

VoIP: Balancing the Security Equation

VoIP, with its packetized transmission of voice, raises the security bar above the relatively easy-to-access TDM platform. But as with all data networks, it is not completely airtight. There are many sophisticated security options available to secure 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.

Here are a few examples: Microsoft Windows is the most widely-used operating system 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. Linux is an operating system in the unique position of offering robust security inexpensively. VXWorks, and industrial-quality platform found in everything from automotive applications to pacemakers to the space shuttle, is a bulletproof operating system for embedded applications. But of course, switching your entire operating system is a major investment in time, expense and labor.

There are far 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 ports on your router. This cuts off the attacker's ability to access applications on the network. But now you've also cut off application access to legitimate employees who may need it.

Some companies deploy Virtual Private Networks (VPN) to tunnel their remote users through the public Internet. They may also employ remote user verification devices such as biometric systems 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.

VoIP Security: The Smart Approach

So what's the right answer 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 network, and then look at the overall impact to your company if that network were to go down due to an attack—Denial of Service (DoS), virus, worm, etc.. 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.



Is all of this worth it?

Yes. Deploying VoIP for your voice communications can definitely offer benefits offsetting the additional security requirements. All of the steps listed above are simply to lockdown your network for voice traffic.

VoIP is based on technology that converts voice into data packets that are in turn sent over your network along with conventional corporate data. In order for a conversation to be intercepted, an intruder first must gain access to the local area network. The intruder must then hope the VoIP vendor uses a standard compression algorithm that he has the ability to decode. Keep in mind, one voice packet will only have a fragment of an actual conversation. Unless someone can intercept and decode all of the packets, the possibility of corporate espionage is remote.

Now compare this against a traditional TDM network. It's true that TDM is a closed circuit-to-circuit system. However, if someone does tap into the system trunks they will have access to every outbound conversation in an entire building. And they will need a comparatively simple level of technology in order to do it. When you look at the complexity involved between breaching a TDM system or breaching a locked down, secure VoIP system, VoIP quickly becomes a very attractive option. And once you've performed a proper analysis of your security environment, you may find that a firewall and basic VPN access for remote VoIP users are all you need to keep your system protected. After all, VoIP is only as secure as the data network.