

CC: BETRIEB & SICHERHEIT

Dipl.-Medieninf. Hai Dang Le
Software Engineer
hhdang.88@gmail.com

SS 2017



AGENDA

3. BETRIEB & SICHERHEIT

- a. Gast-Vortrag: Rechenzentrumsbetrieb
- b. Studentenvorträge
- c. Sicherheit bei Cloud Computing

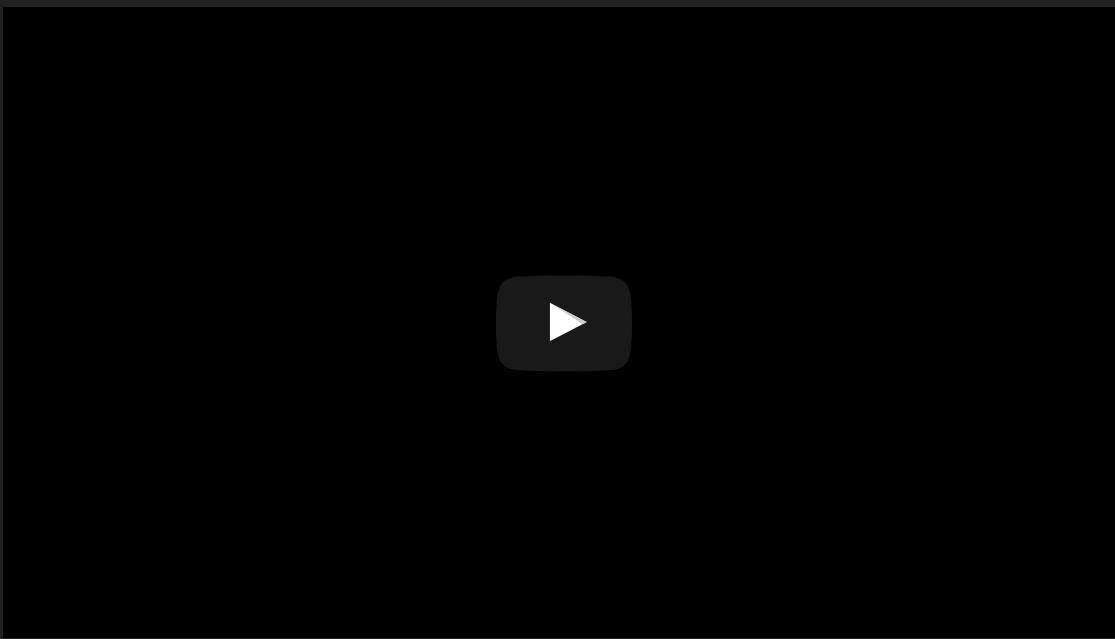


3. BETRIEB

A. RECHENZENTRUMSBETRIEB

GAST-VORTRAG: RECHENZENTRUMSBETRIEB

- Gast-Redner: M.Sc. Gerrit Schmitz
- Security Expert
- Connected Services, Robert Bosch GmbH
- Dozent DHBW Stuttgart



RECHENZENTREN & SICHERHEIT

WAS IST EIN RECHENZENTRUM?

Simpel: Ein Raum in dem Informationstechnik
betrieben wird.

Aber es gibt Qualitätsunterschiede.

DATA CENTER TIERS

Das Uptime Institute hat schon in den 90ern Rechenzentren anhand ihrer Infrastruktur klassifiziert. Dabei kamen vier aufeinander aufbauende "Tiers" zustande.

<https://journal.uptimeinstitute.com/explaining-uptime-institutes-tier-classification-system/>

Basic Capacity

Dedizierter rund um die Uhr klimatisierter Raum mit unterbrechungsfreier Stromversorgung und Generator.

Redundant Capacity Components

Sowohl Klimaanlage als auch Stromversorgung sind redundant, um Anlagenausfälle abzufangen.

