Qualquer empresa moderna que usa um sistema telefônico de Voice over Internet Protocol (VoIP) sabe que manter a segurança é essencial para a confidencialidade, a confiança do cliente e a conformidade regulatória.

Setores como o de saúde, por exemplo, têm regulamentações rígidas que regem as comunicações, e os provedores de VoIP compatíveis com HIPAA oferecem ferramentas de segurança, privacidade e gerenciamento de acesso para ajudar as empresas a seguir essas regulamentações, mesmo quando os funcionários acessam a rede de locais distantes.

Enquanto isso, criptografia e segurança deficientes também podem afetar seus resultados financeiros, pois golpistas e fraudadores encontrarão maneiras de explorar pontos fracos para cometer fraudes de VoIP em sistemas telefônicos não seguros. A fraude tarifária funciona sequestrando o sistema telefônico de uma empresa para fazer chamadas de longa distância artificiais e de alto volume. O proprietário do sistema é cobrado por essas chamadas (muitas vezes sem perceber), e então os fraudadores recebem uma parte da receita proveniente de serviços de operadoras coniventes.

Junto com a fraude tarifária, existem muitas outras vulnerabilidades dos sistemas VoIP – mas se você estiver usando um dos melhores serviços telefônicos comerciais, seu fornecedor assumirá as partes desafiadoras da segurança e criptografia VoIP. Basta promover a segurança básica da rede na sua organização (senhas fortes, controle de acesso, etc.).

O que você vai ler:

Bons provedores lidam com segurança e criptografia VoIP

Um serviço VoIP hospedado é uma solução de comunicação baseada em nuvem que oferece chamadas de voz e mensagens seguras pela Internet.

A beleza desses serviços é que a segurança e a criptografia estão integradas. Os provedores de VoIP atualizam software e firmware, mantêm hardware e ajudam a seguir a conformidade regulatória para você.

É claro que fraudadores e golpistas estão constantemente evoluindo seu jogo, mas os

provedores de VoIP respondem a esses ataques em tempo real e mantêm seu sistema protegido contra as ameaças mais recentes.

Com um serviço VoIP hospedado, seus funcionários têm credenciais de login individuais para acessar suas contas VoIP, e todas as chamadas feitas pela sua empresa passam pela rede do provedor de serviços. Isso significa que o provedor de VoIP cuida da segurança e da criptografia durante o roteamento das chamadas, não você.

Isso também significa que sua empresa é mantida segura, não importa onde seus funcionários estejam, porque um serviço VoIP permite que eles acessem a rede de comunicação segura a partir de qualquer softphone. Seus funcionários também não terão a tarefa de realizar nenhuma tarefa extra relacionada à segurança, pois os serviços VoIP aplicam as medidas mais recentes em toda a rede. Muitas das dores de cabeça envolvidas com a segurança do trabalho remoto agora estão totalmente fora de seu controle.

O que um provedor de VoIP seguro deve ter?

Um bom provedor de VoIP deve ter protocolos de criptografia robustos para manter seus dados seguros enquanto estão em trânsito. Dessa forma, as chamadas de voz e mensagens ficam indecifráveis até chegarem ao destino, onde somente o destinatário poderá decodificá-las.

Da mesma forma, um firewall com estado e/ou sistema de detecção de intrusão ajuda a prevenir ataques e acesso não autorizado. Medidas aprimoradas de segurança de login, como autenticação multifator (MFA) e autenticação de dois fatores (2FA), por exemplo, acesso mais seguro e um sistema de senha e token também podem ser uma medida eficaz contra infiltrações indesejadas.

As seguintes tecnologias ajudam os provedores de VoIP a proteger suas redes:

- **Controladores de borda de sessão (SBCs):** Um SBC atua como o guardião da rede, regulando o fluxo de comunicação IP. Os SBCs são particularmente úteis para proteção contra ataques de negação de serviço (DoS) e DoS distribuído (DDoS).
- **Segurança da camada de transporte (TLS):** Os protocolos TLS usam criptografia para proteger a sinalização e os canais de mídia de uma rede VoIP. Os protocolos TLS usam um handshake digital para autenticar as partes e estabelecer comunicações seguras.
- **Protocolo de transporte seguro em tempo real (SRTP):** SRTP é uma medida de criptografia de mídia que atua como um certificado de autenticidade, que pode ser exigido antes de conceder acesso à mídia.

Nem todas as organizações exigem SBCs, mas qualquer pessoa que use um sistema telefônico em nuvem pode ser alvo de um ataque VoIP DDoS. Trabalhe com seu fornecedor para implantar um sistema telefônico VoIP preparado para o futuro que siga as melhores

práticas de arquitetura de segurança de rede.

A indústria de VoIP possui padrões e estruturas para orientar as empresas com as melhores práticas de segurança disponíveis. Na verdade, a Organização Internacional de Normalização (ISO) publica diretrizes que abrangem este setor.

