



RESILIENZ, EFFIZIENZ UND DATENSCHUTZ

Stärkung der **Resilienz** mit global redundanter Infrastruktur von **AWS**

11.02.2025

Daniel Caduff

Principal Security Assurance DACH
Amazon Web Services Switzerland

Resilienz: Herausforderungen

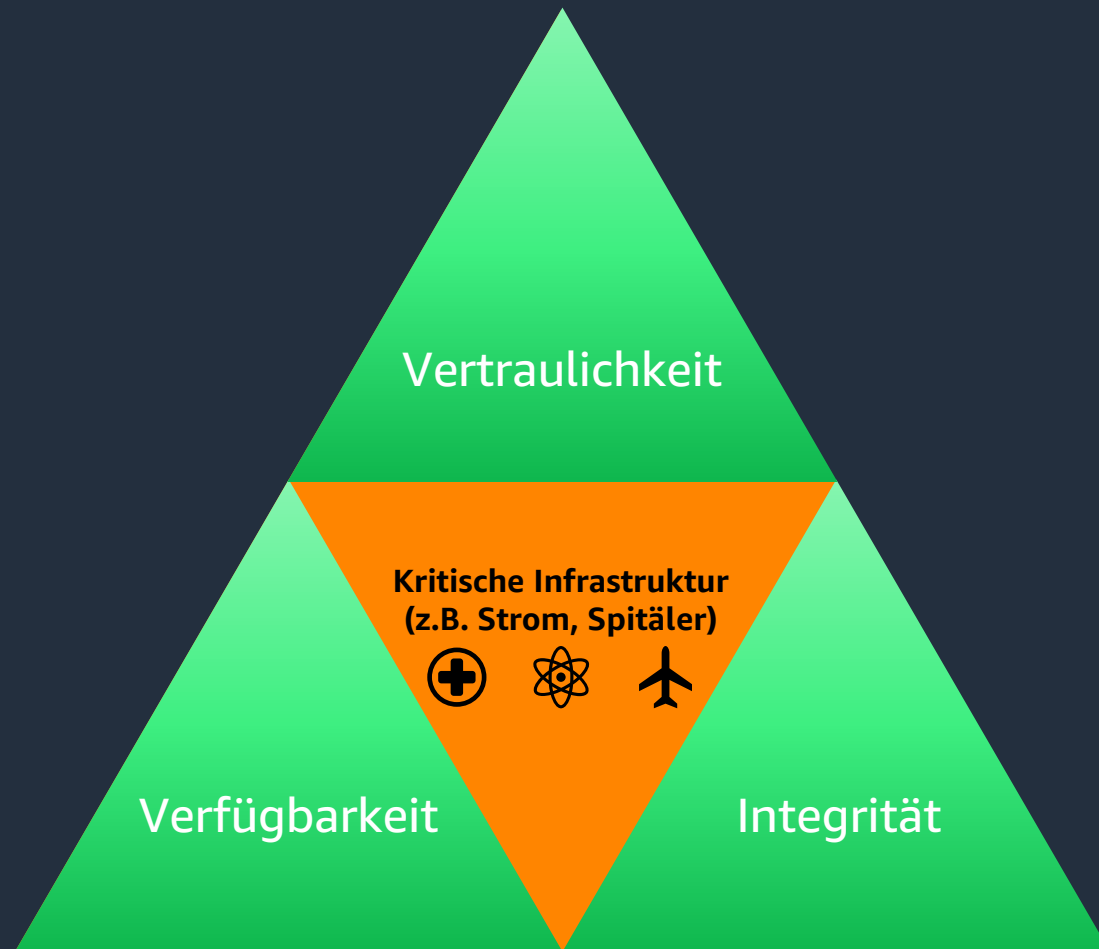


Definition



Resilienz:	Akzeptiert Risiken und bereitet sich auf sie vor
Resilienz:	Reduziert <i>nicht</i> die Eintretenswahrscheinlichkeit
Resilienz:	Bedeutet einen Schlag <i>einstecken</i> zu können

Bedrohungen



Verfügbarkeit

- Elementarschäden (Feuer, Wasser, etc.)
- Infrastrukturausfall (Stromausfall, Leitungsbruch)
- Cyberangriff (z.B. Ransomware)
- Hardwareschaden

