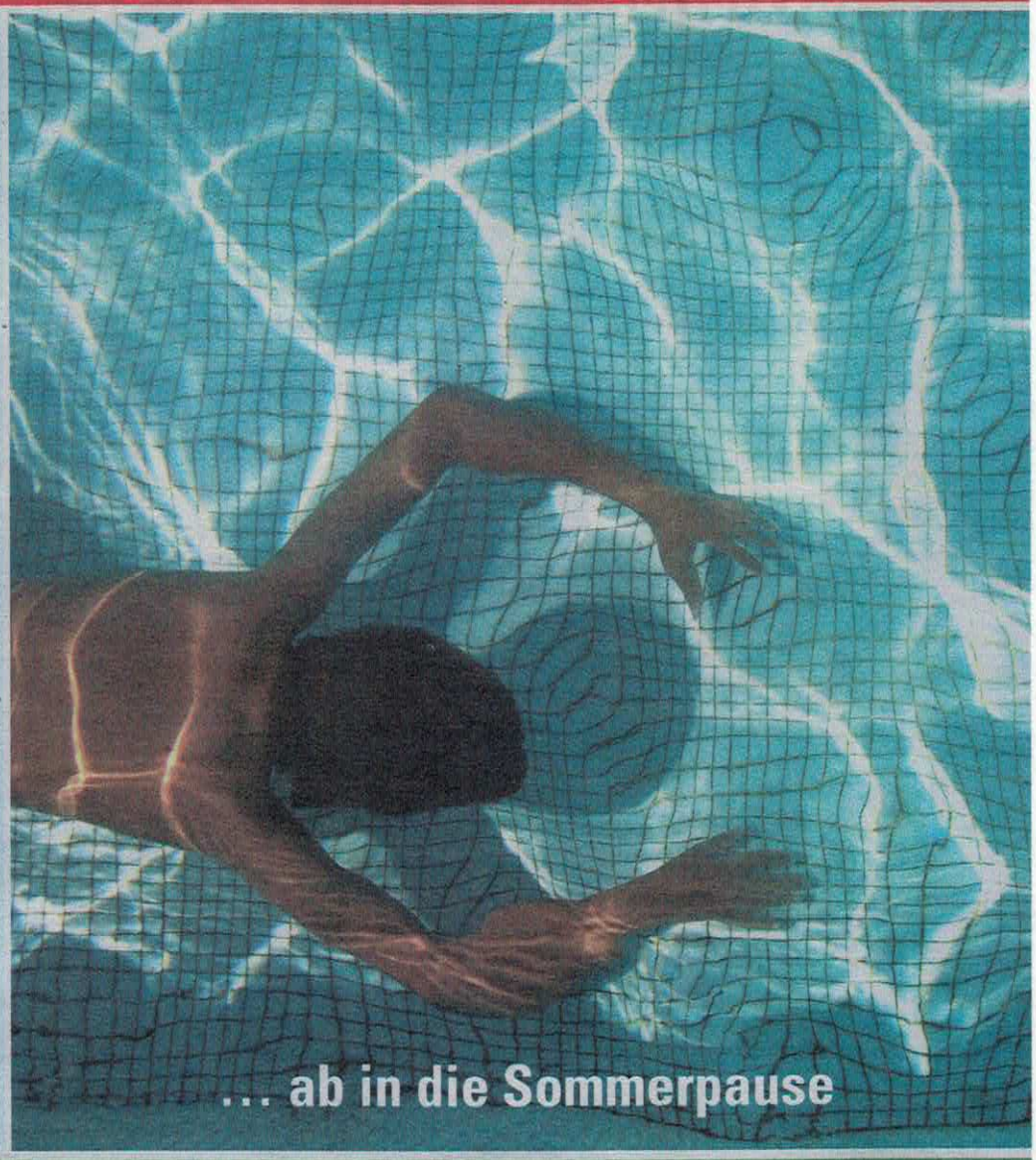
ERFOLG

Die starke Zeitung für Selbstständige, Unternehmer und Existenzgründer

Offizielles Organ des Schweizerischen KMU Verbandes

Nr. 6/7 · Juni / Juli / August 2018 · 12. Jahrgang · Preis CHF 3.90 · www.netzwerk-verlag.ch · AZB 6300 Zug



So schützen Sie Ihre VoIP-Telefonie vor Risiken

Wie anfällig ist VoIP-Telefonie für Störungen? Diese Frage haben sich viele Unternehmen nach Ausfällen bei grossen Telekommunikationsanbietern und nach breit gestreuten Cyberattacken gestellt. Was bei der Suche nach Sicherheitslösungen oft vergessen geht: Die Schwachstelle ist meist der Mensch.

Sprachtelefonie, Internet und Datenverkehr – alles läuft heute über das Netzwerkprotokoll IP (Internet Protocol). Dies vereinfacht vieles, die Technologie macht Unternehmen aber abhängig von der Verfügbarkeit des Internets. Gerade in Bezug auf Telefonie hat sich zu Beginn dieses Jahres wohl manch einer die alten Zeiten des analogen Telefonnetzes und von ISDN zurückgewünscht. Denn die Häufung von Ausfällen des Festnetzes sowie der Mobiltelefonie haben gezeigt, dass die IP-Technologie anfällig sein kann.

