



Das Faust-Prinzip

Cloud oder eigenes Rechenzentrum? Dieser für alle Firmen drängenden Frage ging eine Veranstaltung der Karlsruher IT-Sicherheitsinitiative nach

Die aktuelle Frage aller Fragen im IT-Bereich stellte die Karlsruher IT-Sicherheitsinitiative (KA-IT-Si) dieses Mal gleich an zwei Experten: Wie hältst du's mit den Daten? Eigenes Rechenzentrum betreiben oder die Daten in die Cloud auslagern? Wie schon bei Goethes Faust bleibt die Antwort offen, oder besser: Sie musste offen bleiben. Zu unterschiedlich die Anforderungen, zu unterschiedlich die Sicherheitsempfinden in den Firmen. Hinzu kommt die Tendenz, dass innerhalb der Unternehmen einzelne Abteilungen immer häufiger ein IT-Eigenleben führen. Jede wählt die für sie praktikabelste Lösung. Gesamtkonzept? Meist Fehlanzeige. Sehr zum Leidwesen der IT-Verantwortlichen. Das ist nicht wünschenswert, aber nicht zwangsläufig schlecht. Je größer die Vielfalt, desto mehr Aufwand muss ein Datendieb betreiben und desto geringer seine Beute.

Der Schritt von der Vielfalt zum Chaos ist ein kleiner. „93 Prozent der IT-Verantwortlichen bevorzugen ein eigenes Rechenzentrum und bezeichnen ein solches als Schlüssel zum wirtschaftlichen Erfolg“, zitiert Andreas Kühne vom

Rechenzentrums-Anbieter Rittal eine aktuelle Umfrage. Vor allem die Betriebskosten stehen im Blickpunkt bei der Entscheidung für oder gegen die Datenlagerung im eigenen Haus. Und da haben Cloud-Dienste wiederum die Nase vorn. Sie bieten hundertprozentige Kalkulationssicherheit – Controller-Herzen schlagen höher. Standardisierung lautet die Antwort der Rechenzentren-Anbieter darauf. „Die Kosten sind ebenso im Vorfeld bekannt wie der zu erwartende ROI“, erklärt Kühne und ergänzt: „Das ist die überraschungsfreie Variante.“ Verbunden mit dem Wissen, dass die unterschiedlichen Komponenten harmonieren und störungsfrei funktionieren. Ein solches Modulmodell verringert ebenso den Zeithorizont. Langwierige Planungen entfallen. Sechs Wochen nach der Bestellung erfolgt die Inbetriebnahme – das ist die Regel.

Was jedoch keineswegs bedeutet, dass mit der Entscheidung für ein eigenes Rechenzentrum auch alle Daten im eigenen Unternehmen bleiben. „Manche lagern beispielsweise das Back-up in die Cloud aus“, berichtet Kühne aus der Praxis.

Andere wiederum „entscheiden sich gegen die Inhouse-Lösung – aufgrund eines stark schwankenden Kommunikationsverhaltens. Schnell ist da bei der Serverwahl die falsche Entscheidung getroffen“, lautet die Erfahrung von Matthias Kess. Der technische Leiter von Befine Solutions registriert seit der Snowden-Affäre ein deutlich gestiegenes Interesse am Thema Sicherheit. Und dabei setzt seine Firma auf die gute alte E-Mail. „Ginge es nach dem Silicon Valley, wäre die längst mausetot.“

Die neueste Technologie ist die E-Mail sicherlich nicht, 30 Jahre alt inzwischen und seither kaum weiterentwickelt. „Aber die Vorteile sind immens, was sich in einer unglaublichen Akzeptanz ausdrückt.“ Und mit der Kommunikations-Lösung Cryptshare blieben die Vorteile, ergänzt um die Komponente Sicherheit. Kein Austausch von Sicherheits-Zertifikaten, kein Einrichten von Benutzerkonten, ein Server genügt und schon läuft der geschützte Datenaustausch. Über Schnittstellen integrierbar in die gängigen E-Mail-Programme. Zwar stellt sich auch hierbei die Gretchenfrage. Aber

die Antwort fällt salomonisch aus: „Der Cryptshare-Server lässt sich inhouse betreiben, beim IT-Dienstleister des Vertrauens hosten oder in die Cloud auslagern.“ **mh**

KA-IT-Si
Karlsruher IT-Sicherheitsinitiative

Anti-Prism-Party

Schon zweimal sorgte die größte „Cryptoparty“ Europas mit 650 und über 900 Teilnehmern im Karlsruher ZKM für Raumnot. Nun folgt die dritte Auflage, dieses Mal an neuem Ort.



Wo Foyer des Staatstheaters Karlsruhe,
Wann 11. Oktober 2014,
14 Uhr

Mehr Infos unter
www.ka-it-si.de sowie
www.anti-prism-party.de