Disaster Recovery

Synchronisierung & Konsistenz

Michael Weinberger 5BHIT, 2. März 2016

Überblick

- Grundlagen & Definitionen
- Disaster Recovery Plan, Business Continuity
- Was ist eine Katastrophe? Problem der Downtime & Kosten, Fehlertoleranz
- Aufstellen eines DRP, Cluster <-> Disaster Recovery
- Seven tiers of disaster recovery
- DRaaS

Grundlagen & Definitionen

- Katastrophenwiederherstellung
- Vorbereitung und Reaktion auf sogenannte Katastrophen, die IT-System betreffen

- Cyberattacken, Infrastrukturausfälle ebenso wie Naturkatastrophen
- Schritte zur Wiederherstellung von Servern

- Wieso das alles?

Disaster Recovery Plan

- Richtlinien, Verfahren und Maßnahmen, um Störungen zu begrenzen
- Innerhalb eines Zeitrahmens zurück auf Normalzustand

- Macht Geschäftsbetrieb unmöglich!
- Kosten, Imageverlust?

- Norm: ISO27001

Business Continuity

- Weiterführung von wichtigen Geschäftsprozessen
- Aufrechterhaltung der Geschäftstätigkeit

- Business Continuity und Disaster Recovery eng verbunden, manchmal kombiniert

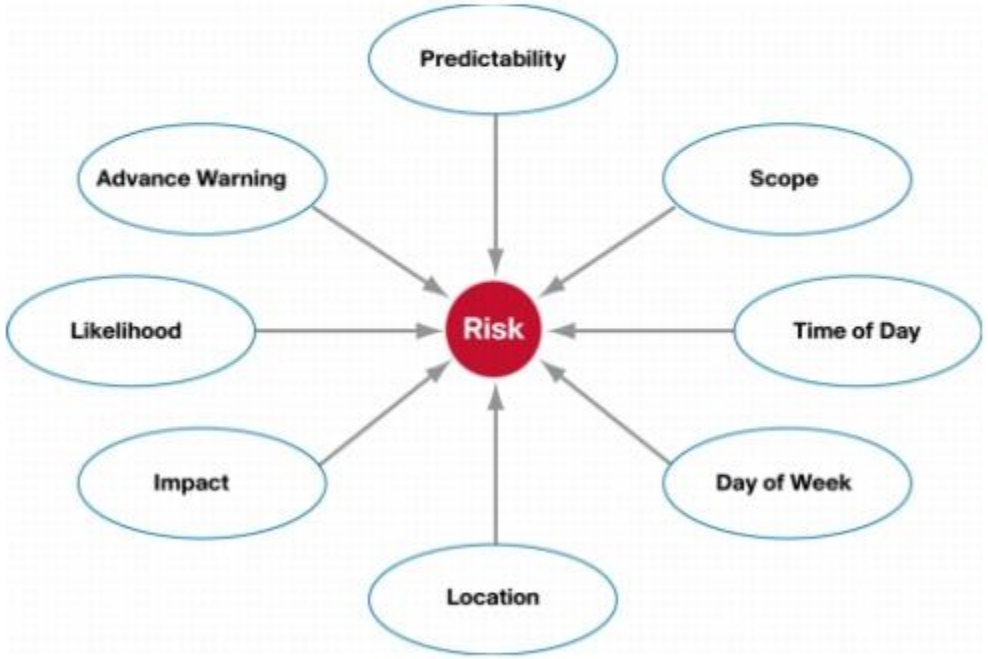
- Norm: BS25999

Was ist eigentlich eine Katastrophe?

