PBX Fraud Alert

How to protect your business

Important information on how you can better protect your business against PBX hacking.

OPTUS

PBX Hacking...

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

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

Who pays the bill?

PBX 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 PBX 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 PBX system.

In some circumstances Optus may alert it's customers to possible PBX security breaches, but it is not responsible for the security maintenance of your system.

As a professional courtesy, if Optus becomes aware of possible PBX fraud it may provide a notification to you but this only occurs after the fraud has commenced.

No responsibility will be taken by Optus should your PBX system become compromised. At the end of the day you will be required to pay any charges generated as a result.

How do they do it and why?

Hackers fraudulently use a company's PBX 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 PBX systems become, so do the hackers and their software. Hackers exploit weaknesses in the company's PBX system by figuring out voicemail pins. Once they penetrate the voicemail they are then able to re-program the PBX 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 PBX 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.

Protection...

How to protect your business

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

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

- Regularly change voicemail pins. Do not use default passwords such as 1234.
- Disable any call forwarding or outbound call ability from your voicemail ports.
- Cancel any unused voicemail boxes.
- Block all International calls access unless absolutely necessary.
- Block International call access to countries that you don't usually dial.
- Ensure your PBX 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.

Due to the ability of carrier overide codes (eg. 0018 – Telstra Easy Half Hour, 0019 – Optus International Fax line) hackers can even determine which company bills you.

Therefore you may receive a bill from a phone provider you are not currently a customer of.

Look for the signs!

You should consult with your PBX 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.

PBX Fraud can have a serious impact on your business:

Case study 1:

A prominent Australian bank was the victim of PBX Fraud. Hackers had accessed the company's system through the company's main switchboard and jammed the phone to constantly dial a number in Sierra Leone. The following business day, the staff noticed that their voicemail boxes were constantly busy and thought that there may have been an IT problem but didn't think to alert their maintainer. Optus noticed the breach several days later and notified the customer that approximately $10,000 worth of calls to Sierra Leone had been run up in a period of only 6 days.

Case study 2:

A government department was a victim of PBX hacking. Optus noticed the unusual call traffic and alerted the customer within 24 hours of the fraud occurring. Due to problems with finding the correct person to handle the issue, the problem was not rectified for approximately 14 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 PBX 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.

Prepared by Tim Little for Optus External Fraud Risk Management.

GMO_N 0445 0916MZ