Blog for MPA Networks

https://www.mpa.com/blog.aspx?p=100000-phone-bill-office-voip-phone-system-next-target

The $100,000 Phone Bill:
Is Your Office VoIP Phone System the Next Target?

Posted March 20, 2015

How would you react if your company's next phone bill revealed a major cost spike—to the tune of over $100,000? It's actually happening now to small businesses across the U.S., thanks to international VoIP toll fraud—perhaps the fastest growing cyber-threat today.

While many small companies have adopted VoIP (Voice over Internet Protocol) as a cost-effective alternative to traditional phone service, the trade-off is increased security risks. Primarily in Africa and Eastern Europe—those usual hotbeds of cybercrime—**hackers have discovered that a VoIP-based PBX system (like other online networks) contains multiple vulnerabilities**, which most smaller companies fix only rarely, if ever. Once they successfully hack into a U.S. company's VoIP network, they can literally hijack its entire PBX and begin placing thousands of calls from that company's local office lines—typically over a weekend, when nobody will be there to notice.

Long-Distance Robbery

Who do they call? In most cases, they've leased international phone numbers with "premium" surcharges (think adult chat or psychic hotlines), resell the calls, and rack up the pay-per-minute profits. And unlike a conventional landline, a single hacked VoIP line can dial several hundred calls simultaneously! Do the math; it all adds up to a lot of money, very quickly.

International law guarantees that *somebody* must pay those long distance charges—either the victimized company or their VoIP service provider.

As with so much other cybercrime from the Third World, the chances of U.S. law enforcement tracking down the culprits are slim at best. Meanwhile, the victim faces, at the very least, a major multi-week headache contesting that ridiculously huge bill.

Protect Yourself

Your VoIP phone system should be secured as much as any other network. There are **steps you can take right now** to shield your company from a costly telephone cyberattack:

- Deactivate Call Forwarding, to prevent rerouting calls to third party numbers—particularly those outside the U.S.
- Set strong passwords for central root access as well as every phone line and voice mailbox. Then schedule company-wide password changes every six months.
- Protect your VoIP network behind its own high-security firewall, configured to only accept access from pre-approved IP addresses.
- Consider Secure Shell encryption (SSH) for an added level of security.
- Physically isolate your VoIP system from the rest of your network infrastructure—down to the cables and Ethernet switches. If a lucky hacker can use your phone system as a front door for infiltrating your entire company network, then you've got even more trouble.

The stakes are simply too high for a do-it-yourself approach to VoIP security, or to think "it won't happen to us." Trust an experienced IT partner who not only knows the nuts and bolts of VoIP, but also specializes in cutting-edge network security. Learn more here.