



Krisensichere und resiliente Netzinfrastruktur und Konnektivität

Strategische Schwerpunkte und Technologien

WAS BEDEUTET KRISENSICHERHEIT UND RESILIENZ?



Es geht nicht nur um Redundanz und Ausfallsicherheit

Krisensicherheit

Fähigkeit, Krisen vorzubeugen, zu erkennen und deren Auswirkungen zu minimieren

Resilienz

Fähigkeit, Störungen zu überstehen und sich anzupassen



Zentrale Merkmale und Prinzipien

**Cyber-
Resilienz**

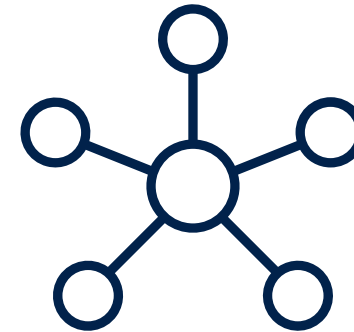
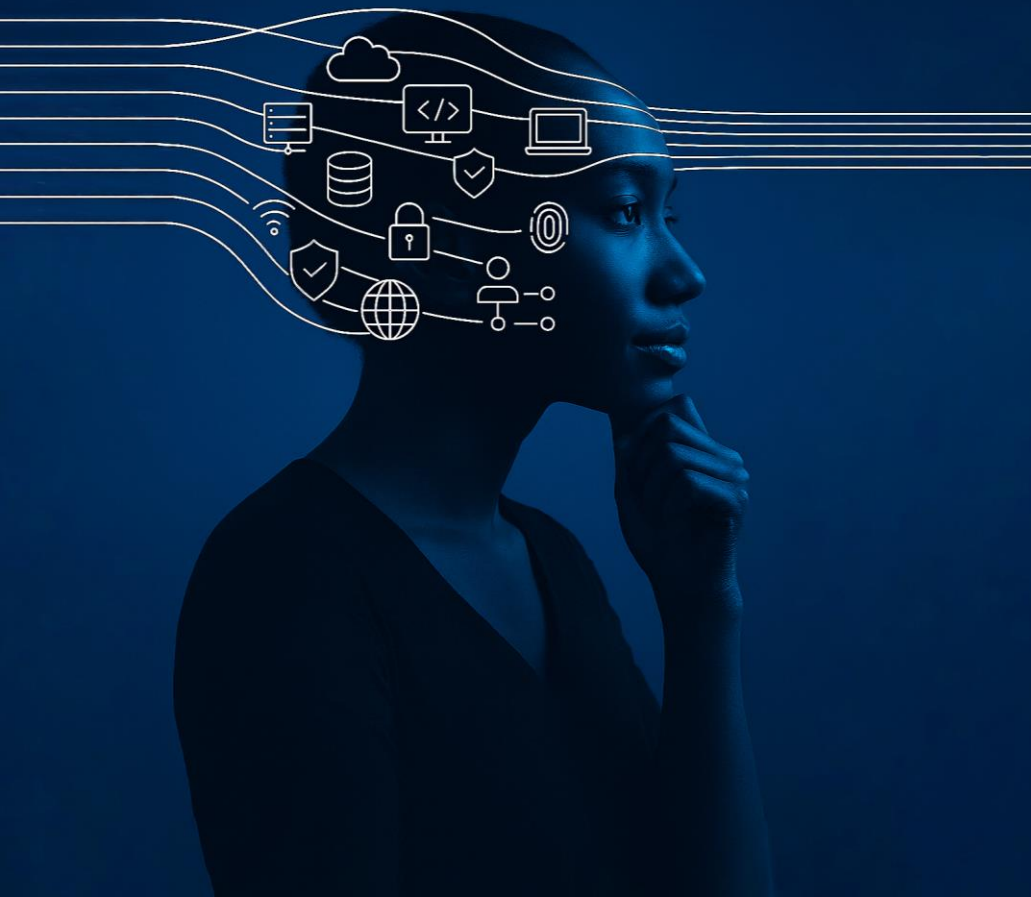
**Kontinuierliche Überwachung
und
Wiederherstellungsfähigkeit**

