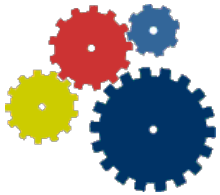


Sicherheitsanalyse von Private Clouds

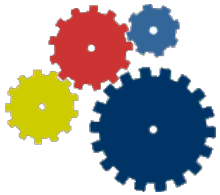
Alex Didier Essoh und Dr. Clemens Doubrava

Bundesamt für Sicherheit in der Informationstechnik

12. Deutscher IT-Sicherheitskongress 2011

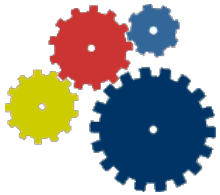
Bonn, 10.05.2011

Agenda



- Einleitung und Motivation
- High-Level Architektur einer Private Cloud
- Gefährdungen beim Betrieb einer Private Cloud
- Maßnahmen zum sicheren Betrieb einer Private Cloud
- Fazit

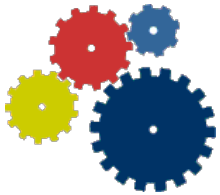
Was ist Cloud Computing?



NIST-Definition (wird in Fachkreisen meist genutzt)

Cloud Computing ist ein Modell, das es erlaubt bei Bedarf, ***jederzeit und überall*** *bequem über ein* ***Netz*** *auf einen* ***geteilten Pool*** *von konfigurierbaren* ***Rechnerressourcen*** *(z. B. Netze, Server, Speichersysteme, Anwendungen und Dienste) zuzugreifen, die schnell und mit* ***minimalem Managementaufwand*** *oder geringer Serviceprovider-Interaktion zur Verfügung gestellt werden können.*

Was ist Cloud Computing?

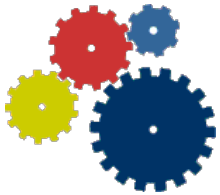


BSI-Definition

*Cloud Computing bezeichnet das **dynamisch** an den Bedarf angepasste Anbieten, Nutzen und Abrechnen von IT-Dienstleistungen über ein **Netz**. Angebot und Nutzung dieser Dienstleistungen erfolgen dabei ausschließlich über **definierte technische Schnittstellen und Protokolle.***

*Die Spannbreite der im Rahmen von Cloud Computing angebotenen Dienstleistungen umfasst das **komplette Spektrum der Informationstechnik** und beinhaltet unter anderem Infrastruktur (z. B. Rechenleistung, Speicherplatz), Plattformen und Software.*

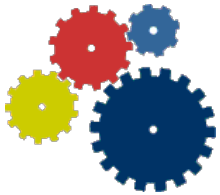
Private Cloud



Cloud Bereitstellungsmodelle (Deployment Models):

- In einer **Public Cloud** können die angebotenen Services von beliebigen Anwendern genutzt werden
- In einer **Private Cloud** wird die Cloud-Infrastruktur nur für eine Institution betrieben. Sie kann von der Institution selbst oder einem Dritten organisiert und geführt werden und kann dabei im Rechenzentrum der eigenen Institution oder einer fremden Institution stehen
- Werden aus einer Private Cloud heraus Dienste einer Public Cloud genutzt, so wird dies als **Hybrid Cloud** bezeichnet

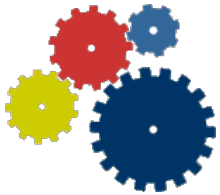
Private Cloud



Vorteile von Private Clouds

- Nutzung der potentiellen Vorteilen von Cloud Computing
- Beibehaltung der Kontrolle über die IT-Infrastruktur
- Vermeidung möglicher Risiken

