Otel Protects Vulnerable Sme Voip Users

Voice over Internet Protocol (VoIP) voice and data communications technology is often touted as a major cost saver for Small and Medium-sized Enterprises (SMEs) under pressure to reign in non-core expenditure.

"A typical SME with ten or less employees can save up to 60% on phone calls and Internet charges, for example, simply by making the switch from a traditional telecoms operator to one of the new breed of independent telcos," says Rad Jankovic, Chief Executive Officer of Otel Communications Pty (Ltd).

The irony, as Mr Jankovic explains, is that SMEs opting for VoIP voice and data solutions because of significant cost benefits could be opening themselves up to international premium number fraud should they not property secure their VoIP connection.

Phone line fraudsters primarily operating from Eastern Europe employ software that identifies unsecured VoIP connections around the world. Once a vulnerable connection with no proper firewall has been located, and its username and password determined, the fraudsters use the South African VoIP connection to call premium telephone numbers around the world. The criminals collect substantial sums of money through network operator revenue-sharing models.

"OTEL is proactively marketing a highly-effective VoIP fraud prevention solution targeted at SMEs that might not have the in-house expertise to effectively secure their VoIP connection," adds Mohammad Patel, OTEL's Chief Technical Officer.

VoIPGuard is an active voice and data fraud prevention system that loads a an intelligent sensor into an SME's VoIP-based PBX system. "It is not merely a passive firewall that can be bombarded by fraudsters until it gives way," says Mr Patel.

The software immediately starts monitoring the packets of data flowing into the VoIP system for four types of alerts that could indicate suspicious incoming calls. These include unusually high concurrency detection, unusually high registration attempts on a VoIP account, foreign country IP change detection and unusually high SIP packets detection on a VoIP account.

If any of the above are detected, VoIPGuard will prevent access, identify the suspect IP (Internet Protocol) address, and add this to a global database of blacklisted IP addresses which further enhances

international VoIP connection protection.

"Because no intervention by the SME's owner or staff is necessary to experience top-notch security, VoIPGuard is ideal for the SME wanting to concentrate on its core business," concludes Mr Patel.