

Securing the PBX – Security Considerations for PBX/Phone Systems

The age of hacking began over four decades ago, but the first ‘hackers’ were far less interested in computers than they were in breaking into phone systems.

Phone hackers (phreakers) broke into phone networks to make free calls. One particular phreak, Cap'n Crunch (real name John Draper) found out that the toy whistle given away inside Cap'n Crunch cereal generated a 2600-hertz signal which was the exact frequency used to access AT&T's long-distance switching system. Of course, the phreaker community grew up and moved on to bigger and better things like hacking computers but they never quite gave up their roots. Which begs the question...

Do you know who is accessing your phone switch and PBX system? If you haven't checked lately, the Office of Information Security (OIS) recommends you do so. In fact, we recommend you expand your regular threat and vulnerability management program to include regularly reviews of your phone system and for unauthorized charges that may occur as a result of a compromise. One agency recently discovered that someone had exploited a simple, yet known vulnerability and hacked their switch, running up thousands of dollars in fraudulent charges. Once they discovered the problem, it was an easy fix and they were able to get the charges removed but the fact that such a common vulnerability even existed is cause for concern. So again, do you know who is accessing your phone switch and PBX system?

A couple of major telecommunications service and hardware providers (AT&T and Nortel) were kind enough to provide some recommended best practices when it comes to reviewing the security of your phone system. OIS recommends that you take the time to read these documents, accept the premise that you may be compromised, investigate, and remediate if necessary. People always seem to forget that a PBX is just a computer. Because it's just a computer, you should harden it just like you do your servers and other computers. If you find a compromised PBX or phone system, the incident is probably reportable so please give us a call and we'll help you work through it.

Resources

AT&T's Recommendations to Secure your PBX/Phone System:

http://www.oispp.ca.gov/government/documents/pdf/ATT_PBX_Security.pdf

Nortel's Recommendations to Secure your PBX/Phone System:

http://www.oispp.ca.gov/government/documents/pdf/Nortel_PBX_Security.pdf