Private Cloud

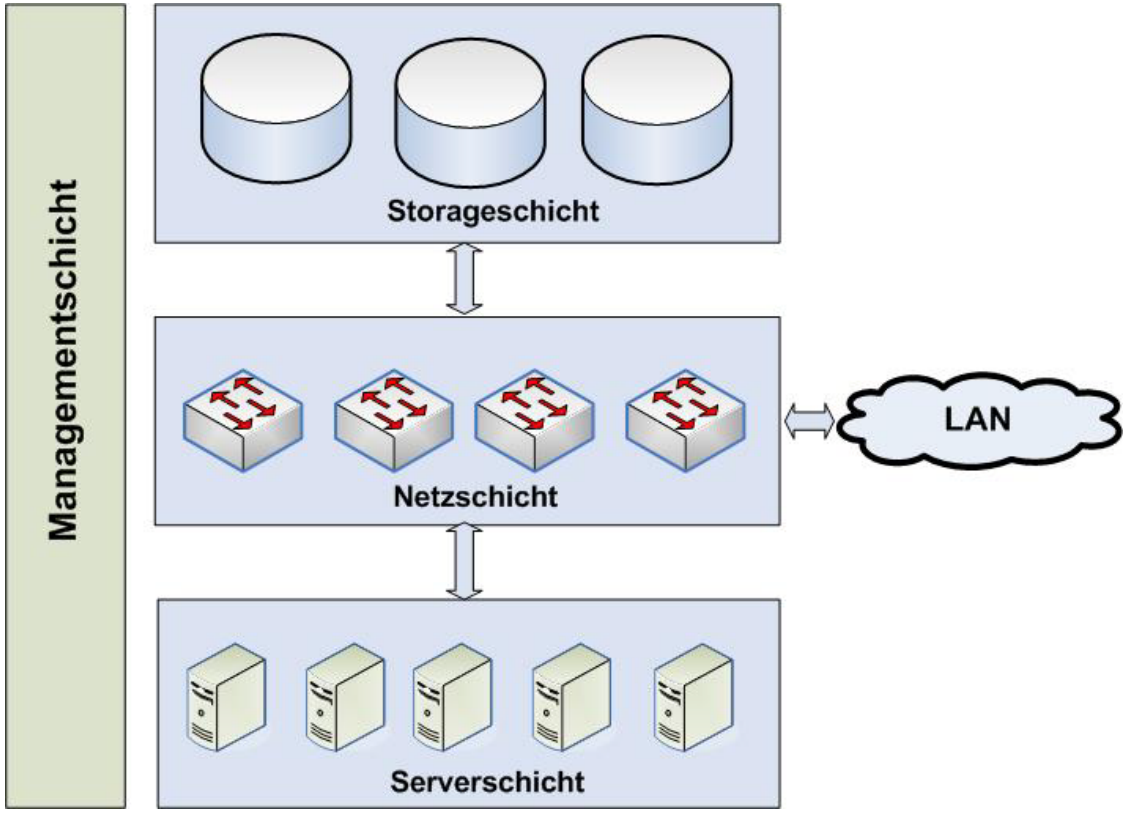


Was sind die Risiken bei einer Public Cloud?

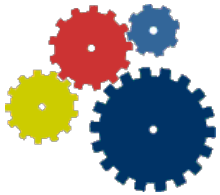
- **Verlust der Kontrolle** über die Daten und Anwendungen
- **Verletzung** geltender Vorgaben und Richtlinien (z.B. **Datenschutzanforderungen**)
- **Viele, unbekannte Nutzer teilen** sich eine **gemeinsame Infrastruktur**. Risiko einer Verletzung der Grundwerte der Informationssicherheit steigt
- Daten bzw. Anwendungen werden über das Internet genutzt, so dass ein **Ausfall der Internetverbindung** den Zugriff unmöglich macht
- Zunahme von verteilten **Denial-of-Service Angriffen** auf Cloud-Computing-Plattformen
- Sehr hohe Komplexität kann zu zahlreichen Sicherheitsproblemen führen (**Ausfall von Diensten**, **Datenverlust**, etc.)