Vertraulichkeit

- Cyberangriff (z.B. mit Phishing)
- Menschliche Fehler

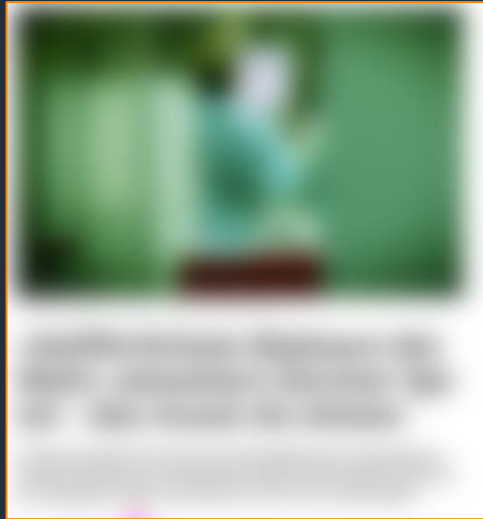
Integrität

- Cyberangriff (z.B. Man-in-the-middle)
- Fehlerhafte Sensoren / Messgeräte
- Menschliche Fehler

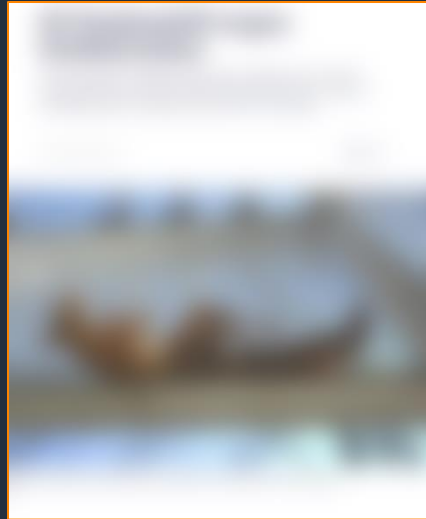
Risiken



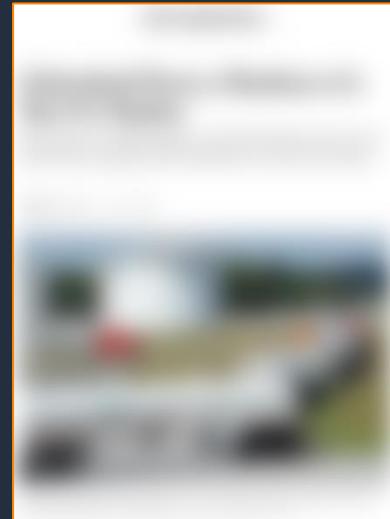
Daylimail.co.uk



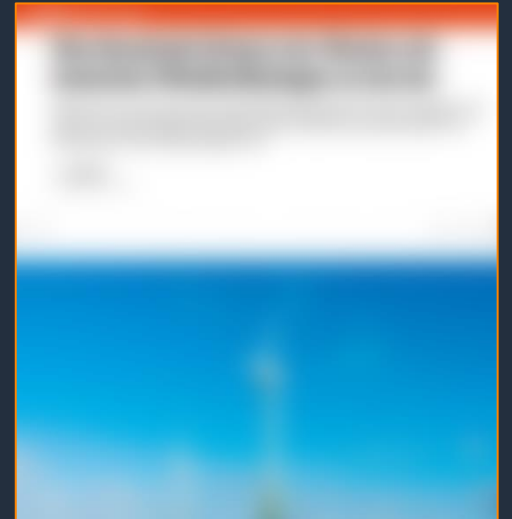
Watson.ch



Tagi.ch



nytimes.com



Spiegel.de

Verfügbarkeit: Risiko von Personenschäden



Vertraulichkeit: Reputationssrisiko, rechtliches Risiko

Integrität: Risiko von Personenschäden



*Resilienz ist niemals Selbstzweck. Systeme müssen resilient sein, weil der **Ausfall** der Systeme potenziell **Menschenleben gefährdet**.*

Die Vertraulichkeit des Patientendossiers ist niemals wichtiger, als das Überleben der Patientin!

