
NETAPP-DATENSICHERHEIT

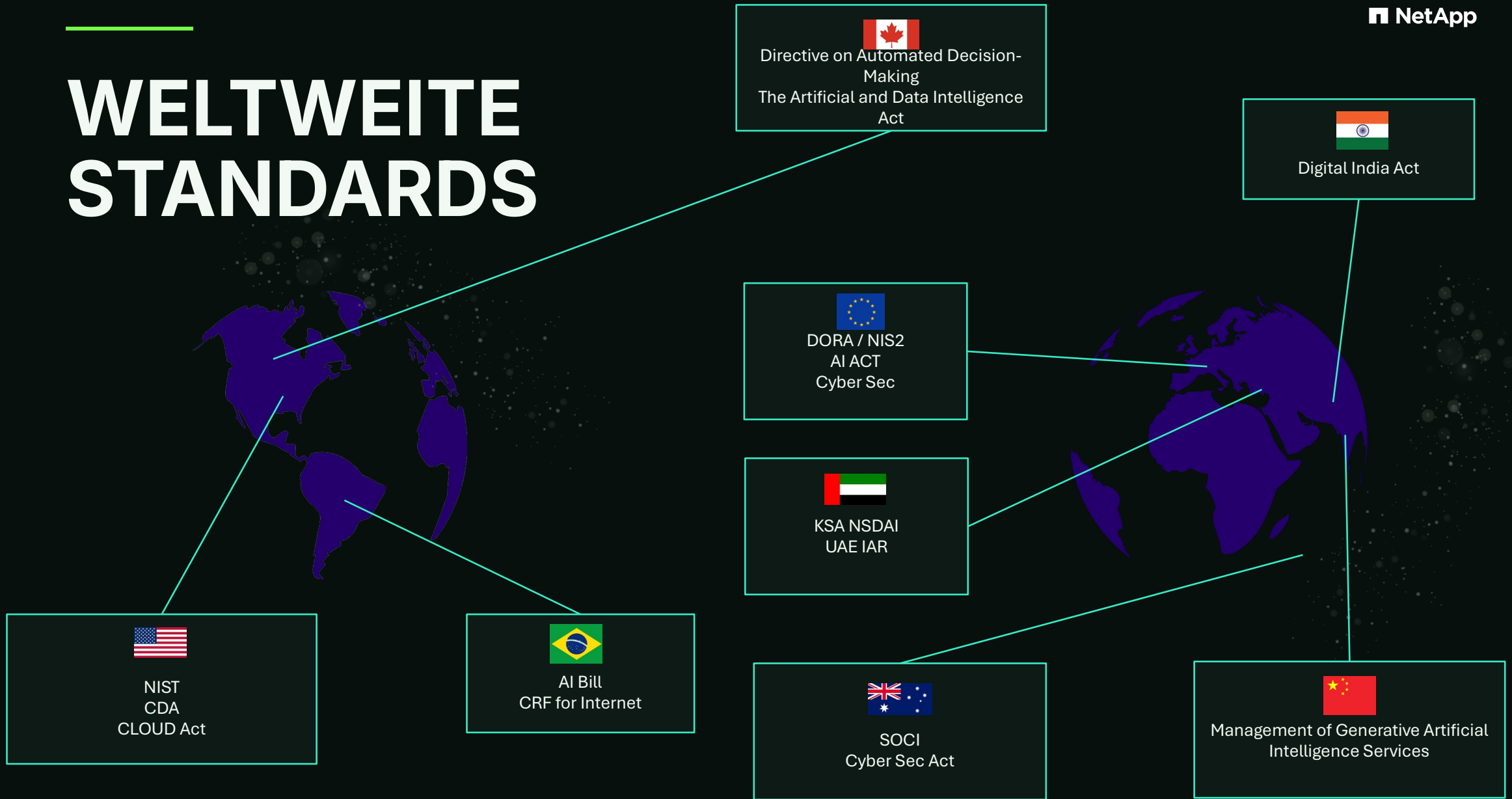
Digitale Souveränität beginnt wo die Daten liegen

Executive-Briefing für IT- und Sicherheitsverantwortliche



PETER HERMANN

WELTWEITE STANDARDS



Souveränität beginnt mit drei klaren Entscheidungsrechten

Nicht der Speicherort allein entscheidet, sondern wer Daten, Schlüssel und Betriebswege kontrolliert.

