Sicherheit und Redundanz in VoIP-Netzwerken

Ausfälle bei grossen Telekommunikationsanbietern und breit gestreute Cyberattacken haben Unternehmen verunsichert. Wie anfällig sind All-IP und VoIP für Störungen oder Angriffe von aussen? Was viele bei der Frage nach Sicherheitslösungen ausser Acht lassen: Die Schwachstelle ist oft der Mensch.

DER AUTOR

Roger Vogler
Partner Manager, Peoplefone

Sind die bisherigen Technologien doch die besseren? In Bezug auf Telefonie hat sich mancher in der letzten Zeit wohl die alten Zeiten mit analogen Leitungen und ISDN zurückgewünscht. Denn die Häufung von Ausfällen des Fest- und Mobilnetzes sowie des Internets haben gezeigt, dass die IP-Technologie anfällig sein kann.

Nicht jeder braucht Redundanz

Wie sich also absichern? Internetanschlüsse mit verschiedenen Servicelevel sind eine Möglichkeit. Wer schnellstmöglich wieder erreichbar sein möchte, sollte eine überwachte Internetleitung wählen, bei der eine kurze Wiederherstellungszeit garantiert wird.

Wer permanent erreichbar sein muss, ist auf verschiedene Anbieter angewiesen, 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 Verfügbarkeit auch zu einer Kostenfrage. Daher empfiehlt es sich, zu überlegen, ob und ab wann eine zeitweise Unterbrechung der Kommunikation schädlich fürs Unternehmen ist.

Bei der grossen Mehrheit steigert VoIP-Telefonie die Gefahr, gehackt zu werden, nicht.

Ist Ihr Unternehmen gefährdet?

Die Auseinandersetzung mit Optionen, die einen vor dem Totalausfall schützen, ist nur ein Faktor der Diskussion um die Verfügbarkeit. Gleichzeitig wird die Sicherheit von VoIP in Bezug auf Hackerangriffe auf die Telefonie-Infrastruktur mitdiskutiert. Doch bei der grossen Mehrheit der Unternehmen steigert VoIP-Telefonie die Gefahr, gehackt zu werden, nicht. Dies 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, sich per Fernzugriff Zugang zu den Datennetzen zu verschaffen, lässt jedes Unternehmen zum potenziellen Angriffsziel werden. Zum Beispiel, um anhand von absichtlich herbeigeführten Störungen, Gelder zu erpressen oder um Telefonnummern für Phishing oder Spoofing zu missbrauchen.

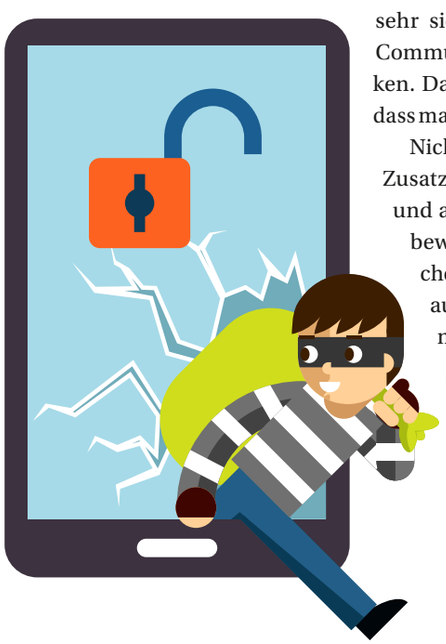

Illustration: Neyro/fotolia.com

Schützen Sie sich selbst!

Telekomanbieter 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. Man selbst und die Mitarbeitenden werden so ohne böse Absicht zu den Hauptgefahrenquellen. Alle Sicherheitslösungen helfen somit nichts, wenn im Unternehmen nicht ausreichend sensibilisiert wird.

Weniger kann ausreichen

Die IP-Technologie fordert die IT-Verantwortlichen 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 Prozent Redundanz und absolute Sicherheit investieren. Die bewährten Sicherheitsansätze und Sicherheitsprodukte lassen sich oftmals auf die VoIP-Infrastruktur ausdehnen, sodass mit bestehenden Mitteln gearbeitet werden kann. Sind ausserdem alle im Unternehmen für potenzielle Gefahren sensibilisiert, ist die benötigte Sicherheit meist gewährleistet.