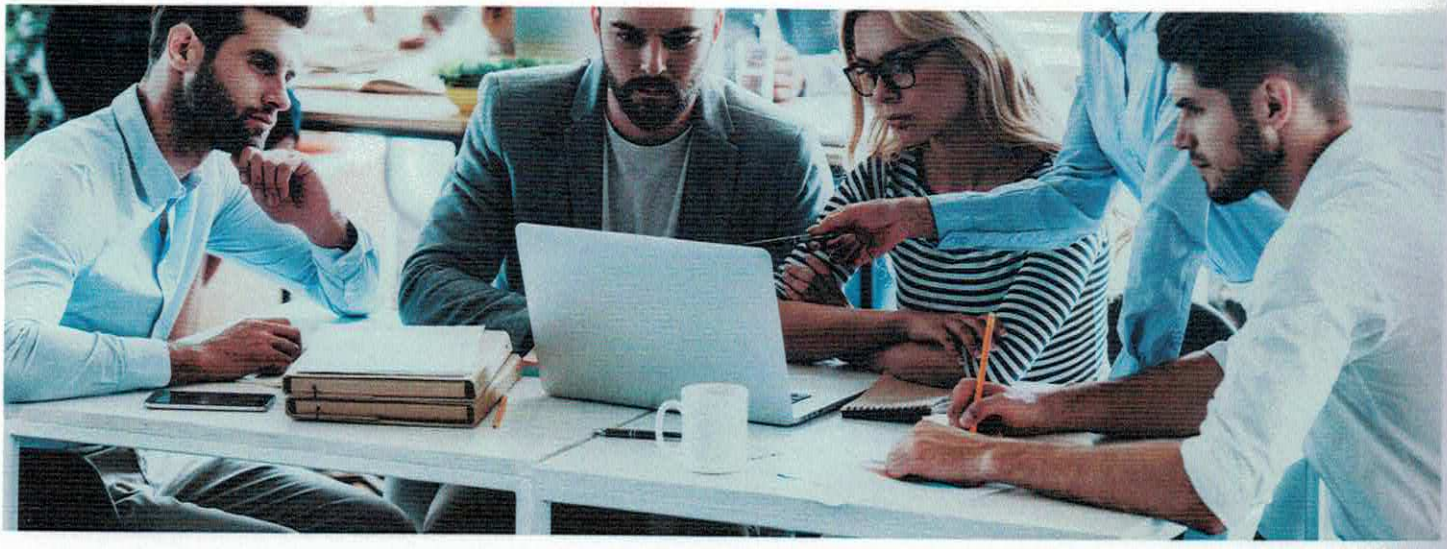
AUSGABE **02/2018**

kmu RUNDSCHAU

DER SPIRIT IST DA

TEAMBILDUNG IN DER PRAXIS

INDUSTRIE 4.0 I DACH ERP I VERSCHLÜSSELTE KOMMUNIKATION I NÜCHTERNE ANLAGE



Jedes Unternehmen ist potenzielles Angriffsziel.

SICHERHEIT UND REDUNDANZ

VOIP-NETZWERKE IM HÄRTETEST

von Christophe Beaud

Unternehmen sind aufgrund der Ausfälle bei grossen Telekommunikationsanbietern und breit gestreuter Cyber-Attacken verunsichert: Wie anfällig sind All-IP und VoIP für Störungen? Was bei der Evaluation von Sicherheitslösungen nicht ausser Acht gelassen werden darf: Die Schwachstelle ist oft der Mensch.

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.

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 Festnetzes sowie der Mobiltelefonie haben gezeigt, dass die IP-Technologie anfällig sein kann.

VERFÜGBARKEIT IST EINE KOSTENFRAGE

Wie können Verantwortliche ihr Unternehmen absichern? Internetanschlüsse mit verschiedenem Servicelevel sind eine Möglichkeit. Wer schnellstmöglich wieder erreichbar sein möchte, sollte eine überwachte Internetleitung wählen, bei der eine kurze Herstellungszeit 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 ein zeitweiser Unterbruch der Kommunikation schädlich fürs Unternehmen ist.

DIE THESE: VOIP, EINE GEFAHRENQUELLE

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 Zugriff auf die Datennetze 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.

SICH SELBST SCHÜTZEN

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. Man selbst und die Mitarbeitenden werden so ohne böse Absicht zu den Hauptgefahrenquellen. Alle Sicherheitslösungen helfen somit nichts, wenn die Mitarbeiterinnen und Mitarbeiter im Unternehmen nicht ausreichend sensibilisiert werden. Eine Sicherheitsphilosophie lebt von Vorbildern aus der Führungsetage.

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 hinausschiesst. 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. ■

Mitarbeiterinnen und Mitarbeiter auf mögliche Gefahren sensibilisieren.

CHRISTOPHE BEAUD

ist CEO der peoplefone AG.

www.peoplefone.ch