The Real Story on Conference Call Security

Security breaches are on the rise. According to a report by the Identity Theft Resource Center and CyberScout, U.S. companies and government organizations suffered from over 1,000 data breaches in 2016, up 40% from 2015, with hacking and phishing attacks accounting for the majority of incidents. It's no wonder businesses are going to ever greater lengths to safeguard their networks and protect customer information.

According to Cybersecurity Ventures, global cybersecurity spending will increase by 12-15% year-over-year through 2021. This increase in security spending is driven by a number of factors, including the desire to protect sensitive data, comply with regulatory requirements and reduce the overall number of security incidents and breaches.

But despite the ever-increasing attention paid to security, there is one area that remains notably absent from the list of security priorities – remote working and remote meetings. Rarely does one hear security concerns voiced about this business activity that's been around for over 25 years.

What's the worst that could happen?

In a survey by Research Now, 99% of conference callers admitted to hosting meetings where they were unsure of who was in attendance. Perhaps even more alarmingly, 60% considered this lack of security to be the norm.

How is this possible?

The answer is fairly obvious: dialing in. Dialing in is the most common way people join conference calls. While it can be a frustrating process, it's pretty easy to do, so most people default to this basic method. However, the biggest downside to dialing in is the lack of visibility of who's actually on the call. With dial-in, every call is essentially a 'black box.'

This security challenge is compounded even further by 'reservationless' conferencing, the technology breakthrough from years ago that led to the ubiquity of conference calling we now know. With reservationless, meeting hosts have their own dedicated conferencing facility with a dial-in number and access code that they can use whenever they like and share widely with guests – colleagues, clients, or external partners and vendors. These numbers and codes are used time and again, perhaps years on end, and will often end up in many different hands. The value that reservationless provides is severely undercut by the security issues introduced by dial-in.

Understanding the risk factors

In recent years, there have been some high-profile cases that call out this security hole. During the 2008 presidential primaries, Barack Obama's campaign lawyer managed to obtain the dial-in details for a media conference hosted by the Clinton camp. Not only was he able to join unnoticed, he even started speaking to the press attendees, taking his opponents by surprise.

In 2012, the FBI admitted that they hosted a conference call with Scotland Yard and other foreign police agencies about a joint investigation of a hacker group and its allies, only to find that the hackers themselves were on the call. To add insult to injury, the eavesdroppers didn't even need to hack into the call. They simply obtained an email containing the dial-in details.

These are very high profile examples, but the implications are just as real for the average business.

Like with any area of security, conference call threats fall into two broad categories: the malicious, and the unintentional. Malicious actors can include professional phishers, disgruntled former employees or even competitors. These perpetrators see rich pickings in the highly sensitive nature of many business calls, and will use the opportunity to gather information for competitive advantage, blackmail, or worse.

Most professionals have neither the time nor inclination to attend training on how to host secure conference calls.

Then there are the non-malicious, accidental breaches. These include scenarios where the host has scheduled back-to-back meetings and a guest inadvertently gatecrashes a confidential conversation, or when someone simply gets the day or time of the meeting wrong. Even wellintentioned meeting organizers can make fairly serious security gaffes – like posting conference call credentials on an event website – without realizing the repercussions (phishing, fraud, etc).

So, how do you address security on conference calls?

Training is the first obvious non-starter. Most professionals have neither the time nor inclination to attend training on how to host secure conference calls.

What about adding roll-call? Most conferencing services offer the capability, but there are two problems that emerge when trying to use it. First, it's painful. Calls get interrupted as anyone joins or leaves. Second, it just doesn't work for the case of the malicious actor. An unwelcome guest could simply not record their name. Then what?

Some of the more capable software products for remote meetings do offer a level of visibility to guard against security breaches. The challenge is that many of the major players' products tend to be quite feature-heavy or complicated, so users shy away from them and resort to the easy option of dialing in.

The best way to address conference call security is to move users away from dial-in to an alternative that provides visibility and is easy to use. Dial-out (where the conferencing product calls the user on a number of their choice when they're ready to join) is one such alternative that not only offers a better user experience, but can also provide visibility of who's on the call and who's speaking with great accuracy.

Ultimately, working towards a world where dial-in diminishes – and one day disappears – will make conference calls and remote meetings so much more secure.