XORCOM
Business Telephony Solutions

Choosing the Wrong IP-PBX Can Cost You $$$$$...on Day One!

- Telecom industry lost $46 billion in fraud.*
- An unprotected IP-PBX on the Internet will usually be hacked within 30 minutes.
- A few hours of unauthorized access can cost as much as your entire phone system.

Avoid the Risk – CompletePBX is Your Best Defense Against Cyber Attacks

With second-to-none security, CompletePBX includes these four layers of protection:

Camouflage

Using stealth technology, CompletePBX systems disguise themselves to avoid the attention of malicious users who know how to identify VoIP systems on the Internet.

Vigilance

Xorcom's intrusion detection feature is constantly on the watch, recognizing potential threats and diverting them before they reach the PBX.

Alert

Any attack in progress generates an immediate e-mail message directly to your system administrator.

Defense

If any unauthorized entity attempts to approach the PBX, Xorcom's integrated **session border controller** software will block it before it can do any damage.

Camouflage

CompletePBX Operates in Stealth Mode

By using non-standard identification methods, CompletePBX systems are essentially camouflaged on the Internet, essentially reducing the probability of cyber-attacks by bots to zero.

Secure VoIP Settings

By default CompletePBX will reject unwanted SIP requests without disclosing the reason for rejection. This greatly hampers brute-force attackers from guessing the SIP username and passwords.

Vigilance

Intrusion Detection and Prevention

CompletePBX features built-in detection of unauthorized attempts to access the system based on permission parameters set up by the system administrator. A potential intrusion is a user-defined number of unsuccessful attempts to access the system within a specific timeframe.

After a potential intruder has been detected, the intruder's IP address will be blocked from further access to the system for the defined ban period, and an email alert will be sent to the administrator.

Alert

CompleteAlert™: Built-in Real-Time Alarm System

Unauthorized activity on the phone system immediately generates real-time alerts, in the form of e-mail messages sent directly to the system administrator.

Defense

CompleteSBC™: Integrated Session Border Controller (SBC) Application

Carriers and customers alike will appreciate the ability of CompleteSBC, a software-based Session Border Controller (SBC) that effectively seals off the IP-PBX, to protect and defend the CompletePBX IP-PBX from misuse.

A sophisticated set of predefined yet customizable rules, supported by an intuitive GUI interface, enables easy configuration of its many features. CompleteSBC acts as a "SIP firewall" for access control.

A trial version of the CompleteSBC, supporting multiple calls with limited call duration, is integrated into every CompletePBX system (version 4.6 and up). Purchasing an electronic license will remove the call duration limitation, and can also be used to increase the number of unconditionally protected channels.

Built-In Firewall

The point at which a system is opened up so it can be remotely administered is almost always the point of compromise in an intrusion. Our recommendation is to lock down the system from the outside world, installing CompletePBX on a LAN protected by a firewall/NAT router. As an additional means of protection, CompletePBX features its own built-in firewall. The default rules in the built-in firewall can be modified to accommodate specific applications relevant to your business.

Initial Configuration is Locked by Default

CompletePBX is preconfigured to use restrictive security policies. For example, in the default configuration CompletePBX does not accept SIP calls from endpoints not located on the LAN. Customers who want the PBX to be able to receive inbound calls from Internet sources must explicitly enable this behavior in the CompleteSBC/Firewall configuration.

Password Strength Assessment

Setting strong passwords is imperative for SIP and IAX2 extensions, as well as for Direct Inward System Access (DISA) and call-back functions. In addition, defining passwords for all outbound routes used for international calls significantly deters intruders from making malicious calls. In CompletePBX, a special algorithm detects potentially problematic passwords and issues a warning to the administrator.

Secure Remote Access via Rapid Tunneling™

Allowing remote access to authorized users such as system administrators or technical support staff working offsite is a challenge met via Xorcom's Rapid Tunneling feature. Secure Shell (SSH) tunneling is used to access the CompletePBX Web interface in a secure and controlled fashion.

Administrator Accounts for Employee Turnover Protection

CompletePBX features different levels of user-defined access; administrator accounts can have their access restricted to a specific extension range or a specific set of features in the PBX. By creating separate administrator accounts for all CompletePBX system administrators, staffing changes simply require user account removal to ensure they no longer have access.

Don't take a costly risk.

CompletePBX provides the best protection against cyber-attacks in the industry.

* *According to the Global Fraud Loss Survey 2013 of the Communications Fraud Control Association (CFCA)*

XORCOM

XPP Technology by XORCOM

Installed in 100+ countries

Xorcom Headquarters
Misgav Industrial Park
20174 Israel
Tel: +972 (0)4 995-1999
Fax: +972 (0)4 999-0287
E-mail: info@xorcom.com
Web: www.xorcom.com

Xorcom USA
145 S. Jefferson Ave., Suite G
Cookeville, TN 38501
Tel: 1-866-XORCOM1/1-866-967-2661
Fax: (931) 854-9114
E-mail: info.usa@xorcom.com
Web: www.xorcom.com