How secure is your cloud PBX solution?

By Rob Lith

21 Sep 2011

Doing business today, they say, is a bit like going to war. Would you fight alongside a soldier whose actions put you at risk? Would you let him reload your rifle, and can you trust him to have your back?

You'd think twice.

Then you probably agree that accepting an unprotected Internet Protocol (IP) connection from your VOIP partner is not the safest tactic either. Besides inviting eavesdropping on your most sensitive business dealings it also puts you at risk of sponsoring thousands of rands in phone calls made on your account.

A real threat?

How real is the threat of VOIP hacking? First of all, telephone hacking is a much more time-honoured tradition than many people realise. "Phreaking" - breaking into analogue networks to make free calls - dates back decades.

Since then, techniques have become much more sophisticated and telephony has migrated onto IP networks, which are more open to interference than analogue lines. Mainstream tools that are meant to help companies assess their network vulnerability are, in fact, used by hackers for the opposite purpose - to exploit vulnerabilities.

For these reasons it is much more common today to hear of hackers hijacking lines to make calls to high-value destinations, or diverting them via expensive routes and taking a cut of the termination fee.

Ultimately, the cost is born by the consumer. A prepaid VOIP customer may be many thousands of rands down on his account before noticing anything, unless the proper systems are in place to halt illicit activity.

What can be done?

So what can be done to keep your PBX safe from spilling your trade secrets and bleeding out your cash resources? The good news is that both VOIP providers and customers can pitch in. Here are some ways to safeguard your telephony:

Customer side:

- Password generators - Cloud PBX customers should use only securely generated random passwords. Passwords

chosen by humans are often the weakest link in a company's security posture, so invest in tools that manage and retrieve passwords easily and securely. 1password from AgileBits (http://agilebits.com/products/1Password) is a good example.

- Strong access policies - It can be as basic as allowing only known IP address ranges access to the voice platform. But this approach, while highly secure, sacrifices flexibility - for instance the ability to access the voice server while roaming overseas.
- Cloud customers can also load tools that monitor VOIP accounts for repeated failed password attempts and block the IP address from which the attempts are coming, pending administrator investigation. Fail2ban (www.fail2ban.org) is one such tool.

Provider side:

- Tools like Zabbix (www.zabbix.com) monitor unusual call patterns, destinations, numbers of live calls and account balances, and trigger alarms when certain values are exceeded (too many calls, a sharp drop in account balance, unusual international prefixes being dialled, etc). Anything out of place is picked up long before too much harm can come to the user enterprise.
- VPN tunnelling used in an enterprise VOIP service shields calls from eavesdropping and line-jacking, making it as secure as line encryption. An MPLS network and VPN technology like ViBE (www.vibesa.co.za) is among the applications that enable secure VPN tunnelling.
- Private cloud solutions are shielded from the public Internet by virtue of the customer's ownership of the hosted domain.

VOIP hacking, while not an everyday occurrence, is very possible. However, with the right tools and a few basic security habits, this form of communication can be highly secure.

ABOUT THE AUTHOR

Rob Lith is a director of Connection Telecom.