneficios de VoIP.....	4
El desafío de la seguridad para VoIP.....	5
La solución de VoIPstudio.....	6
Conclusión	8

Introducción

Los servicios VoIP alojados están en moda y pronto serán el medio dominante para conseguir comunicaciones empresariales eficaces. Según Cavell Group, nos movemos hacia un punto de inflexión de la telefonía alojada: el declive de las soluciones in situ, como las PBX, está a punto de ser superado por la creciente penetración en el mercado de los servicios alojados en el mundo¹.

Gracias a los avances en la velocidad de las redes, su fiabilidad para transportar voz y datos empresariales por las mismas líneas y su mejora de la conectividad, los servicios de VoIP basados en la nube pronto sustituirán a las soluciones tradicionales en la empresa. En pocas palabras, el VoIP alojado se convertirá en el medio dominante para permitir comunicaciones empresariales eficaces.

Por ejemplo, según Cavell Group, el fuerte crecimiento de los últimos 6 meses ha hecho crecer el mercado de VoIP alojado en Reino Unido hasta más de 3 millones de usuarios, convirtiéndolo en líder europeo en este ámbito.

Se prevé un fuerte crecimiento del mercado

La investigación recogida de 94 proveedores de servicios confirma que el mercado ha crecido un 11% en ese periodo, con un millón de usuarios más conectados en los últimos siete trimestres. En comparación, el primer millón de usuarios tardó 3 años en alcanzarse.

Pero no es sólo Reino Unido el que muestra un crecimiento significativo. Francia, Holanda y Alemania tienen ahora entre 1 y 1,5 millones de usuarios cada uno. Cavell predice que el mercado europeo total crecerá en más de 17 millones de usuarios en los próximos 5 años a una tasa de crecimiento (TCAC) de casi el 25%.

Por otro lado, los análisis de la firma IHS Markit muestran una disminución de las licencias de PBX locales, con una caída del 8% comparando 2017 con 2016 (casi 5.000 mill. de euros). El total de líneas de PBX se redujo en un 9% año tras año en 2017, y cada segmento se vio afectado.

La autora del informe y directora senior de investigación de VoIP, UC e IMS en IHS Markit, Diane Myers, culpa el hecho de que las empresas hayan estado postergando las actualizaciones y las nuevas compras, y que el paso continuo a los servicios en la nube esté teniendo un impacto en el mercado.

Tampoco es sólo un signo de reducción de gastos. Según IHS Markit, el gasto de las empresas es saludable, pero se da una baja prioridad a las actualizaciones y expansiones de las instalaciones, lo que sugiere que están cambiando los recursos hacia los despliegues en la nube.

**EL MERCADO EUROPEO
DE VOIP ALOJADO
CRECERÁ MÁS DE
17 MILLONES**

**DE USUARIOS EN LOS PRÓXIMOS 5 AÑOS,
CON UNA TCAC DE CASI EL 25%.**

1. <https://www.cavellgroup.com/cavellvoice/cloud-communications-starting-to-bite-into-traditional-operators-revenues/>

Beneficios de VoIP

Dados sus múltiples beneficios, las empresas buscan cada vez más soluciones de telefonía alojada. Muchas empresas y usuarios se sienten atraídos por el bajo coste. Los servicios en la nube reducen el CAPEX - el coste de comprar, instalar o actualizar un sistema PBX tradicional es mucho mayor que la instalación de un sistema VoIP alojado. De hecho, ampliar o actualizar el hardware heredado para modernizar los servicios suele costar más que un nuevo despliegue completo de VoIP.

Menor coste, mejores características

Muchas soluciones de VoIP ofrecen un paquete de llamadas gratuitas o inclusivas, lo que reduce el OPEX. Las soluciones hospedadas no requieren mantenimiento o actualizaciones, y ofrecen planes de actualización tecnológica gratuitos, que son responsabilidad del proveedor.

Las soluciones alojadas en la nube ofrecen la última tecnología actualizada constantemente, sin coste adicional para el cliente. Ofrecen servicios inclusivos como llamadas en conferencia, mensajería instantánea y comunicaciones móviles, mientras que los trabajadores remotos pueden hacer llamadas en conferencia sin coste adicional. Los mensajes pueden transmitirse a grupos, transcribirse si son de voz y enviarlos por email, para no perder nunca un mensaje o una llamada.

