



CDP – eine sinnvolle Option zur Wiederherstellung nach einem Ransomware-Angriff!

Alwin Kohl

Senior Solution Architect

Agenda

- Wer ist DataCore?
- Bedrohungspotential Ransomware
- Klassische Gegenmaßnahmen
- Continuous Data Protection – Was ist das?
- Wie hilft mir CDP im Falle eines Angriffs?
- Q&A

Wer ist DataCore?

Über uns: Global bewährt.



Über 30.000 Installationen weltweit

Über 10.000 Kunden

Produkt der
10. Generation

Kunden in allen Branchen und Größen

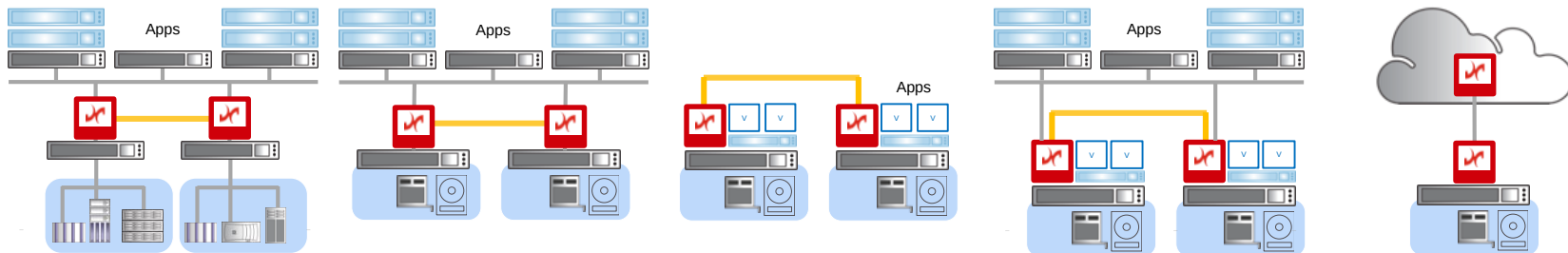
konzeptionell: **Software-defined Storage**
Hyper-Converged

technologisch: **Speicher-Virtualisierung**
Parallel I/O



- Australien
- Deutschland
- Frankreich
- Japan
- UK
- USA

Eine Softwareplattform für jede Verwendungsform



DataCore

Traditional	Converged (Server SAN)	Hyper-Converged	Hybrid-Converged	Cloud
Integriert, verwaltet und optimiert bestehende Speichersysteme	Nutzt internen Speicher, reduziert die Komplexität und unterhält den Compute-Level separat	Konsolidiert alle Funktionen auf kleinster Stellfläche mit höchster Leistung sowie externer Speicher Bereitstellung	Konsolidiert alle Funktionen auf kleinster Stellfläche mit höchster Leistung	Stellt einen zusätzlichen Replikationsort zur Verfügung um Daten und Anwendungen zu sichern

Einheitliche high-end Speicherfunktionen für jede Speicherhardware



UNIFIED ENTERPRISE STORAGE SERVICES

VERFÜGBARKEIT

-  Synchrones Spiegeln
-  Asynchrone Replikation
-  CDP
-  Snapshots / Backups

PERFORMANCE

-  High Speed Caching
-  Auto-Tiering
-  Random Write Accelerator
-  Quality of Service (QoS)

EFFIZIENZ

-  Speicher-Pooling
-  Thin Provisioning
-  Daten-Migration
-  Deduplication/Compression

MANAGEMENT

-  Zentrales Management
-  Analyse & Reporting
-  VVols
-  NAS/SAN (Unified Storage)
-  Cloud Integration

Bedrohungspotential Ransomware



Was ist Ransomware?