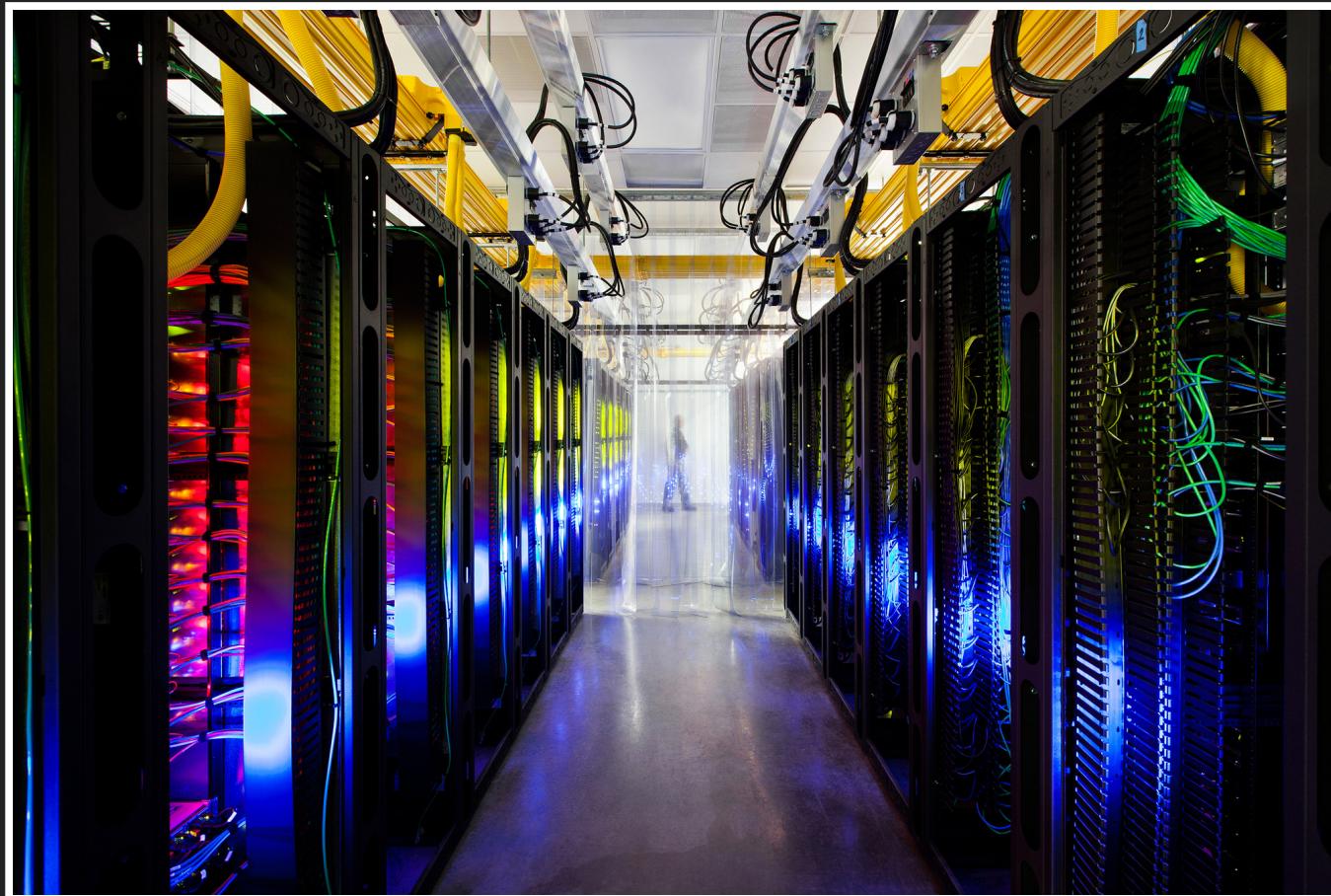
Concurrent Maintainable

Alle Anlagen können gewartet werden, ohne den Betrieb einzuschränken.

Fault Tolerance

Alle Komponenten und Versorgungspfade können einzeln ausfallen, ohne den Betrieb einzuschränken.

Ein ordentliches Rechenzentrum schaut etwa so aus:



Mehr Bilder unter

<http://www.google.com/about/datacenters/gallery/#/te>

Ein einzelnes Rechenzentrumsgebäude bzw. je nach Aufbau auch -stockwerk nennt man im Cloud-Speak Availability Zone.

VERSORGUNGSPFADE

Dank der immer fortschreitenden Verkleinerung sind heutzutage nicht mehr m^2 das Problem, sondern Kühlung (MW) oder Stromversorgung (kA).

Und auch beim Strom gibt's Unterschiede.

Bei manchen Stromanbietern verläuft die Spannung nicht genau sinusförmig. Das führt zu elektrischem "Verschleiß".

Nahezu alle Geräte transformieren die Wechselspannung intern zu Gleichspannung. Auch da kann man helfen, indem man die verschiedenen Stromversorgungspfade phasenverschiebt.

NATURKATASTROPHEN USW.

Aber wie vermeidet man kleinere (Baustelle kappt Strom) und größere Katastrophen (Erdbeben, Feuer, Überflutung)?

Man muss auch das Rechenzentrum selbst redundant machen :) Das heißt dann bei den meisten Cloudanbietern "Region".

INHALT

Man kann die verwendete Hardware grob in drei Kategorien aufteilen:

- Netzwerk
- Storage
- Server

Die Geräte stecken dabei in einem...

RACK

Ein 60-80cm breiter, etwa 2m hoher Schrank.
Üblicherweise aufgeteilt in 42 Höheneinheiten von je
1,75 Zoll und 19 Zoll Breite. Die Tiefe variiert von 60-
120cm. Der Extraplatz kann dabei für saubere
Verkabelung oder Türen benutzt werden.

