Members Telecom

Ideas | Solutions | Results

URGENT NOTICE WITH RECOMMENDATION TO TAKE IMMEDIATE ACTION

PABX FRAUD…

Also known as Toll Fraud causes multi-million dollar losses to organisations each year. This is now beginning to have a substantial impact on business' in Australia.

Whilst PABX features seem attractive to businesses for their convenience, most are unaware that this poses an extreme security risk.

WHO PAYS THE BILL?

PABX fraud results in substantial unauthorised call charges being incurred on your telecommunications accounts.

As a company **you** are responsible for maintaining the security of your phone system. Your PABX maintainer should also have briefed you on the security risks associated with your system. It might even be worthwhile contacting them for further preventative advice that is more relevant to your particular PABX system.

In some circumstances we may be able to alert our customers to possible PABX security breaches, however it is not our responsibility for the security maintenance of your system or the charges incurred during breaches.

As a professional courtesy, if we become aware of possible PABX fraud we may provide a notification to you but this only occurs after the fraud has commenced. No responsibility will be taken by our company should your PABX system become compromised. Your company will be required to pay any charges generated as a result.

HOW THEY DO IT AND WHY?

Hackers fraudulently use a company's PABX system to make long distance telephone calls, usually to obscure international destinations at no cost to themselves. The costs are bared by the organisation and can be quite considerable.

The more sophisticated PABX systems become, so do the hackers and their software. Hackers exploit weaknesses in the company's PABX system by figuring out voicemail pins and gaining access via the PABX maintenance port or 'Direct Inward System Access' (DISA) point of the PABX.. Once they

penetrate the voicemail they are then able to re-program the PABX system to make International telephone calls.

The fraudsters will often then either on-sell the calls as a phone operator themselves or they may even divert the calls to their own premium rate services. Both methods derive income for the hacker, while the business is left with the bill. Due to the unlimited numbers of lines that most PABX systems have, the cost to the business can escalate rapidly as many calls can occur during any one time. The hacker will often breach the system late at night when the business is not operating so they can attempt to avoid detection.

HOW TO PROTECT YOUR BUSINESS

How you protect your business is a matter for you to determine in consultation with your PABX maintainer.

Here are just some of the ways that you can protect your system:

- Regularly change your voicemail pins and do not use default pins such as 1234.
- Disable any call forwarding or outbound call ability from your voicemail ports.
- Cancel any unused voicemail boxes.
- Block International call access to countries that you don't usually dial.
- Ensure your PABX admin access unit is kept in a secure location.
- Restrict the 'after hours' outgoing call access.
- Disable DISA access unless absolutely necessary.
- Look for heavy call volumes at nights or on weekends and public holidays.
- Review system call records for discrepancies and unusual use.

LOOK FOR THE SIGNS!

You should consult with your PABX maintainer to determine if your system may have been a target. Here are some possible warning signs.

- While retrieving voicemail the system returns a 'busy' error message.
- Heavy call volumes late at nights or on weekends and public holidays.
- International calls on your bill to places you don't usually call.
- Calls of very short duration on your bill i.e. calls under ten seconds.

PABX FRAUD CAN HAVE A SERIOUS IMPACT ON YOUR BUSINESS

Case Study 1: A Melbourne based real estate company was the victim of PABX Fraud. Hackers had accessed the company's system through the roaming sales executives' voicemails. Over 4000 calls were made to Sierra Leone during a 8 hour period . Luckily the customer was alerted and international calls barred within a 24 hour period however the customer had $12,000 worth of calls to Sierra Leone. After a lengthy TIO investigation the customer was ordered to pay the charges.

Case Study 2: A government department was a recent victim of PABX hacking. Although advised, the problem was not rectified for a number days after the initial breach. The customer eventually received their bill to find out that $80,000 worth of calls to Columbia occurred as a result. The customer was liable to pay the charges.

Case Study 3: A small construction business suffered a recent PABX attack. The business was a customer of Telstra and was surprised when they received a bill from Optus featuring calls to Liechtenstein totalling $8,500. The customer did not usually make calls overseas but still had International access on their phone system.