**Bessere Verfügbarkeit
und
Stromausfallsicherheit**

**Redundanz
und Diversität**

**Automatisierung und
Selbstorganisation**

**Dezentrale Strukturen
und Modularität**



SELBSTTHEILENDE UND INTELLIGENTE NETZWERKE



SELBSTTHEILENDE UND INTELLIGENTE NETZWERKE

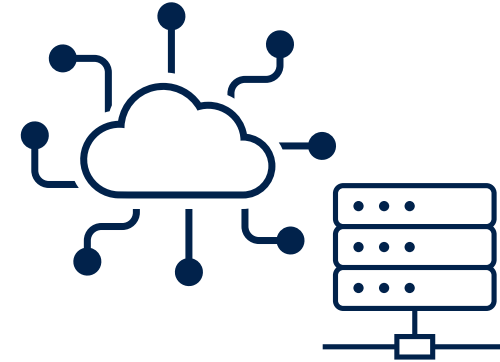
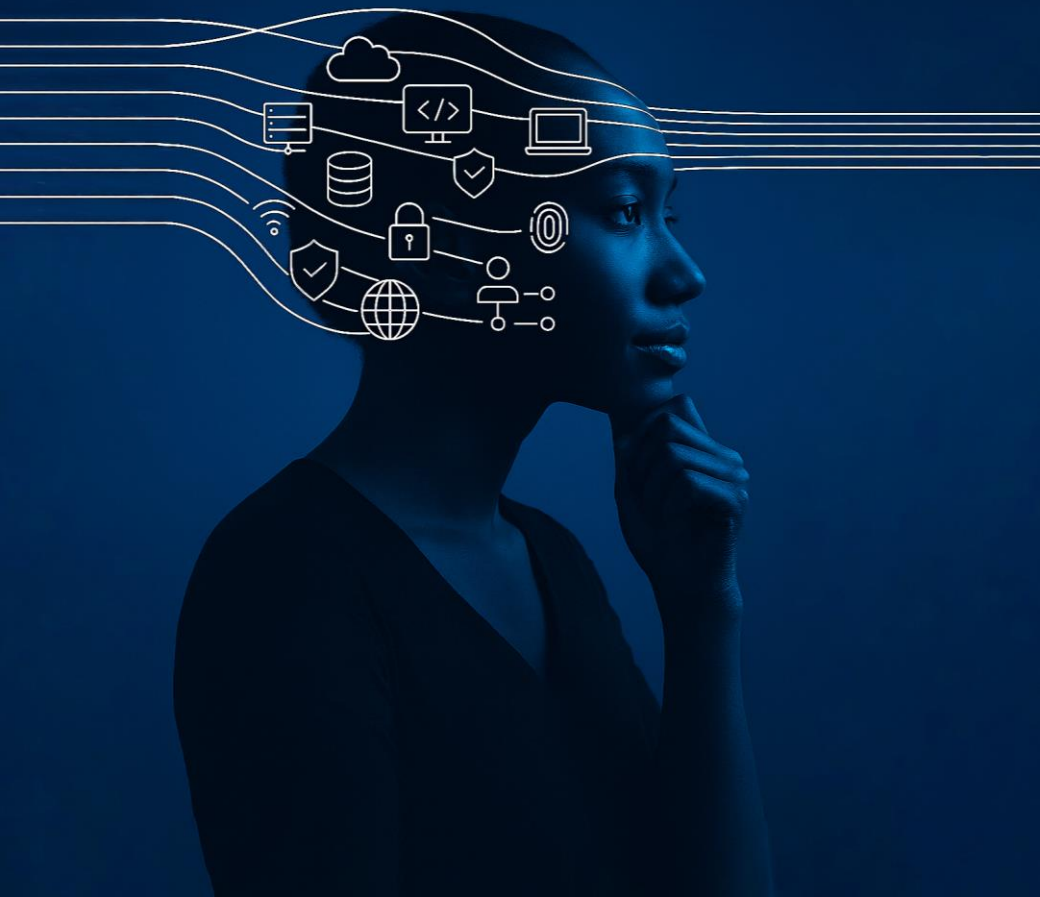
KI-gestützter **Betrieb und Automatisierung** (AIOps)

KI erkennt **Anomalien oder Verschleißmuster** frühzeitig und vermeidet Ausfälle, bevor sie auftreten

KI leitet **automatische Gegenmaßnahmen** bei Erkennung von Störungen oder Angriffsmustern ein