NETZWERK

Das Netzwerk muss je nach Bedarf die Daten zwischen den anderen Kategorien transportieren.

Dabei kommen üblicherweise Ethernet mit 1 - 10GBit/s zum Einsatz.

Infiniband kommt aber auch auf bis zu 290 GBit/s.

Ein typischer Router:



Ein typischer Switch:



STORAGE

Storage bezeichnet Plattensysteme alle Größe und Protokolle. Das können sein:

Direct Attached Storage (DAS)

Blockstorage für einen Server

Storage attached network (SAN)

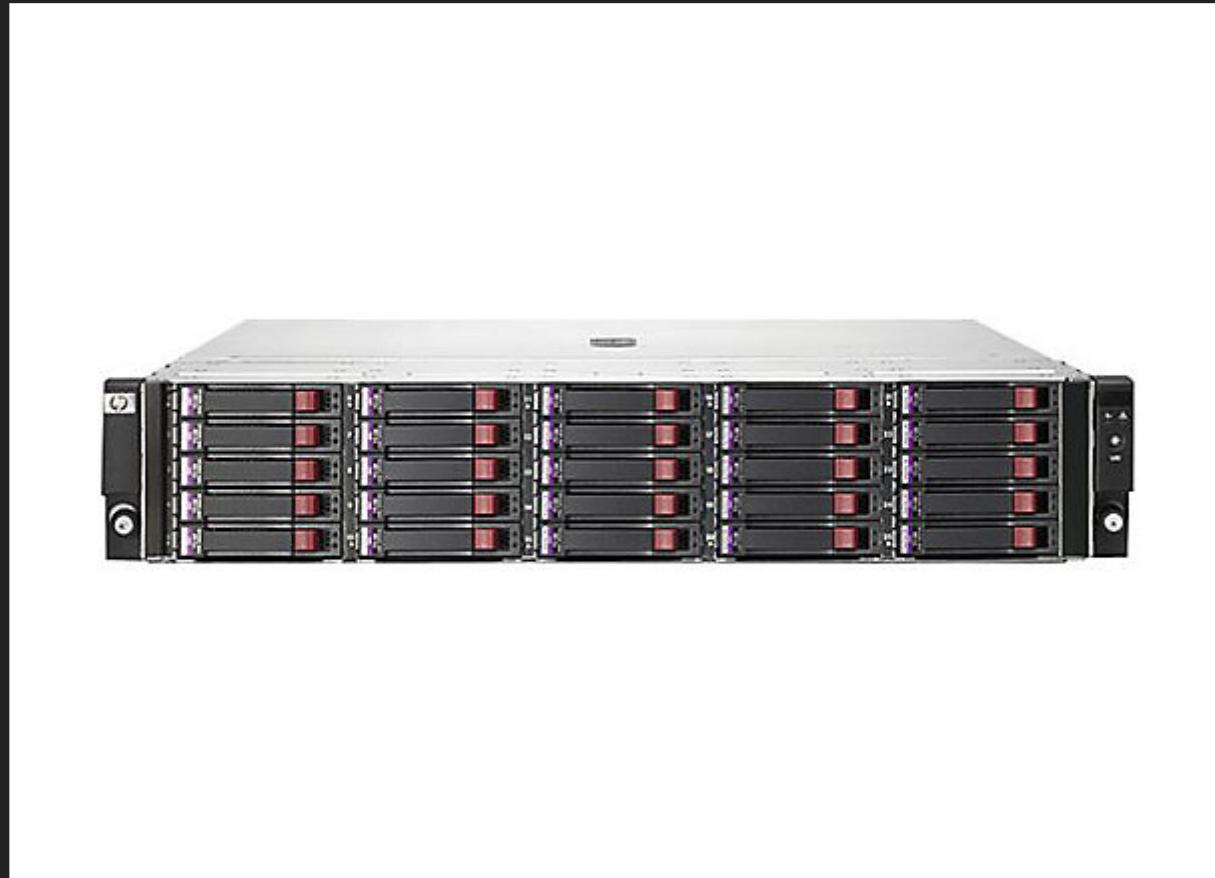
Blockstorage für mehrere Server. z.B. AWS EBS

Network Attached Storage

Fileshares wie bsp. Volume Services in Cloud

Foundry

Ein kleines DAS:



Ein großes SAN:



SERVER

Server zeichnen sich primär durch CPU (Architektur, Kerne, Takt) und RAM (Anzahl Module, Größe, Takt) aus. Dabei ging der Trend immer mehr zum Outsourcen der Platten (siehe Storage) und anderer Komponenten hin.

Ein klassischer Server:



Ein Blade:



Ein Blade Center:



PHYSISCHE SICHERHEIT

Menschen müssen natürlich im Rechenzentrum arbeiten.