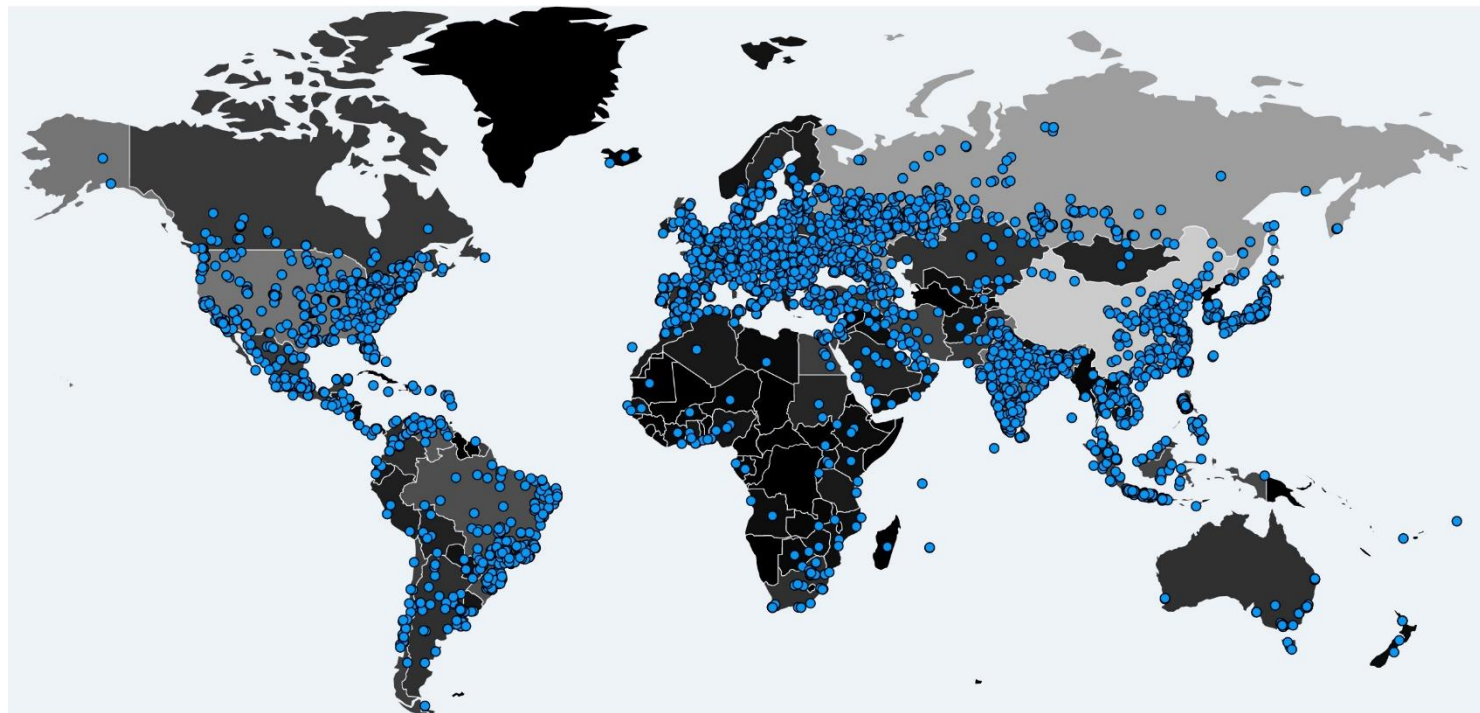
- Ransomware [...] sind Schadprogramme, mit deren Hilfe ein Eindringling den Zugriff des Computerinhabers auf Daten, deren Nutzung oder auf das ganze Computersystem verhindern kann. Dabei werden private Daten auf dem fremden Computer verschlüsselt oder der Zugriff auf sie verhindert, um für die Entschlüsselung oder Freigabe ein Lösegeld zu fordern.[...]

Eines der aktuellsten Beispiele ist WannaCry, welches seit Mai über 230.000 Computer in 150 Ländern infiziert hat.

CNN schätzt, dass innerhalb von 3 Monaten, \$209 Mio an Cyber-Kriminelle bezahlt wurden. (Q1/16)

Source: <https://de.wikipedia.org/wiki/Ransomware>, <https://de.wikipedia.org/wiki/WannaCry>

Verbreitung von WannaCry



Source: <https://intel.malwaretech.com/botnet/wcrypt/>

Infektionswege

- Dienste und Anwendungen mit Sicherheitslücken
 - SMB file sharing (WannaCry wurde auf diesem Weg verbreitet)
- Emails (Phishing ähnlich, von vertrauenswürdigen Quellen)
 - z.B. BKA, Polizei, GEMA, Microsoft, PayPal, etc.
- Telefonischer Kontakt
 - „Microsoft ruft an...“
- Browser
 - Silverlight, Flash oder Java Exploits
- Dropbox
 - Downloads von (nicht) vertrauenswürdigen Quellen, z.B. Bewerbungsunterlagen

Bedrohungspotential

- Lokale Platten des kompromittierten Systems
- Aktive UNC Pfade
 - Home Shares
 - Gruppen Shares
- Inaktive UNC Pfade
 - Temporäre Laufwerke mit hinterlegtem Password im Cache