WO

RESIDENZ

- 01 Primärdaten in freigegebenen Regionen
- 02 Backups und Replikate mitführen
- 03 Datenflüsse dokumentieren

ERGEBNIS: überprüfbare Datenresidenz

WER

AUTORITÄT

- 01 Schlüsselverantwortung festlegen
- 02 Admin- und Supportzugriff begrenzen
- 03 Audit- und Freigabepflichten definieren

ERGEBNIS: klare Kontrollhoheit

WIE

HANDLUNGSFREIHEIT

- 01 Wiederherstellung im Zielraum testen
- 02 Daten und Metadaten exportierbar halten
- 03 Providerwechsel im Runbook abbilden

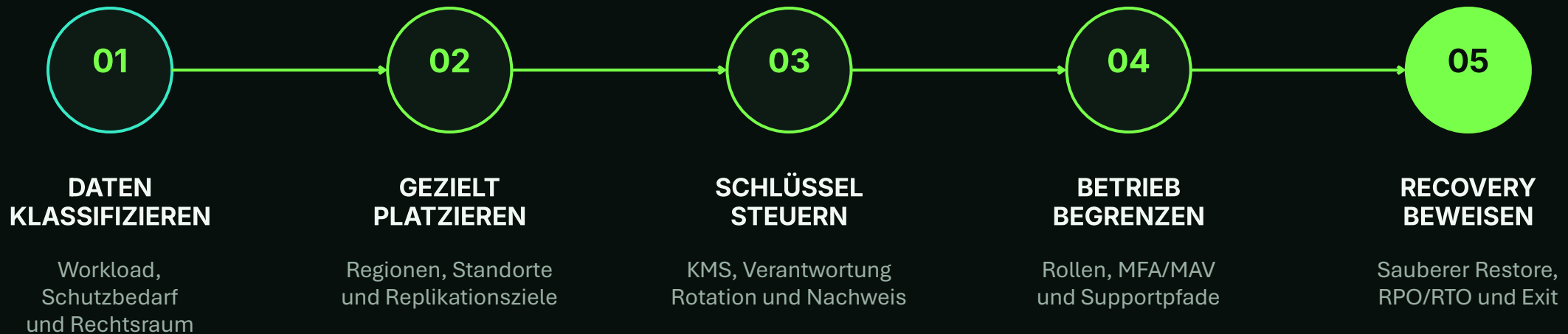
ERGEBNIS: geübte Exit-Fähigkeit

Prüfen: Region • Schlüssel • privilegierter Zugriff • Wiederherstellung • Exit-Fähigkeit

Kontrollen machen Souveränität belastbar

Fünf verknüpfte Entscheidungen übersetzen Rechtsraum und Risiko in ein belastbares Datenbetriebsmodell.

ABLAUF



Souveränität ist belastbar, wenn jede Entscheidung dokumentiert, technisch erzwungen und regelmäßig getestet wird.

Anforderungen und verfügbare Kontrollen variieren nach Rechtsraum, Plattform und Betriebsmodell.

Globale Regeln unterscheiden sich – das Kontrollmodell bleibt konsistent

Ein gemeinsames Steuerungsmodell muss lokale Vorgaben abbilden, ohne Datenbetrieb und Wiederherstellung zu fragmentieren.

01

AMERIKA

USA + BRASILien

NIST • CDA • CLOUD Act
AI Bill • Internet CRF

02

EUROPA

EU-RAHMEN

DORA • NIS2
EU AI Act • Cybersecurity

03

NAHER OSTEN

REGIONALE REGELN

KSA NSDAI
VAE IAR

04

ASIEN-PAZIFIK

INDIEN + AUSTRALIEN + CHINA

Digital India Act
SOC1 / Cyber Security Act
GenAI-Service-Regeln

1x

Gemeinsamer Nenner: Daten inventarisieren • Zugriff und Schlüssel steuern • Residenz und Recovery nachweisen.

Bezeichnungen dienen als Orientierung; Geltungsbereich und Pflichten sind je Rechtsraum und Organisation zu prüfen.