Werden Sie öfter angegriffen?

Im Zusammenhang mit der Einführung von VoIP-Telefonie werden oft auch potentielle Sicherheitsrisiken mitdiskutiert. Wird beim Einsatz dieser Technologie das Unternehmen über die Telefonie-Infrastruktur vermehrt angegriffen? Bei der grossen Mehrheit der Unternehmen trifft dies nicht zu. Aus einem einfachen Grund: die meisten besitzen keine Daten oder Informationen, die für organisierte Kriminalität im grossen Stil von Interesse sind. Dennoch darf die Sicherheit nicht vernachlässigt werden. Die Möglichkeit per Fernzugriff auf die Datennetze zuzugreifen, lässt jedes Unternehmen zum potentiellen Angriffsziel werden. Zum Beispiel, um anhand von absichtlich herbei geführten Störungen, Gelder zu erpressen oder um Telefonnummern für Phishing oder Spoofing zu missbrauchen.

Schützen Sie sich selbst

Telekom-Anbieter schützen ihre eigenen Infrastrukturen mit hohen Sicherheitsstandards und bieten ihren Kunden verschiedene Sicherheitslösungen für deren VoIP-Infrastruktur an. Dazu gehören sichere Leitungen ebenso wie die Verschlüsselung des Datenverkehrs. Der sorglose Umgang mit E-Mails, offene Internetzugänge, für jeden ersichtliche WLAN-Passwörter im Sitzungszimmer oder Standardpasswörter bei der Sicherheitsinfrastruktur erleichtern Kriminellen jedoch den Zugriff auf die Datennetze. Die Mitarbeitenden werden so ohne böse Absicht zu den Hauptgefahrenquellen. Alle Sicherheitslösungen helfen somit nichts, wenn im Unternehmen nicht ausreichend sensibilisiert wird.

Autor: Christophe Beaud, CEO peoplefone AG

So bleibt die Telefonie verfügbar

Wer abseits von kriminellen Machenschaften die Verfügbarkeit der VoIP-Telefonie sicherstellen möchte, hat verschiedene Optionen. Internetanschlüsse mit unterschiedlichem Servicelevel sind eine Möglichkeit. Wer schnellstmöglich wieder erreichbar sein möchte, sollte eine überwachte Internetleitung wählen, bei der eine kurze Wiederherstellung der Betriebsbereitschaft garantiert wird. Wer permanent erreichbar sein muss, setzt am besten auf verschiedene Anbieter, die nicht die gleichen Leitungen und Technologien verwenden. Zusätzlich bieten VoIP-Anbieter den Service an, bei Ausfällen die Festnetztelefonie auf Mobiltelefone umzuleiten. All diese Optionen machen die Verfügbarkeit auch zu einer Kostenfrage. Daher empfiehlt es sich, zu überlegen, ob und ab wann ein zeitweiser Unterbruch der Kommunikation schädlich fürs Unternehmen ist.

Nutzen und Aufwand abwägen

Die IP-Technologie fordert IT-Verantwortliche auf diversen Ebenen. Mit VoIP kommt eine Komponente hinzu, die es im gleichen Masse abzusichern gilt wie die restliche Infrastruktur. Dies geht noch oft vergessen, da bezüglich Missbrauch die Festnetztelefonie bisher als sehr sicher galt. Mit All-IP und Unified Communications braucht es ein Umdenken. Dabei sollte darauf geachtet werden, dass man nicht über das Ziel hinaus schiesst. Nicht jedes Unternehmen muss mit viel Zusatzaufwand in 100% Redundanz und absolute Sicherheit investieren. Die bewährten Sicherheitsansätze und Sicherheitsprodukte lassen sich oftmals auf die VoIP-Infrastruktur ausdehnen, so dass mit bestehenden Mitteln gearbeitet werden kann. Sind ausserdem alle im Unternehmen für potentielle Gefahren sensibilisiert, ist die benötigte Sicherheit meist gewährleistet.

Sicherheit in VoIP-Netzwerken

- Strukturieren Sie Ihre IT- und VoIP-Komponenten nach Sicherheitszonen, die den Schutzbedarf festlegen.
- Setzen Sie bewährte Security-Ansätze ein und dehnen Sie bestehende Sicherheitsprodukte auf die VoIP-Infrastruktur aus.
- Schalten Sie Firewalls einen Session Border Controller (SBC) zur Kontrolle von Echtzeitströmen nach.
- Installieren Sie nur die Software, die für den Betrieb nötig ist.
- Reglementieren Sie den Zugang zum Netzwerk und nutzen Sie Funktionen zur Authentifizierung und Autorisierung von Nutzern und Geräten.
- Nutzen Sie digitale Zertifikate und sorgen Sie für ein Zertifikats-Lifecycle-Management.
- Schützen Sie Remote-Zugänge und gewähren Sie Dritten nur die unbedingt erforderlichen Rechte.

peoplefone
VoIP Solutions Provider

peoplefone AG
Albisstrasse 107 · 8038 Zürich
Telefon 044 552 20 00 · www.peoplefone..ch