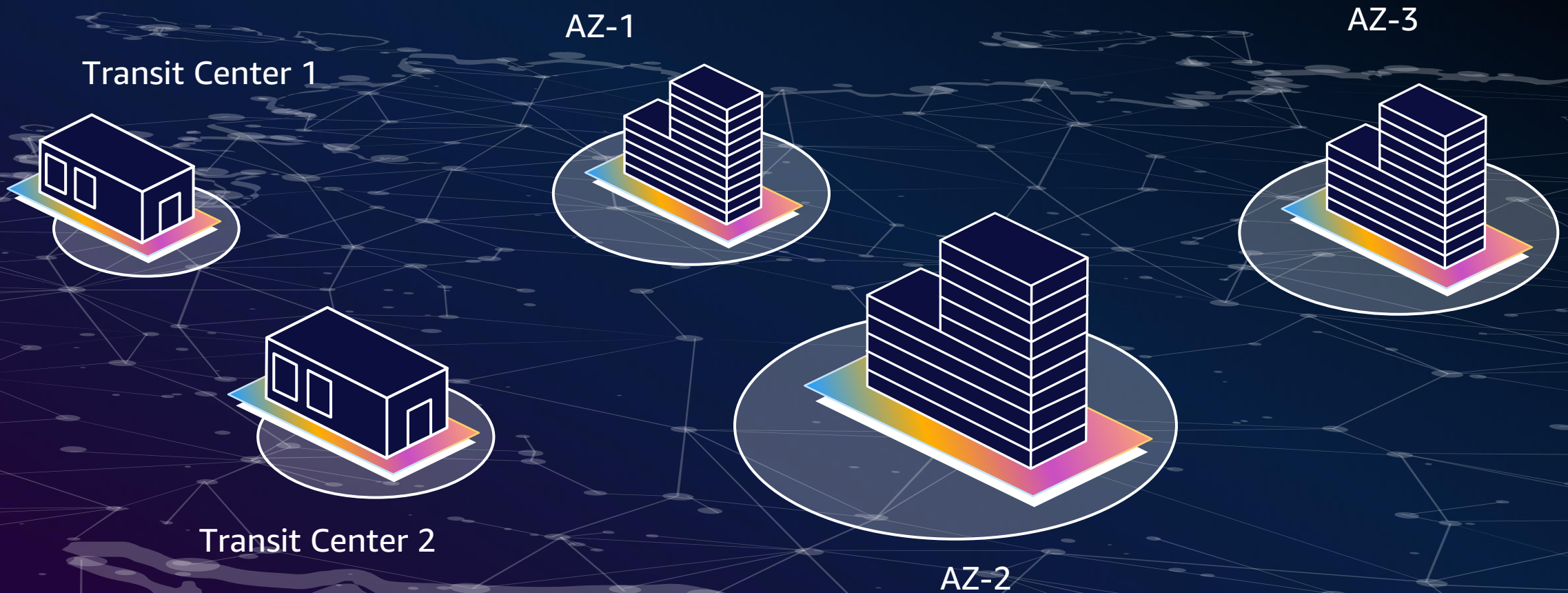
Resilienz: Antworten



Verteilte, global redundante Infrastruktur



Design einer Availability Zone

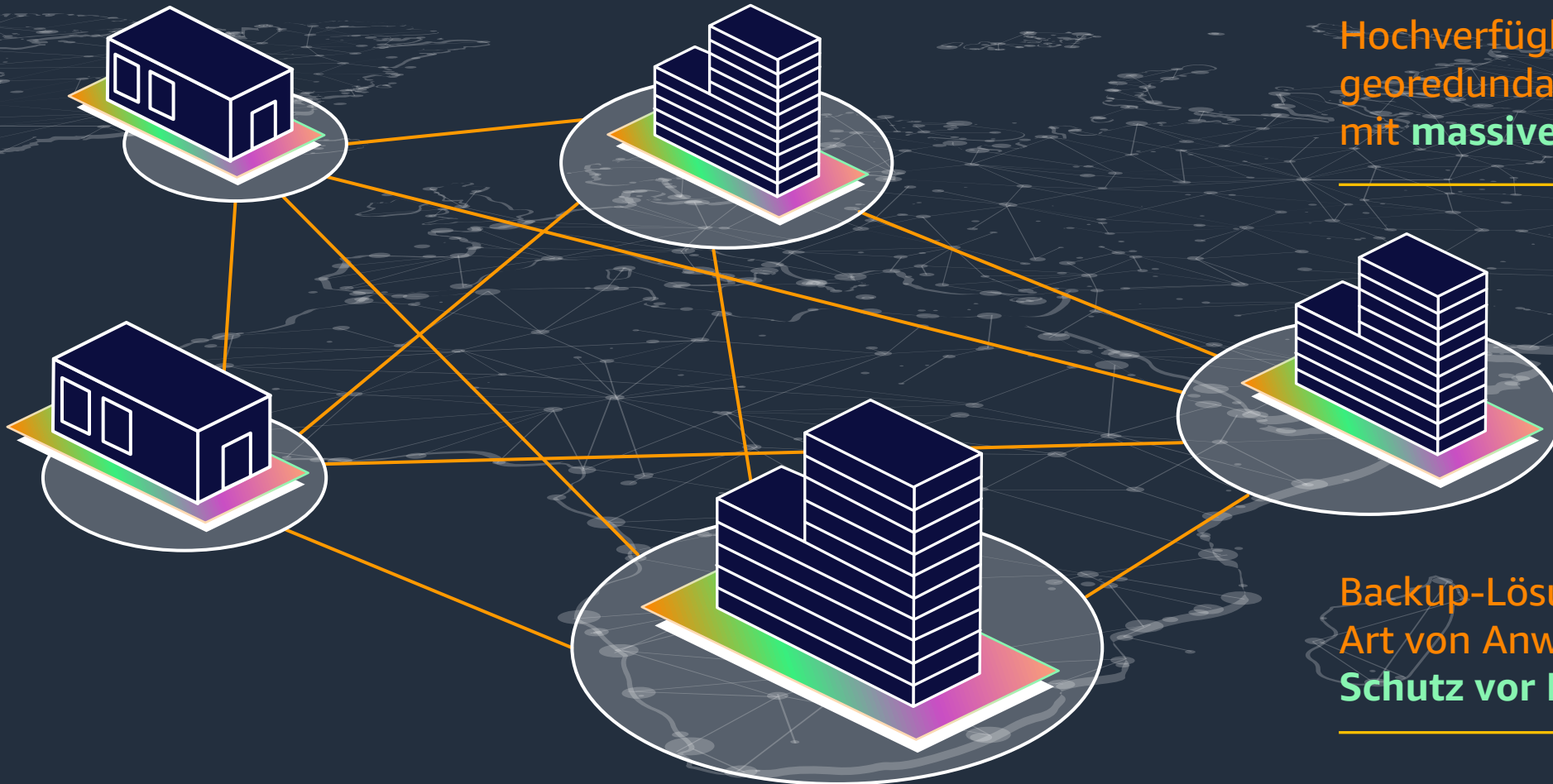


Resilienz durch Redundanz



Highly redundant
regional network
with **massive**
capacity

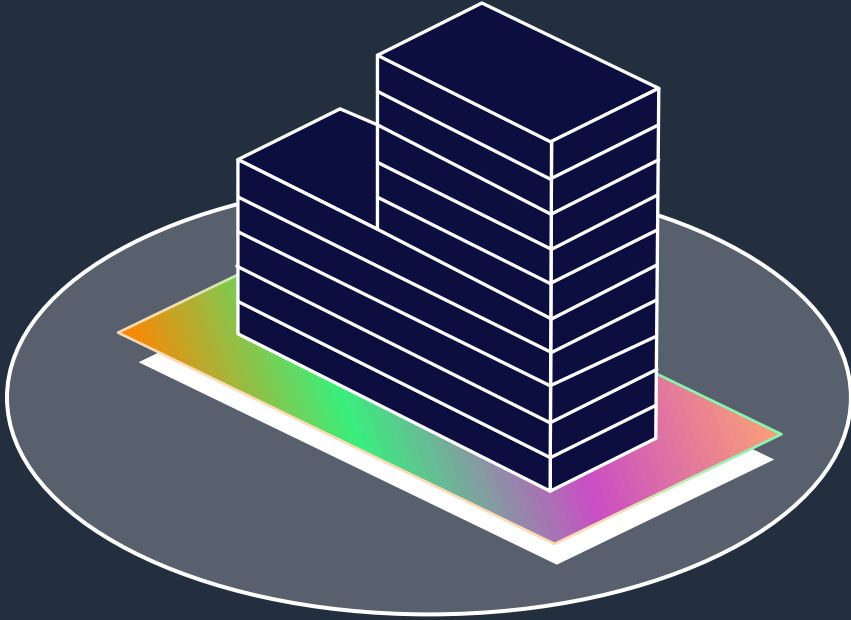
Resiliente Verfügbarkeit



Hochverfügbares, mehrfach
georedundantes Netzwerk
mit massiver Kapazität

Backup-Lösungen für jede
Art von Anwendung als
Schutz vor Datenverlust

Resiliente Datencenter



Sicheres Design

- Standortauswahl (vertraulich)
- Redundanz
- Kapazitätsplanung

Physische Sicherheit

- Perimeterschutz
- Sicherheitsstechnik
(Kameras, Bewegungsmelder, Brandmelder, etc.)
- Bewachung durch Sicherheitspersonal 24//7

