9 Tips to Secure Your Unified Communications System

The voicemail hacking scandal at News of the World has led many people to wonder about the security of their own voicemails and phone calls. Voicemail hacking is possible with some technical skills and caller ID spoofing – especially if the user doesn't take the most basic step of using a password to protect their voicemail account. Organizations should follow best practices to protect the privacy and security of their unified communications (UC) systems.

- **Enforce strong passwords.** Don't let employees use common passwords like "123456" or "iloveyou." Many people choose simple passwords, despite the glaringly obvious risks. Make sure your organization follows best practices for choosing strong passwords: between 8-14 characters long with a combination of lower and upper case letters, numbers, and a special character. However, remember not to make the password requirement too burdensome, or they'll just write it down on a sticky note and paste it to their screens.

- **Use firewalls to protect the corporate network.** Protecting the UC system means first protecting the network with defenses including firewalls, intrusion prevention/detection (IDP), and in some instances session border controllers (SBCs). Firewalls prohibit unauthorized traffic from entering or leaving the network, which protects the organization from external attacks. IT can create rules to control what types of applications and traffic are allow to pass to the internal network. An IDP is another layer of protection, as it can block malicious traffic and help protect against denial-of-service attacks, worms and Trojans. If you use an IPS, make sure it provides protection from application-level VoIP attacks.

If your organization uses SIP trunks to connect to the wide-area network, then you should also use a SIP-capable firewall or an enterprise SBC. With a SIP-capable firewall or an SBC, IT can maintain control over what traffic can travel between the LAN and the outside world.

- **Protect against eavesdropping.** Unscrupulous employees or outsiders may eavesdrop on key employees' VoIP conversations, which could lead to the exposure of confidential information. IP voice should be protected against unauthorized recording, playback and other forms of electronic snooping. When protecting sensitive communications, you should demand 128-bit media encryption, which is the strongest protection against electronic eavesdropping and replay attacks and SSL/TLS to protect instant messaging sessions.

- **Prevent service fraud and thefts.** Service thefts are a well-known threat to telecom managers, as people may try to break into the phone system to make hundreds of costly international calls. You can take steps such as using strong passwords, limiting the redirection of incoming calls to outside numbers and using call detail reporting to monitor and log international call activity.

- **Use VPNs to protect remote workers.** Many remote workers use the public Internet to connect to corporate headquarters. It's key to secure this connection so that communications cannot be snooped. Organizations can use a VPN Concentrator to connect remote IP phones to the rest of the system. Remote workers simply connect an IP phone to a broadband router and, with minimal effort, a secure tunnel is established to the VPN Concentrator. Once connected, the phone acts as if it was located in the office—and the connection is secure.

- **Prioritize voice over data traffic.** Organizations can use a variety of bandwidth management methods to ensure that bandwidth is readily available for time-sensitive voice communication and collaboration. Organizations can use virtual LANs (VLANs) to separate voice traffic from data traffic, which improves both performance and security. With some solutions, VLANs can be set up automatically, which saves time. In a larger or multi-site network, you may consider using quality of service (QoS) to prioritize voice traffic over data traffic. Traffic shaping can be used to allot bandwidth to specific applications, so even if the network is under attack, there is still bandwidth available for voice traffic.

- **Pay attention to physical security.** Physical security is your first line of defense, but it is often overlooked. Your buildings, data centers and wiring closets must be locked and secured and accessible only by authorized personnel.

- **Perform regular security maintenance.** Perform regular patching and keep security protections up to date all systems, including desktops, laptops, and servers—as well as the UC system itself. Administrators can use the Web-based ShoreTel Director to manage all voice applications across all locations. Multiple levels of administrative privilege are permitted, which for example allows day-to-day access for administrative staff while a few key personnel have complete system access.

- **Consider the security architecture of the platform.** Security should be built into the system architecture with an embedded system platform, distributed intelligence, and network-independent call control. Look for software that runs on a hardened appliance that has no moving parts other than a fan. If you're looking for system that can deliver 99.999% availability then we should talk. Call control is distributed, with no single point of failure. Voicemail and automated attendant are also distributed in the Voice Switches as well, which provides remote survivability.

To learn more or schedule a meeting call 330.335.7276 or email the BCS Team.