Pipeline Knowledge is Power.

VoIP Security - Is It Really an Issue?

By Chris Thatcher

Consumer exposure to threats in the data world have consistently and exponentially grown over the past five years – a fact reinforced in the media each day, with reports of breaches in data security at lending institutions and retail outlets nationwide. The number of vulnerabilities grows daily, as does the simplicity of pre-packaged hacker tools. The potential loss of revenue or a tarnished reputation in the event of compromise is high.

Though there have been no major threats to date to VoIP security, the multitude of security threats that plague today's data networks will be inherited by VoIP infrastructures down the road. The addition of VoIP as an application on the network makes those threats even more dangerous. For example, a distributed Denial of Service (DoS) attack may slow down someone browsing the Web, but on a VoIP network this same attack could prevent 911 calls. Other potential breaches include: spam calling (SPIT), tapping into calls, viruses, user identity management issues, and of course the unknown.

If the right steps are taken, VoIP can be made as secure -- if not more secure -- as its traditional counterpart. However, when it comes to securing VoIP networks, the traditional business mentality has been to focus on "probable," near term security issues. Then, if there is budget left, businesses are considering the "possible." Companies currently view many vulnerabilities as "too complex" or "too unlikely" to spend money on.

Improving VoIP Security

Waiting to secure a VoIP infrastructure is not only dangerous from a security perspective, but it is also more costly. Proper security for VoIP can change the logical topology and the bill of materials in network configuration. It requires tuning and changing controls that could temporarily affect voice services. For these reasons it is best if an organization can begin by building security into initial VoIP deployments rather than bolting it on afterwards.

The key to success is making security a priority and working with a vendor and/or solutions provider that offer an integrated, end-to-end approach to converged network security that includes the following components:

- Establish trust zones by segregating the converged network from the data-only network—either physically or through virtual LANs. Segregating the voice traffic onto separate networks and enforcing the separation will limit access from both internal and external users.
- Apply the same defense-in-depth strategy you would with any business critical network. The extended perimeter must be protected with multi-layered solutions such as firewalls, network and host based intrusion prevention, anti-virus, encryption, and more.
- Stop many attacks before they enter the network with network intrusion prevention. Be sure to protect the call manager and voice gateways as well.

So Whose Problem is it?
Lack of awareness and flawed implementations are perhaps the biggest VoIP security threats -- as they are for any technology implementation. When enterprises move to replace legacy PBX systems with VoIP, they tend to look for performance and quality of service (QoS) first, thinking of security as an afterthought, if at all. This is a mistake: telephony is a business-critical application, and any insecure converged network represents a significant security risk. Mis-configurations, partially completed implementations, and not abiding by known standards of risk mitigation will be attributed as the cause of most compromises.

Service providers are in a virtual land grab for VoIP market share. As a result, the risks are often overlooked and security is rarely even mentioned in most service descriptions and FAQs about service offerings. It is important for service providers to look into potential risks and address them, and for enterprise and government organizations looking for VoIP services to ask questions. Subscribers and prospective subscribers should not only be asking about service availability, but also about what steps the service provider has taken to secure that service.

There is no sole owner of responsibility here. Vendors must secure their applications and platforms and provide guidance. Governing bodies must provide leadership, and those who implement must be sure to abide by guidelines and continue to develop and brand secure solutions. End users are also responsible for educating themselves and buying the products and services from the vendors who have the best security postures for their solutions.

As converged networks grow in strategic importance, concerns about security should be top of mind for vendors and customers. As long as security is given utmost importance, VoIP systems can be made at least as secure as PBXs and the public switched telephone system.

Bottom Line

Security risks in VoIP networks are real, and network architects need to understand that a single attack to a VoIP network can simultaneously shut down both data applications and phone service, causing significant impact to business. Companies need to take responsibility for securing their VoIP networks today.