

MANAGED SERVICES

Mehr Freiräume für mehr Sicherheit

Im Zuge der fortschreitenden Digitalisierung von Geschäfts- und Kommunikationsprozessen rückt das Thema Sicherheit bei Unternehmen in den Fokus. Denn: Mit der Flexibilität steigt auch das Risiko für Netzwerke, wie eine aktuelle Bitkom-Studie belegt. Im Jahr 2020/21 waren rund neun von zehn Unternehmen von Angriffen betroffen.

Innere Verfügbarkeit und äußerer Schutz – das A und O

Im Kern muss ein Sicherheitskonzept die Verfügbarkeiten der Infrastruktur auch bei Lastspitzen sowie den Schutz gegen Hacker-Angriffe abdecken. Verfügbarkeit bezieht sich auf die Leistungsfähigkeit des Systems: Sind die Datenleitungen in der Lage, Daten-Traffic und Sprache gleichzeitig und reibungslos zu übertragen? Ein Thema, das schon lange nicht mehr nur den Call- und Contactcenter-Bereich umtreibt, sondern nahezu alle Branchen, die die Erreichbarkeit ihrer Mitarbeiter gewährleisten wollen.

Der zweite Sicherheitsaspekt nimmt die Abwehrfähigkeit einer IT-Infrastruktur gegenüber illegalen Zugriffen von außen in den Blick. Hier zählen Firewalls zu den wichtigsten Instrumenten der IT-Security. Dabei wird oft der Schutz der Telefonie, genauer gesagt der SIP-Telefonie, nicht ausreichend berücksichtigt. Denn auch moderne IP-Telefone und -Telefonanlagen sind ein Einfallstor. Die Angreifer können enorme Kosten verursachen, indem sie Anrufe über die Telefonanlage absetzen oder sensible Daten abgreifen. Die Absicherung von Kommunikationsdaten sollte daher nicht auf die leichte Schulter genommen werden. Damit weitere blinde Flecken ausgeschlossen werden, sollten Unternehmen auch eine vollständige Aufstellung der einzelnen Anwendungen und Dienste, die via Cloud verfügbar sind, vornehmen und im Zweifel individuell absichern.

Managed Service Provider für aktive Sicherheit

Sind alle Sicherheitsmaßnahmen erfasst, ist es mit der Installation der Hardware nicht getan. Ohne eine permanente Überwachung und Wartung kann der erforderliche Sicherheitsstandard nicht erreicht werden. Hierfür bieten sich Managed Service Provider an: Ein sicherer Betrieb erfordert Fachpersonal sowie ein proaktives Monitoring und laufende Anpassungen. Das umfasst die sofortige Alarmierung und Behebung bei Problemen – im Idealfall durch einen 24/7-Support. Regelmäßige Backups und Reportings gehören ebenfalls zu den Grundlagen einer zeitgemäßen Firewall-Lösung. Dabei können Unternehmen verschiedene Managed-Service-Pakete je nach Anforderung auswählen:

Neben der Absicherung der Datenströme gegen Cyberangriffe durch Managed-Firewall-Lösungen oder für Telefonie durch eine Managed-SBC-Variante, gibt es auch Managed Services für komplexe Netzwerkinfrastrukturen im SD-WAN-Bereich. Insbesondere wenn ein Unternehmen mehrere Standorte unterhält, sind verschiedene Breitband-Anbindungstechnologien verfügbar. Beim Einsatz von SD-WAN werden die Softwareservices von der Hardware entkoppelt. So werden auch heterogene Technologien unter einer einheitlichen Schnittstelle vereint. Damit können flexible Topologien realisiert sowie kostenoptimierte (Sicherheits-)Erweiterungen quasi auf Knopfdruck bis zum Netzwerkrand eingebunden werden. Wird SD-WAN zudem als Managed Service genutzt, bieten die Provider die komplette Installation, Betreuung, Überwachung und Wartung an. Neben dem Vorteil der Planbarkeit der monatlichen Kosten verschafft das dem IT-Team wieder mehr Luft, sich um relevante Projekte, wie beispielsweise der Optimierung des Kundenservices, zu kümmern. Denn im Gegensatz zu anderen Lebensbereichen gilt die Devise „no risk, more fun“ – oder mehr Zeit fürs Geschäft.

Die Vorteile auf einen Blick:

- **Spart Zeit und Kosten:** Einfache Planung durch monatlich festgelegte Kosten. Unternehmen wissen immer, wieviel sie bezahlen und wofür. Zusätzlich sparen sie dabei Zeit ein.
- **Geschulte IT-Fachkräfte:** Durch das Auslagern von Teilbereichen oder der gesamten IT können Unternehmen auf Spezialisten zugreifen, die das vorhandene Know-how ergänzen.
- **Regelmäßige Updates:** Ein regelmäßiges Monitoring findet statt, sodass Updates aktuell und teilweise automatisiert eingespielt werden können.



Alexander Nohles,
Head of Technical Department
bei byon GmbH
www.byon.de

byon
communicate