KI verbessert und optimiert das **Traffic-Management**

KI unterstützt die Implementierung von **Intent-based Networking**



EDGE COMPUTING UND DEZENTRALE INFRASTRUKTUR



EDGE COMPUTING UND DEZENTRALE INFRASTRUKTUR

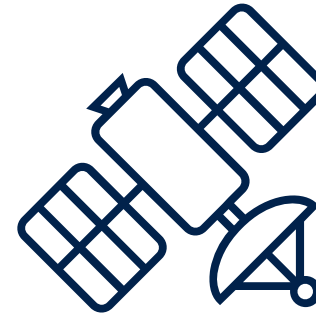
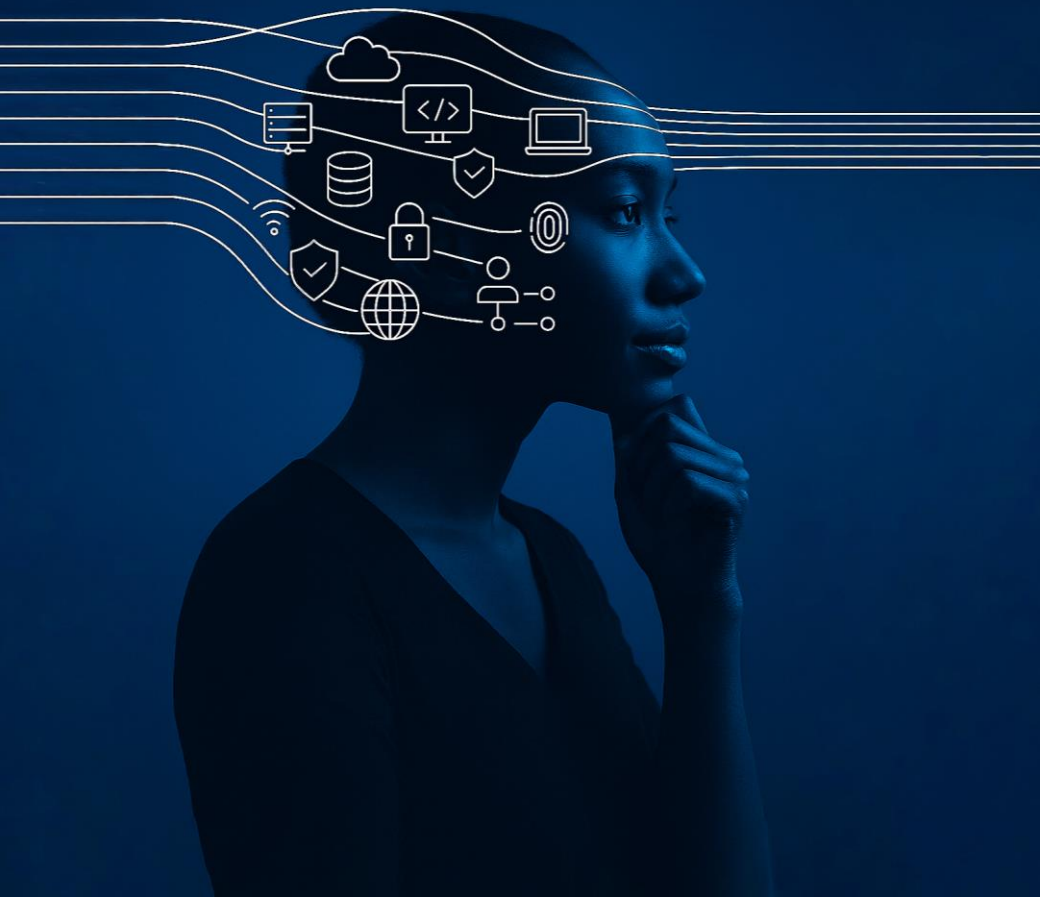
Reduzierung der Abhängigkeiten von zentraler Infrastruktur

