

Secure VoIP: Deciding What Protection Level is Best for Your Organization

As with any data network, VoIP has its own security vulnerabilities that need to be addressed. There are many sophisticated security options available to protect your VoIP network, but there will be an impact in terms of internal process and cost expenditure for each level of security that you add. The goal of this article is to provide a roadmap to deciding what level of VoIP security is right for you.

The first thing to consider is the direct physical access to your network. Most security threats to businesses are internal in nature. Disgruntled employees or any non-authorized persons entering the building present a threat of someone actually tapping into your physical network. Therefore, you should always take security measures to keep your server room and other sensitive areas locked down. What you must decide is how much to spend on such measures. In some cases, a simple lock may suffice. But if you're really concerned about your level of vulnerability, advanced measures such as biometric access may be necessary.


Network Security

Microsoft Windows is the most widely used network in the world for business applications. As such, the overwhelming majority of malevolent entities target this system. Switching to another platform reduces your risk by the simple fact that you are removing yourself from the hacker's crosshairs. VXWorks, an industrial-quality platform found in everything from automotive applications to pacemakers, would be a good choice to greatly reduce your risk. But of course, switching your entire operating system is a major investment in time, expense and labor.

There are simpler security measures that you can employ within the Microsoft Windows framework, but each can have an impact on the overall usability of your network. One common solution is to block Port 80 on your router. Since Port 80 is responsible for HTTP access, blocking this port cuts off the attacker's ability to access your network and any configuration screens. But now you've also cut off access to important applications, such as Microsoft Exchange and WebEx, to legitimate employees who may need it.

Some companies deploy Virtual Private Networks to keep their remote users off the public Internet system. They may also employ remote user verification devices such as biometrics or remote security keys with randomly generated passwords. But all of these methods limit where the user can access the system, how long it takes to access the system, and what features that users have access to. Not to mention that VPN typically costs about 10% more per station than a non-VPN network.

A simple cost-effective change that you can make is to set up two separate virtual LANs (VLANs) to run your data and voice networks. Even though there are possible attacks in a VLAN-based network, good VLAN security practices such as removing VLAN1 (default) and not using DTP (Dynamic Trunking Protocol) will prevent someone from accessing your data network from the voice side, and it's an inexpensive solution to put into place. Most equipment today already support VLANs, and unless you



wish to remotely access your data network via phone, there's really no reason not to setup a VLAN infrastructure.

Phone Security

One final consideration is the deployment of phones to any public areas, such as your main lobby. Many IP-enabled phones today have two external jacks, one for the network cable, and one where a PC or laptop may be plugged in. Use your L2/L3 Switch's port security or other features to block packets from the PC/laptop connected to the phone. Otherwise, anyone could walk up, plug in, and access your network.

Securing VoIP: The Balanced Equation

So how can you determine the right security mix, balancing protection with smooth workflow and affordable cost for your organization? We recommend an examination of three different elements to get a complete picture of what will work best for you. First, perform a security analysis to determine the kinds of information that may be passed across your VoIP system, and then look at the overall impact to your company if that network were to go down due to a virus or worm attack. Second, perform a usability analysis to look at the impact that additional security measures will have on your internal processes and the frustration level of your employees. Finally, perform a traditional cost/benefit analysis to determine the real implementation cost of putting additional security measures into place. By looking at all three elements together, you can start to get a true sense of what extra VoIP security measures you realistically need to put into place.

VoIP communications security is a combination of sophisticated technology and specific setup configurations, and some basic common sense. Your VoIP vendor should be able to provide guidance as you move through this process and help your organization gain the right level of protection that it deserves.