Ironton Global

Cloud communication: reliable, simple & affordable

PBX FRAUD EDUCATION INFORMATION

Ironton Global
PBX Fraud Education Information
August 2015

FOLLOW US

Ironton Global

RESOURCE:

PBX FRAUD EDUCATIONAL INFORMATION FOR PBX CUSTOMERS

Telephone hackers hit where it hurts: your wallet

Telephone hacking is unauthorized or fraudulent activities that can affect your telephone system, and potentially cost your business significant amounts of money and resources if they occur. Unfortunately, most of the times the owner of the PBX isn't aware of the "hacking" until an enormous bill from their toll provider arrives or malicious events start occurring via their phone system.

Why do these activities occur?

Telephone hackers can infiltrate vulnerable PBX systems to make international and long distance calls, listen to voicemail or monitor conversations. Victims of hacked PBX systems unknowingly allow the hackers to "sell" the use of their telephone system to others or provide the hackers with an opportunity to maliciously reprogram the system.

How do they do it?

1. Typically, hackers gain unauthorized access through the PBX's maintenance port, voicemail (if voicemail can be accessed remotely) or the Direct Inward System Access (DISA) feature of a PBX.
2. Since most PBXs today are software driven, when configured improperly, allow hackers access to the system remotely. PBX administrators usually manage via a PBX maintenance port, by interconnecting from their remote service centers via modem. By controlling this PBX maintenance port, hackers can change the call routing configuration, passwords and can delete or add extensions or shut down a PBX, all of which adversely impact business operations.
3. Some voicemail systems can be accessed remotely and programmed to make outbound voice calls. Hackersmake use of this feature to forward calls to a "phantom" mailbox that will give a dial tone, allowing them to make calls from anywhere, on your business account. Hackers can also gain access to your mailbox to listen to your messages, change your greeting or delete your messages.
4. DISA is a feature enabling remote users to access an outside line via a PBX with authorization codes. This is a very useful feature for employees who are on the road a lot or who frequently make long distance calls or need to access international call conference after business hours. By gaining access to this feature, hackers can make access on an outside line and make tolled calls at the cost of your businss.

What can you do about it?

Having a properly secured telephone system is your responsibility and is the best way to prevent telephone hacking and mitigate the potential damage and cost that could be incurred by your business as a result. The following are some industry best practice guidelines that, if followed, could help reduce the risk of telephone hacking. Read below about the best practices for securing your PBX.

Ironton Global

Education

1. Familiarize yourself with the dangers of telephone hacking and the financial exposure you have to your toll provider.
2. Educate staff that utilize your PBX on security procedures and ensure they have an appreciation for the importance of adhering to set procedures.
3. Establish after-hours contact protocol so appropriate personnel can be notified timely.
4. Take time to evaluate your current settings and disable any features that are not in use.

Authorization Code/Password

1. Treat each of your IP phone as a gateway to hacking. Each phone's user name and password MUST be different and changed from the defaults. Never ever use admin and admin (as user name and password). That is 100% recipe for failure and hacking. Immediately change the user name AND the password to strong and long and never found in any dictionary. See below for further instructions.
2. On your PBX: do not use any default codes and passwords that come pre-configured. Be sure to change those settings as soon as possible after the PBX is installed and update them regularly.
3. Your router is an entry to your network, thus your phone. Your router should have its administrative and all user's names changed. NO DEFAULT USER NAMES OR PASSWORDS OF ANY KIND. Use a strong encryption password never found in any dictionary. Your router's password should be changed every 90 days
4. Choose random, lengthy passwords (at least 10 digits). Chose lengthy user's names too. Never ever use admin or administrator or any names that can be guessed. User names need be something like: h!A9ds89&dE and passwords to be as complex if not more complex.
5. Force password and authorization code changes for employees periodically.
6. Ensure that only trusted system administrators know the administrator password and be sure to change passwords as soon as possible after any staffing changes.
7. Do not keep extensions active for former personnel or positions. If there are staff changes, cancel the associated extension, including any associated features, access rights (i.e. LD/IDD) and codes and passwords.
8. Never ever leave IP phones at their default user name and password either. EACH phone must be changed to a different user name and complex password (not found in the English language – i.e. Uywi*2!dehj23)
9. ALL your gateway devices must also be taken into consideration and changed from default user names and passwords. Servers, PCs, anything that is on the Internet is susceptible for hacking

DISA

1. Limit the DISA access number and authorization codes to only employees who have a real need for such a feature as this can be a big security hole.
2. If possible, ensure the first few digits of the access number for DISA are different from the voice line.

Voicemail

1. Disable the external call forwarding feature in voicemail, unless it is absolutely required. Understand the risks that come with this.
2. Remove any inactive mailboxes.

Ironton Global

Toll Call

Restrict access to international or long distance destinations to which your company does not require access. Restrictions should include 1-900 calls.

Extensions

When an extension is no longer required, it should be canceled, along with associated features and access rights such as LD/IDD.

Ongoing Monitoring

1. Familiarize yourself with your business' call patterns and monitor them regularly.
2. Look for any suspicious call activity after hours, including weekends and public holidays. While hackers can "hit" anytime/anyplace, their favorite time is after hours and on week-ends and Holidays because they know that no one is usually monitoring during these times.

Equipment Room Access

1. The PBX system should be kept in a secured location to which only authorized users have access.
2. Verify any technician's identity, or anyone who requests access to your PBX equipment and be suspicious of any person you do not know or have hired that is working on your PBX, locally or remotely.

IRONTON GLOBAL

P: 855-226-0530
E: sales@irontonglobal.com

4242 Mauch Chunk Road
Coplay, PA 18037

FOLLOW US