Plan B

Sicherheits-Strategien für Datenvorhaltung und Storage-Technologien

Jens Katzwinkel
Lead Technical Consultant
Competence Center Data Center Infrastruktur

19.09.2025, Congress Park Hanau

Was erwartet uns?

- Ein Blick auf die Bedrohungslage
- Techniken zur Früherkennung von Angriffen(Ransomware und Co.)
- Schutz meiner Daten auf dem Produktionsspeicher
- Sicheres Backup Design
- Disaster Recovery und Business Continuity
- Fragen und Antworten

Die Bedrohungslage

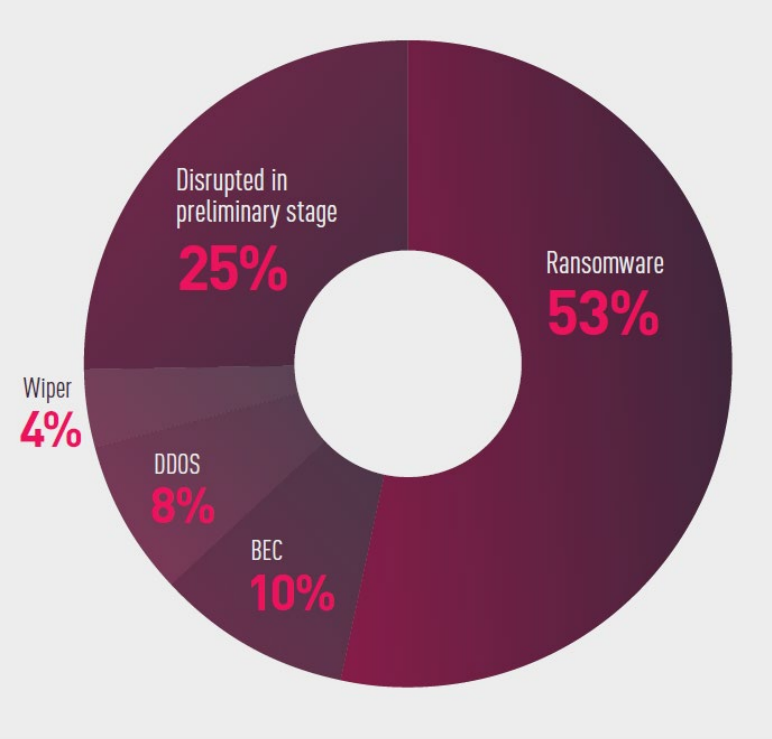
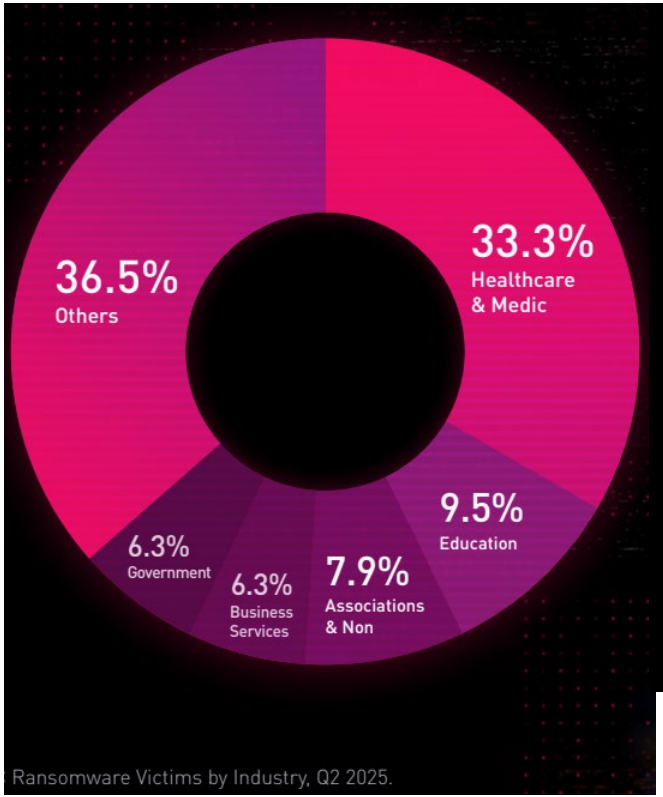


Figure 6 - Main attack categories in CPIRT 2024 cases.

