Understanding and Addressing VoIP Security Concerns

VoIP is a comprehensively featured low-cost telephone service that businesses are increasingly using to minimise their hardware investments and leverage cloud-based solutions. At the same time, they need to ensure that their VoIP telephony is secure against call fraud, DoS, malware, viruses and other threats that loom in IP networks. By deploying the system on MPLS VPN and incorporating some custom security tools, the integrity of VoIP can be significantly enhanced.

Security of their data is a major concern for enterprises of all sizes, and IT teams work continuously to detect and rectify vulnerabilities in their systems. Of late, there have been concerns about Voice over Internet Protocol (VoIP) phone systems that can bring security issues for users.

When VoIP was initially introduced, not many were worried about security. Businesses were more concerned about the technology’s functionality, call quality and reliability. Today, when VoIP is a part of mainstream communication technology and is used not only by enterprises but on a majority of personal devices, the security factor has become more critical.

With its infrastructure rooted in traditional Internet protocol (IP) data network, VoIP inherits all of the security vulnerabilities that affect the network. An organisation with VoIP phone systems without implementing security measures faces the risk of its privileged and crucial business conversations getting routed over various ISP networks and Internet backbones.

Call fraud is a major threat faced by enterprises using VoIP. It happens when unauthorised people (known as phone hackers or ‘phreakers’) take over the system to make illicit calls and misuse user IDs, passwords, phone numbers and other information to steal financial information.

Other common threats that can impact a VoIP network and even bring it down entirely include malware, viruses, Denial of Service (DoS) attacks, call hijacking and man-in-the-middle (MITM) attacks.

Safeguarding against vulnerabilities and threats

Given such concerns and their gravity for a business, the question is: how to secure a VoIP setup and keep all information shared through it restricted to authorised users?

Here are some measures that your organisation can take:

**Use Virtual Private Networks (VPNs):** By using a VPN, you create an encrypted tunnel over the Internet through which your business communication, including VoIP traffic and online transactions, pass. A VoIP VPN protects the network and secures it against phreakers.

**Upgrade to Multiprotocol Label Switching (MPLS):** A step ahead of basic VPNs, MPLS adds Asynchronous Transfer Mode (ATM)-like capabilities to the IP network. It creates a private IP network to segregate your voice calls traffic from other traffic types and dedicates bandwidth to a VoIP system for high-quality communication. This implies that instead of letting your VoIP service operate over the public Internet, it creates a dedicated and private circuit connecting you directly to your service provider. The Quality of Service (QoS) that is typical to MPLS secures business-critical voice calls and ensures consistent VoIP performance on the network. Organisations with high call
volumes can boost communication quality by leveraging MPLS. The technique also helps businesses meet their compliance protocols.

**Deploy better ways for authentication:** VoIP systems are secured by usernames and passwords. However, password authentication can be weak and may get exploited by hackers. A different mechanism for security known as Challenge Handshake Authentication Protocol (CHAP) employs a three-step process to check the authenticity of a person trying to make a VoIP call. It prevents fraudulent calls by allowing access only when encrypted messages coming from both the sides match. Leading hosted VoIP vendors offer such solutions to businesses.

**Use antivirus software, patches and upgrades:** VoIP systems have softphones that are vulnerable to malware and viruses. Do not forget to take antivirus safeguards in the form of unified threat management (UTM) software if you are using a VoIP service. By subscribing to UTM, you get critical security functions comprising antivirus, intrusion detection and prevention, firewall and anti-spam systems to keep your VoIP and other Internet-based applications secure.

Like other software systems, VoIP applications also need periodic maintenance, security updates and patches. These should be arranged for by the service provider.

**Implement Deep Packet Inspection (DPI):** DPI helps VoIP vendors to check for and block any threatening or unauthorised data from creeping into the network. It can also help to enhance network performance and avert peer-to-peer abuse that can occur due to fraudulent use of VoIP.

In addition to taking such preventive measures, it is also good to monitor VoIP network in real time. Your service provider can offer custom tools for such processes.

As a leading brand offering connectivity and communication solutions for businesses, Tata Tele Business Services provides the MPLS VPN and threat management tools that you need to streamline and secure your VoIP system. Please call us on 1800 266 1800 if you wish to know more about these packages.