Ransomware macht Präventionslücken zur Krise

Perimeterkontrollen bleiben wichtig. Entscheidend ist, ob saubere Daten isoliert, verifiziert und wiederhergestellt werden können.

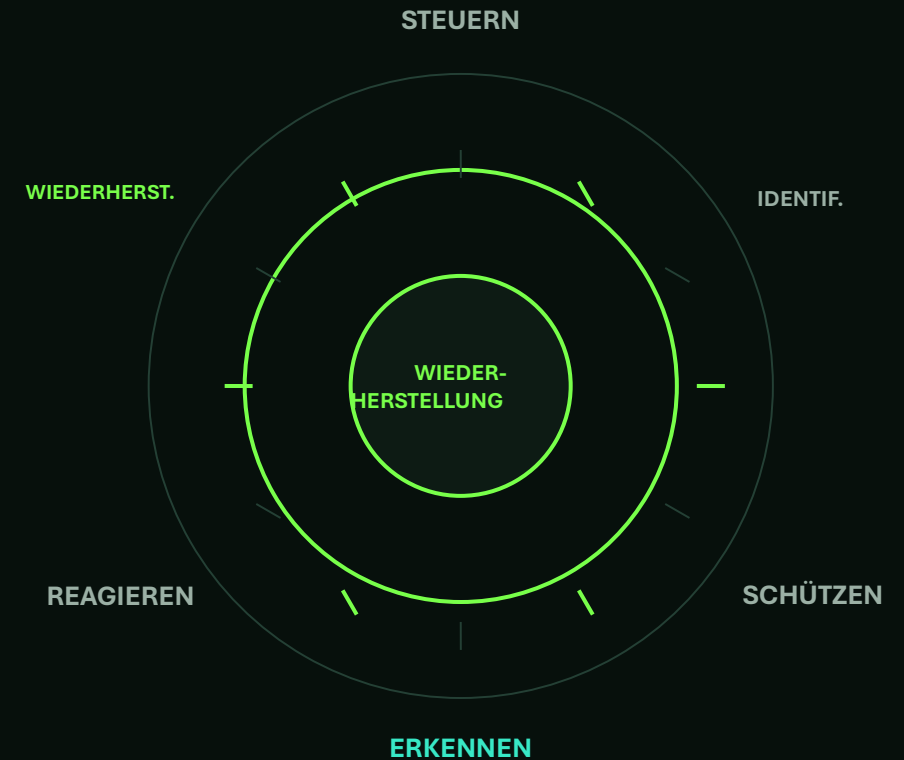
44%

der Sicherheitsverletzungen im Verizon-Datensatz 2025 waren mit Ransomware verbunden

5,08 Mio.

USD – durchschnittliche Kosten eines Ransomware-Datenverstoßes in der IBM-Studie 2025

Die Sicherheit muss den gesamten NIST-Kreislauf abdecken – insbesondere die Wiederherstellung.



NetApp schließt den Kreislauf direkt im Datenpfad

Storage-native Erkennung, geschützte Kopien und orchestrierte Wiederherstellung bilden eine letzte Verteidigungslinie unter Netzwerk- und Identitätskontrollen.

01

ERKENNEN

ARP/AI

Analysiert die Datenaktivität in Echtzeit und schützt unterstützte NAS- und SAN-Workloads ohne Lernphase.

02

SCHÜTZEN

GESCHÜTZTE SAUBERE KOPIEN

Manipulationssichere Snapshots und SnapLock-Aufbewahrung schützen vor versehentlicher oder böswilliger Löschung.

03

ORCHESTRIERUNG

NETAPP CONSOLE

Ransomware Resilience bewertet die Lage, empfiehlt Kontrollmaßnahmen, erkennt Bedrohungen und leitet die Wiederherstellung.

04

WIEDERHERST.

ISOLIEREN + WIEDERHERST.

Isolierte Cyber-Vault-Architekturen und geführte Wiederherstellung bringen kritische Workloads zurück in Betrieb.

99% Erkennungsrate ohne Fehlalarme in den von SE Labs getesteten dateibasierten Szenarien (2024).

Abdeckung und Verhalten hängen von ONTAP-Version, Protokoll, Workload und Lizenzierung ab. Ransomware Resilience ist separat lizenziert; laut aktueller Dokumentation nur im Standardbereitstellungsmodus.