- Über 50% aller Angriffe sind Ransomware
- Nur 25% können aufgehalten werden
- Die Folgen eines Angriffs
  - Produktionsausfälle
  - Finanzieller Schaden
  - Kostspielige und lange Wiederherstellung
  - Reputationsverlust
  - Rechtliche Konsequenzen

Die Bedrohungslage



Ransomware Victims by Industry, Q2 2025.

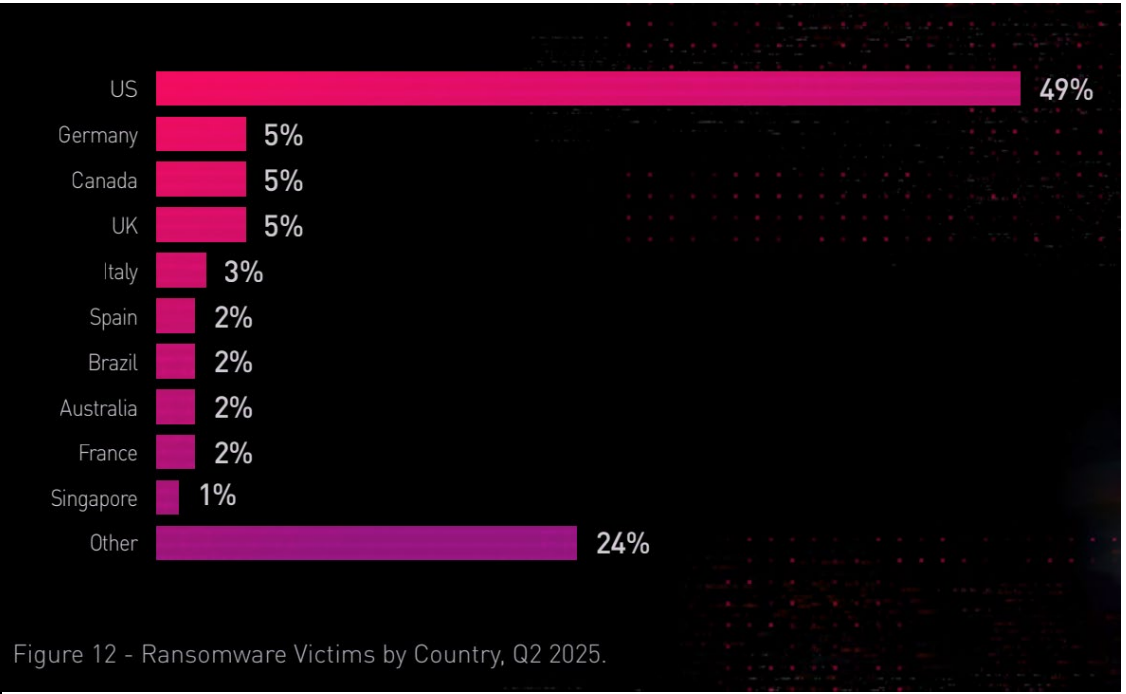


Figure 12 - Ransomware Victims by Country, Q2 2025.