In Kolokation können u.U. sogar mehrere Kunden Hardware im eigenen Rack installieren.

Dafür gibt's es dann spezielle Racks:



Die Racks benutzen aber auch reguläre Betreiber, die die Zugänge ihrer Mitarbeiter und Dienstleister gerne strenger regeln.

Dabei erhalten die MA dann nur genau die Schlüssel, die sie benötigen.

Das Ganze geht natürlich auch mit Fingerabdrücken oder Retinascannern.

Sollte der Mechanismus dann noch am Netzwerk hängern, kann man genau feststellen, wer was wann geöffnet hat.

Dieselbe Sensorik verwendet man natürlich auch für den Zutritt zum RZ selber.

Dabei werden oft auch noch Personenschleusen eingesetzt, um sicherzustellen dass sich auch wirklich jede Person authentifiziert.

LOGISCHE SICHERHEIT

Will sich jetzt ein Cloudkunde von den anderen Kunden abschotten (Mandantenfähigkeit, Noisy Neighbor), greift er in der Regel auf dedizierte Systeme zurück.

Das klappt auch ganz gut bei Servern. Entweder Host werden VMs auf vorbestimmter Hardware isoliert bzw. man kauft Root-Server.

Warum nicht bei Netzwerk und Storage?

Platt gesagt: die Hardware ist zu teuer.

Server gibt es für wenige Tausend Euro.

Soviel kostet auch ein Rack-Switch oder kleines DAS,
aber ohne Router und SAN macht Cloud nicht wirklich
Spaß.

Dank Firewall (VPC) und SAN-Zoning kann man aber zumindest Vertraulichkeit und Integrität gewährleisten.

Aber selbst Vorreiter AWS garantiert weder Latenz noch Durchsatz.

Spätestens wenn diese Metriken entscheidend werden, sollte man Colo in Betracht ziehen.

Dann muss man sich aber auch der Hardwareredundanz bzw. dem -support widmen.

Einerseits kann man versuchen Applikationen vorzugsweise über AZ hinweg zu clustern.

Oder man gönnt sich einen teuren Vertrag mit dem Hersteller, der dann innerhalb von x Stunden Ersatzteile liefern muss.

Im Bereich der Netzwerkredundanz / -kontrolle gibt es noch sehr speziellen Mechanismus bietet auf WAN-Seite noch das Internet.

Wenn man sich seinen eigenen IP-Bereich geleistet hat, kann man den zwischen Internetprovidern wechseln bzw. aufteilen (BGP).

Das erlaubt eingehenden Verkehr über die Provider zu verteilen. Ausgehende Verbindungen kann man ja sowieso routen, wie man will.

FRAGEN ?



NOW, ARE THERE
ANY QUESTIONS?



3. SICHERHEIT

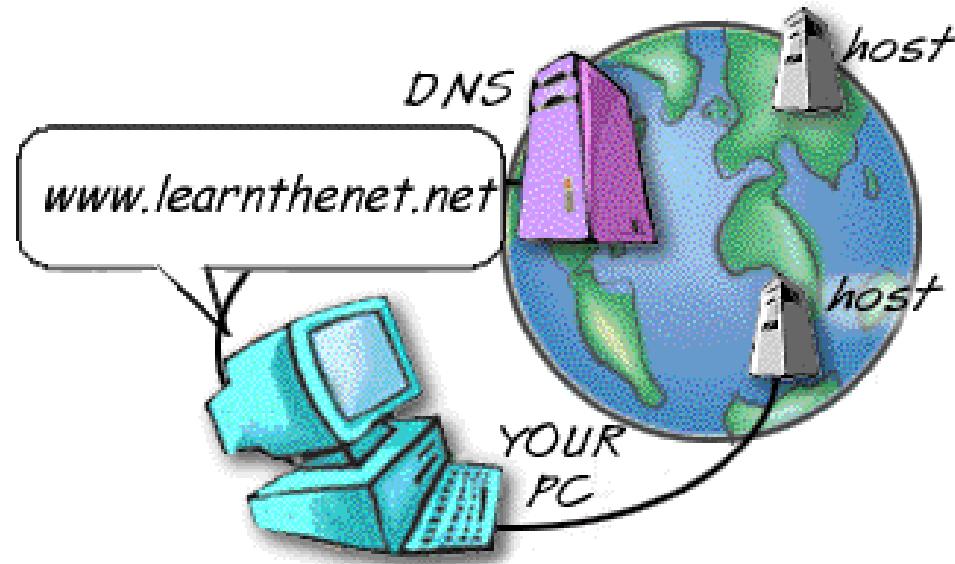
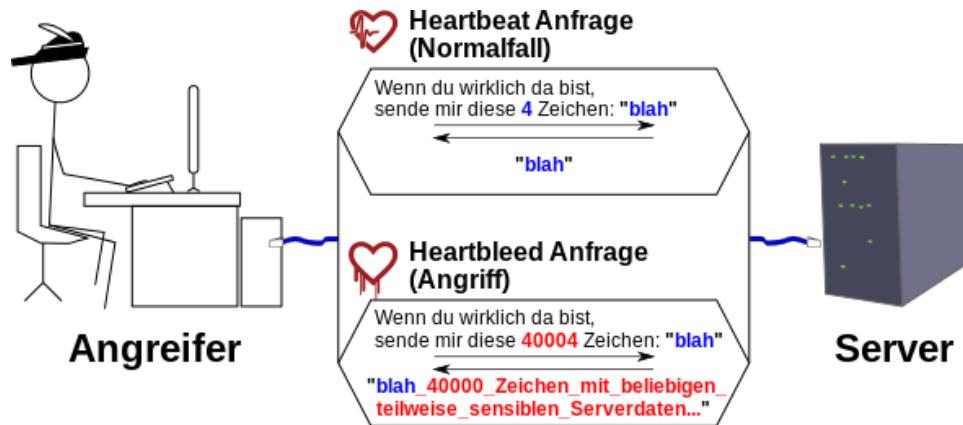
B. CLOUD SECURITY