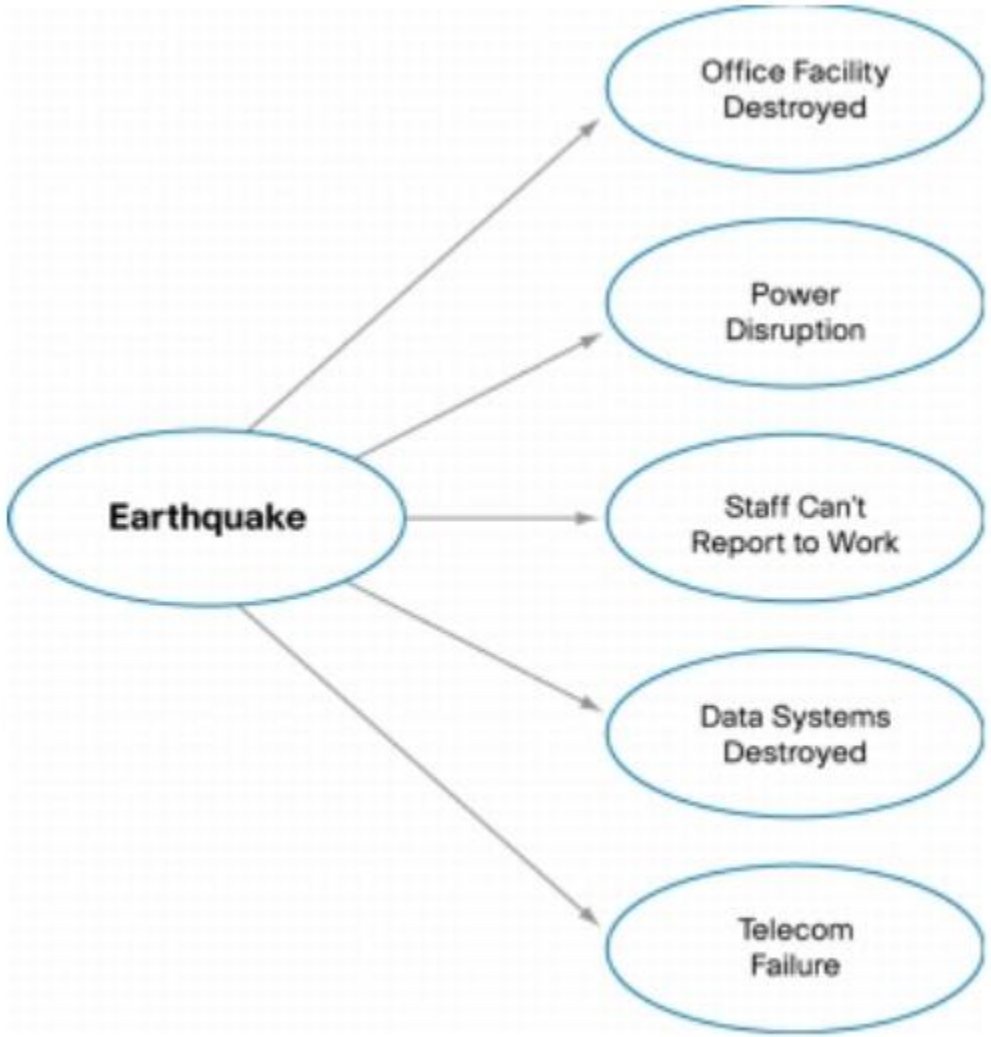
- Vierlei Ausmaß, primäre und sekundäre Auswirkungen
- Im schlimmsten Fall ohne Vorwarnung

- Wasserrohrbruch, Feuer, Viren, Datendiebstahl, Stromausfall, ...

- Kleinere Desaster häufiger, möglichst alle Faktoren berücksichtigen!



(a) Risikofaktoren [11]



(b) Extrembeispiel Erdbeben [12]

Abbildung 1: Katastrophe & Auswirkung, Risikoabschätzung

Problem der Downtime, Kosten

- Beispiel Facebook
- Schaden > 500.000 $

- Nutzer und Werbetreibende bauen auf dessen Zuverlässigkeit
- 20% der Unternehmen schätzen Ausfall = 1 Stunde Verlust über 100.000 $

- Zeigt, wieso Disaster Recovery/Hochverfügbarkeit wichtig ist!