Otros servicios inclusivos son la captura de llamadas, numeración única, recepcionista virtual, mensajería instantánea en el navegador y permitir el uso simultáneo de teléfonos de escritorio y softphones.

Muchas empresas, como los contact centers, necesitan escalar sus sistemas de comunicaciones rápidamente para hacer frente a la demanda. Los servicios VoIP son independientes de los dispositivos y simples de usar, así que se pueden añadir o quitar líneas y usuarios rápidamente. Comparado con los sistemas tradicionales, VoIP también elimina la necesidad de pagar por la capacidad innecesaria. En esas plataformas, las líneas suelen comprarse “por si acaso”, pero sólo se utilizan durante los períodos de máxima actividad.

Mejoras en la eficiencia y la productividad

Otros beneficios incluyen la consolidación de costes, mientras otros servicios se migran a la nube, mientras que los modelos ‘aaS’ ofrecen mayores ahorros de costes y racionalización de los procesos de negocio. Las soluciones de VoIP se integran fácilmente con los CRM, lo que da lugar a una mejora de los servicios de atención al cliente y de la gestión de las llamadas, así como a la opción de “upselling” o prospección.

Sin embargo, el mayor beneficio es que los servicios VoIP alojados pueden aumentar la productividad y la eficiencia de los empleados, al tiempo que proporciona flexibilidad y agilidad empresarial con un menor coste.

“Las soluciones alojadas en la nube ofrecen servicios inclusivos como llamadas de conferencia, mensajería instantánea y comunicaciones móviles, mientras que los trabajadores remotos pueden hacer llamadas de conferencia sin coste adicional. Los mensajes pueden transmitirse a grupos, transcribirse si son de voz y enviarlos por email, para no perder nunca un mensaje o una llamada.”

El desafío de la seguridad para VoIP

Sin embargo, quizás uno de los mayores desafíos que frenan a las empresas a migrar su contenido a soluciones alojadas es la percepción de poca seguridad. Los costes asociados a la protección y defensa contra los ataques han aumentado para todas las empresas, en consonancia con la frecuencia de esos ataques.

VoIP también puede ser vulnerable. Los teléfonos VoIP dependen de Internet, lo que les expone a posibles problemas de seguridad. El coste de recuperación tras un incidente de seguridad puede ser elevado, así que un servicio VoIP barato, pero no seguro, puede resultar caro. Lamentablemente, no todas las soluciones VoIP alojadas son seguros.

¿Cuáles son los requisitos de seguridad para VoIP?

Una solución de VoIP segura necesita protegerse contra amenazas y vulnerabilidades, desde la política de privacidad y las debilidades de los datos, hasta las amenazas técnicas en la red y en los centros de datos. Por ejemplo, muchos ataques se centran en los sistemas operativos de VoIP, protocolos de Internet, o en las interfaces de teléfonos y softphones. Todos ellos son vulnerables al acceso no autorizado y los virus. Además, los ataques de denegación de servicio (DoS) pueden hacer caer sistemas enteros.

En general, las amenazas a la seguridad de la VoIP se pueden dividir en 3 grandes áreas:

1. ¿Puede alguien no autorizado acceder a mi llamada?
2. ¿Están seguras mis redes y dispositivos?
3. ¿Puede alguien no autorizado acceder a mi cuenta?

Algunas de las amenazas de las que las soluciones VoIP deben protegerse, aunque no solo se limiten a estas, son:

- Ataques de phishing: donde engañan a empresas o empleados para que den información confidencial.
- Ataques de denegación de servicio.
- Falsear la identificación de llamadas. Los hackers hacen llamadas y suplantando otra identidad.
- Secuestro de llamadas - las llamadas son desviadas a diferentes lugares o son "escuchadas" por personas ajenas al negocio.
- Robo de servicios: los hackers irrumpen en las cuentas de empresas o empleados y dirigen el servicio a otro lugar, mientras bloquean el acceso del usuario a su cuenta.
- Malware - los hackers descargan spam o malware en los dispositivos locales a través del software de VoIP.

La seguridad es tan esencial para los servicios de VoIP como para cualquier otra aplicación empresarial. Los costes asociados a un ciberataque aumentan cada año.

Un informe reciente de Accenture encontró que las empresas se enfrentan a una media de 130 brechas de seguridad al año, y un coste medio de resolución de esas incidencias de 7,5 M€ en Reino Unido y de 15,5 M€ en EE.UU., para empresas de todos los tamaños².