High-Level Architektur einer Private Cloud

- Netzschicht
- Serverschicht
- Storageschicht
- Managementschicht

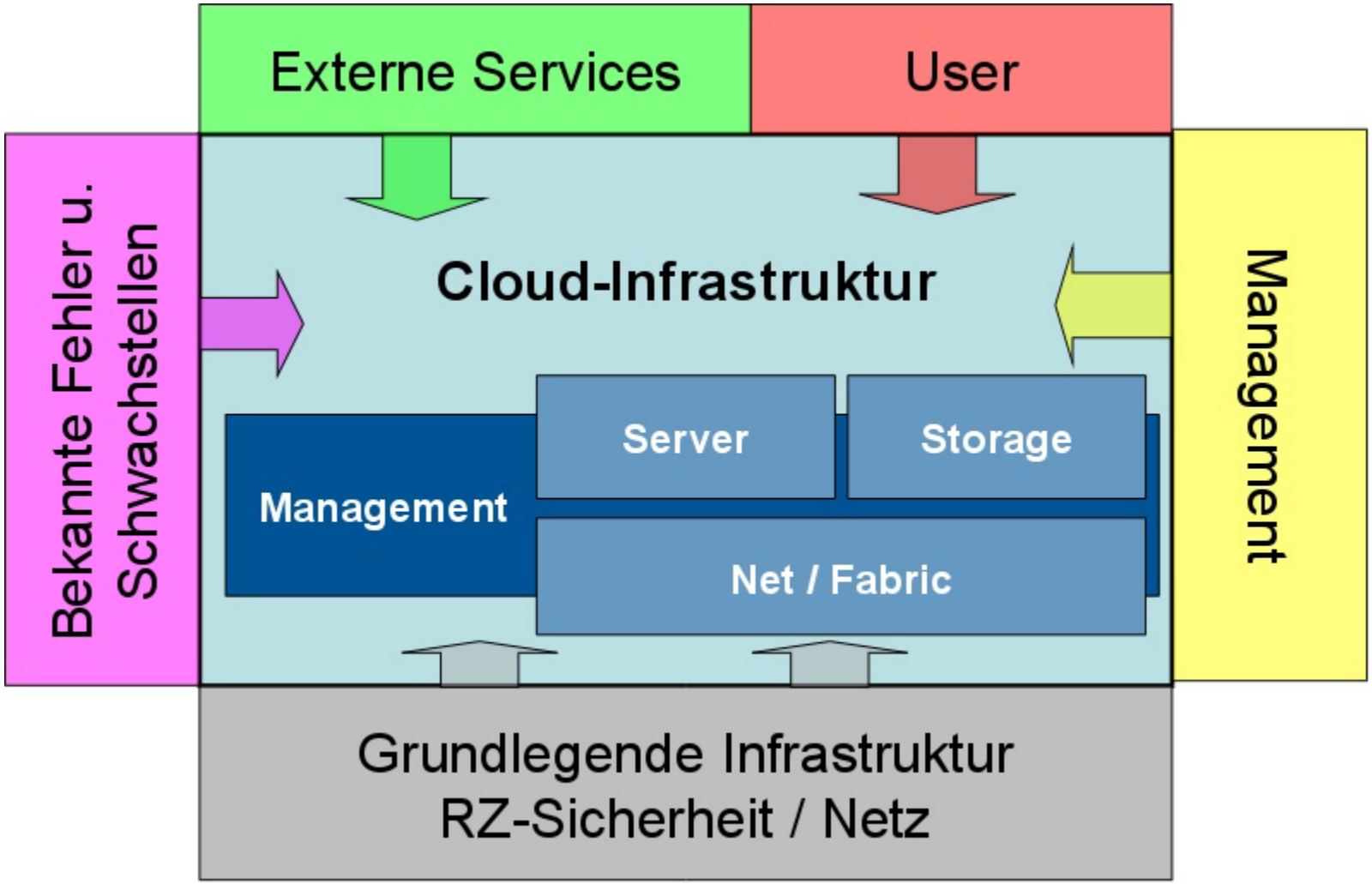


Agenda

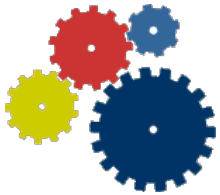


- Einleitung und Motivation
- High-Level Architektur für eine Private Cloud
- **Gefährdungen beim Betrieb einer Private Cloud**
- Maßnahmen zum sicheren Betrieb einer Private Cloud
- Fazit