Fehlertoleranz

- Fehler selbstständig und automatisch ausgleichen
- Reduziert Auswirkungen auf das System, Prozess läuft weiter

- Wichtige Systeme höheren Grad, hohe Toleranz = hohe Kosten

Aufstellen eines DRP

- Desasteridentifikation, Kommunikationsrichtlinien, Koordinieren der Prozesse
- Ausweichmöglichkeiten, → Rückkehr zu Normalzustand

- Priorisierung, was ist für Einsatzfähigkeit wichtig?
- Auferlegte Uptime

- Möglichst viele Daten sammeln, händisch, an Fall angepasst

Schaffung eines zuverlässigen Systems Cluster und deren Vorteile

- Clusterlösung = Garant für Hochverfügbarkeit
- Failover- oder Aktiv/Aktiv-Cluster

- Sehr teuer in Aufbau und Wartung
- Eher nur für große Unternehmen mit großem Budget

Schaffung eines zuverlässigen Systems Wozu dann Disaster Recovery?

- Für Systeme, wo < 100% Uptime in Ordnung, oder aus Budgetgründen

- Cold Standby, Eingriff des Administrators, ‚der Betrieb steht‘
- Normalzustand im Normalfall schnell erreicht, billiger als Cluster

- Auf Fehler reagieren, nachdem sie passiert sind

Schaffung eines zuverlässigen Systems Wozu dann Disaster Recovery?

- Mit gutem DRP Wahrscheinlichkeiten verringern, Recovery beschleunigen

- Unterbrechungsfreie Stromversorgung
- regelmäßige Backup-Routine
- RAID

= einfache Methoden, die viel helfen!