CLOUD COMPUTING SICHERHEIT

- allgemeine Sicherheitsrisiken betreffen auch Cloud Services (Anwendungen)
- durch Verlagerung (Outsourcing) in die Cloud, gibt es mehr Sicherheitsrisiken zu beachten
- potentiell größere Angriffsfläche als im Intranet

ALLGEMEINE SICHERHEITSRISIKEN

- Netzwerk
 - (D)DoS
 - Man-in-the-Middle, Abhören
 - DNS Hijacking
- Software
 - Exploits (Exploitable Bugs)
 - SQL Injection, Buffer Overflows
 - XSS - Cross-site-scripting, Cross-Site-Token-Forgery
 - Sicherheitslücken in OS, Programmen, Runtime, Protokollen etc.



ALLGEMEINE SICHERHEITSRISEN

- User
 - Unachtsamkeit, unsichere Passwörter
 - Phishing, Spoofing
 - Social Engineering, Scams
- Physisch
 - Naturkatastrophen
 - Stromversorgung, Netzausfall
- Mitarbeiter
 - Spionage, Sabotage
 - Inside Jobs, Malicious Insider
 - Unterbeauftragung, Subunternehmer



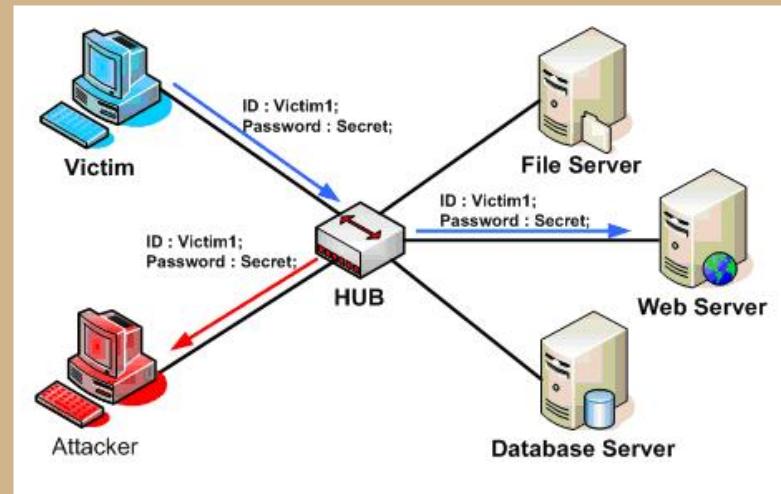
haveibeenpwnd

ABWEHRSTRATEGIEN & MASSNAHMEN

- Compliance
- Security Policies, Awareness
- Security Patches
- Data Encryption, End-to-End Encryption
- Audits, penetration tests

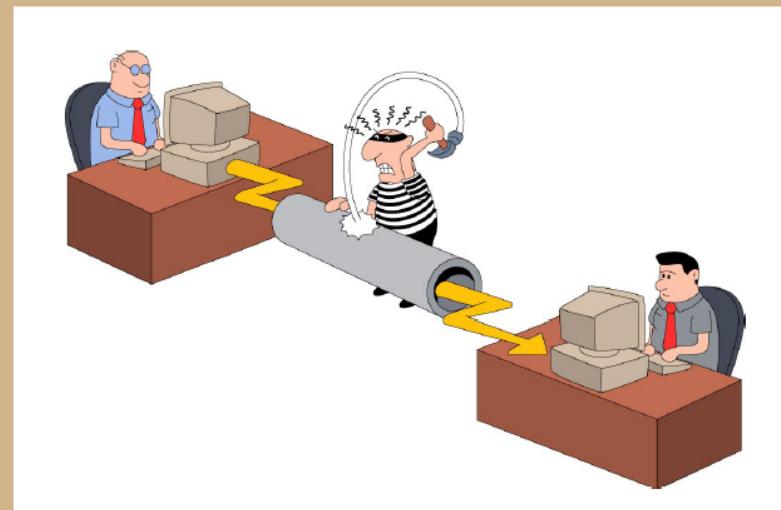
BEISPIEL: ABHÖREN ÜBER HTTP-KOMMUNIKATION