Um bom fornecedor deve ter os seguintes credenciamentos e certificações:

- **Conformidade com PCI:** A conformidade com PCI é um padrão de segurança da informação para pagamentos com cartão. Ter esta certificação facilita pagamentos seguros dos principais cartões de crédito.
- **ISO/IEC 20071:** Este Sistema de Gerenciamento de Segurança da Informação (SGSI) descreve um conjunto global de padrões que ajuda a proteger os dados de negócios.
- **ISO/IEC 27002:** Este Código de Práticas para Controles de Segurança da Informação descreve os controles e as melhores práticas para proteger as informações.
- **ISO/IEC 27005:** Esta certificação refere-se ao Gerenciamento de Riscos de Segurança da Informação. Ele fornece diretrizes para avaliar e gerenciar riscos de segurança da informação.
- **ISO/IEC 27017:** Isso estabelece protocolos para provedores de serviços em nuvem. Ajuda a proteger explicitamente os serviços em nuvem e seus ecossistemas.
- **ISO/IEC 27018:** Isto descreve como proteger informações de identificação pessoal (PII) em nuvens públicas.

Os provedores de VoIP seguro também precisam estar cientes de sua segurança na camada humana. Muitos golpes se originam de erro humano, portanto, uma empresa só estará segura se seus funcionários forem confiáveis. Como tal, as empresas são vulneráveis a ataques de engenharia social.

Engenharia social é o processo de manipulação de indivíduos para que forneçam informações confidenciais. Em vez de confiar em vulnerabilidades técnicas, muitos golpistas usam a psicologia humana para obter senhas, detalhes de login e outras informações confidenciais.

Os golpistas costumam usar técnicas de phishing para ganhar confiança. Essa técnica envolve o envio de mensagens e e-mails que parecem legítimos, levando os indivíduos a revelar senhas ou novos detalhes de login após confiarem na legitimidade da fonte.

Os provedores de VoIP podem limitar as oportunidades de engenharia social implementando 2FA ou MFA como parte dos fluxos de trabalho de autenticação IVR. Simplificando, quanto mais etapas de autenticação forem necessárias, mais informações um golpista precisará extrair, e quanto mais informações um golpista precisar extrair, menores serão suas chances de infiltração.

A formação e a sensibilização dos funcionários são também factores críticos na redução dos ataques de engenharia social, uma vez que a monitorização dos padrões de comunicação e a

identificação de irregularidades podem erradicar as tentativas de engenharia social antes que ganhem qualquer força.

Para combater essas medidas e educar ainda mais os funcionários, Udemy, Coursera e edX oferecem cursos de segurança cibernética que incluem módulos de engenharia social. Da mesma forma, Black Hat e DEFCON incluem workshops sobre a relação entre psicologia e segurança.

Segurança e criptografia de VoIP auto-hospedado são um desafio

Algumas empresas optam por hospedar seu próprio servidor VoIP nas instalações da empresa. Isso traz algumas vantagens, pois a criação de um sistema auto-hospedado do zero oferece mais opções de personalização e controle.

No entanto, vários desafios tornam a hospedagem de um serviço VoIP impraticável para muitas empresas. Essas áreas incluem:

- **Custo:** Configurar um sistema VoIP é caro em relação à assinatura de um serviço existente. Um provedor de serviços VoIP já possui a infraestrutura, o hardware e o back-end necessários em funcionamento.
- **Responsabilidade:** A auto-hospedagem oferece personalização e controle a um custo. Com seu próprio sistema VoIP, você deve atualizar software, gerenciar hardware e solucionar problemas técnicos.
- **Escalabilidade:** Aumentar a capacidade do seu sistema VoIP auto-hospedado pode exigir atualizações de hardware e outras configurações. Você pode conseguir o mesmo aumento de capacidade com apenas alguns cliques usando um serviço VoIP.
- **Segurança e criptografia:** Com um sistema VoIP auto-hospedado, a segurança e a criptografia são de sua responsabilidade. Para muitos proprietários de empresas, isso por si só é suficiente para rejeitar a auto-hospedagem.

Além disso, a auto-hospedagem geralmente só é possível com uma equipe de TI dedicada ou um provedor de serviços gerenciados. Sem ele, sua segurança e criptografia provavelmente não serão tão boas quanto as de um provedor de serviços hospedado — que possui sua própria equipe dedicada a executar os protocolos de segurança mais recentes.

Usar um VoIP auto-hospedado também traz complicações para equipes remotas, pois você deve configurar a rede para acesso remoto e ao mesmo tempo manter a segurança. Esse processo geralmente envolve uma rede privada virtual (VPN) ou outros métodos seguros de acesso remoto.

Deixe os profissionais cuidarem da segurança e criptografia de VoIP

A segurança de VoIP é complexa e está em constante evolução, portanto, a terceirização para um serviço VoIP faz sentido por vários motivos.

Mesmo os provedores de serviços telefônicos VoIP mais baratos fazem o trabalho pesado para você, então não há necessidade de comprar, configurar e manter uma infraestrutura VoIP local cara que ficará obsoleta em alguns anos.

Enquanto isso, segurança e criptografia são os pilares de um bom negócio de VoIP, e a maioria dos provedores de serviços de VoIP terá melhor segurança e criptografia do que soluções auto-hospedadas no longo prazo.

Portanto, a menos que você esteja no setor de telecomunicações e tenha grandes conhecimentos de segurança de comunicação, provavelmente é melhor deixar os profissionais cuidarem disso.