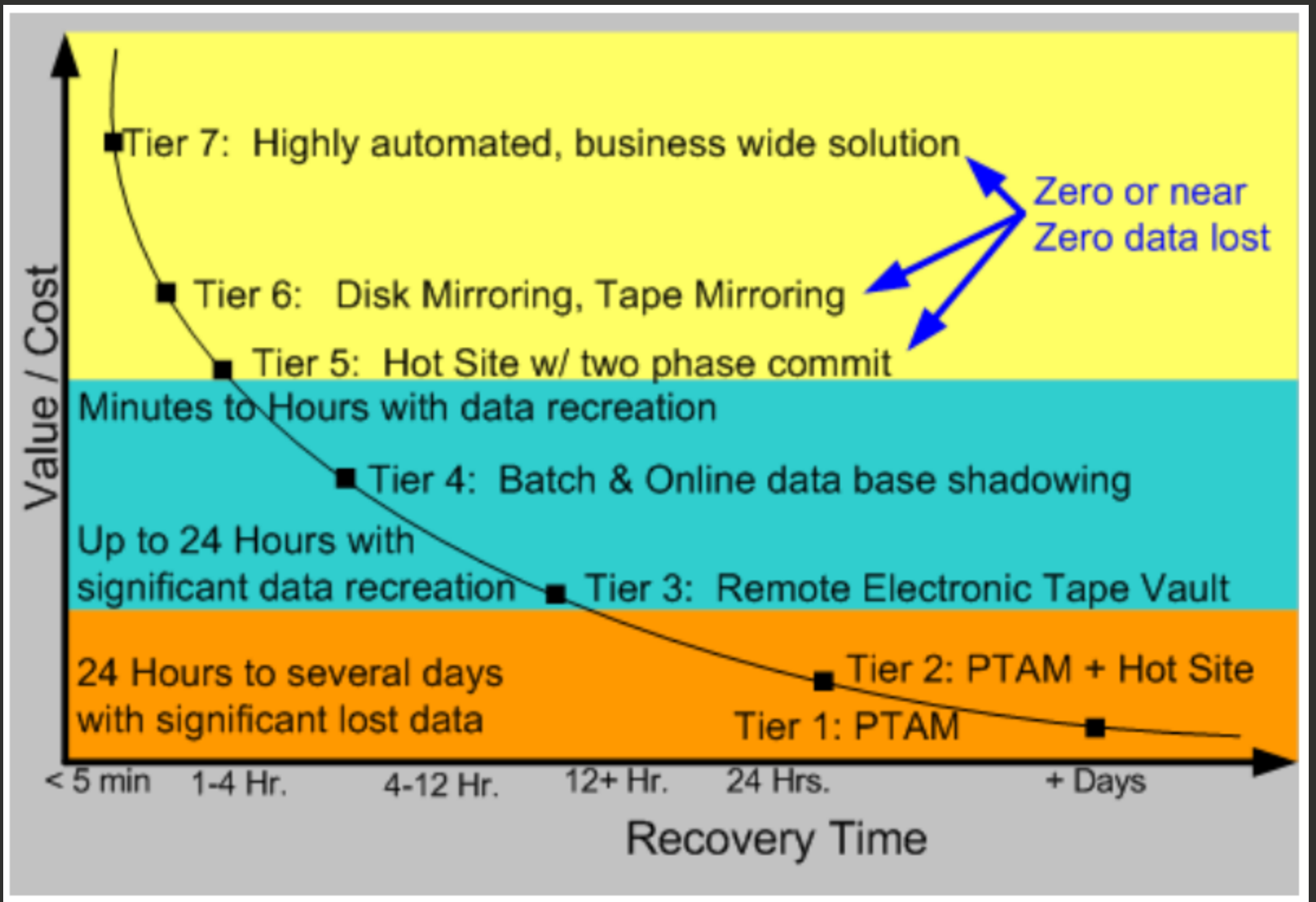


Abbildung 2: Seven tiers of disaster recovery [13]

Traditional Disaster Recovery

- SHARE / IBM

- Tier 0: No off-site data – Possibly no recovery
  - Keinen Plan, keine Backups
  - Recovery unvorhersehbar, wenn nicht sogar unmöglich

- Tier 1: Data backup with no hot site
  - Regelmäßiges Backup, PTAM
  - Einige Tage/Wochen Datenverlust möglich

Traditional Disaster Recovery

- Tier 2: Data backup with a hot site
  - Regelmäßige Sicherungen, Tapes
  - ‚Hot Site‘
  - Ausfall einige Stunden oder Tage möglich, Dauer besser vorhersehbar

- Tier 3: Electronic vaulting
  - Basiert auf Tier 2
  - Kritsche Daten abgekapselt
  - Weniger Datenverlust

Traditional Disaster Recovery

- Tier 4: Point-in-time copies
  - Hoher Wert auf Datenkorrektheit und schnellerer Wiederherstellung
  - Vorrangig mit Disks
  - Mehrere Stunden Datenverlust möglich
  - Einfache Backups dank fixem, variablen Zeitpunkt

- Tier 5: Transaction integrity
  - Wenn zwingend erforderlich, dass Daten konsistent
  - Kaum bis gar kein Datenverlust

Traditional Disaster Recovery

- Tier 6: Zero or near-Zero data loss
  - Höchstes Maß an Datenrichtigkeit
  - Für Systeme, wo kein Verlust tragbar
  - Erfordert Disk Mirroring

- Tier 7: Highly automated, business integrated solution
  - Übernimmt Tier 6, fügt Automatisierung hinzu
  - Desaster automatisch erkannt
  - Beschleunigt Prozesse, Wiederherstellung automatisch
  - Downtime: wenige Minuten oder Sekunden

Disaster Recovery as a Service

- Unterkategorie des Cloud Computing
- Zuverlässige Form des Disaster Recovery

- Abgrenzung zu cloudbasierten Backups
- Effizienter, billiger als Warm Site & Hot Site
- Sandboxes