Por supuesto, no todos son ataques a los servicios y sistemas de VoIP, pero según un informe del Grupo de Inteligencia de Seguridad de IBM, el 51% de sucesos de seguridad analizados en 2016 fueron ataques que utilizaron el protocolo de iniciación de sesión (SIP)³ de VoIP.

Es una extrapolación fácil para entender los costes asociados con los ataques de VoIP - claramente en el rango de millones de dólares.

Como conclusión, la seguridad debe ser un criterio de selección clave al elegir una solución de VoIP. ¿Qué factores garantizan la seguridad de las soluciones de VoIP?

La seguridad de VoIP tiene su propio conjunto de desafíos además de los problemas de seguridad propios de las redes de datos. Además de las vulnerabilidades de los centros de datos, las amenazas a la seguridad de VoIP se extienden a los softphones, los clientes móviles, los puestos remotos y a menudo a los proveedores y trabajadores temporales, que tienen su propio conjunto de desafíos vinculados a la negligencia de los empleados.

Como tal, la seguridad de VoIP requiere un enfoque por capas que incluya datos, dispositivos, redes, aplicaciones y personas.

2. https://www.accenture.com/t20171006T095146Z__w_/us-en/_acnmedia/PDF-62/Accenture-2017CostCybercrime-US-FINAL.pdf#zoom=50

3. <https://securityintelligence.com/hello-youve-been-compromised-upward-attack-trend-targeting-voip-protocol-sip/>



La solución de VoIPstudio

VoIPstudio es una plataforma de comunicaciones alojada en la nube, con una sólida infraestructura que permite conexiones flexibles y seguras dondequiera que estén los usuarios. La seguridad es nuestra prioridad y adoptamos un enfoque múltiple para garantizarla. Nos dedicamos a proporcionar un servicio resistente y seguro, y como tal, nos adherimos a todas las principales regulaciones y normativas de aplicación. Realizamos pruebas, escaneos y auditorías regulares en nuestra infraestructura, y proporcionamos a nuestros clientes información transparente con respecto a nuestras políticas de seguridad y privacidad.

Nuestra red, sistemas y aplicaciones están totalmente protegidos. Por ejemplo, toda la conectividad a nuestras redes o servidores que albergan los datos de los clientes se defiende con mecanismos de seguridad como IPsec, Seguridad de la Capa de Transporte (TLS) y Seguridad de la Capa de Transporte de Túnel (TTLS), proporcionando una fuerte encriptación y autenticación en las redes de VoIP.

La seguridad de VoIP requiere prácticas culturales y procesos de apoyo claros, comenzando desde casa, nos aseguramos de que todos nuestros empleados se adhieran a los procesos definidos por la empresa y a los registros de auditoría para garantizar la integridad de las cuentas y asegurar que no haya accesos no autorizados a los datos. Realizamos escaneos de seguridad mensuales y llevamos a cabo una auditoría regular de la infraestructura para el cumplimiento de la PCI. Realizamos pruebas de vulnerabilidad contra los vectores de amenazas y ataques para detectar cualquier vulnerabilidad de seguridad en los procesos de pago, evitar los ransomware y otras amenazas.

Esto ha dado lugar al establecimiento de las siguientes normas y procedimientos de vigilancia de seguridad y cumplimiento interno:

- Normas y procedimientos de seguridad de la organización definidos y documentados.
- Todos los empleados y contratistas deben firmar un acuerdo de confidencialidad.
- Verificación de antecedentes de todos los empleados que tienen acceso a los datos de los clientes.
- Acceso restringido a empleados que necesiten gestionar datos clientes o administrar los servidores que los alberguen.
- Proceso para eliminar el acceso a datos de usuarios por parte de empleados o proveedores que abandonen la empresa o que ya no requieran acceso.
- Capacitación continua del personal en políticas de seguridad interna y conciencia general de seguridad.

VoIPstudio está también certificado por la Oficina del Comisionado de Información del Reino Unido y cumple con los próximos requisitos de la Regulación General de Protección de Datos de la UE (RGPD), es decir, nuestros clientes pueden estar seguros de que adoptamos y cumplimos las regulaciones actuales y a medida que evolucionan.

Centros de datos, cifrado y alojamiento

La seguridad requiere un sistema y unas operaciones sólidas. Todas las llamadas realizadas a través de VoIPstudio se enrutan a través de tres centros de datos en el Reino Unido, EE.UU. y Japón, proporcionando un mejor enrutamiento y una red robusta con recuperación instantánea de datos en caso de cualquier imprevisto.