Klassische Gegenmaßnahmen

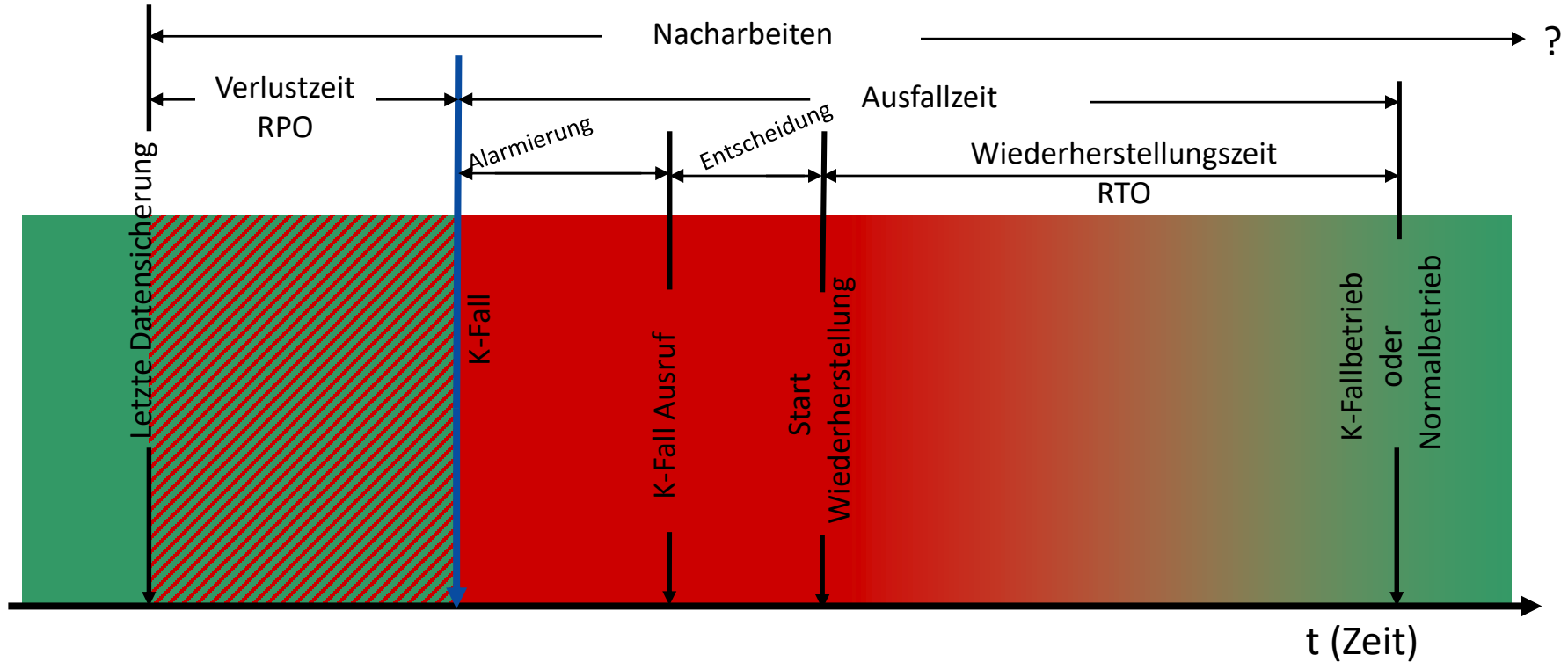
3 Schritte zum Schutz vor Ransomware

- Regelmäßig Updates und Patches auf Computern und Servern installieren
 - Nach Möglichkeit automatisierte Updates nutzen
- Anwender sensibilisieren keine Anhänge zu öffnen und Dateien herunterzuladen
 - Leichter gesagt als getan!
- Backups machen!
 - Um an einen sicheren Punkt im Falle einer Cyber-Attacke zurückkehren zu können

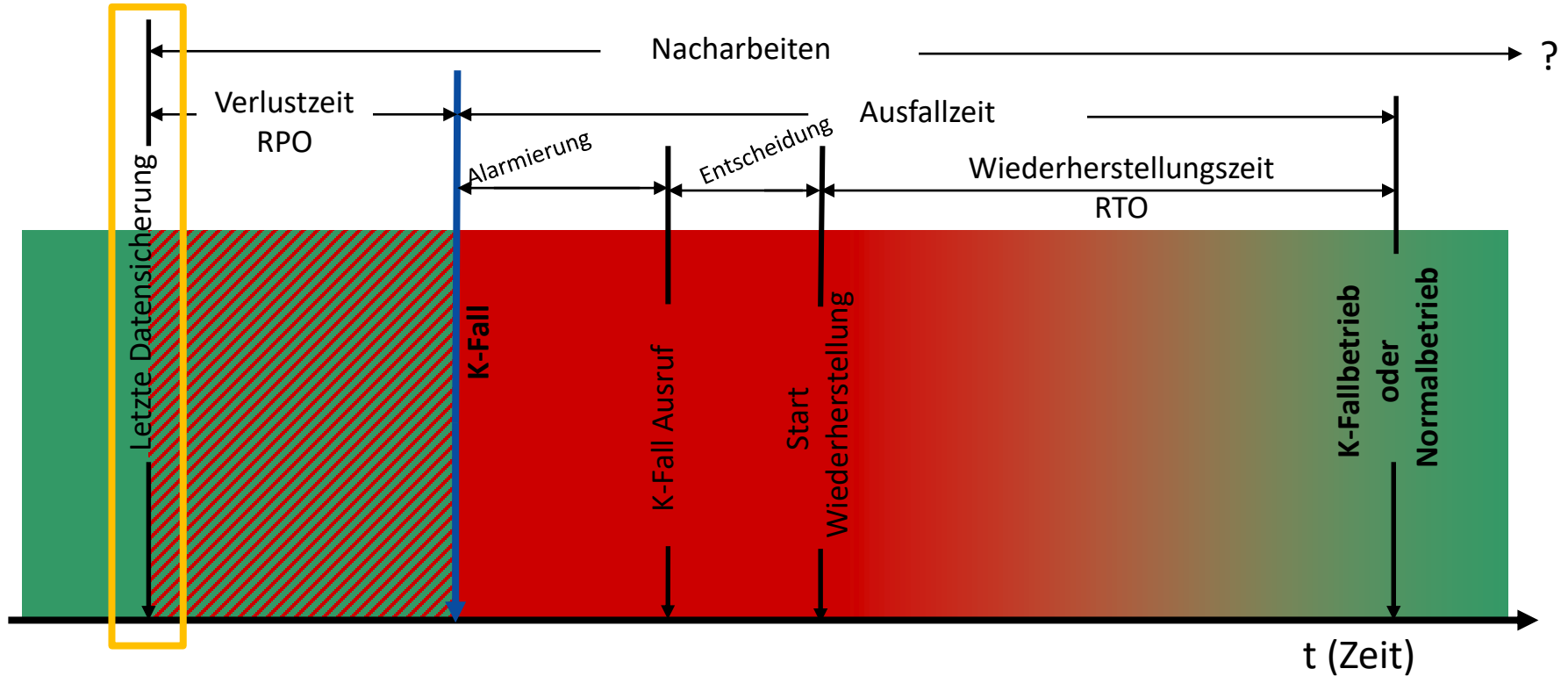
Was tun wenn's zu spät ist?

