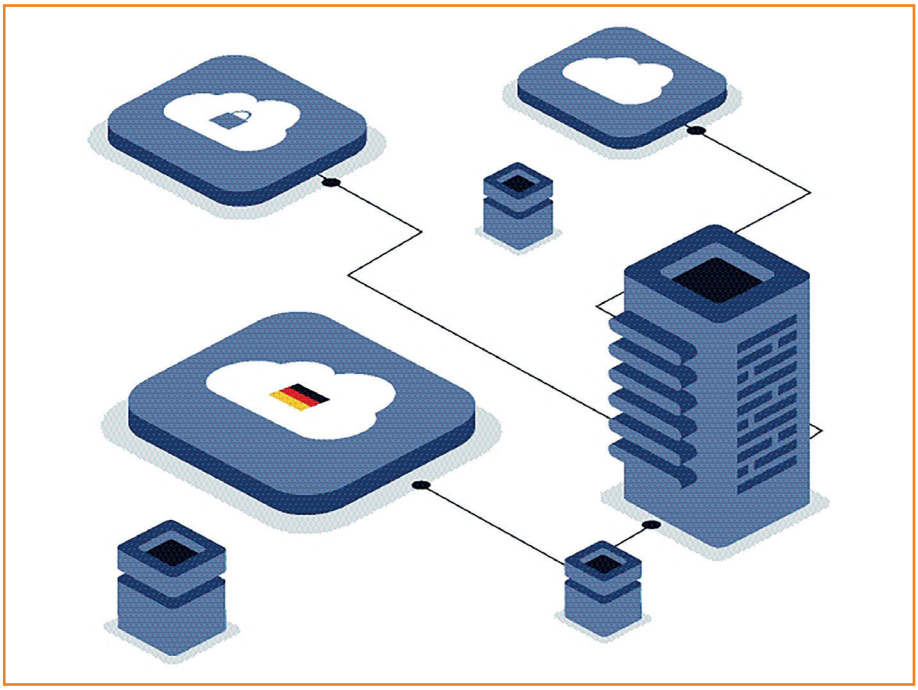
Digitale Souveränität

Kommunikationslösungen sicher hosten – aber wie?

Tobias Stepan

Der Anbietermarkt von SaaS-Lösungen wächst und die Nachfrage nach flexiblen und skalierbaren Infrastrukturen nimmt zu. Parallel steigen die Anforderungen an Datenschutz und -sicherheit. Leider vervielfacht sich auch die Anzahl von Hackerangriffen und Vorfällen, die die Cybersicherheit gefährden. Dabei ist vielen Organisationen nicht bewusst, dass sie mit ihren IT-Lösungen ins Visier von Cyberkriminellen geraten können oder sich rechtlich auf sehr dünnes Eis begeben. Worauf kommt es bei der Wahl einer Kommunikationslösung also an und welche Rolle spielt dabei das Hosting der Software?



Viele Tools und Kommunikationslösungen, die hierzulande im Unternehmensalltag zum Einsatz kommen, basieren auf Lösungen US-amerikanischer Cloud-Provider. Das Problem hierbei ist, dass es keine Rechtsgrundlage gibt, um personenbezogene Daten in den USA oder von US-Unternehmen verarbeiten zu lassen. Der sogenannte transatlantische Datentransfer wäre nur zulässig, wenn die USA als Drittland ein angemessenes Datenschutzniveau vorweisen könnten (Artikel 44 DSGVO) – oder ein sogenannter Angemessenheitsbeschluss (Artikel 45 DSGVO) vorläge. Beides ist nicht mehr gegeben, seit der Europäische Gerichtshof (EuGH) auch das Privacy-Shield-Abkommen 2020 für ungültig erklärte.

