Pipeline
Technology for Service Providers.
www.pipelinepub.com Volume 12, Issue 5

PBX Fraud Detection

By Colin Ayer, Ph.D

Protecting Your PBX and Your Profit Margins

Your telecom costs were already too big for your burgeoning business, but being slapped with a $20,000 bill because you weren't paying attention to abuse of your own telecom infrastructure hurts your profit margins even more. How did they do that and how do you stop it?

As the world increasingly moves toward IP communications and hosted PBXs, VoIP services have become a fertile hunting ground for fraudsters who attack your business, steal your telecom services, and rack up bills you'd rather not pay. This is being done by organized, tech-savvy telecom fraudsters who illegally access your PBX, either by stealing credentials, through an unsecured maintenance port or via an unprotected Direct Inward Dial (DID) account. These fraudsters can then steal expensive long-distance service, re-sell that service to third parties, or just pump their own traffic to an International Revenue Share Fraud number, using your enterprise PBX as a gateway. What makes this type of fraud so detrimental is that it is often discovered long after the fact, alerted only by a highly-inflated phone bill. The criminals are careful to break into your PBX after everyone has gone home for the weekend, and are constantly searching for a new system to tamper with when the next weekend rolls around. VoIP systems like yours are constantly being probed for open ports and other security weaknesses. Perhaps even more damaging are the potential legal ramifications of disputing fraud-related charges with your carrier or other partner, debating over which party is ultimately responsible. This wastes your time and money, and can negatively affect your partner relationship.

Why has this type of fraud increased over the past several years, and why have companies deployed new technology to help fight it? Because the move to VoIP and the global reach of the internet has made it all too easy for the perpetrators to reach and cause damage to enterprises all over the world while also making themselves very hard to track down and prosecute. While the larger carriers commonly have expensive and complex fraud protection systems in place to alert them to fraudulent activity, smaller businesses often use local carriers, which may not yet have been the target of an attack and who probably don't have those sophisticated fraud detection solutions in place. PBX hacking is one of the most popular methods of perpetrating telecom fraud. In 2013, hacking of IP PBXs was used in schemes that siphoned off $3.6 billion of global telecom revenue, with an additional $4.4 billion related to more traditional PBX installations, according to the bi-annual survey from the Communications Fraud Control Association. Unfortunately, legal action isn't always the most effective remedy to combat fraudsters. Attempting prosecution is not only very costly, it is very difficult to find and prosecute criminals who are hiding behind multiple layers of internet redirection across multiple international borders.

So if legal action isn't the answer, what is the best way forward? An ounce of prevention is worth a pound of cure (said Ben Franklin) and there are several simple and effective ways to safeguard both your business and your profit margins:

Make sure your available security features are all turned on

The strength of your security is determined by the weakest link. Go through the entire security chain looking for weaknesses. How did those phones get provisioned? Don't use TFTP which can send unencrypted passwords across your network. How did the passwords get chosen? If your PBX can enforce strict password rules, make sure it does. I bet those phones have a web interface, probably admin/admin will do the trick! Is your local network physically secure? Are you sure? Keep your network infrastructure current with all the latest security updates and patches. Put rules in place on who can call which numbers when. Premium Rate, really? Fraudsters target companies at the weekend when nobody is looking. If your company never calls (pick your favorite expensive per-minute calling destination), then make sure this is noted and alerting rules are put in place.

Insist your teams follow basic security procedures

Your telecom system has all sorts of passwords, for extension registration with the SIP server, voicemail, Web user and administration interfaces. But let's be honest; many people, even the IT guys, often create short and overly simple passwords that are vulnerable to brute force hacking. Or worse, the factory defaults never get changed! That's why a strict password policy is critical. Create long complex passwords that combine special characters, numbers, and upper and lowercase letters (e.g., w#$*&b@!DoT) and enforce regular password changes. When employees leave, immediately disable all telephony-related accounts.

Beware the social engineering capabilities of the fraudster. All those hard-to-remember passwords are stored in central password stores protected by accounts whose password can often be recovered by knowing the answer to a couple of security questions, and you are not always looking too far away for the culprit. An unscrupulous disgruntled employee may know both where you got married and your dog's name.

Fraudsters want your trash, too. There is a treasure trove of information "stored" in your paper waste and even your physical e-waste. Keep "dumpster divers" away with a solid document shredding program in place, using lockable shredding receptacles that are emptied often. Send a trusted employee on a midnight raid of the office to look for all those passwords written on post-it notes and inside notebooks left lying on desks. And don't forget that old router, the one with the VoIP ports, that still has the default admin password that is just waiting for an unsuspecting network to plug into. Always factory-reset any e-waste before you dispose of it.

> *There is little point relying on a compromised network component protecting itself given that the first thing an accomplished hacker will do is disable any protection mechanism.*

Use an application-level call monitor

VoIP telephony is controlled with the SIP protocol, an easy-to-read message-based protocol for managing the establishment, progress and termination of each call. Application-level call monitors look at these packets in real-time to look for unusual traffic that might signal fraudulent activity on the network, both from within (people with late-night access to the office placing expensive international and premium rate calls) and external (the hacker intent on using your network to pump traffic to their dubious International Revenue Share numbers). Look for a fraud protection solution that can process the expected calls-per-second of your network and can apply a number of strategies for alerting you to possible fraud and let you quickly identify that hacked SIP extension or IP PBX in your network.

Look for a solution that works independently of your PBX. There is little point relying on a compromised network component protecting itself given that the first thing an accomplished hacker will do is disable any protection mechanism.

Make good use of firewalls and session border controllers

Many PBXs have built-in SBC functionality, a VoIP firewall if you will, that will focus on enforcing communications policies, managing external traffic, hiding the topology of your internal network and providing denial-of-service protection.

Use offline call record and billing analysis to look for longer-term trends

Locking down the network and getting instant alerts at the first sign of trouble is good; but, for the complete solution, track your call and billing records over time to look for unexpected calls from non-existent extensions to irrelevant destinations.

We will never eliminate telecom fraud entirely. Make one approach unprofitable for the fraudster and they will surely find another one; the only good trick is to try and stay one step ahead of the fraudster. Make sure you have people who know how VoIP fraud works, and the methods fraudsters use. In this environment, no one can afford to be thinking, “this can never happen to me”. It is imperative you implement a reliable anti-fraud solution combined with solid security policy controls including a robust staff training program in order to monitor and protect your business against fraud and significantly reduce the risk of revenue loss.