Bandbreitenoptimierung und geringe Latenzzeiten

Vermeidung von Single Points of Failure

Diversifizierung: Multi-Cloud, Multi-Provider

Hybride Architekturen: Cloud und Edge



HYBRIDE UND NEXT-GEN KONNEKTIVITÄT



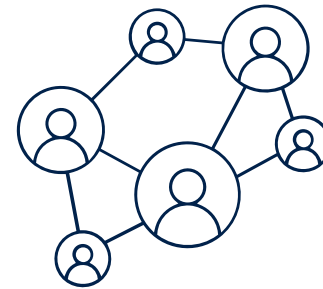
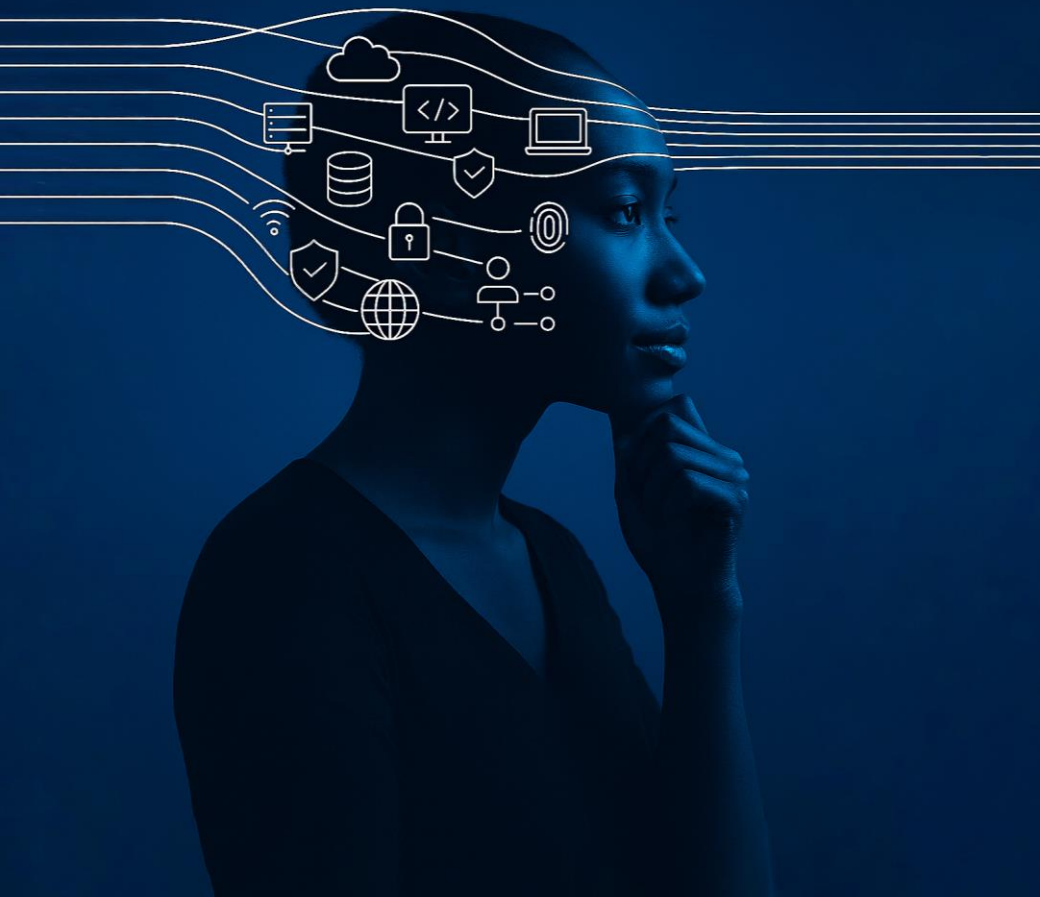
HYBRIDE UND NEXT-GEN KONNEKTIVITÄT

Nutzung von mehreren, **heterogenen Netzwerkverbindungen**
(Glasfaser, 5G/6G, Satellitenverbindungen)

Automatisierung von **Failover, Routing und QoS**

Nutzung von **SDN- und SD-WAN-Technologien**

5G/6G-Netzwerk-Slicing: Nutzung von **virtuellen, logisch getrennten Netzwerken**