- Lösegeld zahlen?
 - Keine „Freilassungsgarantie“
- Backup einspielen?
 - Verlustzeit (Recovery Point Objective /RPO)?
 - Kalkulierter Datenverlust
 - Wo ist mein Backup?
 - Wurde mein Backup ebenfalls verschlüsselt?
 - Wiederherstellungszeit (Recovery Time Objective/RTO)?

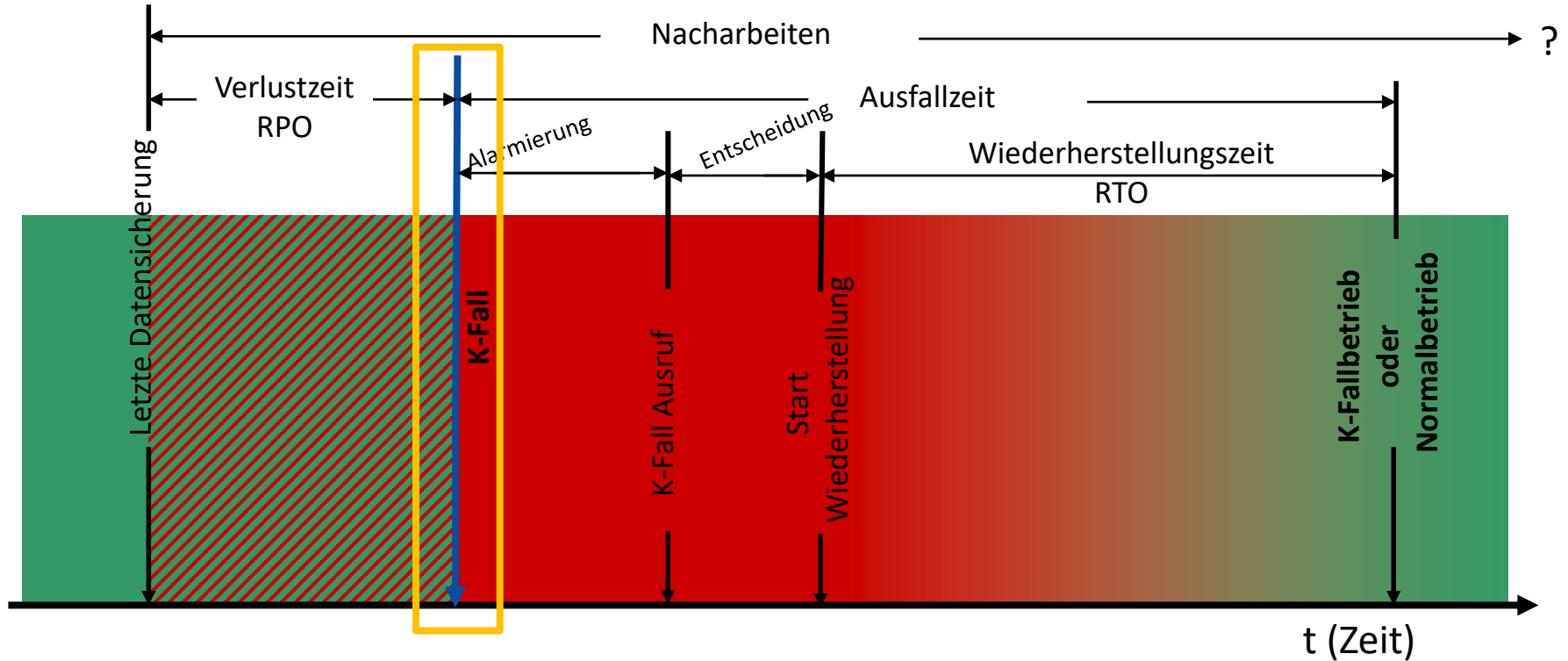