Kontrollen sichern den sauberen Neustart

Das Designziel ist nicht nur "ein Backup". Es handelt sich um eine verifizierte Kette von geschützten Produktionsdaten zu einer isolierten, wiederherstellbaren Kopie.

DATENPFAD



Die Abdeckung umfasst On-Premises ONTAP, Cloud Volumes ONTAP, Azure NetApp Files und Amazon FSx für NetApp ONTAP.

Designhinweise: Multi-Admin-Verifikation ist mit Cloud Volumes ONTAP nicht verfügbar; Service-Modi, Ziele und Funktionen variieren je nach Umgebung.

Datensouveränität bedeutet Kontrolle – nicht nur Standort

Souveränität verbindet Datenresidenz mit Kontrolle über Zugriff, Schlüssel, Schutz und Wiederherstellung über den gesamten Lebenszyklus.

01

RESIDENZ

STANDORT AUSWÄHLEN

Workloads und Backup-Kopien werden nur in genehmigten Regionen oder Standorten platziert; Servicegrenzen und Datenflüsse dokumentiert.

02

AUTORITÄT

ZUGRIFF KONTROLLIEREN

Identitäten, Admin-Trennung, Supportzugriff, Auditprotokolle und Schlüsselverantwortung mit Richtlinien und Rechtsraum abstimmen.

03

SCHUTZ

VERSCHLÜSSELN + BEHALTEN

Verwenden Sie Plattform- und Cloud-Verschlüsselung sowie erhaltene, manipulationssichere Kopien im jeweiligen Design.

04

PORTABILITÄT

AUSSTIEG + WIEDERHERST. TESTEN

Wiederherstellung und Migration auf genehmigte Ziele testen, damit die Kontrolle Angriffen, Ausfällen und Anbieterwechseln standhält.

4×

Vier Entscheidungen machen Datenresidenz zu belastbarer Souveränität: Standort • Autorität • Schutz • Portabilität.

Datenresidenz folgt der Wahl von Bereitstellung und Backup-Ziel. Anforderungen variieren nach Rechtsraum, Cloud-Service, Workload, Schlüsseln, Verträgen und Betriebsmodell.

Von exponiert zu erprobt – in 90 Tagen

Die Arbeit auf Wiederherstellbarkeit ausrichten: Umfang festlegen, den Kopierpfad härten und das Betriebsmodell unter Druck nachweisen.

0–30

BESTANDSAUFNAHME

- 01 Kritische Workloads inventarisieren
- 02 Aktuelle RPO / RTO erfassen
- 03 ARP- und Kopierschutz bewerten

ERGEBNIS: priorisiertes Lückenregister

31–60

HÄRTEN

- 01 Unterstütztes ARP/AI aktivieren
- 02 Aufbewahrung definieren + Kopien sperren
- 03 Admin- und Vault-Domänen trennen

ERGEBNIS: geschützte Kopierkette

61–90

ERPROBEN

- 01 Saubere Wiederherstellung üben
- 02 Zeit von Erkennung bis Isolation messen
- 03 Verantwortungs- und Eskalationslücken schließen

ERGEBNIS: bestätigter Wiederherstellungsnachweis

Messen: Abdeckung kritischer Workloads • unveränderbare Kopien • Wiederherstellungserfolg • tatsächliche RPO/RTO • Übungsabschlussquote

Wiederherstellung als Sicherheitskontrolle finanzieren

Nicht als Notfallplan: Eine resiliente Datenschicht macht Ergebnisse messbar – saubere Kopien, begrenzte Zugriffe und geübte Wiederherstellung.

-
- 01 ABDECKUNG** Sind die Workloads, die das Geschäft steuern, auf der Speicherschicht geschützt?
 - 02 INTEGRITÄT** Kann privilegierter Zugriff jede Wiederherstellungskopie löschen oder beschädigen?
 - 03 NACHWEIS** Wann haben wir zuletzt eine saubere Wiederherstellung gegen die vereinbarten RPO/RTO-Ziele nachgewiesen?



BESTAND / SPERREN / NACHWEISEN

Optionale Zusicherung: Die NetApp-Wiederherstellungsgarantie gilt nur für qualifizierte Arrays, validierte Konfigurationen und erforderliche Services; sämtliche Programmbedingungen gelten.