VIRTUALISIERUNG VON NETZWERK- FUNKTIONEN



VIRTUALISIERUNG VON NETZWERK-FUNKTIONEN

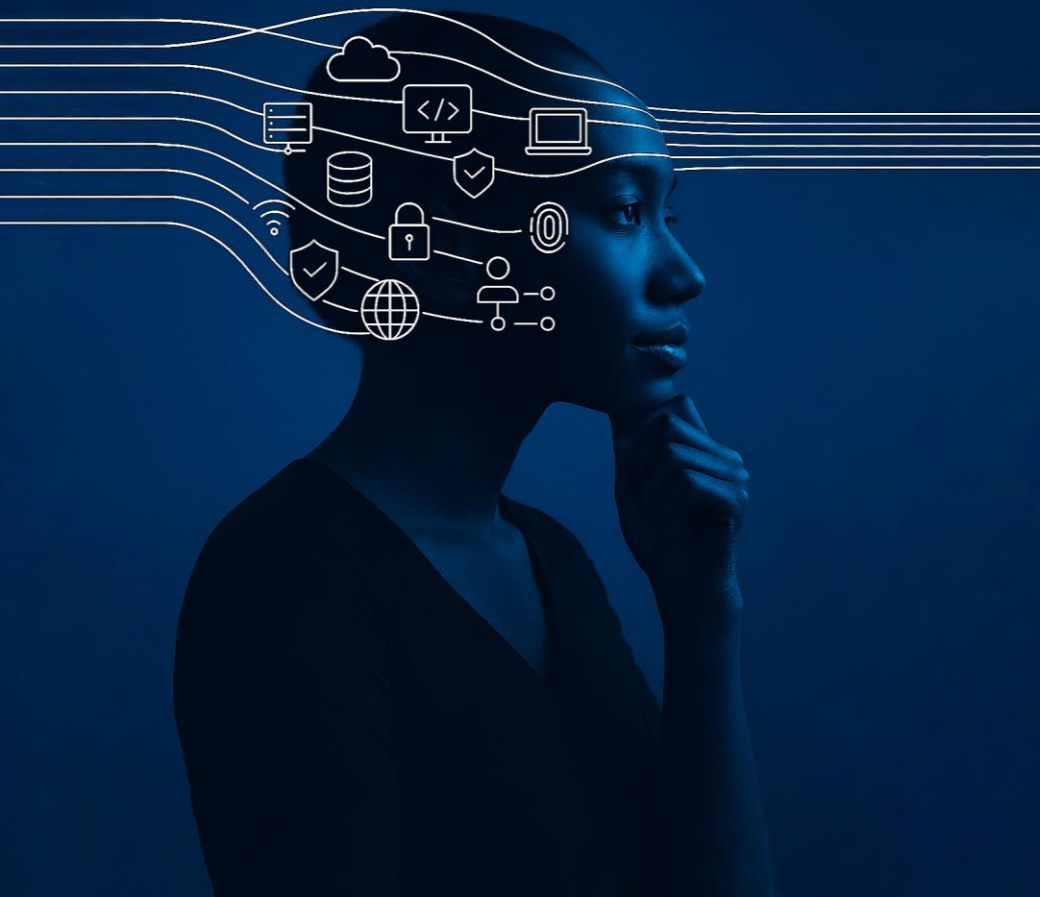
NFV (Network Functions Virtualization)
virtualisiert klassische Netzwerkfunktionen

Entkopplung von **Software und Hardware**

Integration mit SDN für dynamische Netzwerke

Hohe Flexibilität und geringe Bereitstellungszeiten

Aber auch **mehr Komplexität** und potenzielle Sicherheitsrisiken



ZERO TRUST UND MIKROSEGMENTIERUNG



ZERO TRUST UND MIKROSEGMENTIERUNG

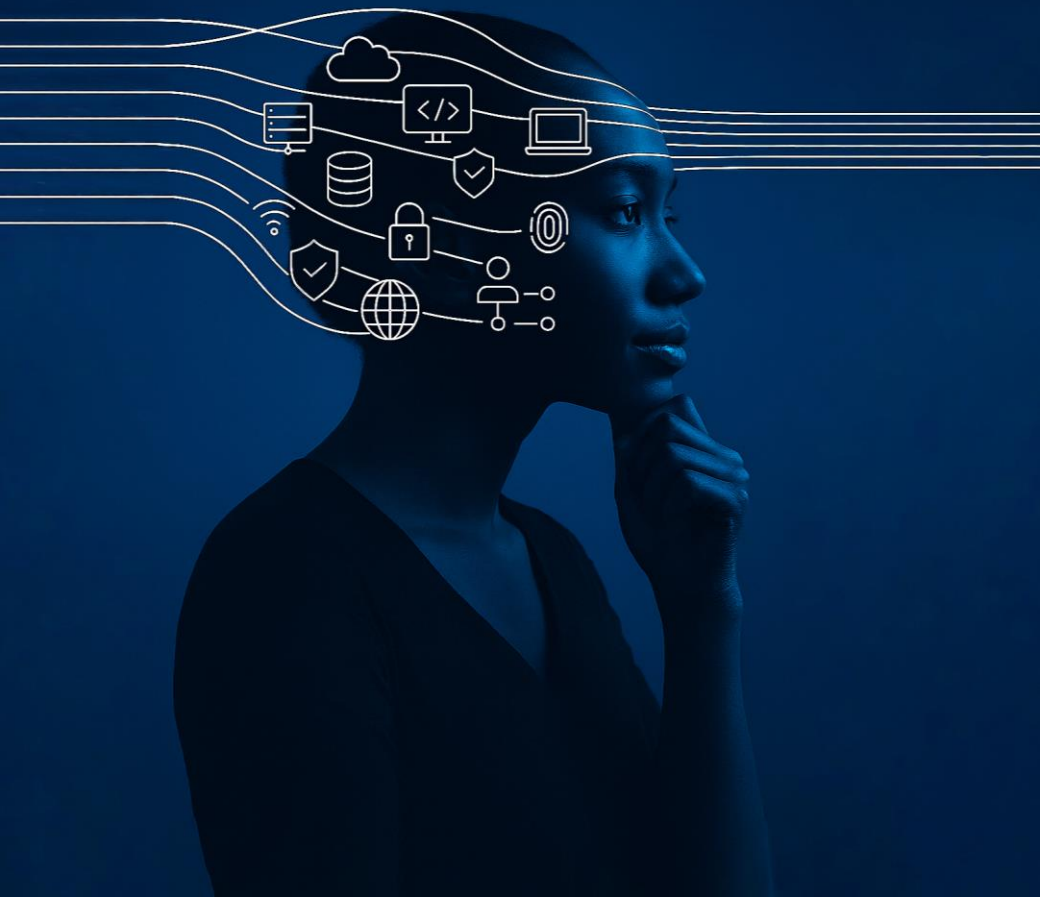
Umsetzung von **Zero Trust Architekturen** wird zum Standard

