Stop Voip Threats Before They Start With A Licensed, Local Voip Operator

To any regular consumer of media content, the following has become a familiar story. A web user trawling the bowels of the Internet discovers a database containing gigabytes of call logs, messaging data and internal system credentials.

The exposed Cloud-hosted database most often belongs to a fixed, mobile or IP-based telecoms operator that has mistakenly left data exposed on a development system. Examples typically include credentials for customer login pages and the telco's own internal data such as hostnames, usernames and passwords.

Sometimes, the telco that has left sensitive details out in the open is a VoIP operator. Fortunately, South Africa licenses its VoIP operators who are governed by the Electronic Communications and Transactions Act 25 of 2002 and Number Portability Regulations, amongst others.

The country's independent telcos, of which OTEL is a leading example, have been expected to comply with the onerous consumer protection, record keeping and data security requirements entrenched in this Act for almost two decades.

In addition, compliance with the Financial Advisory and Intermediary Services (FAIS) Act, the Financial Intelligence Centre Act (FICA) and the Consumer Protection Act (CPA) ensures local VoIP users are well-protected in the information stakes compared to many of their data-vulnerable overseas counterparts.

Legislation aside, OTEL CTO Anthony Engelbrecht advises telecoms users that setting up two-factor authentication should be the first port of call when it comes to protecting VoIP accounts from unauthorised use and access. Two-factor authentication provides an extra layer of security that goes beyond a standard password and username and typically means accounts can only be accessed on trusted devices.

"Two-factor authentication stops VoIP fraud before it starts while minimising the threat from client log-in details inadvertently exposed online, or acquired by traffic scanning systems on infected networks," said Mr Engelbrecht. "It is critical that VoIP operators start providing SSL encryption for SIP registrations rather than the traditional plain text authentication traditionally and still widely used in the industry."

OTEL CEO Rad Jankovic adds that VoIP users setting up their voice and data networks for the first time should always be sure to never leave the default password on any IP phone, router, switch, firewall or any other IP-based device that requires a password. "The best passwords are long strings of characters that don’t include common phrases. Make liberal use of special characters and always use a different password per device.”

VoIP's cost-saving potential and its ability to easily offer a plethora of value-added services means it is quickly overtaking traditional landlines as the world's telecoms technology of choice. Greater usage means greater visibility and VoIP has certainly been noticed by the world's fraudsters," Mr Jankovic said.

Fortunately, OTEL's VoIP services include multilayered fraud detection for end user clients as well as resellers. “At the end of the day; strong passwords, two-factor authentication and making sure to contract with a reputable local VoIP Operator licensed in terms of the ECT Act are the most effective ways to fight back against telecoms fraudsters,” concluded Mr Jankovic.