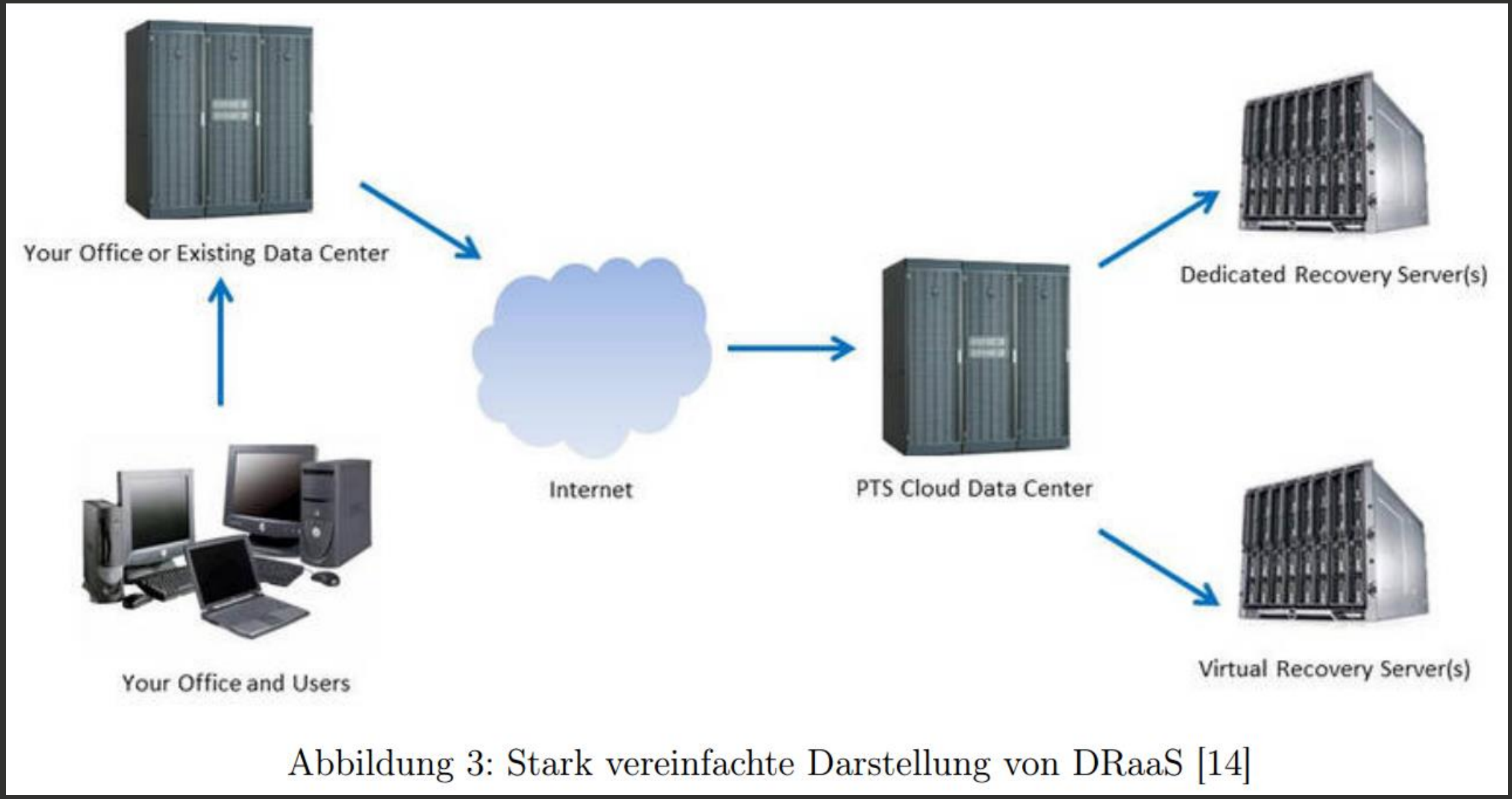


Abbildung 3: Stark vereinfachte Darstellung von DRaaS [14]

RaaS Architektur

- To-Clooud RaaS → Zielanwendung privat, Backup in der Cloud
- In-Cloud RaaS → Zielanwendung und Recovery-Sites in Cloud
- From-Cloud RaaS → Primärdaten in Cloud, Backup-Target privat
- Namhafte Hersteller bieten Implementierungen:
  - VMware, Zerto, Amazon AWS, Bluelock, Microsoft Azure
    - Preis nicht fix, je nach System, selber verhandelbar mit Hersteller

Vielen Dank für eure Aufmerksamkeit!

Gibt es Fragen?