Protecting Your Business from Telephone Fraud: 5 Things to Watch For

2016-06-14 - Tom Collins - Comments (0) - Blog Posts

Every IT pro's worst nightmare is to suffer an information security incident. Not only can a data breach act as a black mark on your resume, it can devastate your employer's profitability and reputation. The average cost of a data breach resulting from telephone fraud, phishing, or other attack is now $3.8 million, a $0.3 million increase over the past year. In some cases, these figures can be much higher. Target estimates their data breach several years ago cost over $148 million.

Needless to say, information security is a top priority for many IT professionals. A comprehensive approach to network protection should include attention to your voice communications platform. In this blog post, you'll gain insight into the state of voice-over-IP (VoIP) security, as well as a little bit of information on how VoIP stacks up to plain old telephone service (POTS) in terms of risks. You'll also learn the most important signs to watch for if you're monitoring for an attack.

VoIP is More Secure than Plain Old Telephone Service

If you're under the impression that VoIP is automatically a risk because it's not traditional phone lines, stop right there. Phone fraud, which is known as phreaking, has been around for well over 50 years. While publicly-switched telephone networks (PSTN) have improved security since the 1960s and 70s, POTS did not equal security.

Research actually indicates that VoIP users are less likely than their POTS-using peers to suffer an attack. That's right, VoIP isn't as risky. Implementing VoIP could make your company less-likely to suffer from eavesdropping or other forms of attack.

However, it's important to remember that VoIP is exactly as secure as a number of factors, including your network, your vendor, and your implementation measures. By investing in effective firewalls, a trustworthy VoIP vendor, and smart implementation, you can significantly reduce your chances to falling prey to an attack.

Categories of VoIP Threats

Understanding the types of risks can be important to developing an effective monitoring strategy. VOIPSA (Voice over IP Security Alliance) has created the following categories to organize common VoIP threats:

- **Social Threats** – e.g., eavesdropping
- **Service Abuse Threats** – e.g., premium rate service fraud
- **Intentional Interruption of Service** – e.g., Denial of Service (DoS) attack
- **Physical Threats** – e.g., power failure
- **Interception and Modification** – hacker gains full access to the communication signal between two or more parties

Researchers report that, most often, VoIP hackers leave one or more of the following signs in their wake:

- Multiple failed password attempts and registration hijacking
- Abuse of long distance and premium calls
- Failed attempts to log in and make calls (which could possibly lead to unavailability of service to legitimate users)
- Attacks on the application layer

5 Tell-Tale Signs Your Business VoIP Service May Be Hacked

The following signs aren't necessarily indicative that your VoIP served as a gateway for an attack. Some are signs of general security issues, which could indicate that you've fallen prey to phishing or another form of incident. In general, the following are important to monitor for:

1. Call History

Regularly monitoring your call history is a VoIP security best practice. A sudden spike in unusual calls, as denoted by volume or area code, can indicate that you've suffered service abuse and a hacker has successfully gained access to use your system.

VoIP security experts report that criminals may make an enormous volume of international calls or route calls to 900 numbers for the purpose of making money. The majority of VoIP security incidents take place outside of business hours. A single weekend of unusual calls can result in thousands of dollars of charges. Constant monitoring is key. Blocking such activity is a recommended best practice. If you don't need to make 900 number or

International Long Distance calls, block them.

2. Sudden Quality of Service (QoS) Issues

A sudden spike in call delays, cracking noises, or other sound problems may be a red flag. Any drop in VoIP call quality can indicate a number of factors. It may indicate you've suffered a denial of service (DOS) attack, which occurs when an attacker floods the network with large amounts of data resulting in disruption of services.

A massive decline in Internet quality that appears out of nowhere can also be connected to other information security issues, which may or may not be connected to your VoIP security. Depending on your network structure, a high demand for bandwidth that results in poor voice QoS can be the result of criminals exfiltrating a massive amount of data from your network.

3. Fake Antivirus Messages

If your organization has invested in antivirus protection and regular updates, antivirus messages should raise an alarm in your users. If a hacker has gained access to your network through your VoIP system or another point of vulnerability, you could notice a flood of fake antivirus messages. Fake antivirus messages are a general security warning sign that's rarely connected to VoIP, but it's still important to monitor.

All of your end users should be informed that any antivirus messages on any device, from a desktop within your building to a laptop taken home, should be reported to IT immediately for further investigation. Users should avoid using potentially compromised devices, particularly to enter credentials.

4. Activated Hardware

VoIP service isn't limited to just calls made from a handset located on-premises. VoIP service can also encompass calls through laptops or mobile devices and web conferencing. Reuben Yonatan reports that mysteriously self-activated microphones and web cams can be a sign that entry to your VoIP system, possibly though a cracked password, has been completed. However, this can also indicate a general network breach through a different point of entry. Hackers may use microphones or webcams to eavesdrop or visually spy on your operations in the hopes of gathering sensitive information. Any time hardware from a mobile device to a webcam appears to have been mysteriously modified or activated, employees should immediately report it to IT.

5. Strange Internet Changes

Regardless of whether hackers enter your system through your VoIP or another point of vulnerability, changes to your company Internet connectivity can be an early warning sign. Browsers that begin running slowly can point to weird or criminal network activity. Similarly, toolbars that appear without having been downloaded or redirected internet searches can be clear signs of compromise.

How to Protect Your Business from VoIP Hackers

With the right vendor, VoIP security isn't a risk. It's just a component of smart implementation and maintenance. Depending on your businesses risks, needs, and your vendor, you may decide to:

- Block international calling and/or 900 numbers
- Monitor traffic regularly
- Educate end users on suspicious signs to watch for
- Enforce effective password policies
- Adopt adequate firewalls
- Utilize encryption tools
- Implement a segregated VPN

How to Improve Your Voice Security

If you're currently using analog or PRI service or a VoIP vendor with poor security, it may be time to consider making the switch. While VoIP is typically more secure than traditional phone systems, a sloppy implementation can leave your organization vulnerable to attack.

Atlantech Online has invested in a culture of secure VoIP for business communications customers. This includes a best-of-class approach to implementing VoIP technology, with specialized attention to a customer's unique risks. It also involves investment in cutting-edge tools for automated monitoring of risks 24/7. This dedication to security isn't the cheapest way to do business, but it's how we do right by our customers. To learn more about Atlantech's secure VoIP services, click here.