VoIP Security Risks: Is the Back Door to Your Business Wide Open?

VoIP hackers are busier than ever these days, and it appears no business is too big or too small for their destructive reach, including yours.

According to the 2020 Annual Internet Crimes Report, released by the FBI and the Department of Homeland Security, malicious cyberattacks are on the rise against established companies' telecommunications systems, causing massive disruptions and billions of dollars in revenue losses.

VoIP (Voice over Internet Protocol) is rapidly becoming the new standard for commercial phone systems and has already been adopted by the majority of modern businesses. For folks all around the world, conducting business over the phone has never been easier, clearer, or more streamlined. But is it safe?

With their extensive capabilities and integrated networks, these digital phones may save both time and money. However, due to their increased internet connectivity, VoIP networks are potentially more vulnerable to security breaches than traditional telephone services ever were.

As a result, it's critical to recognize that, while VoIP provides a number of productivity and financial benefits, cybersecurity safeguards must be taken to avoid inherent hazards.

Sweating bullets yet? Not to worry! A closer look at 3 of the most common VoIP breaches can help you and your organization stay on top of your game.

1. Denial of Service (DoS) Attacks

First up, Denial of Service (DoS) Attacks. This type of cybersabotage aims to interrupt and impede an organization's whole phone service by flooding its VoIP network with redundant Session Initial Protocol (SIP) call-signaling data, thereby gobbling up all available bandwidth, resulting in terrible call quality, frustrating downtimes, and delays.

To add insult to injury, DoS attacks don't even necessitate a high level of expertise. They are, in fact, relatively easy and inexpensive to run. Anyone can launch a pretty

catastrophic denial-of-service strike with just a little cash, basic technical know-how, and enough ill intent.

A growing number of DoS attackers are capable of gaining access to a system's administrative tools without ever needing to enter your primary network.

Your VoIP system's TCP (Transmission Control Protocol) and UDP (User Datagram Protocol) ports are often all that an attacker needs to take control of your company's communications infrastructure.

2. Malware and Viruses

All of your electronic gadgets are vulnerable to virus and malware contamination. VoIP networks are no exception. Viruses, worms, spyware, and other similar harmful programs can infect VoIP equipment and software just as easily as any other internet application.

Malware is the general term applied to any software program with a malevolent motive (and it's a cybercriminals bread & butter). The following are five types of malware that are sadly all too common.

Spyware: Covert software that allows a hacker to stealth monitor another's computer activities.

Keyloggers: Keyloggers record your keystrokes. This data is used to access your accounts.

Trojans: A Trojan is a malicious program that masquerades as genuine software.

Worms: Devouring bandwidth to cause system crashes, worms quickly infect entire networks.

Ransomware: Ransomware encrypts your data, preventing any access until a ransom is paid.

- ➔ "Ransomware attacks are currently causing serious disruptions in the US healthcare sector, risking economic destabilization", says retired Sgt. Jason Haak, former head of the Abilene PD Cyber Crimes unit. AffordaCare, a network of walk-in urgent care clinics in Abilene, Texas, was one such victim, having been forced to shut down completely after refusing to pay the $55 million ransom.

These heinous assaults on our privacy have the potential to cause irrevocable damage, such as the loss of sensitive client information, data corruption, password leaks, and even the complete hijacking of your personal computer.

Softphones (phone-like software) are one of the most enticing targets for cybercriminals because almost every VoIP system uses them. When they are not at their desk, many people utilize VoIP apps on their smartphones to make and receive calls. If your mobile device is infected with malware, it will be capable of transferring data without your knowledge.

3. Eavesdropping

Each time your VoIP system connects to an unprotected WiFi network, attackers from any location on the planet have the potential to weaponize the internet, essentially turning it into a point-and-click wiretapping machine.

Eavesdropping is commonly used by hackers to monitor calls in order to get essential company information such as user names, passwords, payment authorization information, private phone numbers, and other vital business data.

The terrifying thing about this form of attack is that, unlike the others, it's extremely likely you won't ever know about it, making it virtually impossible to catch these culprits.

Imagine some dubious character having unrestricted access to your personal, intimate discussions, while they themselves operate in perfect anonymity. It's an atrocious thought, yet it occurs hundreds of times every day.

Top 10 Ways to Protect Your Business from VoIP Cyber-Attacks

Despite the fact that VoIP systems pose certain security risks, you can take steps to mitigate these risks and protect yourself from hackers and eavesdroppers. Here’s a quick and helpful top-ten list of suggestions to get you started.

1. Promote a data-safe workplace
2. Avoid sketchy websites and links
3. Use strong passwords (changing them regularly)

4. Assist team members in understanding all security procedures and policies
5. Keep your computer's operating system and anti-virus software updated
6. Keep your IPS and VoIP firewall updated
7. Use VPNs (virtual private networks) to encrypt calls made over wireless networks
8. Speak up. Notify your service provider of any unusual or suspicious activities
9. Don't rely on old tech. Utilize modern encryption and authentication technology
10. Start with choosing a VoIP service provider you trust and can depend on

Advanced VoIP Solutions

As you can see, maintaining effective VoIP security is a full-time job, and because VoIP security breaches can be extremely costly in a short period of time, it's a job you can't afford to neglect.

Given the increasing prevalence of cybercrime around the world, the need for a secure solution has never been greater. If VoIP security risks have been keeping you awake at night, it's time to find a solution that offers you complete confidence and peace of mind.

From independent school districts to managed service providers, it's no surprise that enterprises of all sizes are transitioning their telecommunications operations to Advanced VoIP Solutions. With over 20 years' experience, 25 industry honors, 15,000+ delighted clients, and a job satisfaction rating of 100%, Advanced VoIP Solutions is a true "client first" VoIP service provider.

Learn more about how Advanced VoIP Solutions can help you simplify and safeguard your organization with cutting-edge communication services.

Want to hear why strengthening your cybersecurity will simultaneously improve customer experience at your organization? Schedule your no-cost, no-obligation consultation today.

Resources:

- FBI National Press Office
- 2020 Annual Internet Crimes Report
- 2020 Texas State Cybercrimes Report
- DataBreaches.net | Abilene, TX News
- Hendrick Health System | Network Security Threat
- 2021 Ransomware Attack List and Alerts