Die Bedrohungslage

Chart 8: Recovering data via backups and ransom payments 2020–2025

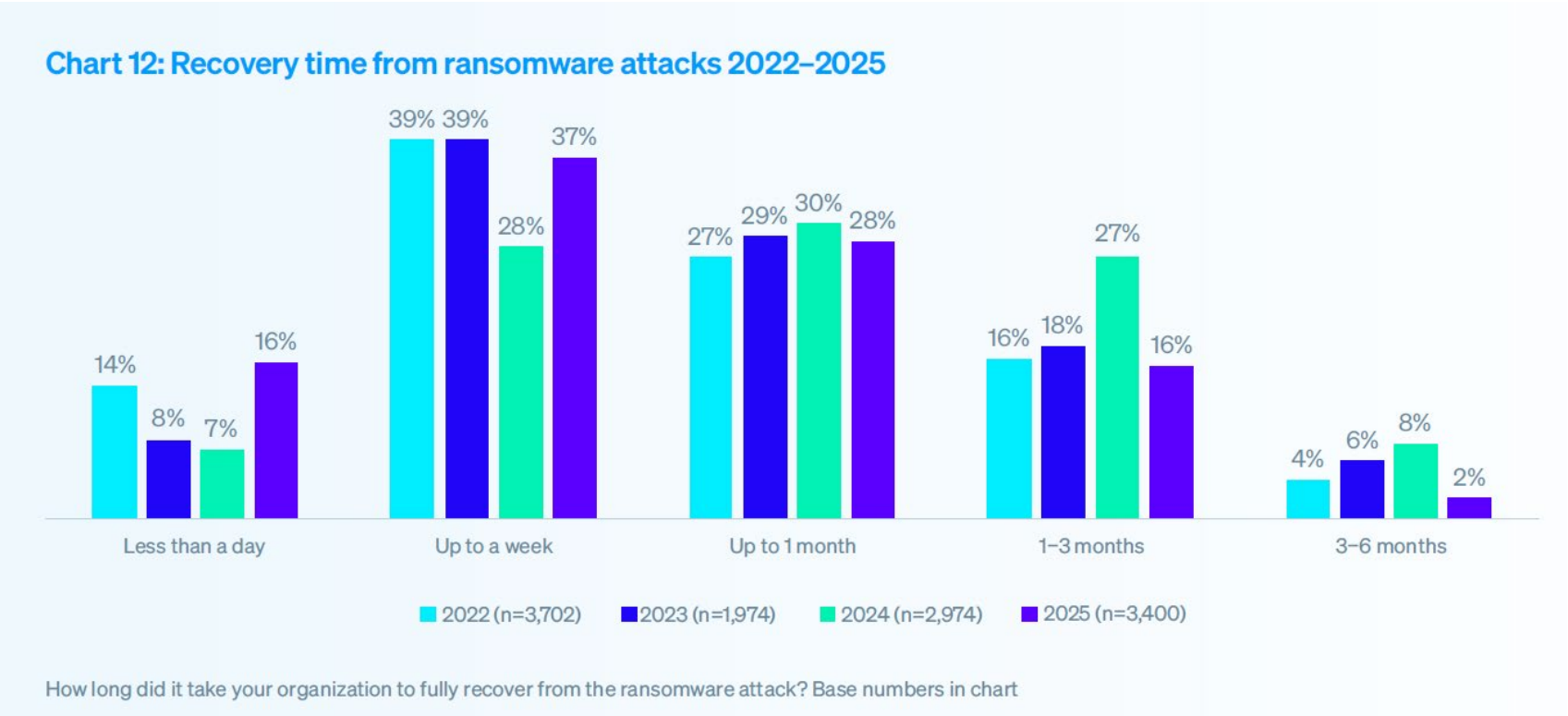
Did your organization get any data back? Yes, we paid the ransom and got data back; Yes, we used backups to restore the data. Base numbers in chart

Die Bedrohungslage

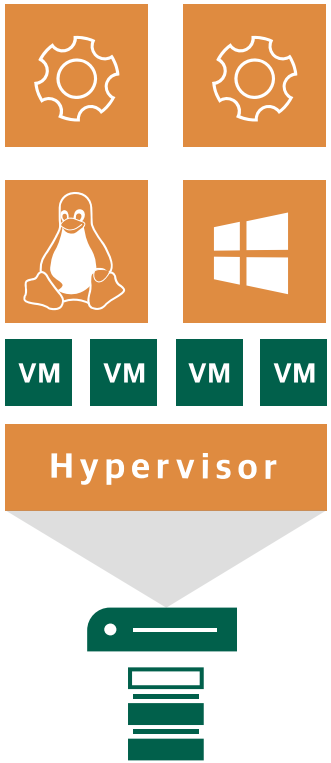
Chart 9: Ransom demands split by company annual revenue

How much was the ransom demand from the attacker(s)? Base numbers in chart.