Versorgungssicherheit

- Redundante Stromversorgung
- Notstromversorgung
- Klimakontrolle (Temperatur, Feuchtigkeit)
- Prozesse zur Wartung im laufenden Betrieb

Ukraine



Resilienz in der echten Welt: Ukraine



Verfügbarkeit



42
Behörden



10 Mio GB
(10 Petabyte)



AWS
Snowball



PrivatBank



3500 Server



45 Tage

Resilienz in der echten Welt: AWS Snow Family



AWS Snowball

- Datenmigration im Petabyte-Bereich
- Case hält Kräfte bis 8.5 G aus
- End-To-End Verschlüsselt
- 80 TB Kapazität / 10 GB Netzwerk
- Transferiert 250 TB in einer Woche



AWS Snowball Edge

- Compute und Storage in einem
- 100 TB lokaler Speicher
- Entspricht einer EC2 m4 Instanz
- 10GBBase-T / SFP28 / QSFP / Kupfer / Optisch



AWS Snowmobile

- Vollausgestattetes Datacenter auf Rädern
- Datenmigration im Exabyte-Bereich
- Bis zu 100 PB Kapazität
- End-to-End Verschlüsselung
- Eigenes Sicherheitspersonal
- GPS-Tracking, 24//7 Überwachung

Resilienz in der echten Welt: Ukraine

BUSINESS

How Amazon put Ukraine's 'government in a box' — and saved its economy from Russia



Amazon conducts a disaster response training exercise using Snowball Edge data storage units. Similar units have been used to transfer Ukraine government data to the Amazon cloud. (Noah Berger / Amazon)

Ukraine Tech Chief: Cloud Migration 'Saved Ukrainian Government and Economy'



LAS VEGAS, NEVADA - NOVEMBER 29: Liam Maxwell, Director of Government Transformation at Amazon Web Services (AWS) and Ukrainian Deputy Prime Minister Mykhailo Fedorov (C) sign a Memorandum of Understanding stating Amazon's ongoing support for Ukraine at AWS re:Invent 2022 at The Venetian Las Vegas on November 29, 2022 in Las Vegas, Nevada. PHOTO BY NOAH BERGER/GETTY IMAGES FOR AMAZON WEB SERVICES)

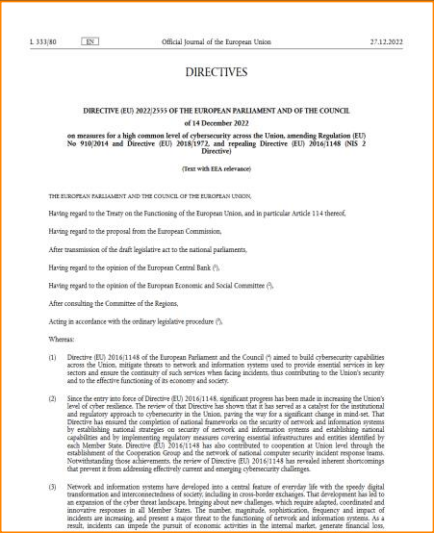


Regulierungsumfeld



Europäische Regulierungsanforderungen (Auswahl)

