Modern IP Communication bears risks

How to protect your business telephony from cyber attacks

Voice-over-IP (VoIP) provides many new features over PSTN. However, the interconnection with your IT infrastructure also carries risks affecting the security and integrity of your IP services. As IT networks are targeted by attackers, insufficient prevention can endanger not only the network but your telecommunication infrastructure that is build on top of it. This paper aims to educate you about possible risks, common attacks and how to prevent them from being successful.

1. Network Meets VoIP

Analog and ISDN phone systems are connected to the public switched telephone network (PSTN) but usually not to the internet. IP phone systems or PBXs on the other hand, are more vulnerable as they are connected to the internet through the local network (LAN) or directly through the SIP protocol.

If the phone system is connected to the service provider (ISP) through the SIP protocol, it should access the internet through a firewall. However, even if is not directly connected to the internet, it can still be attacked through the LAN as IP devices are accessible from each point within. Furthermore, network switches with management features enable eavesdropping from any location within the LAN, and service access points of some routers enable eavesdropping from the internet.

If an attacker gets access to the LAN, the phone system can be attacked as well. Therefore, all IP devices and the access to your router, ISP and IP devices need to be secured at best.

Another possibility, which we advise against, is the IP phone system being directly connected to the Internet and either having a public IP address, or certain firewall ports being open. This case often occurs if external phones are to be connected to the system through the internet, such as for traveling employees or home office usage.

2. Common Forms of Attacks

2.1 Fraud

Typically, attackers perform a port scan to look for public IP addresses. If, for example, a SIP server is located behind port 5060 and an internal extension is known, a brute force attack can be used to determine the password.

Another possibility is the use of publicly available third-party SIP-proxies or gateways. Also, services may be used illegally by means of identity spoofing. If an attacker uses the highjacked system for oversea calls, victims may face high costs. For example, calls may be routed through PSTN instead of the IP network, or expensive service numbers and hotlines may be called. If a server gets hijacked, call credits may be sold to third parties.

Identity spoofing affects SIP but also other communication protocols. It can be done by simply having the victim's phone displaying another identity, but also by manipulating registration or by man-in-the-middle attacks. In the latter case, incoming calls for the victim are forwarded to IP devices of the attacker. Stealing registration information can provide attackers with passwords in order to act as a valid user. This can be done in different ways, such as through eavesdropping or faking identity and asking the victim for the registration information. Attackers may aim for call recordings, call detail records, or further data misuse for fraud or spam.

2.2 Eavesdropping

Contrary to ISDN and analog telephony, eavesdropping of IP phone calls is much easier. As for network convergence, separate access to physical phone lines or special equipment are no longer required. Many programs are available online that allow eavesdropping of VoIP calls. User names and passwords can be spied out, but also habits and patterns in the way the victim communicates and both social and business contacts. A common approach is a man-in-the-middle attack, where an attacker acts as a proxy between communicating parties and can listen to or even manipulate all of the communication, even for encrypted SSL or SSH connections.

The address resolution protocol (ARP) is used to map IP network addresses to the hardware addresses used by a data link protocol. ARP-Poisoning can only be used in LAN, but is most efficient and dangerous. Connections get redirected transparently and can only be detected by stations in the same subnet. In order to listen to connections outside your own LAN, a server is usually simulated and the traffic is routed there by means of spurious DNS information. If the connection needs to be redirected, this server then works as a proxy. It can also be set as a target server.

Alternatively, it is possible to highjack standard gateways and eavesdrop the data traffic. These gateways introduced to victims by means of DHCP spoofing. DHCP stands for Dynamic Host Configuration Protocol. DHCP allows to automatically acquaint computer systems with a network configuration. By means of DHCP spoofing, victims receive forged DHCP responses for the standard gateway and DNS server. This allows an attacker to eavesdrop or manipulate all data packets that are being sent outwards of the subnet, but also to forge responses to DNS requests.

Another approach is infrastructure hijacking. Potential targets include servers, IP phones or other network devices. Attackers may gain access to IP devices by means of weak authentication mechanisms and guessed or stolen passwords, or via security gaps in corrupted server services. In case of a hijacked server, the attacker may at least protocol the connection, but may also eavesdrop calls, or redirect them to record them or act as the actually requested callee.

2.3 Denial-of-Service

Denial-of-Service (DoS) stands for the unavailability of a service and can be provoked in a number of ways. DoS attacks aim to create malfunction of system operations. In worst case, a system may become completely inoperative.

As attackers want to remain unidentified, they usually indicate a faked return address. This approach is named IP spoofing. For DoS attack on lower network layers, mostly only requests have to be send without the need of a response. IP spoofing can also be used to overload the victim with response packets.