RPO/RTO erklärt



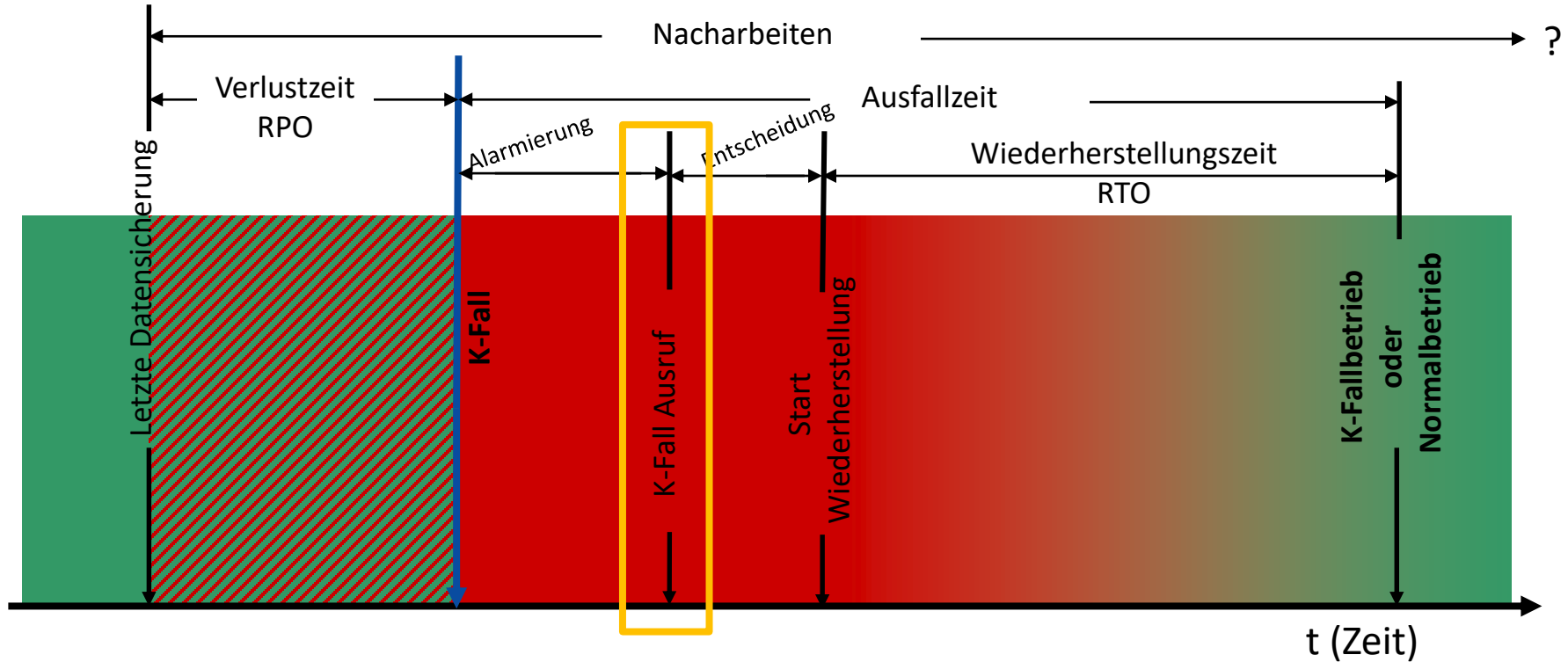
RPO/RTO erklärt



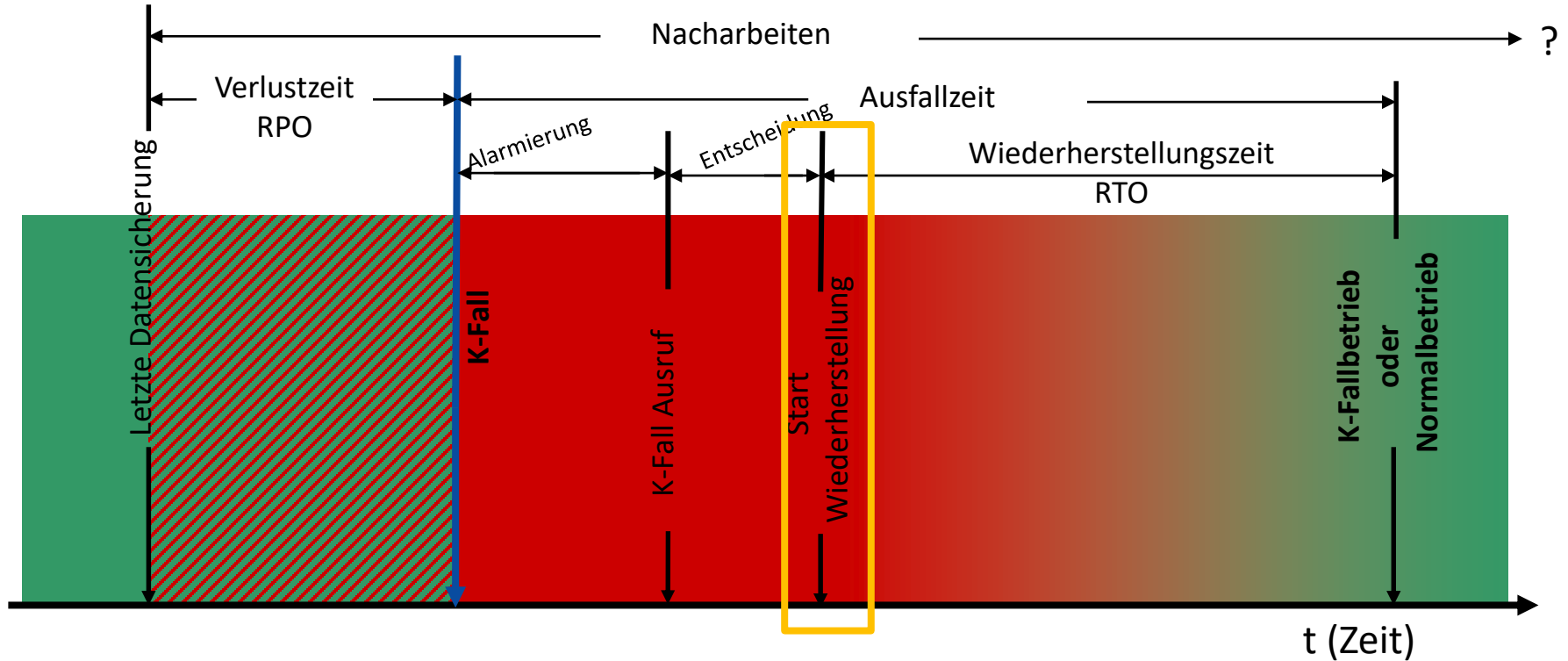
RPO/RTO erklärt



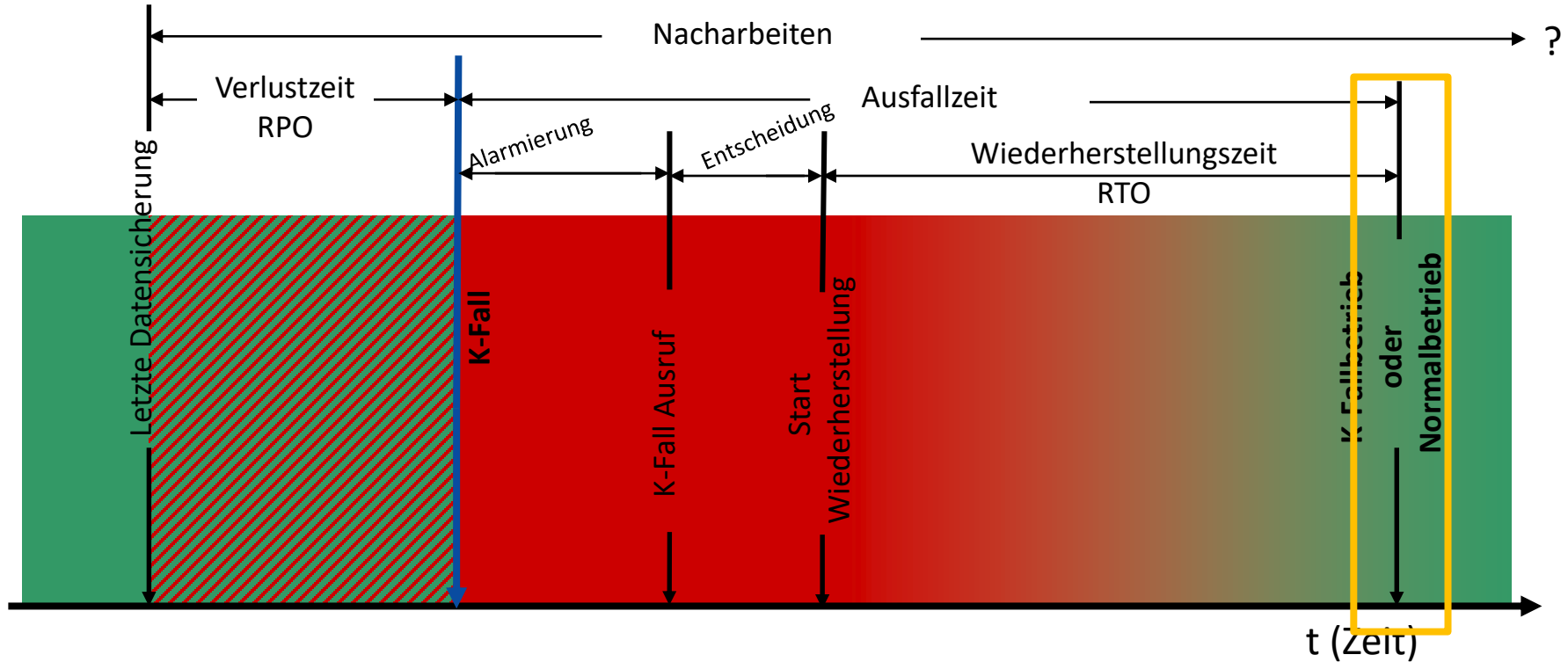
RPO/RTO erklärt



RPO/RTO erklärt



RPO/RTO erklärt



Continuous Data Protection

Was ist das?

Continuous Data Protection (CDP)