NIS 2

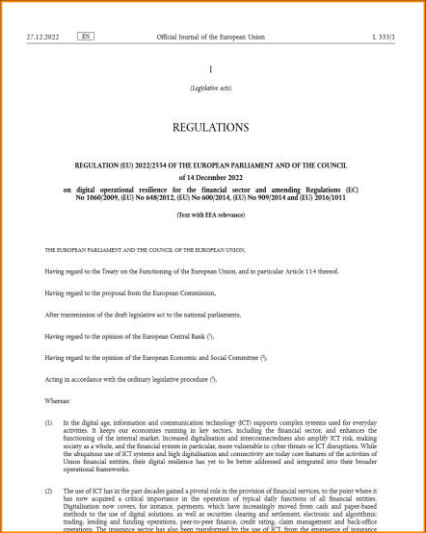


NIS2 Directive / Eur-Lex



Cybersicherheit

DORA

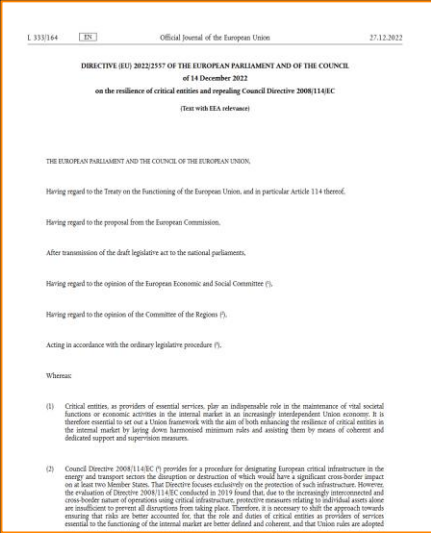


DORA / EUR-Lex



Operative Resilienz

CER

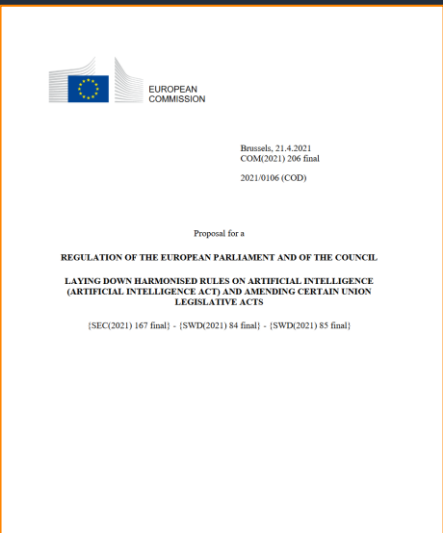


CER / EUR-Lex



Schutz Kritischer Infrastrukturen (CIP)

AI ACT



AI Act / EUR-Lex

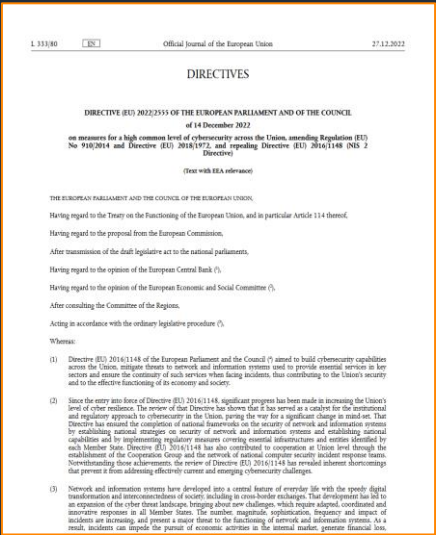


AI Regulierung



NIS2: National implementations (DE)

NIS 2



Law	the change	NIS2UmsuCG
BSI Act	NIS2 changes	Article 1
BSI and Telecommunications Act	Reference umbrella law and annexes	Article 2
BND Act, SÜFV, TTDSG, GleibWV	References	Articles 3-6
IT Security Act 2.0	Evaluation cancelled on 1 May 2025	Article 7
BSIZertV, BSI-ITSiKV, De-Mail-Gesetz, PassDEÜV, PAuswV, KassenSichV, ATG,	References	Articles 8-15
Energy Act	NIS2 changes	Article 16
TKG	NIS2 changes	Article 23
MsbG, EnSiG, SGB V, DiGAV, SGB VI, BfSGV, TKG, KHSFV, MessEV, AWW, VDG,	References and definitions	Articles 17-27
NIS2UmsuCG	Evaluation	Article 28
NIS2UmsuCG	Come into effect	Article 29

Tabelle: Legal changes, as of May 2024

NIS2 Directive / Eur-Lex

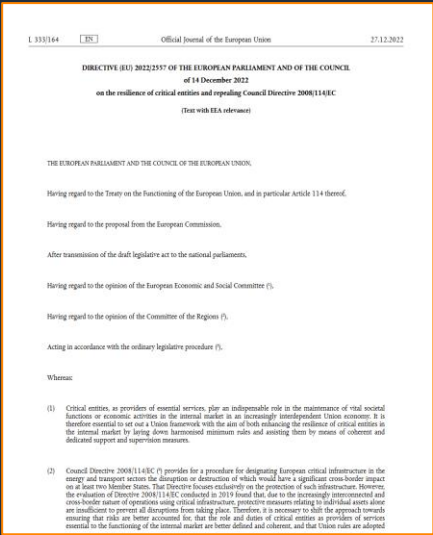


Source: openkritis.de



CER: National implementations (DE)

CER



CER / EUR-Lex



Critical Infrastructure Protection

sector §4 (1)	Critical service* §3 (3)	Critical facilities §16 (1)
energy	Power supply Gas supply Fuel/heating oil Production of hydrogen	still missing
Traffic transportation	Air traffic Rail traffic Sea and inland waterway transport Road traffic Weather forecast (DWD)	still missing
Finance/Insurance †	Cash supply Payment transactions Securities Insurance Social insurance Basic security	still missing
Health	still missing	still missing
Water sewage	still missing	still missing
IT and telecommunications †	Voice and data transmission Data storage and processing	still missing
space	Ground infrastructures	still missing
Nutrition	still missing	still missing
disposal	still missing	still missing
Country §5 (1)	Federal Administration Facilities	Federal Chancellery Federal Ministries