Traditionelle Netzwerkarchitekturen und statische Konfigurationen verschwinden

Dynamische **Richtlinien** und **Zugriffskontrolle**

Mikrosegmentierung zur **Verhinderung lateraler Ausbreitung** bei Vorfällen

Zero Trust ist ein zentraler Baustein für **Cyber-Resilienz**



CYBER-RESILIENZ STATT NUR CYBERSICHERHEIT



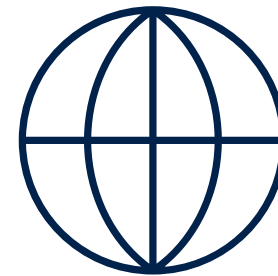
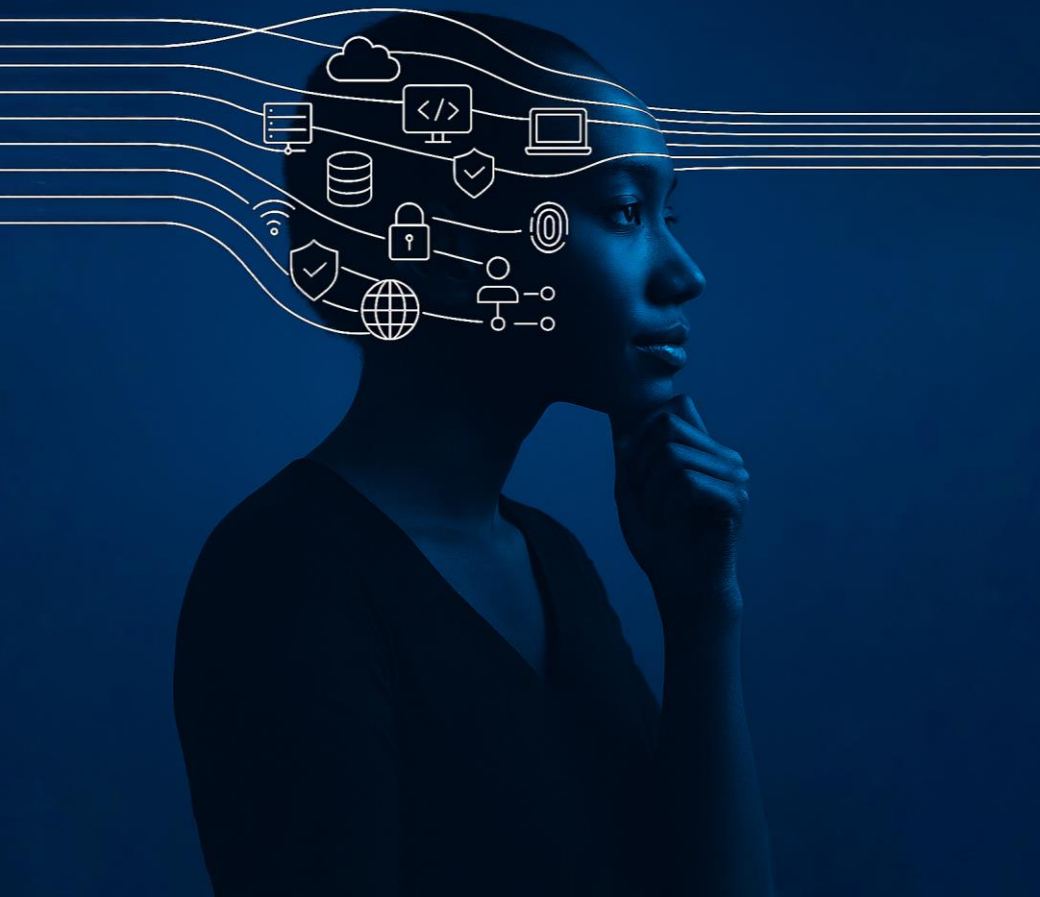
CYBER-RESILIENZ STATT NUR CYBERSICHERHEIT