2.4 Spam Over Internet Telephony

The fusion of IP telephony and computer networks increases SPAM over internet telephony (SPIT), whereby IP phone systems get hijacked and misused to spread SPAM phone calls. As with e-mail SPAM, back-tracing is very difficult as actual originators can not be clearly identified. In order to stay hidden, attackers may use identity spoofing and bot networks formed by multiple hijacked devices. Another possible approach to spread SPIT is the insertion of forged RTP packets.

Despite the similarity to SPAM, opposing SPIT is much more difficult. As for e-mails, a pre-classification may likely be unreliable. A content filter may require too many resources and act too late during a phone call as the callee has already been bothered. A content filter may still be of help for recorded voicemail messages on a mailbox.

If a hacker controls an IP device, he can access the network and the services it offers. Hijacked systems can be misused as bots for SPIT or for attacks on other users. Victims often can trace back the trail only to the hijacked server but not the actual attacker.

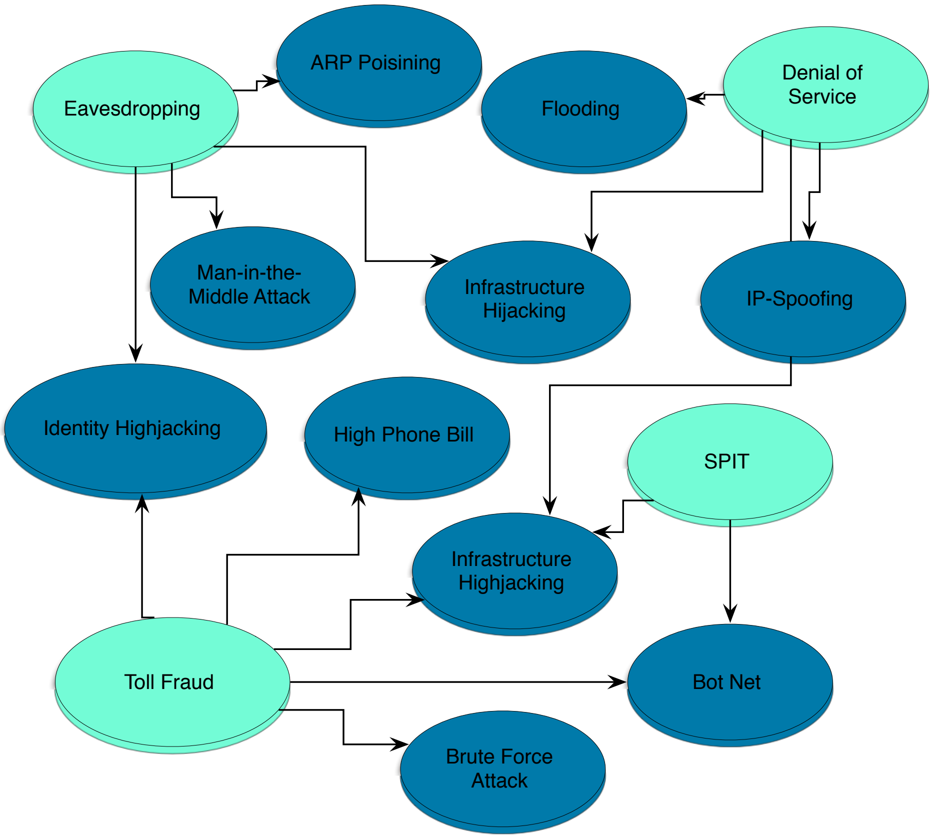

fig.: common threats for IP telephony

3. Security measures

In this section, we are going to take a look at security measures. We recommend to implement as many of these as possible to secure your IP network and telephony at best.

Generally, a company guideline should be defined and strictly implemented to guarantee network safety. This guideline should cover the following measures and be regularly reviewed and updated.

Securing the IP PBX alone, is not sufficient to prevent it from being attacked though. All relevant network components need to be secured. PBXs and terminal devices need to be protected, even if the PBX is not directly connected to the internet, as an attack on any other network component may still be a threat to the PBX.

3.1 Secure Passwords

For increased protection against all attacks, long and secure passwords are required. Instead of names, birthdays, or entire words, secure passwords need to contain letters, numbers, and special characters. If users still use simple passwords, the administrator should consequently enforce secure passwords, either through strict guidelines or by assigning passwords to every user. AskoziaPBX automatically generates a secure password for each newly created phone account.

3.2 Firewall

A packet filter included in a corporate network firewall can filter the incoming and outgoing data traffic. This increases network protection from attackers as well as unwanted outgoing data packets, for example to avoid network devices being misused as parts of a bot network.

