

WISSENschafft
Vorsprung



IT-Sicherheit im Zeitalter des Cloud-Computing

Sven Geisel
Staatliche Studienakademie Bautzen

Wrocław, 29.10.2015



Teilausfälle bei Amazon sorgten für Kundenfrust
@ heise online 16.02.2015 13:15 Uhr - Holger Bleich

amazon.de

Alle Kategorien ans...

Bücher

(Bild: dpa, Frank May)
Am Abend des gestrigen 15. Februar war Amazon.de zeitweise nicht zu erreichen. Damit verbunden streikten auch an die Domain gekoppelte Services, etwa Instant Video.

Gehackte Bundestags-Rechner: Cyber-Angriff kam per E-Mail

In Apples AppStore hunderte Anwendungen mit Trojanern verseucht!

Hacker stellen Millionen Fremdgeher im Internet bloß

Android: Und noch eine schwere Sicherheitslücke UPDATE
12.08.2015 18:23 Uhr - Christian Kirsch



(Bild: dpa, Britta Pedersen)
Forscher von IBM haben in Googles mobilem Betriebssystem eine Lücke entdeckt, die über die Hälfte aller Android-Geräte betrifft. Sie erlaubt das Übernehmen privilegierter Prozesse durch einen Angreifer. Google hat die Lücke bereits geschlossen.

IT-Sicherheit

Datensicherheit

Bedrohungen

durch Menschen

...



Maßnahmen

technische

organisatorische

personelle

Datenschutz

Internet

Public/Private
Cloud Computing

Anwendungen
Plattformen
Infrastruktur

Unter-
nehmen

Private
Cloud

Cloud Anbieter

- > Keiner kann 100%ige Sicherheit garantieren!
- > Sicherheitsniveau kann oft im "Service Level Agreement" ausgehandelt werden
- > Zertifikate wie **ISO 27001** schaffen Vertrauen
- > Ihre Mitarbeiter sind schon in der Cloud!