Fokus verschiebt sich von reiner Prävention hin zur **Resilienz und Widerstandsfähigkeit**

Automatisierung ist unverzichtbar – insbesondere bei Incident Response und Orchestrierung

Kontinuierliche Überwachung

Sichere und **resiliente Lieferketten**



DIGITALE SOUVERÄNITÄT



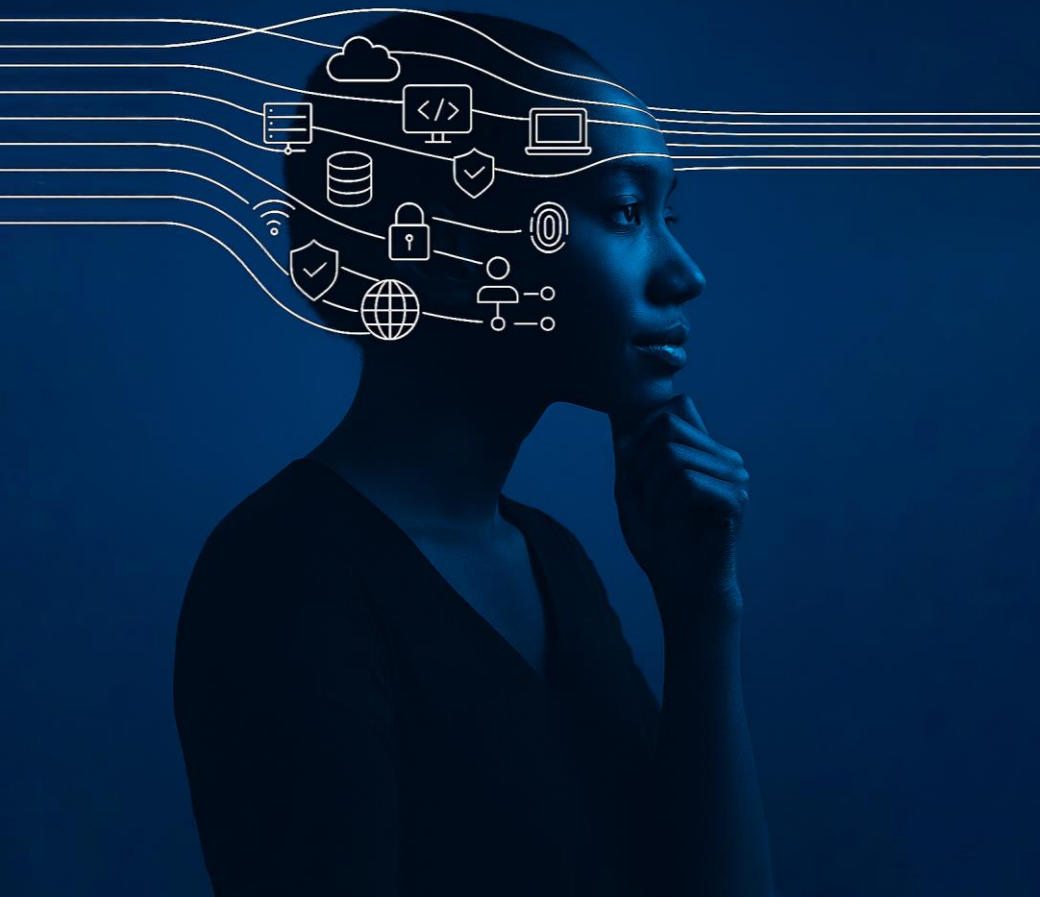
DIGITALE SOUVERÄNITÄT

Risiken ergeben sich aus geopolitischen, sicherheitsrelevanten und wirtschaftlichen Abhängigkeiten

Digitale Souveränität ist ein strategischer Hebel für **Resilienz und Krisensicherheit**

Kontrolle und **Minimierung von Abhängigkeiten**

Souveränität von Lieferketten, Netze, Cloud, KI, Daten, etc.