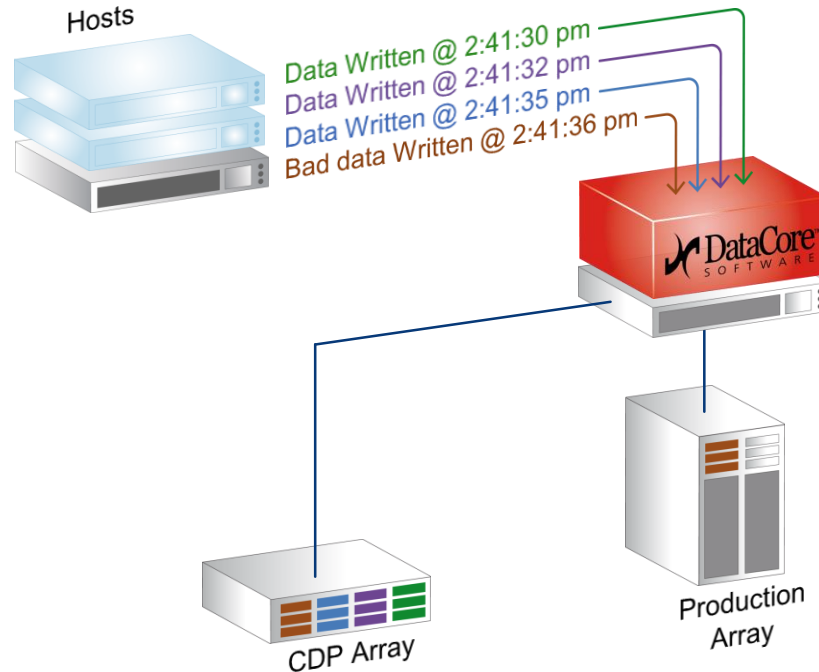


- Zugriff auf beliebige Datenzustände in einem 14 Tage Fenster
- Protokolliert nahtlos jeglichen I/O für geschützte virtuelle Disks
- Keine Anwendungsintegration notwendig
- Agentenfrei
- Einfach einschalten und wiederherstellen
- Konsistenz Markierungen möglich