Gefährdungen der Cloud-Infrastruktur



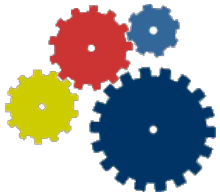
Gefährdungen beim Betrieb einer Private Cloud



Serverschicht

- Kompromittierung des **Hypervisors**
- Kompromittierung des **Management Interface**
- Überbuchung des **Arbeitsspeichers**
- Auslesen des **Arbeitsspeichers**
- Missbrauch von **Schnittstellen**
- Ausfall des **Hosts**

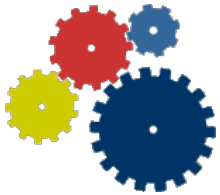
Gefährdungen beim Betrieb einer Private Cloud



Netzschicht

- Interne **Kommunikation zwischen den VMs**
- Ungeeignete **Segmentierung**
- Fehlende **Verschlüsselung**
- **.....**

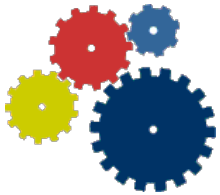
Gefährdungen beim Betrieb einer Private Cloud



Speicherschicht

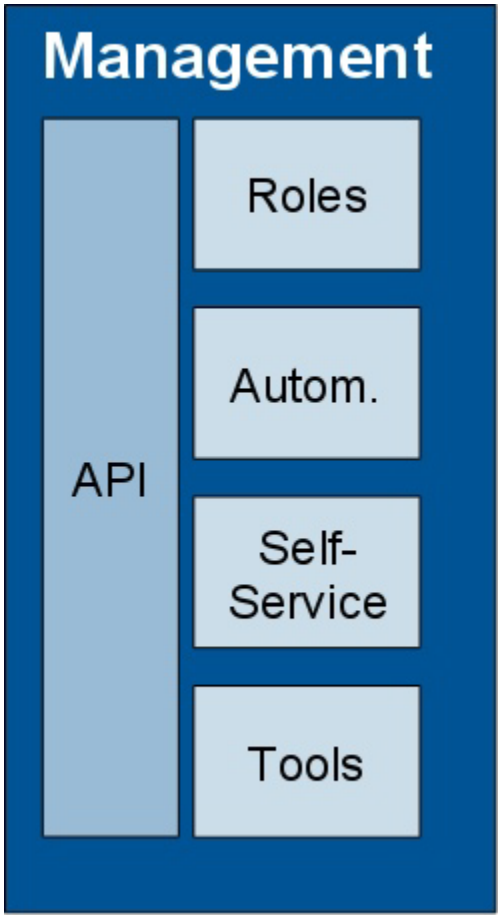
- **Back-up**-System
- **DoS** auf Storage-Systeme
- **Storage-Protokolle**
- **.....**

Gefährdungen beim Betrieb einer Private Cloud

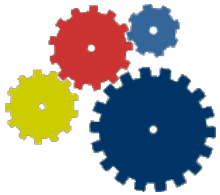


Managementschicht

- Mangelhafte Planung von Rollen und Verantwortlichkeiten
- Integration in Verzeichnisdienste
- Fehlkonfiguration / Fehler bei der Automation
- Management Interfaces
- Unsicheres Self Service Portal

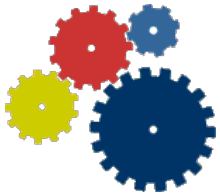


Agenda



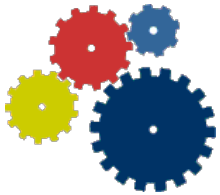
- Einleitung und Motivation
- High-Level Architektur für eine Private Cloud
- Gefährdungen beim Betrieb einer Private Cloud
- **Maßnahmen zum sicheren Betrieb einer Private Cloud**
- Fazit