RESILIENZ DER ENERGIE- VERSORGUNG



RESILIENZ DER ENERGIEVERSORGUNG

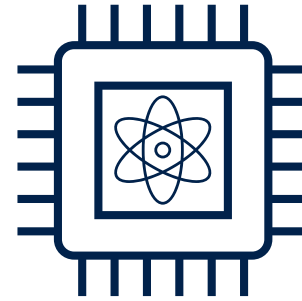
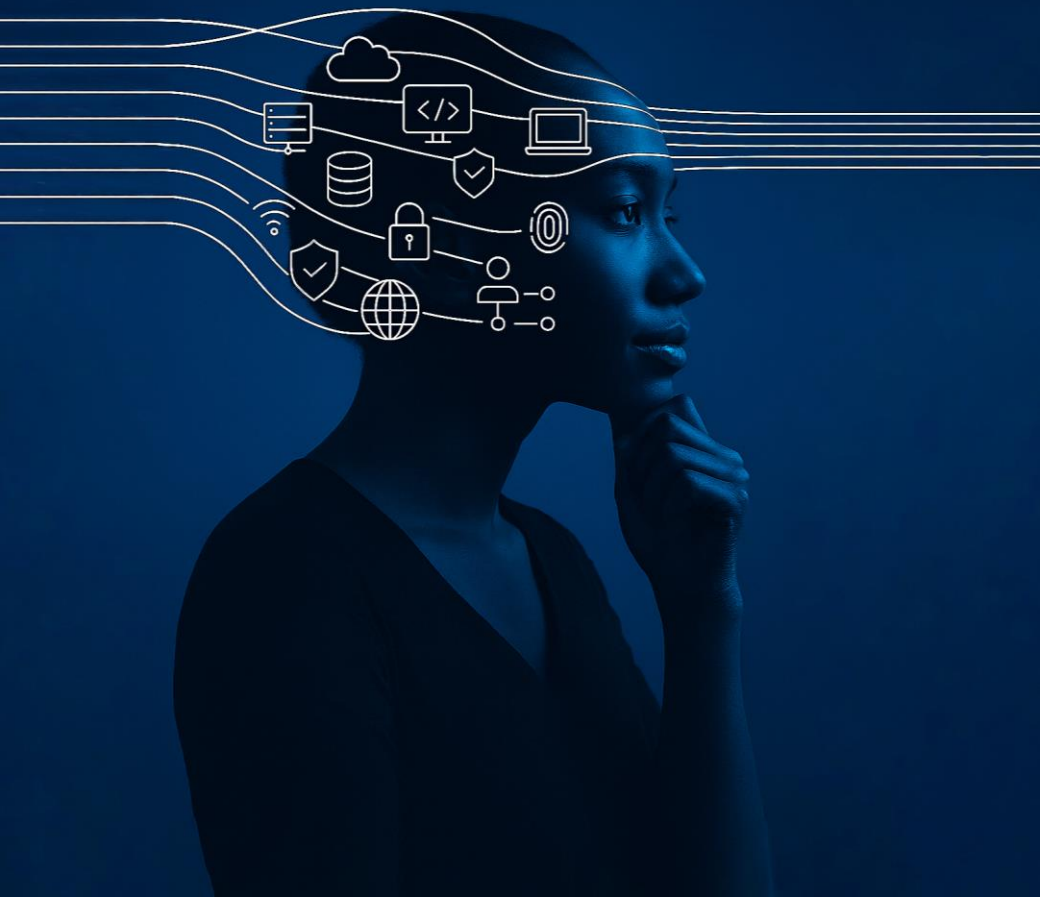
Risiko von Stromausfällen wird gerne unterschätzt – **Netzersatzanlagen** oft zu klein dimensioniert

Diversifizierung und redundante Stromversorgung

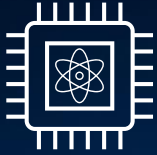
Integration von **Batteriespeicher** – stromgepufferte Netzwerkverbindungen

Intelligentes **Energiemanagement** und Priorisierung kritischer Dienste

Aufbau von lokalen, autarken **Stromnetzen** (Microgrids)



POST-QUANTEN- KRYPTOGRAPHIE (PQC)



POST-QUANTEN-KRYPTOGRAPHIE (PQC)

Klassische **asymmetrische kryptografische Algorithmen** werden durch Quantencomputer **unbrauchbar**

Symmetrische und **Hashing-Algorithmen** verlieren ca. 50% ihrer Sicherheitsstärke

Wahrscheinlichkeit, dass ein **kryptographisch relevanter Quantencomputer** entwickelt wird liegt bei bis zu 14% für 2030 und 34% für 2035

Umstellung auf **quantenresistente Kryptoalgorithmen** unbedingt notwendig

NOTFALLPLANUNG, BUSINESS UND IT SERVICE CONTINUITY

» Resilienz statt nur recovery

Business Continuity Management (BCM)

Fokus auf Unternehmensprozesse

IT Service Continuity Management (ITSCM)

Fokus auf Netz- und IT-Services,
sowie konkrete Definition von Wiederanlaufplänen

» Tests und Übungen sind unverzichtbar



Nur wer sein Ziel kennt,
findet den Weg

