PBX Fraud

Overview

Advances in technology means that PBXs are not only more powerful, but they are now accessible to smaller businesses. Next Generation SIP networks allow companies to run soft PBXs with minimal outlay or effort. There are even some consumer devices that terminate telecoms networks and allow calls to be made over a home's broadband.

While these improvements in communication provide significant benefits to users, they also introduce a number of risks for new, inexperienced users. For instance, unchanged factory default administrator or system passwords, week voicemail passwords, poorly configured controls etc can easily lead to unauthorised access to a PBX. Once unauthorised access is gained a fraudster can place calls that rack up huge expenses in just a few hours. Typical types of fraud include dial-through fraud – where calls are made through the system in order to minimise costs – and International Revenue Share Fraud.

Although contractually the cost of any calls made as a result of PBX hacking are attributable to the business running the PBX, it is often in the communication service provider's (CSP) interest – for business and adverse brand name publicity reasons – to come to an agreement to write off some or all of the costs; even where they have to pay interconnect charges for the calls.

Running on the Ocean Services Platform, Telsis Call Fraud Monitor allows CSPs to monitor calls and identify patterns that may indicate that a PBX has been hacked. These include unusually large number of calls to international or premium rate numbers, calls at weekend, long or fixed duration calls, etc.

International Revenue Share Fraud

International Revenue Share Fraud (IRSF) is a type of premium rate fraud, where calls are made to premium rate numbers across international boundaries. The fraudster makes a call to a premium rate number which they own in a second country. They then take their share of revenue for running the premium rate service.

The originating network usually has to pay the terminating network due to interconnect agreements, even if the call was made fraudulently. (For example, the basic GSMA bilateral roaming agreement states that originating operator must pay for all calls originating from its network — whether it is fraud or not.)

Scope of Fraud

According to the Communications Fraud Control Association's global fraud report for 2013, it was estimated that the global losses attributable to fraud were $46.3bn (USD), around 2% of the total global telecom revenues. Of this, they estimated $4.4bn was as a result of PBX hacking, the second most commonly reported fraud method.

The Telsis Call Fraud Monitor service also supports integration with hot number databases. Such databases contain lists on numbers that have previously been associated with fraud.

Once a hacked PBX has been detected, the Telsis Call Fraud Monitor may raise alerts, allowing the owner of the PBX to take appropriate action, or may block calls made from the business in order to minimise the financial impact of the fraud.

Globally, it has been estimated that PBX hacking is costing the industry over $4.4bn (USD), and accounts for almost 10% of all communication fraud. By monitoring PBXs and detecting hacked PBXs, CSPs can provide a useful service to their customers, limit losses associated with it, and protect their brand against bad publicity.

WHY CHOOSE TELSIS?

Telsis is a leading innovator in communication services, and has a wealth of experience in this area.

Founded in 1987, Telsis has been providing service innovation to both incumbent network operators and other licensed operators for over a quarter of a century. The Ocean range of Voice and Next Generation Network products are in service with some of the world's leading operator groups, including BT, KPN, Telefónica and Vodafone, as well as national and regional operators including EE, Kcom, EWE TEL, M-Net and Neo-Sky.

Telsis provides user programmable platforms that operate in both TDM and NGN environments and fully functional services that can be extended to meet local market challenges.
Telsis – your service innovation partner.

Contact: sales@telsis.com

UK
T: +44 (0) 1489 76 00 00
F: +44 (0) 1489 76 00 76

Germany
T: +49 (0) 6151 827 850
F: +49 (0) 6151 827 8521