- unverschlüsselte Kommunikation (Daten werden im Klartext versendet)
- abhörbar, persönliche Daten, Passwörter können entwendet werden
- Angriffsvektor: z.B. Router-Hijacking



GEGENMASSNAHME: HTTPS-KOMMUNIKATION

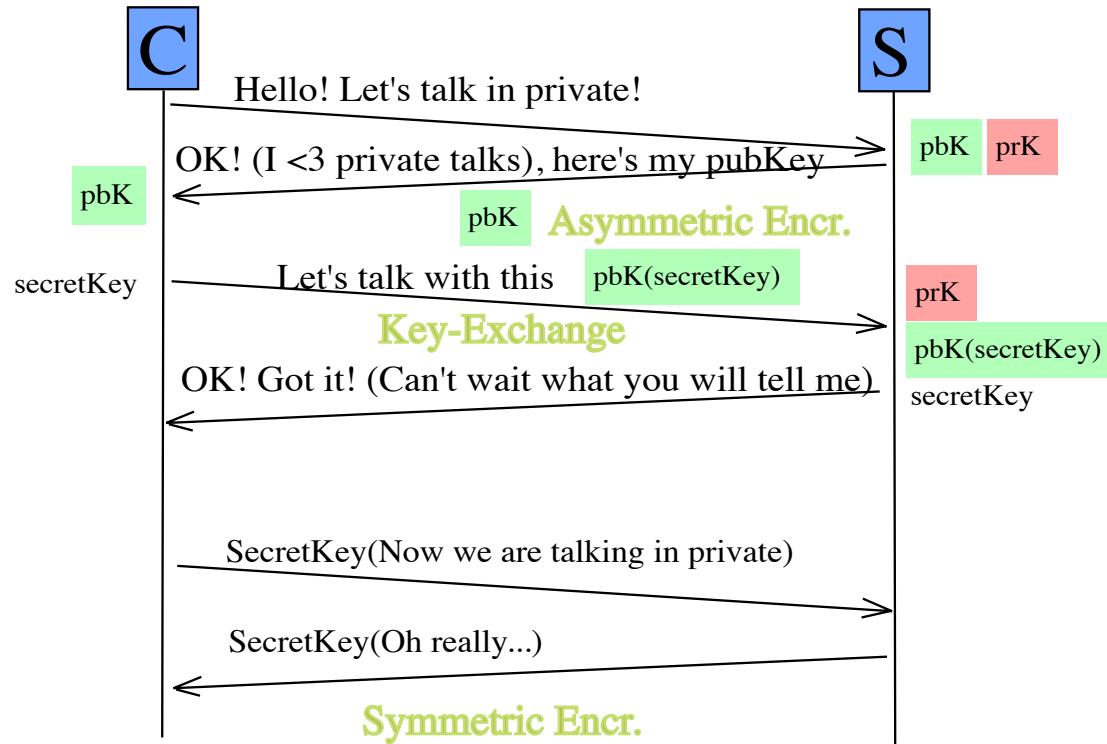
- Kommunikation über einen verschlüsselten Kanal
(Klartext wird zu '%\$nO3s;M2d%W')
- SSL/TLS Protokoll
- Basis: symmetrische + asymmetrische
Verschlüsselung



SSL/TLS PROTOKOLL (VEREINFACHT)