Maßnahmen zum sicheren Betrieb einer Private Cloud



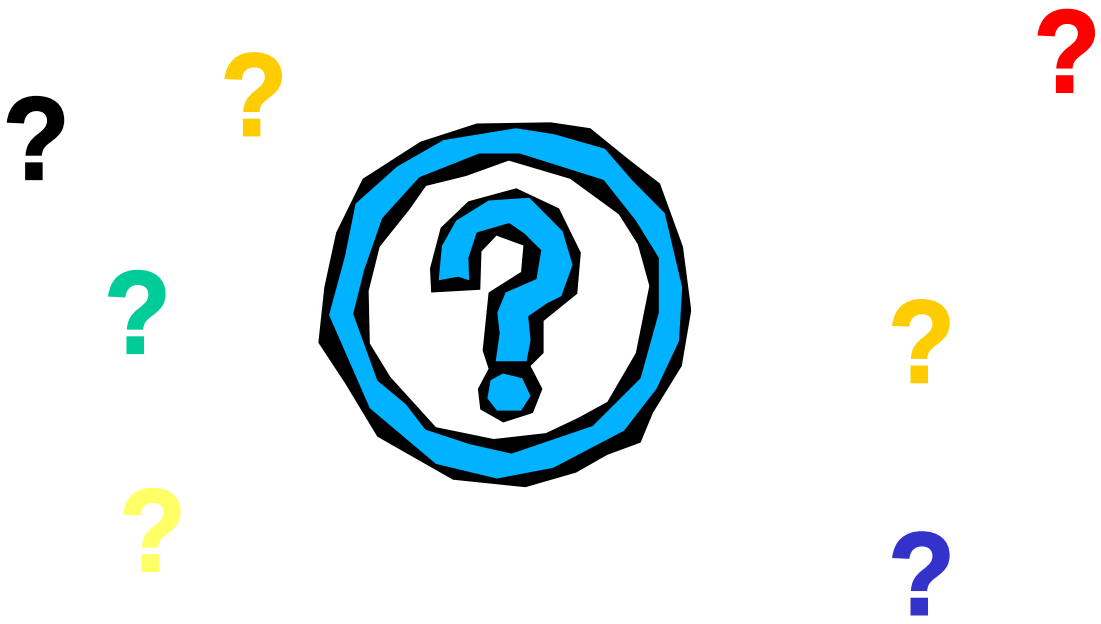
- Sichere Trennung der Mandanten
- Sichere Konfiguration der Komponenten
- Trennung der Rollen und Verantwortlichkeiten
- Schulung der Administratoren
- Schutz der Webschnittstelle

Fazit



- Aufgrund der technischen und wirtschaftlichen Potenziale kann sich Cloud Computing **am Markt durchsetzen**, wenn die Frage der **angemessenen IT-Sicherheit** geklärt wird.
- Zur Minimierung der Risiken werden die Anwender **zunächst auf Private Clouds** zurückgreifen
- Aber auch in einer Private Cloud muss **Informationssicherheit** gewährleistet sein
- Die Erarbeitung und Etablierung von **Standards** für **Interoperabilität** und **Informationssicherheit** wird eine der zentralen Aufgaben in den kommenden Jahren sein

Fragen und Diskussion



Kontakt

Bundesamt für Sicherheit in der Informationstechnik (BSI)

Alex Didier Essoh
Godesberger Allee 195-198
53175 Bonn

Tel: +49 (0)22899-9582-5391
Fax: +49 (0)22899-9582-10-5391

cloudsecurity@bsi.bund.de
www.bsi.bund.de/grundschutz
www.bsi-fuer-buerger.de

Neu: XING-Forum IT-Grundschutz

Kontakt

Bundesamt für Sicherheit in der Informationstechnik (BSI)

Dr. Clemens Doubrava
Godesberger Allee 195-198
53175 Bonn

Tel: +49 (0)22899-9582-5887
Fax: +49 (0)22899-9582-10-5887

cloudsecurity@bsi.bund.de
www.bsi.bund.de/grundschutz
www.bsi-fuer-buerger.de

Neu: XING-Forum IT-Grundschutz