TATA COMMUNICATIONS
GlobalRapide

Tata Communications Fraud Prevention as Service -Customer Security Checklist

Take steps to safeguard your network.

Global telecom fraud losses amount to over 39 billion USD* a year.

- If your network is not secure, you risk criminals seizing and sending traffic via your switches without your knowledge.
- IP fraud is most common on weekends when staff are away.
- Open-source platforms/networks/switches are a core target.
- Fraudsters are sophisticated, organized and should not be underestimated. Given the high profit potential, they tend to be well funded and have access to the latest software tools and the best programmers.

Top fraud methods

- IP PBX Hacking
- Abuse of network configuration weakness
- Call Spoofing
- Subscription Fraud
- Account Takeover
- Wangiri
- SMS Phishing

Security Checklist

- Limit PSTN dialling to essential destinations.
- Do you absolutely require the ability to terminate to A-Z countries.
- Avoid routing plans which facilitate loop access to the PSTN via the PBX.
- Enable call admission controls – Example-. max sessions, registration policies, etc.
- Disable non-essential portranges.
- Interconnect over a trusted interface, when possible, Example-. TLS or IPSec.
- Apply updates and patches on a regular basis.
- Enable dynamic dialling rules if possible – Example-. enabling time of day and/or routing destination policies.
- Secure your edge with an SBC on premise, or via a Service Provider such as TCL.
- Limit access and call processing to known IP addresses.

* Annual loss in 2021, according to the Communications Fraud Control Association Global Fraud Loss Survey (www.cfca.org)

TATA COMMUNICATIONS

GlobalRapide

- Upgrade your devices using the latest stable release.
- Change default passwords for all your devices — especially accounts with administrative privileges.
- Use strong passwords with a combination of capital and lower-case letters, numbers, and symbols.
- Put password expiry policies in place.
- Establish account lockout policies to combat brute force and dictionary-based attacks.
- Set up proper notification policies for locked-out accounts.
- Block all 'lower' TCP ports (<1024) to public Ips.
- Use non-standard ports for web-accessible interfaces if they must be accessible from public IPs.
- Block ICMP responses for mission-critical devices and only selectively allow ICMP responses to trusted IPs.
- Use challenge-response authentication to encrypt communication to any web-based portals over public IP.
- Understand the device you are running. For example, some SBCs allow endpoint registration without a username or password as long as an extension is configured.
- Block administration access from a public IP for VoIP devices.
- Implement strong passwords and only allow access from specific IPs if you require public access. Consider implementing a jump-server architecture such as Citrix.
- Enforce standards for voicemail passwords, including periodic password resets.
- Disable PBX remote dialling and dial-through capabilities.
- Allow only trusted IPs to send to default VoIP ports.
- Require carrier authentication using prefixes that are at least six digits long and change on a regular basis.
- Scan your network from a public IP to discover open ports and secure them.
- Test your security measurements by trying to access your own network from a public IP.
- Send VoIP calls to your own network to test its vulnerability.
- Ignore, or block completely messages from unknown IPs. Some devices will send 100 calls to an unauthorized IP, only to reject the call in a subsequent message. This only serves to inform an intruder that a VoIP device is available and listening.
- Carefully review the rate sheet/deck of your international carriers. Watch out for "premium number ranges". These are typically higher cost/risk numbers that are established for content-based services. Request to block these if not needed.
- Ask your Carrier to establish call monitoring and control capabilities on your voice traffic, i.e., alarming when monetary / minutes thresholds have been breached per CLID/A number and/or destinations with optional auto-call blocking.
- Ask your carrier what fraud prevention forums they are members of. i.e. i3Fourm https://i3forum.org/ , GLF https://www.capacitymedia.com/global-leaders-forum, GSMA https://www.gsma.com/etc.
- Is your carrier compliant with the GLF Code of Conduct Against Fraud.

This checklist is for customers' convenience and is not comprehensive. You may need to take additional steps depending on the type of platform/switches in use. Please check with your IP-PBX vendor on a regular basis for the latest patches and security configurations.