4 Cloud-Based Phone Implementation Errors that Lead to Security Risks

2016-08-17 - Tom Collins - Comments (0) - Blog Posts



Is your cloud-based phone system at risk?

Consultant Fatih Ozavci cites "botnets, malware distribution, vishing, denial of service attacks, and toll fraud" as risks to organizations with gaps in their security. The problem isn't with the technology, though, it's with a "lack of understanding" that can lead to massive holes in protection.

Another study stated 15% of businesses that haven't yet adopted cloud-based phone services are concerned about security issues. If you're in this category, you'll be pleased to learn that attacks are relatively rare. However, smart vendor selection and proper implementation are crucial to further lowering your risks of being a target.

In this blog, you'll learn the most common hosted phone service implementation mistakes that can lead to vulnerabilities in your business.

Are You Experiencing These Security Gaps

1. Using Default Passwords

Far too many organizations are implementing high-quality networking equipment without changing the passwords from default settings.

Researcher Paul Moore recently discovered this frightening trend when observing a series of VoIP deployments.

Many handsets and other types of equipment come with simple default passwords like "admin", which are designed to be replaced at the time of installation. However, too many IT pros vow they'll "deal with it later" and fail to follow up.

Failing to change default logins to appropriately strong passcodes and usernames can make entry easy for hackers, causing you to be vulnerable to eavesdropping, interception, and other types of attack.

2. Inadequate (or Outdated) Network Security

When you make the switch to a hosted phone service, your voice data will become a component of your Local Area Network. Any existing weaknesses in your network security will become vulnerabilities in your phone service as well. Outdated firewall technologies can be a risk post-implementation.

The solution isn't to implement a hosted PBX and cross your fingers that your firewall is tough enough. The answer is to understand your network and security needs prior to implementation.

The right VoIP vendor has the staff and knowledge to walk new clients through a full-scale network assessment as a add-on service, which will include:

Infrastructure Foundation Assessment

- Review of physical cable infrastructure
- High-level review of physical facilities and HVAC systems

- Inventory of active host IP addresses

Core Network Assessment

- Layer 2 configuration analysis (VLANs)
- Layer 3 configuration analysis (routing)
- Availability of switch ports required for phones
- Overview of IP addressing scheme
- Network traffic patterns and analysis
- Check for **ability** of network devices to provide CoS/QoS
- Review of ability to provide DHCP services
- Ability of wireless infrastructure to support VoIP
- Firewall connectivity relative to VoIP traffic
- Ability of WAN to support VoIP and QoS
- Network management overview

- Review of existing documentation

Scorecard Report

- Scorecard with survey results by area
- Recommendations for remediation efforts
- Vendor best practice guidelines

- Physical reporting of full results

For more information on the technical aspects of a phone migration done right, we recommend *How to Move Voice Services to the Cloud.*

3. Weak Encryption Tools

End-to-end encryption of voice data packets is necessary to avoid interception at any point along the transmission path, which may include your network, your internet service provider, and all points in-between.

Voice encryption is slightly complex, and business needs can vary depending on a number of factors, including the sensitivity of transmitted voice data.

However, Cisco's core recommendations for basic encryption best practices include:

- Balancing encryption with business-specific security needs to keep latency and costs as low as possible.
- Ensuring your vendor enables SIP over TLS security via their switch fabric.
- Using packet encryption protocols such as SRTP.

- Encrypting mobile device calls using VPNs when HTTPs or SRTP is unavailable.

4. Using Public Internet Connectivity

Perhaps the single most common security error is implementing IP-based telephony without considering the risks of your internet vendor. Even exceptional network security and smart encryption practices cannot always

compensate for public internet connectivity risks.

One of the fastest and most effective ways to increase information security is to reduce the "attack surface area."

When using a public internet vendor, your data will be transferred from your company's network and through many other locations before reaching it's final destination. After your voice traffic is transmitted to your public internet vendor's network, it's transferred across the wide-open public internet to your VoIP provider's internet service provider. From there, it's moved to your VoIP providers network. This can maximize the potential points of entry for cyber criminals with intent to intercept or interfere with your data.

In addition, traditional copper cable internet technology is inherently less secure than fiber. Data transmitted over copper can be intercepted through splicing of cables or disrupted with equipment designed for interference.

Choosing a unified business communications vendor who also offers fiber-optic internet services can offer significant business benefits. Avoiding shared public internet resources is favor of bundled, business class services can enable:

- Decreased attack surface and higher security
- Lowered risk for interception and interference
- Higher reliability
- Better quality of service (QoS)

- More consistent data transmissions

Is it Possible to Have an Easy and Secure Cloud-Based Phone Migration

Information security can be highly complex, especially as organizations shift to more complicated business networks. While hosted phone service security and network analysis may seem time-consuming, it doesn't have to be.

The right vendor can walk you through a pre-implementation plan to ensure you have the knowledge and tools to mitigate your risks.

To learn more about Atlantech Online's commitment to best-of-class security for hosted voice and fiber connectivity customers, check out the eBook 10 Questions to Ask Before You buy Fiber, Phone, or Data Center Services For Your Business.