Die Bedrohungslage



Techniken zur Früherkennung von Angriffen(Ransomware und Co.)

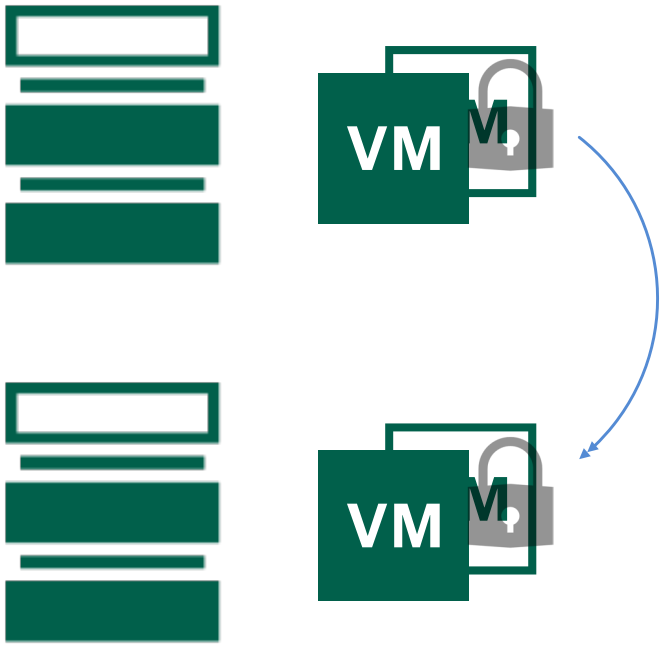


- Applikation
- Betriebssystem
- Virtuelle Maschine
- Hypervisor
- Storage

Techniken zur Früherkennung von Angriffen(Ransomware und Co.)

- Storage
  - Live Analyse
  - Mustererkennung
  - Anomalieerkennung

Schutz meiner Daten auf dem Produktionsspeicher



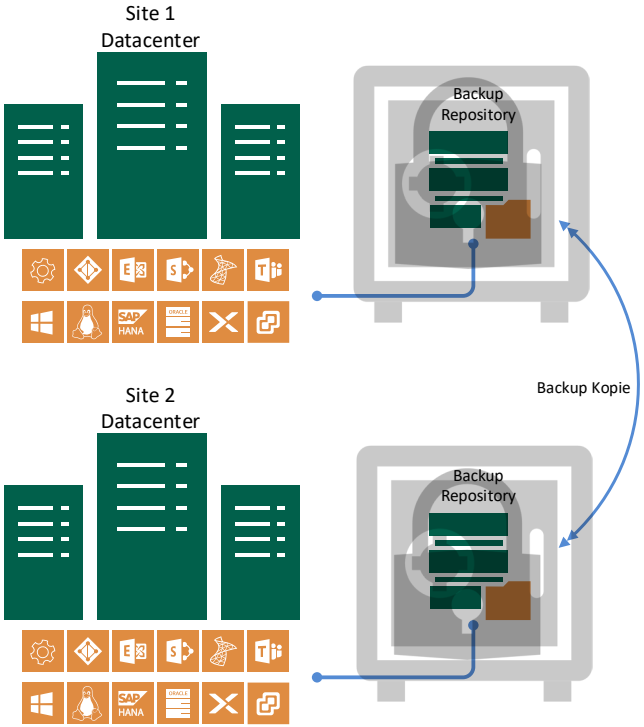
- Storage
  - Snapshot
  - unveränderlicher Snapshot
  - Löschen:
    - Vier Augen Prinzip
    - Wartezeit (Immutability)
  - Replizieren
  - RPO/RTO sehr gut