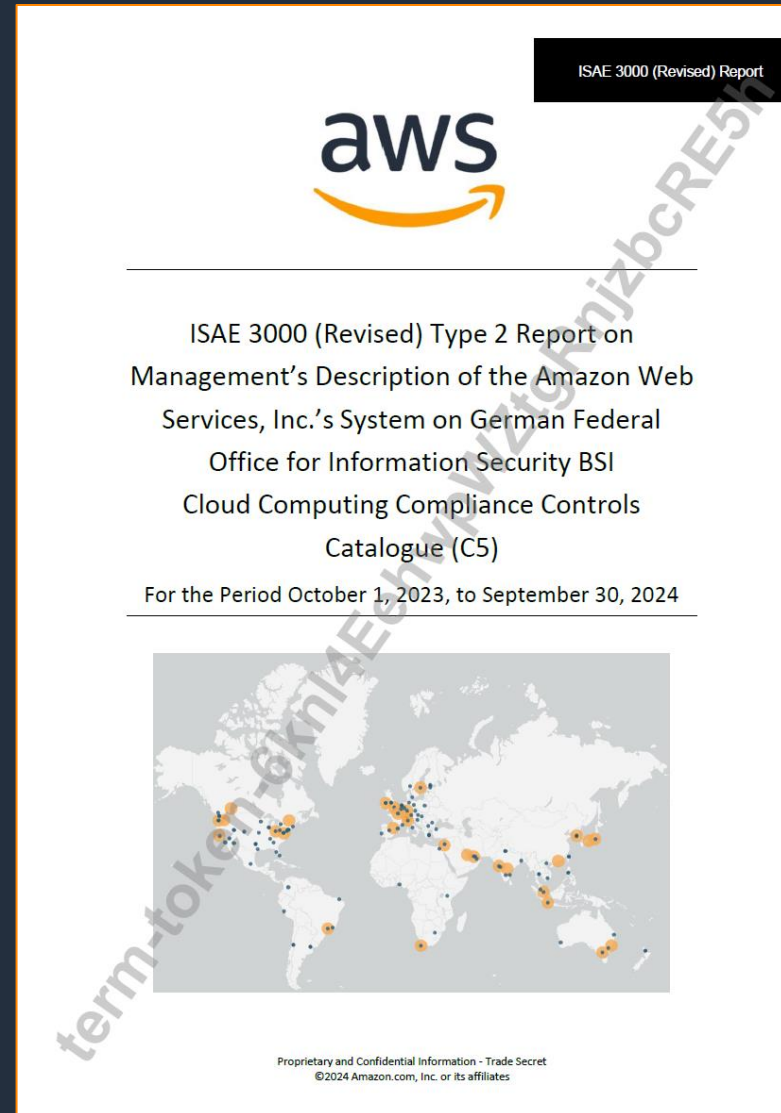
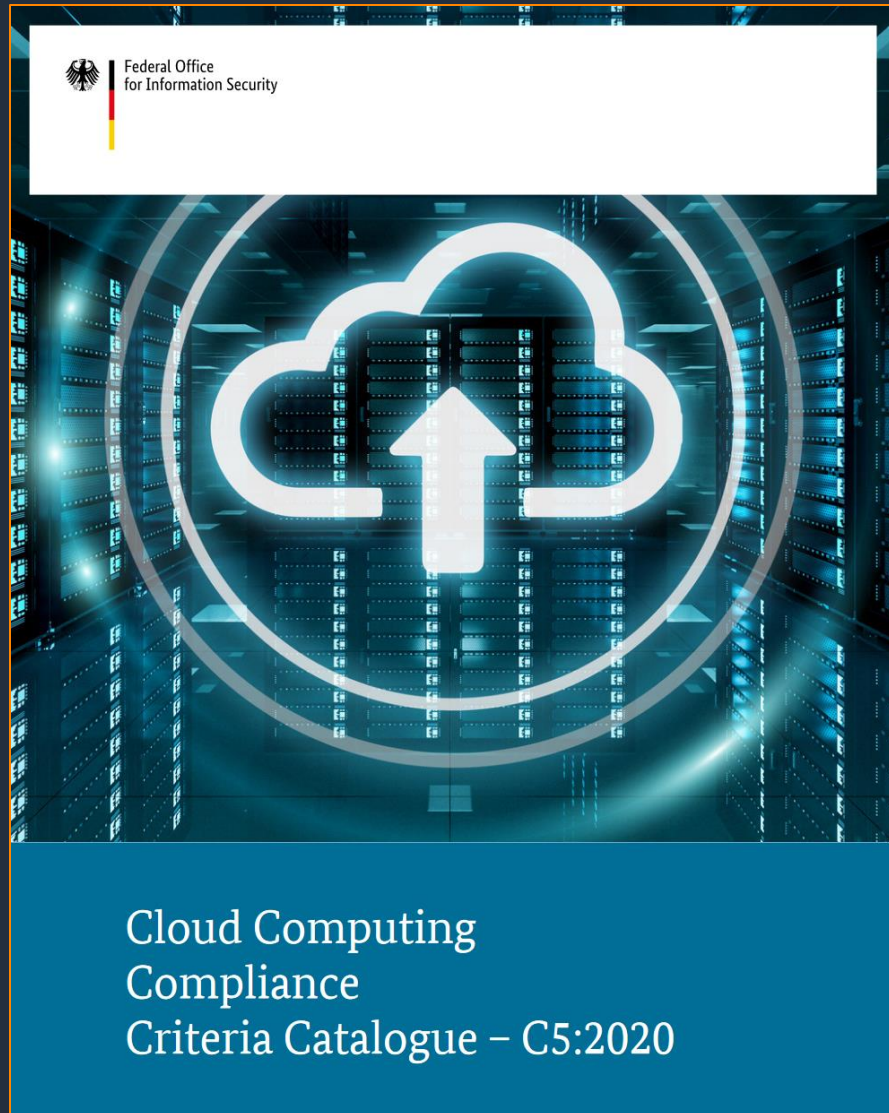
Tabelle: own compilation from the draft of the DachG as of December 2023
* - Federal responsibility
† - with exceptions