AskoziaPBX has an internal firewall. In addition to the network firewall providing basic security, this internal firewall should also be activated. This internal firewall only provides protection for the PBX, but does not replace a network firewall. The network firewall performs an address translation (NAT). Therefore, only the server and address range of the ISP can communicate with the PBX through the internet. This option provides much more security than changing SIP ports. If a server or PBX is running on a public IP address, it is only a matter of time until the changed SIP port is found.

3.3 Fail2Ban

As part of Askozia's internal firewall, Fail2Ban can be activated as a measure against brute-force attacks. IP addresses are blocked if they repeatedly attempt to log in with incorrect passwords within a time window specified by the administrator. To prevent attackers from guessing an internal number, AskoziaPBX also uses the option alwaysauthreject = yes. Answers to requests are always the same, regardless of whether the username is correct or not.

3.4 Avoid Port Forwarding

We strongly recommend to avoid port forwarding, as well as DMZs (demilitarized zones) and hosting on home routers. Instead, access to external devices should be implemented through virtual private networks (VPNs). If at all, port forwarding should only be implemented with a most secure password and active Fail2Ban.

3.5 Call Rights

Limiting call rights should be taken into account, as it may protect both against abuse by internal users and from outside attacks. In AskoziaPBX, restrictive dial patterns can be defined to prevent calls to countries that normally should not be called. At the same time, calls to national phone numbers with high charges should be blocked. Sometimes not all threats can be prevented, for example in case of regular international calls. In that case, at least the number of calls or the call duration should be limited. If these thresholds are exceeded and an attack is considered to be likely, calls can be blocked completely. A further precaution could be a VoIP prepaid credit to limit the impact of a successful attack.

3.6 Separating Telephony and Data

NGN ports (Next Generation Network) for dedicated VoIP lines are already offered by various ISPs. Also, data and telephony networks should be separated by means of virtual local networks (VLAN). A VLAN is a logical subnet within a switch or network. Within a network, a VLAN may expand across several switches. Physical networks are separated into subnets and VLAN-capable switches assure that data packets are not transferred into other subnets.

3.7 SIP Proxy

Considering the costs, it may make sense for larger installations to use an external server as SIP proxy for incoming calls. A proxy server acts as middleman, that receives requests of one party, and establishes a connects to another party through its own IP address.

3.8 Encryption

Encryption between IP PBX and phones based on Secure SIP (SIPS) und Secure RTP (SRTP) can prevent calls from being eavesdropped. In AskoziaPBX, required certificates can be created or uploaded in the settings for secure calling.

3.9 Blacklist and Whitelist

To further prevent potential threats, certain numbers can be blocked or accepted. In the extended provider settings of AskoziaPBX, blacklists allow to block certain numbers from calling through this provider. In the firewall settings of AskoziaPBX, the whitelist allows to add certain numbers as exceptions for Fail2Ban.

3.10 Access Privileges

To further increase security, only required devices should be permitted access to the network. Unused devices should be disconnected. Furthermore, access rights should only be assigned to specific users and only as far as actually necessary. In AskoziaPBX, client user interfaces limit user access to certain settings. This way, only the system administrator has access to the whole PBX and sensitive settings in terms of security.

3.11 System Hardening

To prevent attacks on your network infrastructure, all network devices should always be updated to latest software version available and security updates should be realized as quickly as possible. Beside your IP phone system, this also counts for IP phones, routers, switches, firewalls, and all other network devices. Unused services should be deactivated.

3.12 High Availability

If there is an attack and an attacker successfully forced the phone system to fail, you should have a plan B. This can be high availability (HA) and should particularly be realized by companies with high call loads. The idea is to provide a second phone system with the same configuration in order to quickly replace a failed PBX.

4. Summary

IT and VoIP security can not be separated. To prevent your network and telephony infrastructure from being hijacked, as many security measures as possible need to be implemented. Where complete safety can not be guaranteed, these measures help to strongly minimize the risk of a successful attack. Regular reviews and updating, both your network and IP telephony infrastructure as well as your security guidelines is a key to keep your business save. If your business does not have the required know-how, a specialized network security company can help you through the process. Investing in security is definitely a worthwhile investment.

About Askozia

Askozia started out in 2006 by developing AskoziaPBX, a highly intuitive telephone system firmware for embedded appliances. Over the years, Askozia has evolved into an international developer of realtime IP communication technologies and PBX software for service providers, SMBs and system integrators worldwide.

Askozia uses open standards for interoperability and no proprietary lock-in. The pricing is fair and excludes licenses limiting the numbers of users, phones or phone lines.

All solutions can be used on-site or in the cloud, with IP phones of your choice and can be configured and managed through the most intuitive user interface. No matter if you have questions regarding the installation, configuration or operation of AskoziaPBX, our support team has your back and offers you conditions well-matched with your business needs.

Learn more about how Askozia can boost your business at askozia.com