CDP

Continuous Data Protection (CDP)

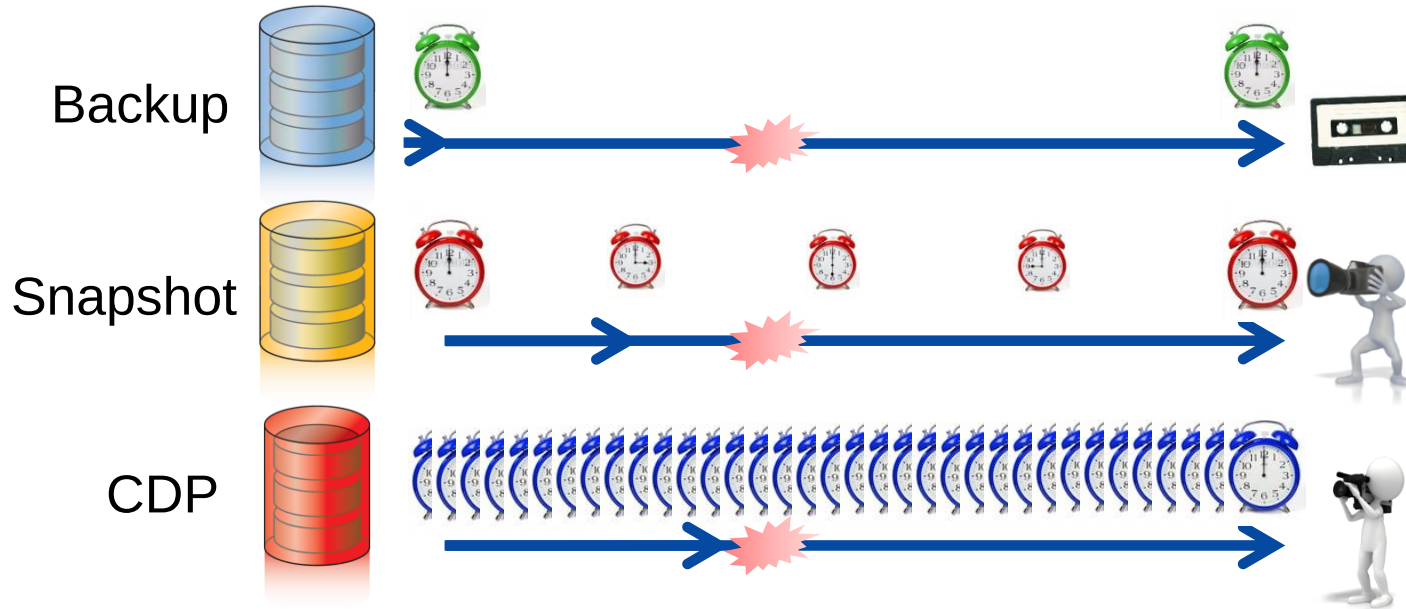




CDP

Wo CDP den Unterschied macht!

