

RZ-Konsultation zur nationalen Rechenzentrumsstrategie

Ein zukunftsfähiger und leistungsstarker Rechenzentrumsstandort muss nicht nur energieeffizient und digital souverän sein, sondern vor allem resilient gegenüber physischen Bedrohungen. Die zunehmende geopolitische Unsicherheit und die Verbreitung asymmetrischer Angriffsformen – etwa durch Drohnen – machen deutlich: Rechenzentren, insbesondere solche mit kritischen Anwendungen, benötigen deutlich stärkeren physischen Schutz. Auch die Kommunikationsnetze und ihre Knotenpunkte selbst sind kritische Anwendungen.

Der physische Schutz tritt regelmäßig gegenüber dem digitalen Schutz in den Hintergrund, obwohl bereits eher kleine Schadensfälle im Frieden schon nicht unerhebliche volkswirtschaftliche Schäden verursachen.

Beispielhaft sei hier ein Brandereignis in einer Telekom-Zentrale in meiner Geburtsstadt Siegen am 21.01.2013 genannt (Zeitungsbeiträge: [Telekom-Brand in Siegen – Unternehmen räumt Defizite ein](#) & [Innenministerium fordert Bewertung an](#)).

Wie viel kritischer sich die Kommunikation gestalten würde, wenn ein potenzieller Feind durch Sabotage oder Drohnenangriffe entsprechende Einrichtungen flächendeckend ins Ziel nehmen würde, kann man sich gut vorstellen.

Zentrale Herausforderungen und Chancen:

- Herausforderung: Unzureichender baulicher Schutz gegen Sabotage, Brand, Drohnenangriffe oder andere militärische Einflüsse.
- Chance: Deutschland kann durch klare Vorgaben für physische Sicherheitsarchitekturen (z. B. Raum-in-Raum-Konzepte, Löschwasserresistenz, Einbruchschutz) zum Vorreiter für resiliente digitale Infrastruktur werden und durch ein resilientes Auftreten im Rahmen einer gestärkten Gesamtverteidigung die Gefahr einer tatsächlichen Auseinandersetzung reduzieren.

Erforderliche Rahmenbedingungen:

- Einführung verbindlicher Mindeststandards für bauliche Schutzmaßnahmen bei Cloud-Rechenzentren.
- Förderung von Investitionen in physische Sicherheitslösungen durch steuerliche Anreize und Förderprogramme.
- Pflicht zur physischen Separierung kritischer Cloud-Infrastrukturen in geschützte Zonen zur Schadensbegrenzung.

Rolle des Staates:

Der Staat sollte regulatorisch und fördernd eingreifen:

- Durch gesetzliche Vorgaben für physische Resilienz bei IT-Infrastrukturen.
- Durch gezielte Förderung sicherheitsrelevanter Innovationen.
- Durch strategische Partnerschaften mit Herstellern und Betreibern kritischer digitaler Dienste.

Konkrete Maßnahmen aus der Praxis:

- Verstärkter Einsatz von Brandwänden, Rauchschutzsystemen und Einbruchschutz-Türen.
- Raum-in-Raum-Lösungen mit brandresistenten (mindestens F90 / EI90) und (weitgehend) löschwasserundurchlässige Hüllen.
In diesem Bereich sind deutsche Unternehmen führend.
- Redundante Spiegelung kritischer Anwendungen in physisch getrennten und geschützten Cloud-Zonen.

Bei Resilienz im Sinne der Gesamtverteidigung darf es keinen Sparzwang geben!

Für Rückfragen oder weiterführende Gespräche stehe ich gerne zur Verfügung.

Freundliche Grüße

Jan-Eric Schacht
Solutions Portfolio IT Projects
Rittal GmbH & Co. KG · Auf dem Stützelberg · DE-35745 Herborn
eMail: SCHACHT.J@RITTAL.DE