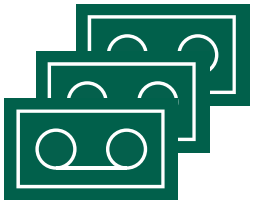
Sicheres Backup Design

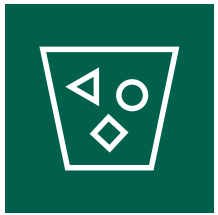
Die geheime Formel:

- Drei Kopien
- Zwei unterschiedliche Medien
- Eine Kopie Offsite
- Eine Kopie Air-Gapped oder Immutable
- Null Kopien, die nicht auf Wiederherstellbarkeit getestet sind

Sicheres Backup Design





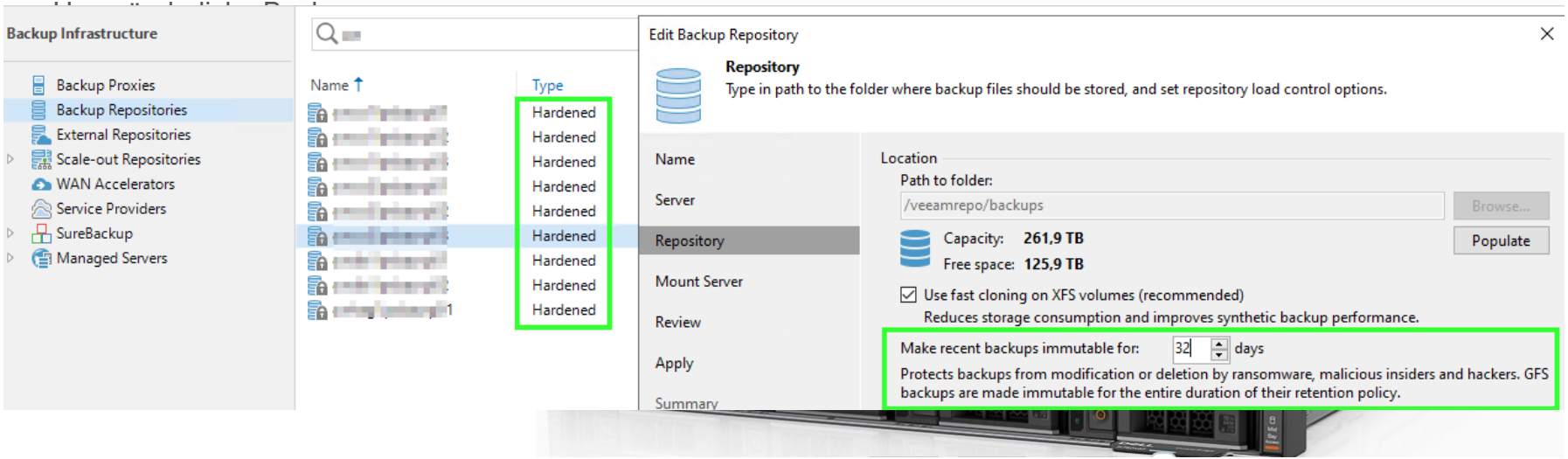


- Mehrere Standorte
- Standortübergreifende Kopien
- Gehärtete Repositorys
- Unveränderliche Backups
- Air-gapped/Offline Kopien
- Tapelibrary
- S3-Objectstore (Azure,AWS,….)