Dringender Handlungsbedarf

Doch es geht nicht nur um den Schutz personenbezogener und unternehmenskritischer Daten, sondern auch um die Gewährleistung des Organisationsbetriebs und der Kommunikation – insbesondere in Krisen- und Notfallsituationen. Laufen bestimmte Dienste einer Organisation in der Cloud großer US-Konzerne, sind Alternativen als eine Art Sicherheitsnetz nötig, um bei einem Ausfall dieser Cloud-Strukturen – ganz gleich ob durch höhere Gewalt, menschliches Fehlverhalten oder gezielte Attacken – wichtige Prozesse wie die interne Kommunikation aufrechterhalten zu können. Hier geht es gezielt darum, digital resilient und souverän zu sein. Denn dann kann auch in Krisensituationen oder im Fall von Cyberattacken im eigenen Unternehmen die volle Funktionsfähigkeit der Softwarelösungen gewährleistet werden. So ist der interne Informationsfluss zu keiner

Mit dem Zero-Trust-Modell können Unternehmen zusätzliche Sicherheit in ihre IT-Infrastruktur integrieren. Die Prämisse hierbei ist: Kein Tool, keine Plattform, kein Anwender ist sicher

Tobias Stepan ist Gründer und Geschäftsführer der Teamwire GmbH in München

Zeit unterbrochen und die Organisation bleibt weiter handlungsfähig.

Mit Netz und doppeltem Boden

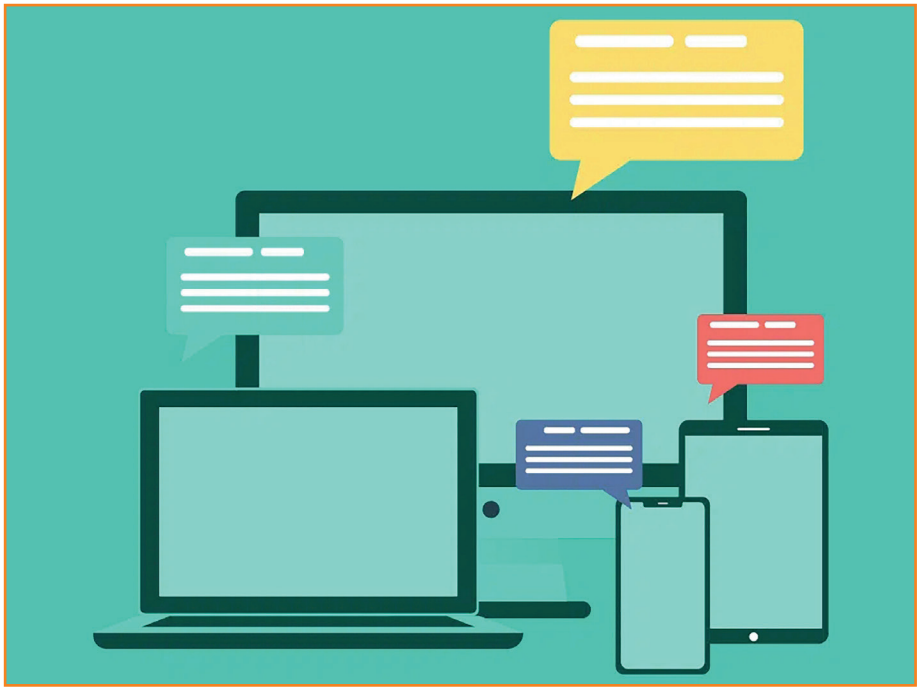
Ein Plus an Sicherheit gewinnen Unternehmen, wenn Sie mit dem Zero-Trust-Modell zusätzliche Sicherheit in ihre IT-Infrastruktur integrieren. Die Prämisse des Modells ist: Kein Tool, keine Plattform, kein User ist sicher. Deshalb werden jede Anforderung, jeder Zugriff und jede Anfrage an das System so geprüft, als käme sie aus einem offen zugänglichen Netz. Bevor also ein Zugriff gewährt wird, gilt es diesen vollständig zu authentifizieren, zu autorisieren und zu verschlüsseln sowie die Identität und den Zustand des Endgeräts zu überprüfen. Umfassende Business Intelligence (BI) und Analytics erkennen zudem Anomalien in Echtzeit und wehren sie ab. Dies macht es Cyberkriminellen erheblich schwerer, die Kommunikationslösung als Einfallstor zu nutzen.