Nuestros centros de datos están certificados por la ISO 27001, asegurando altos estándares de seguridad. Los dispositivos de almacenamiento físico emplean los más altos estándares de encriptación de datos, usando AES-256. También utilizamos señalización SIP encriptada TLS y ZRTP para los flujos de voz encriptados de WebRTC.

Los datos de los clientes son compartimentados para evitar el acceso no autorizado. Los datos individuales están protegidos por contraseñas reforzadas que se rotan cada 90 días.

La seguridad física de nuestros centros de datos que albergan los servidores también está garantizada. Todos nuestros centros garantizan la seguridad cumpliendo los siguientes requisitos:

- Las habitaciones están aseguradas por lo menos por dos mecanismos de acceso (acceso con tarjeta/llave al edificio, trampas, personal de seguridad, acceso restringido a la sala, etc.).
- Sólo los empleados autorizados pueden acceder físicamente a los servidores.
- Seguridad 24/7 en cada centro de datos.
- Todas las copias de seguridad de los datos de los clientes se almacenan en el sitio con acceso controlado.
- El sitio admite niveles adicionales de protección, como energía ininterrumpida y supresión.
- Los componentes de almacenamiento que fallan se someten a un procedimiento antes de su eliminación, aprobado por el Ministerio de Defensa.

Contamos con políticas y procedimientos de seguridad oficiales frente a los virus, los programas informáticos maliciosos y las amenazas conexas. Los antivirus están activos en todas las máquinas basadas en Windows, tienen escaneos completos periódicos automatizados y utilizan archivos de firmas de virus actualizados.

Gestión e integridad de los usuarios

Nos aseguramos de proteger la confidencialidad, integridad y disponibilidad de los datos de los clientes. Por ejemplo, a cada usuario se le asigna una identificación única, y el acceso a los datos de la base de datos de VoIPstudio tiene controles basados en permisos que restringen el acceso, según lo determine el propietario.

También se registra cualquier cambio en el estado de acceso de los usuarios. Estos registros se tratan como información confidencial y el acceso a estos informes puede restringirse mediante el sistema de permisos. VoIPstudio también soporta encriptación SSL de 256 bits entre cada componente de la ruta de comunicaciones para la transmisión de datos confidenciales, datos personales o información de autenticación, añadiendo una capa de protección adicional. VoIPstudio permite la seguridad de extremo a extremo, desde el acceso humano hasta la integridad del centro de datos, pasando por fuertes controles técnicos y tecnologías en toda nuestra red, garantizando la seguridad de nuestra solución de comunicaciones VoIP.

Conclusión

Las soluciones de VoIP alojadas se están convirtiendo en el medio dominante para permitir las comunicaciones empresariales. Pero, al igual que cualquier otra aplicación empresarial (alojada o in situ), necesitan hacer frente a un número creciente de amenazas y vulnerabilidades de seguridad. El alojamiento VoIP es vulnerable a los ataques, lo que puede provocar angustia y costes.

La elección de una solución de alojamiento VoIP que pueda proteger contra todas estas amenazas es primordial. Una solución profesional y de calidad empresarial debe proporcionar las garantías de seguridad y la protección que las empresas necesitan.

VoIPstudio le da tranquilidad al garantizar la protección contra la mayoría de las amenazas humanas y técnicas, con una excelente relación calidad-precio. La seguridad es parte integral de la visión de VoIPstudio, asegurando que sus comunicaciones de negocios son seguras, protegidas y que el servicio es totalmente fiable. No sólo permite a las empresas utilizar su presupuesto de seguridad de manera más eficaz, sino que también hace su vida más sencilla.

Notas

1. <https://www.cavellgroup.com/cavellvoice/cloud-communications-starting-to-bite-into-traditional-operators-revenues/>
2. https://www.accenture.com/t20171006T095146Z__w__/us-en/_acnmedia/PDF-62/Accenture-2017CostCybercrime-US-FINAL.pdf#zoom=50
3. <https://securityintelligence.com/hello-youve-been-compromised-upward-attack-trend-targeting-voip-protocol-sip/>

VOIP \ STUDIO

comercial@voipstudio.es

Tel (ES): +34 919 019 100

Tel (MX): +52 55 4166 2992