- Daten „filmen“ und wiederherstellen

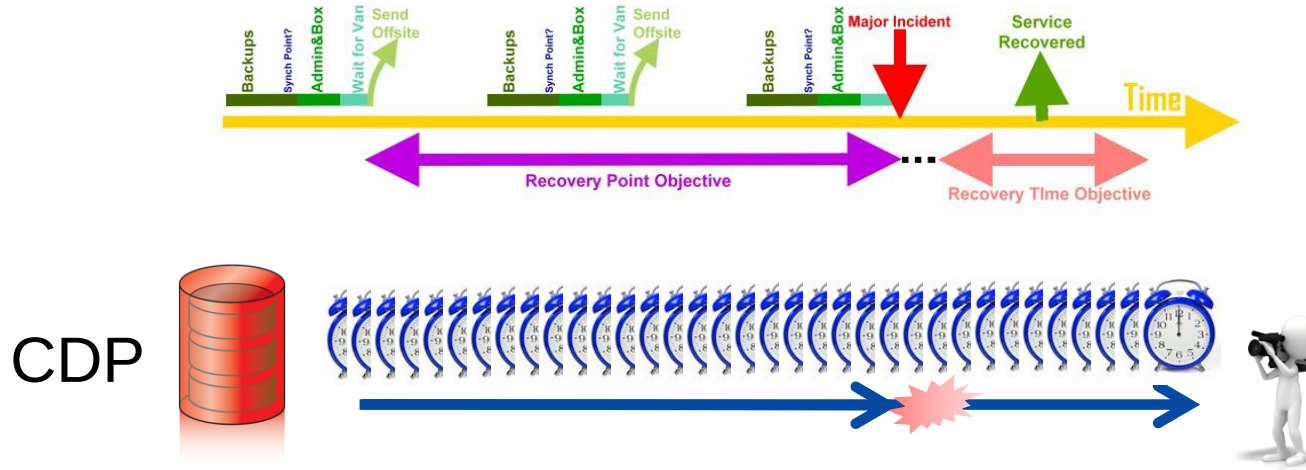




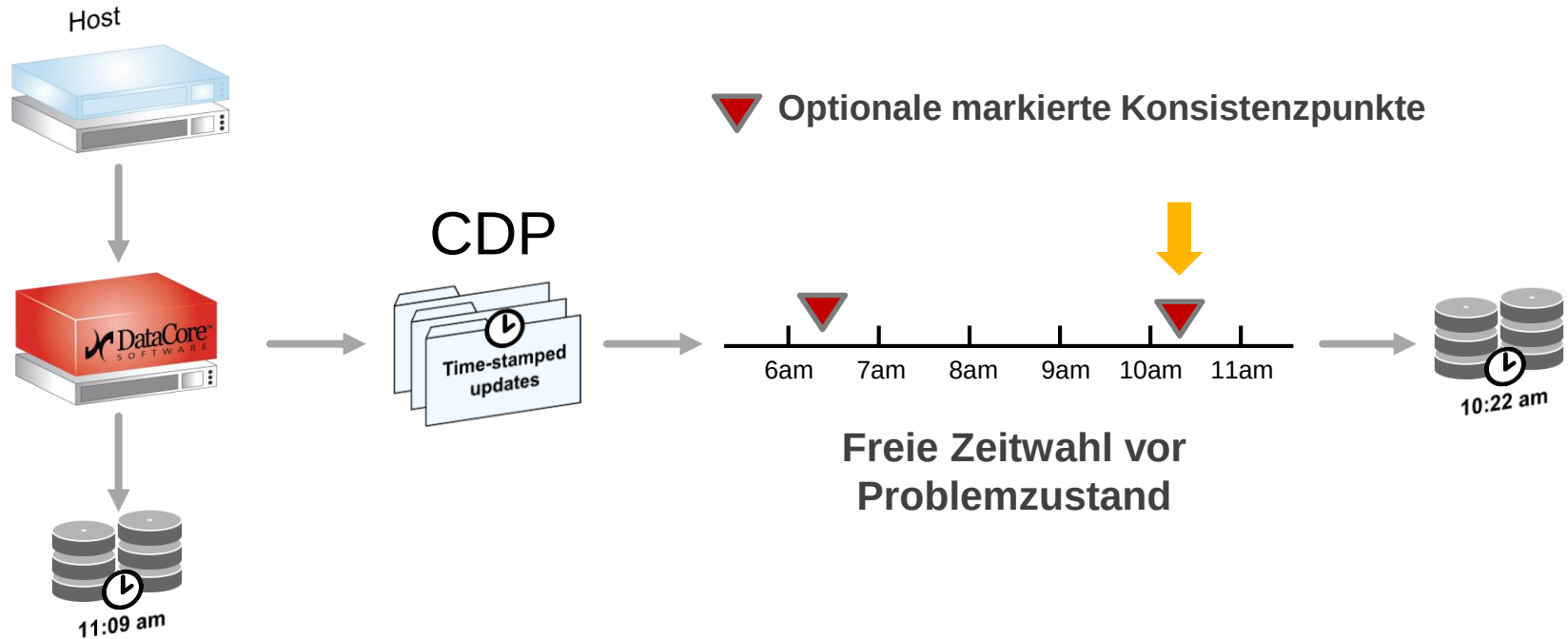
CDP

DataCore CDP

- Erhebliche Verbesserung des RPO- und RTO- Wertes



Rücksprung auf vorherige Zustände





CDP

Vorteile von CDP

- Unabhängig von 'Sicherungszeitfenstern'
- Verkürzung der Wiederherstellungszeit und Verkleinern des Datenverlustes
- Optimierung von RPO und RTO gegen Null
- Forensische Analyse und Troubleshooting

Wie hilft mir CDP im Falle eines Angriffs?

Angriffserkennung

- Verhaltensänderungen von CDP
 - Log wächst schlagartig
 - Retention Time schrumpft schlagartig

☒ Continuous Data Protection Enabled

DataCore Server: System Health Thresholds

Disk pool:

Minimum retention period warning threshold: hours

Maximum history log size: GB

Maximum history log size warning threshold: % of the maximum history log size

Abwehr

- Wiederherstellen der CDP geschützten Platten
 - Nach Alarmierung kompromittierte(n) Rechner sofort abschalten!
 - Zeitpunkt vor Angriff (Sekundenbereich) identifizieren
 - Herantasten durch multiple Rollback-Punkte
 - Verschlüsselungsfreien Datenbestand identifizieren
 - Restore unverschlüsselter Daten oder „instant“ Promotion des Rollback-Punkts zur Datendisk

Bitte beachten Sie...

- Continuous Data Protection (CDP):
 - Ersetzt kein Backup
 - Schafft keinen Medienbruch
 - Ist kein Datenreplizierungstool
 - Ersetzt nicht den „gesunden Menschenverstand“

Nächste Schritte

- Installieren Sie regelmäßig Updates und Patches auf Ihren Computern und Servern
- Schulen Sie Anwender
- Ziehen Sie CDP als Ergänzung zu Ihrem Backup in Betracht
 - Vereinbaren Sie hierzu eine 15-minütige Live-Demo mit einem unserer Solution Architekten
 - <http://info.datacore.com/LiveDemo>
- Testen Sie DataCore CDP in Ihrer Umgebung
 - Schützen Sie Ihre Daten im Falle einer Cyber-Attacke

Zusammenfassung

- Ransomware ist kein Mythos, es kann jeden treffen
- Ransomware bedroht lokale Daten und Server-Daten
- Niemals zahlen! Das ist die direkte Einladung für den nächsten Angriff!
- Sensibilisieren Sie Ihre Anwender
- Seien Sie vorbereitet und treffen Sie Maßnahmen dafür „was ist zu tun, wenn's passiert ist“

Zeit für Fragen...!



Vielen Dank

infoGermany@datacore.com

www.datacore.de