NETWORKWORLD
This story appeared on Network World at
http:// www.networkworld.com/columnists/2007/110607-jericho-forum.html

VoIP security industry: Guilty as charged

Plus, 10 nasty questions to ask your VoIP supplier

The Jericho Forum Outlook By Paul Simmonds , Network World , 11/05/2007

Paul Simmonds is a member of the management board of the Jericho Forum, an organization pushing for innovation in e-commerce security, and is also chief information security officer for a large, global chemicals corporation. Here,Simmonds speaks out about why the Jericho Forum regards today's VoIP systems as "guilty" of not meeting a necessary level of security. For anyone discussing this with your vendors,Simmonds has also drawn up a "Ten 'nasty' questions to ask your VoIP supplier" that's included at the end of this column.

We in the IT security industry are collectively guilty for allowing a fundamentally insecure system such as VoIP to be launched into the market.

We've known for years that only "secure out of the box" should be the default. Yet VoIP is not only insecure by default, it's almost impossible to make natively secure. What's worse, VoIP end-devices (the phones) are a full computer – usually with their own Web browser, and (insecure) File Transfer Protocols to manage the firmware updates. So just as organizations are coming to grips with managing the vulnerabilities on their PCs, we have just doubled the management nightmare.

The return-on-investment claims made for moving to VoIP rarely stand up to proper scrutiny. The phones cost more than a standard "business" phone, and have a reduced replacement cycle. Gartner says in its November 2006 report "IP telephony technology, in many cases, can be more expensive than equivalent TDM-based PBX Systems."

Related Content

The ability to benefit from toll-bypass (routing your voice traffic over your private WAN to take advantage of spare WAN capacity) is frustrated by the fact that peak time for voice traffic is also the peak time for data traffic on the WAN. Most network managers that I know are looking for ways to offload peak traffic from congested, expensive corporate WAN links – not add huge volumes.

The ability to integrate your computer and your phone is another "benefit" that is on the salesperson's list, with features such as Click to Call, Find Me/Follow Me and Unified Messaging, but in reality companies rarely take any advantage of such CTI (computer-telephony integration) options.

Then toss in all the extra Band-Aid solutions you need to add, from VoIP firewalls to specialist VoIP security assessments (just run a Google search for "VoIP security solutions"), to make it even partially secure, and the extra management for firmware upgrades, vulnerability assessment and mitigation, and of course the WAN upgrades and all of a sudden those incredible savings the sales-person promised magically disappear.

VoIP is, in essence, a time bomb, poised for a massive exploit. With VoIP gaining traction in the corporate world, from boardrooms to the world's financial trading floor, VoIP is a public security exploit waiting to happen – with the large potential consequences. But unfortunately, this may be what is needed before the industry agrees to take VoIP security seriously.

The historical problems with being able to listen in to conversations that people assumed were secure (or where people assumed security through complexity) are well known: In the 1980s, the world became aware of problems with analog cell phone security when tabloid journalists printed details of an intimate cell-phone conversation between Prince Charles (than married to Princess Diana) and Camilla Parker Bowles. We're at the stage now with VoIP that something like that is likely to happen, but with consequences far more serious than embarrassment on the part of the British royal family.

At the 2006 Black Hat conference, David Endler and Mark Collier spent a very entertaining hour abusing a mix of VoIP phones, from being able to set up a call and listen in without the called phone ringing to a full corporate denial-of-service attack by making all phones repeatedly ring every 10 seconds (with no one there when answered).

"If it's not broken, don't fix it," doesn't apply here

At the 2007 Black Hat Conference, there were no less than five presentations on the insecurity and general problems with VoIP.

Related Content

VoIP does have advantages in certain business situations, such as running an international follow-the-sun help desk or an overseas call center operation, but those business cases are limited and the security risks of VoIP should far outweigh most ROI cases.

Getting the security right, and according to Jericho Forum principles, will finally give a true business case with real ROI: The ability to securely integrate disparate sources of VoIP phones (from VoIP clients on cellular devices, to BlackBerry, Wi-Fi VoIP phones and PC soft phones, as well as the traditional desk phone) connected on LAN connections that probably will not be on a LAN managed by your organization.

Oddly enough, when I used VoIP to discuss this *Network World* column with a colleague in the United States, the call dropped five times. I gave up and switched back to my cell phone.

Do I like VoIP? It has great potential, but for now the answer is no.

The 10 nasty questions to ask your VoIP supplier:

1. Do all phones and the central infrastructure use 100% secure protocols?

2. Will you warrant this system to operate on the raw Internet with no further add-on devices?

3. Can you manage all VoIP devices automatically, simply, with a scalable, easy-to-manage solution that will support all VoIP end-client including soft phones and end-devices that are connected on the Internet?

4. Explain how phones are, by default, securely provisioned. Including devices that you do not have physical possession of during the provisioning process.

5. Explain how you can conclusively prove that a phone using your system was provisioned by you.

6. Explain how you can conclusively prove that when I make a call, (say from my hotel room) I can be 100% assured that my phone is connecting to the corporate exchange (without using extra security devices such as IPSec).

7. Explain how users are strongly authenticated when connecting their devices. Ideally both device and user should authenticate.

8. Will your system allow federation of identities so we do not need to maintain (yet another) autonomous authentication system?

9. Is there segregation of duties? For example: can the administrator access voice mail and set passwords without the user being aware.

10. Are voice mail systems encrypted, and are all backups encrypted (voice mail, user-names, configuration, passwords)?

All contents copyright 1995-2008 Network World, Inc. http://www.networkworld.com