Wahl einer Kommunikationslösung

Mit dem Ziel, die eigenen Daten bestmöglich zu schützen und die Kommunikation auch im Krisenfall sicherzustellen, müssen Unternehmen ihre bestehende (wie auch jede neu in Erwägung gezogene) Kommunikationslösung und deren Hosting-Anbieter hinsichtlich Datenschutz und -sicherheit überprüfen und sich folgende Fragen stellen.

Im Hinblick auf das Hosting:

- Bietet der Dienstleister für seine Kommunikationslösung verschiedene Hosting-Modelle an (Public Cloud, Private Cloud, On-Premises)?
- Findet bei Public-Cloud-Lösungen kein Datentransfer in die USA oder andere Drittländer ohne angemessenes Datenschutzniveau statt?
- Liegen Sitz des Softwareanbieters und des Cloud-Providers innerhalb der EU?
- Basiert die Kommunikationslösung auf einer ausfallsicheren Serverinfrastruktur in ISO-27001-zertifizierten Rechenzentren?



Unternehmen benötigen eine Art Sicherheitsnetz, um bei einem Ausfall der Cloud-Strukturen wichtige Prozesse wie die interne Kommunikation aufrechtzuerhalten (Bilder: Teamwire)

Bezüglich Datenschutz und -sicherheit:

- Lässt sich das Zero-Trust-Modell damit umsetzen?
- Werden alle Anforderungen der DSGVO und ggf. anderer rechtlicher Vorschriften, umgesetzt? Dazu gehören beispielsweise Dokumentations- und Archivierungspflichten, keine Analyse von Metadaten, Anonymisierung von personenbezogenen Daten, Mehrfach-Authentifizierung u.v.m.
- Folgt der Softwareanbieter den Grundsätzen von Privacy by Design und Privacy by Default?
- Garantiert der Dienstleister dem Anwender die volle Kontrolle und Datenhoheit?
- Bringt der Anbieter der Kommunikationslösung entsprechende Erfahrung im Umgang mit Datenschutz und Datensicherheit mit?
- Kann die Kommunikationslösung mit detaillierten Referenzen überzeugen?

Lassen sich diese Fragen für eine konkrete Kommunikationslösung bejahen, besteht aus datenschutzrechtlicher Sicht und im Hinblick auf Datensicherheit und -souveränität eine gute Grundlage. Natürlich muss anschließend auch die Funktionalität der Lösung überzeugen, darunter Standardfunktionen wie beispielsweise Echtzeit-Messaging, Videotelefonie und die Einbindung mehrerer Endgeräte. Aber auch businessrelevante Aspekte – etwa eine einfache Administrationsoberfläche und Nutzerverwaltung, Alarmierungen und Statusnachrichten sowie die Möglichkeit, organisationsübergreifend zu kommunizieren und auch Drittsysteme anzubinden. Schließlich ist es auch die Qualität von Kommunikationsprozessen, die die digitale Resilienz und Souveränität fördert.

Datensouveränität ist das A und O

Nicht allen Unternehmen ist aktuell bewusst, auf welcher rechtlichen und technischen Grundlage sie ihre Kommunikationslösungen betreiben. Nicht selten fehlt die Transparenz seitens der Lösungsanbieter, auch hinsichtlich der Erklärungen zu Datenschutz und Sicherheitsstandards. Dies sorgt für eine bedenkliche Abhängigkeit der Unternehmen von diesen Anbietern. Dabei trägt jedes Unternehmen rein rechtlich selbst die Verantwortung für die Datenverarbeitung.

www.teamwire.eu