Source openkritis.de

Nationale und globale Zertifizierungen



Deutschland: C5



Source [AWS C5](#)

Source [bsi.bund.de](https://www.bsi.bund.de)



Globale Zertifizierungen



European Sovereign Cloud



European Sovereign Cloud

10 min

May 15, 2024



AWS plans to invest €7.8 billion into the AWS European Sovereign Cloud

Written by About Amazon Team



Physisch getrennt

- Eigenes Netzwerk
- Unabhängig und physisch getrennt
- Gebaut für maximale Kontrolle

Aus Deutschland

- 100% auf Deutschem Boden
- Deutsche Legal Entity
- Nur Personal aus der EU
- Verfügbar ab Q4 2025



Verschlüsselung und Datenschutz



Was ist AWS KMS?



- AWS KMS ist ein verwalteter Service, der Ihnen hilft, die für kryptografische Vorgänge verwendeten Schlüssel einfacher zu erstellen und zu steuern.
- Verwenden Sie AWS KMS, um Daten in Ihren AWS-Workloads zu verschlüsseln.
- Schützen Sie Signiervorgänge mit AWS KMS mit asymmetrischen KMS-Schlüsseln.
- Verwenden Sie AWS KMS, um vertrauliche Datensätze in Ihren Datenbanken einfach zu verschlüsseln und sicher zu durchsuchen.

Benefits



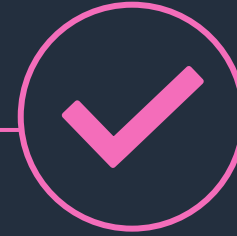
Verwalten Sie Schlüssel zentral und definieren Sie Richtlinien für integrierte Services



Verschlüsseln Sie Daten in Ihren Anwendungen mit der AWS Encryption SDK



Validieren Sie digitale Signaturen mit asymmetrischen Schlüsselpaaren



Gewährleisten Sie **Integrität und Authentizität** durch Hash-basierte Authentifizierungscodes (HMAC)

Was spricht für AWS KMS?

AWS KMS ist ein hochverfügbarer, kosteneffizienter Service zur Verwaltung von kryptographischen Schlüsseln auf AWS



Fragen & Ressourcen



AWS
Resilience
Hub



AWS
Well Architected
Framework



AWS
Infrastructure



AWS
Snow Family



AWS
Ransomware
Defense



AWS
Assisting
Ukraine

VIELEN DANK!



Daniel Caduff
dancad@amazon.ch

Scannen Sie den nebenstehenden QR-Code,
um meine Kontaktinformationen als
elektronische Visitenkarte zu speichern.