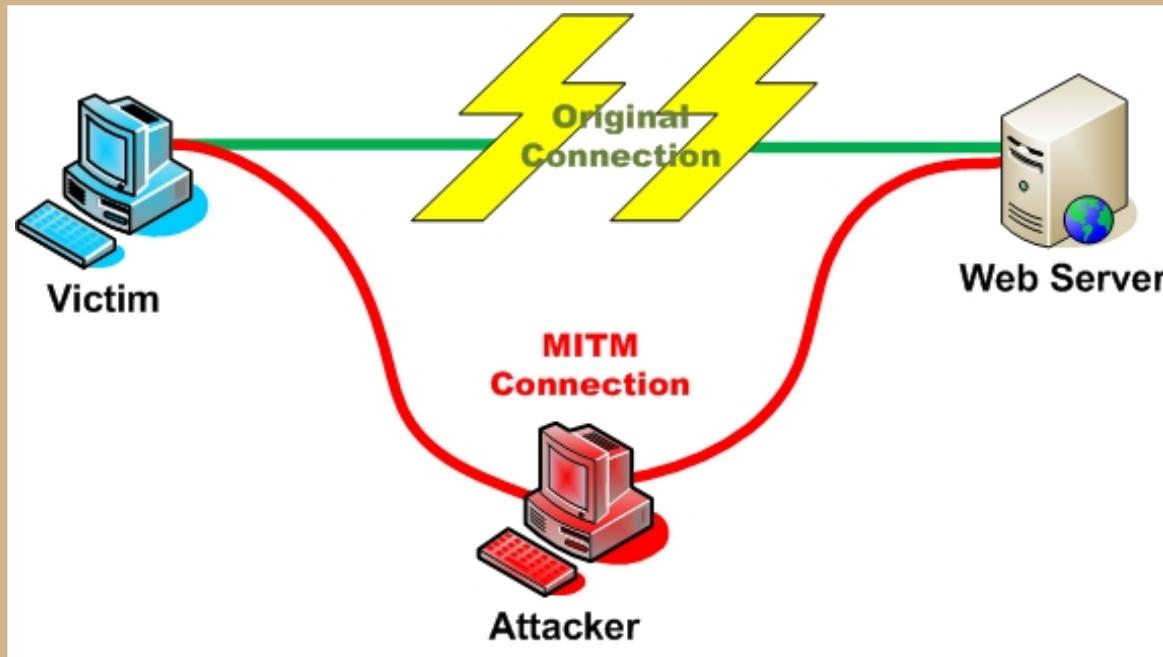
- 'Hello'
- Key-Exchange (über asymmetrische Verschlüsselung)
- Starte Verschlüsselungskanal (über symmetrische Verschlüsselung)

SSL/TLS PROTOKOLL (VEREINFACHT)



MIT WEM KOMMUNIZIERE ICH ?

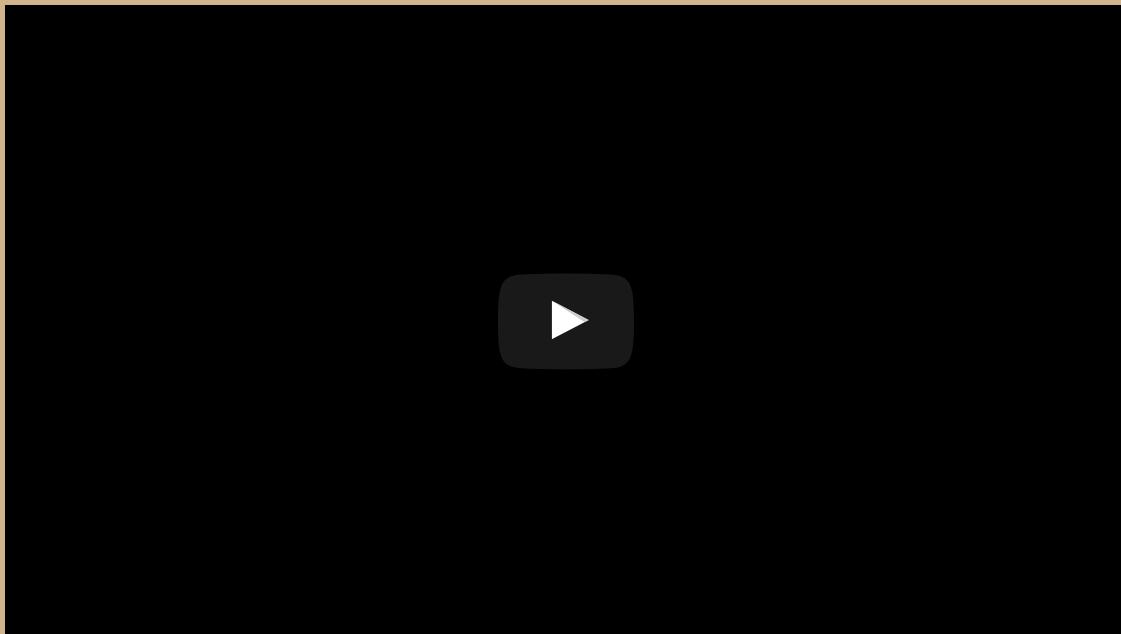
Problem: Man-in-the-Middle



AUTHENTIFIZIERUNG MIT ZERTIFIKATEN

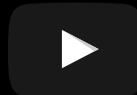
- Zertifikat enthält publick Key
- Certificate Authority (Ausstellungsinstanz) bestätigt Echtheit des Zertifikats und den Kommunikationspartner
- Key-Exchange kann anschließend durchgeführt werden

