Date: 17/12/ 2014
Our Ref: PREVENT17122014
Tel: 01707 355464

ERSOU BULLETIN

This bulletin is issued as a Prevent and Protect message to all schools within the region.

The purpose of this alert is to provide knowledge and prevention advice to help schools protect themselves from PBX and dial through fraud.

The National Fraud Intelligence Bureau (NFIB) has seen a significant rise in the number of reports made in relation to this type of fraud. Since the end of June 2013 there have been nearly 500 reports relating to this - costing victims over £6m.

What is PBX Fraud?

Private Branch Exchanges (PBX) are systems which enable organisations to allow improved communication both internally and externally. PBX/dial-through fraud occurs when hackers target these systems from the outside and use them to make a high volume of calls to premium rate or overseas numbers to generate a financial return.

How does it work?

This type of crime can take one of two forms:

1. Criminals use auto-diallers to identify systems which are easy to hack into, especially voicemail.

2. The system is subject to a sustained cyber-attack to establish the pass code that will give them access to the PBX system itself. This can be relatively straightforward as often victims leave the password/code on default settings.

3. Once access is gained, the criminals can exploit in-built services such as message forwarding and call diversion and can make calls on the organisations account.

The criminal can make their money in two ways:

I. Dialling premium rate numbers to which they are affiliated

II. Dialling international numbers through the compromised telephone system, especially to Eastern Europe, Cuba and Africa.

Who is affected?

The victims are often small to medium-sized businesses, but the NFIB has also noticed that a number of schools, charities and medical/dental practices are being targeted, with losses sometimes up to tens of thousands of pounds. It is anticipated that these types of organizations will be subjected to increased victimisation as criminals identify common flaws in security procedures.

This type of fraud is most likely to occur when organisations are most vulnerable i.e. during times when businesses are closed but their telephone systems are NOT, for example in the early hours of the morning or over a weekend or public holiday.

Prevention

The good news is that some simple steps will significantly reduce your risk of victimisation:

- Use strong pin/passwords for your voicemail system, ensuring they are changed regularly.
- If you still have your voicemail on a default pin/password change it immediately.
- Disable access to your voice mail system from outside lines. If this is business critical ensure the access is restricted to essential users and they regularly update their pin/passwords
- If you do not need to call international numbers/premium rate numbers, ask your telecoms provider to place a restriction on your telephone line.
- Consider asking your network provider to not permit outbound calls at certain times e.g. when your business is closed
- Ensure you regularly review available call logging and call reporting options.
- Regularly monitor for increased or suspect call traffic.
- Secure your exchange and communications system, use a strong PBX firewall and if you don't need the function, close it down!
- Speak to your maintenance provider to understand the threats and ask them to correct any identified security defects

If you do become a victim of this type of crime, report it to www.actionfraud.police.uk

We also recommend www.getsafeonline.org which will give advice about security measures to take into account and the things to ensure that are in place.

Our vision is to contribute, alongside national and international partners, towards the provision of a safer and more secure cyber environment, in support of the National Cyber Security Strategy, that enhances trust and confidence in the Eastern Region as a place to live and conduct business.
http://www.ersourocu.org.uk/