Microsoft



Google Cloud Platform

T-Systems

SAP S/4 HANA

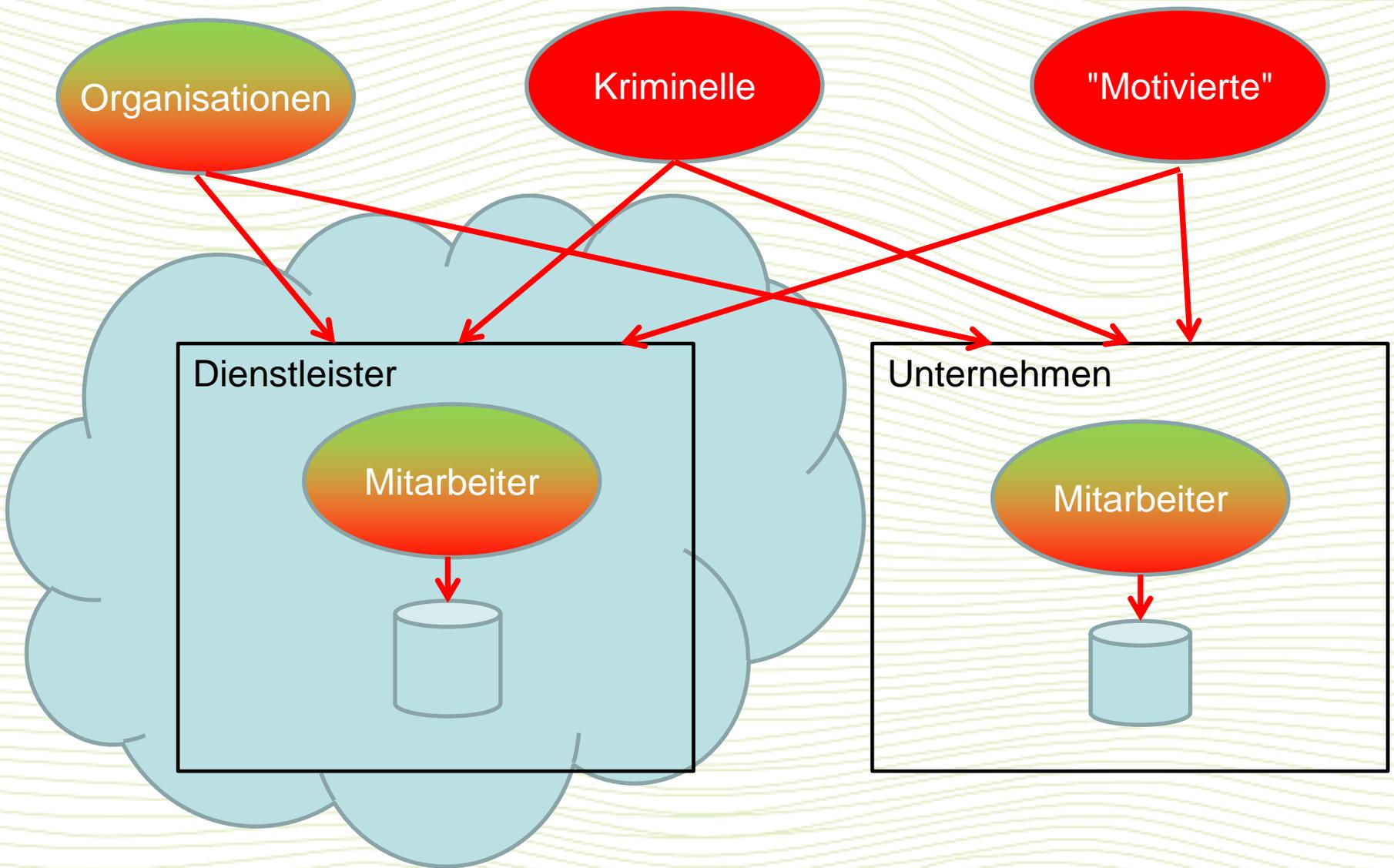


amazon
web services™

itelligence NTT DATA Business Solutions

Dropbox





Vor- und Nachteile

- > Kosten **können** geringer sein
- > bessere Skalierbarkeit
- > Abhängigkeit vom Anbieter
- > oft bessere Sicherheitsmaßnahmen, aber zusätzliche Risiken:
 - beliebtes Angriffsziel
 - Netzwerkverbindung
 - Mitarbeiter des Anbieters
 - Datenschutz (nicht EU-Länder)

Mitarbeiter

- > Datenverluste: 30 % durch IT-Abteilungen, 22 % durch Kunden-Service [Orthus2007]
- > 14 % der Unternehmen bemerkten beabsichtigte Lücken oder ein bewusstes Teilen von Informationen durch Mitarbeiter, und dieses führte bei 36 % auch zum Verlust von geschäftskritischen Daten [Kaspersky2015]
- > 9 % beklagten den Verlust sensibler Informationen durch Softwarelücken, 26% durch Diebstahl oder Verlust mobiler Geräte und 25 % aufgrund von durch Mitarbeiter unabsichtlich verursachte Datenlecks [Kaspersky2015]
- > Die Hälfte aller Mitarbeiter, die ihren Arbeitsplatz gewechselt oder ihre Stelle verloren hat, behält vertrauliche Unternehmensdaten. Jeder Vierte davon will diese Daten beim neuen Arbeitgeber nutzen. [Ponemon Institute 2012]

Was man tun sollte

- > schulen und **sensibilisieren** Sie Ihre Mitarbeiter!
 - Passworte, BYOD, Phishing, Trojaner, Drive-by-Downloads, Zertifikate, Identitätsdiebstahl
- > überlassen Sie die Verantwortung nicht nur der IT-Abteilung oder dem Dienstleister
- > nutzen Sie **aktuelle** technische Maßnahmen wie Antimalware, autom. Updates, Backups, Firewalls
- > stellen Sie ein IT-Sicherheitskonzept auf und **leben** Sie es
- > "**riskieren**" Sie die Cloud



**Vielen Dank für die
Aufmerksamkeit**

geisel@ba-bautzen.de