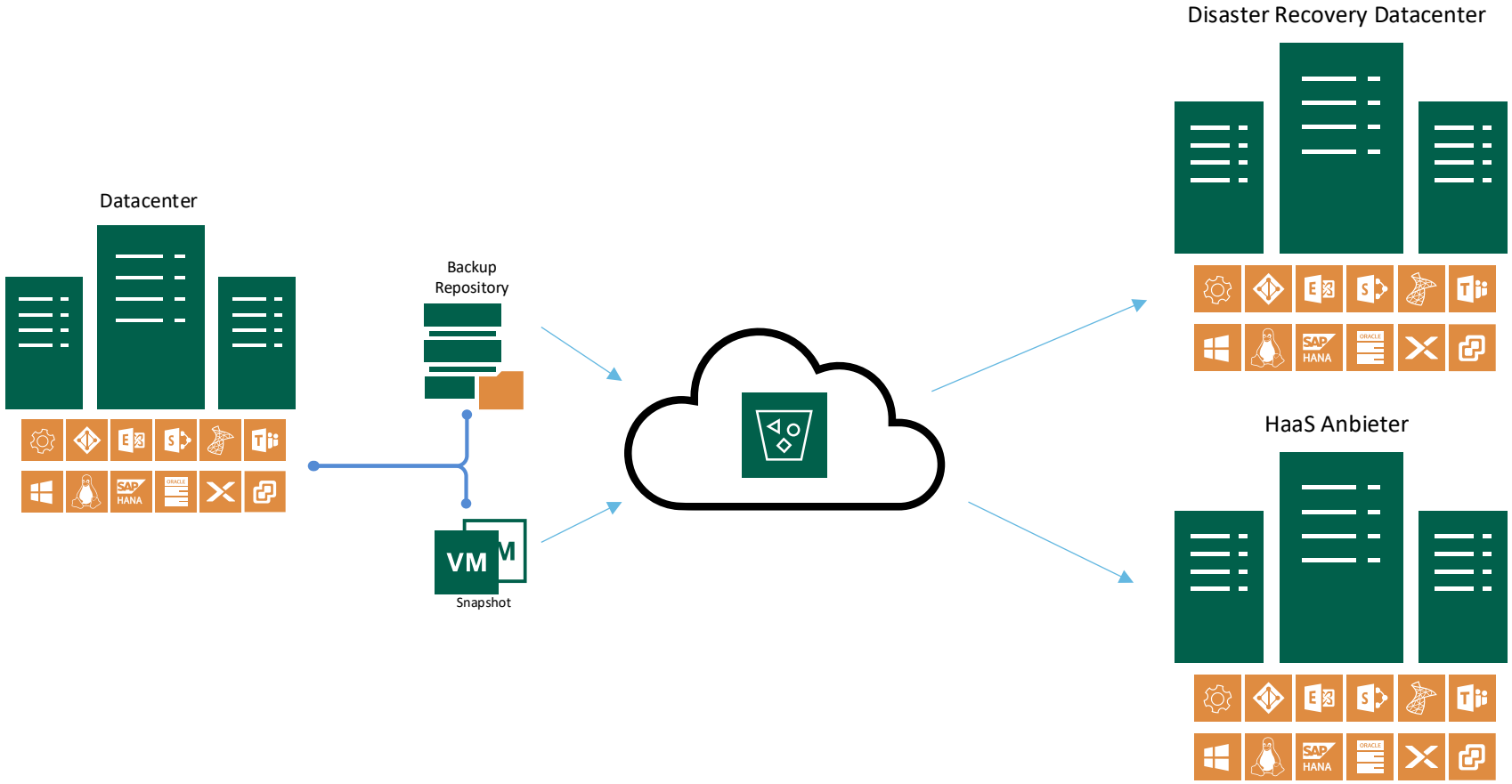
Sicheres Backup Design

CUBA – Controlware Universal Backup Appliance

- Gehärtetes Repository
  - Alle Hard- und Software-Hardening Guides angewendet
  - Minimale Angriffsfläche(keine GUI, kein SSH,..)



Disaster Recovery und Business Continuity



Sicherheits-Strategien für Datenvorhaltung und Storage-Technologien

?

Controlware
Security Day

Danke für Ihre Aufmerksamkeit.
Wir freuen uns über Ihr Feedback!

Bitte geben Sie den ausgefüllten Bogen am Empfang ab und erhalten Sie als Dankeschön ein kleines Präsent.