AUTHENTIFIZIERUNG MIT ZERTIFIKATEN

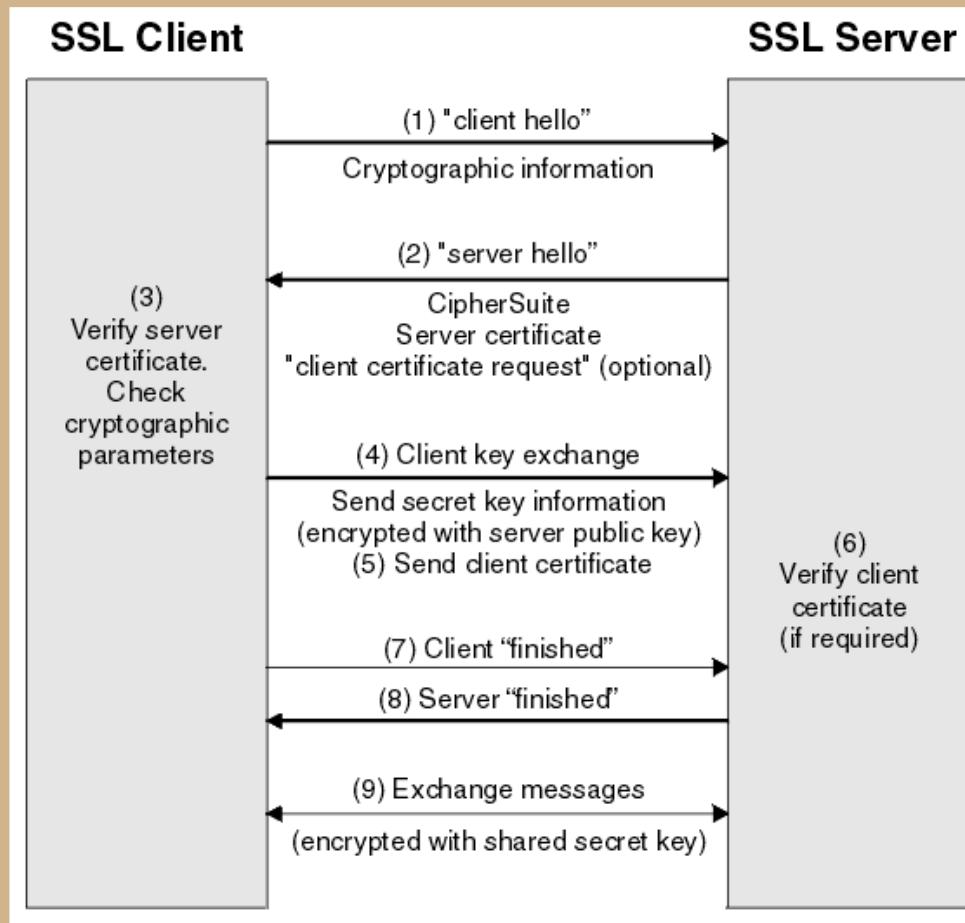


https://www.youtube.com/embed/i-rtxrEz_E8

weiterführende Erklärung: Chain of trust,
<https://youtu.be/heacxYUnFHA>



SSL/TLS PROTOKOLL



ORGANISATIONEN IM BEREICH INTERNET / CLOUD SECURITY

- Cloud Security Alliance
 - Top 12 Cloud Computing Security Threads
 - https://downloads.cloudsecurityalliance.org/assets/research/top-threats/Treacherous-12_Cloud-Computing_Top-Threats.pdf
- Open Web Application Security Project
 - OWASP Top 10
 - https://www.owasp.org/index.php/Top_10_2017-Top_10

TOP 12 CLOUD THREATS

1. Data Breach - Datenleck
2. Ungenügende Identity/Credential/Access Management
3. Unsichere Schnittstellen / APIs
4. Systemlücken, Exploits
5. Account Hijacking
6. Malicious Insider
7. Advanced Persistent Threats (APT)
8. Data loss - Datenverlust
9. Ungenügende Sorgfalt: Cloud-Strategie
10. Missbrauch von Cloud Services
11. Denial of Service (DoS)
12. Shared Technology Vulnerabilities

CLOUD SECURITY: VERANTWORTUNG

Wer ist verantwortlich für Sicherheit in der Cloud ?

Garantiert der Cloud Solution Provider Sicherheit ?

Nein, CSP und Cloud Kunde / Nutzer teilen sich die
Verantwortung

Es kommt auf den Cloud Services, Angriffspotentiale,
Sorgfaltspflicht und Wichtigkeit der Daten an

CSA - UNGENÜGENDER SCHUTZ FÜR CREDENTIALS

- Ursachen:
 - ungenügende Security Policy, schwache Passwörter
- Schaden:
 - Cloud Credentials hosted on Github
- Maßnahmen:
 - strengere Security Policy, Audits
 - Multifactor Authentication (MFA), Single-Sign-On (SSO)

CSA - SYSTEMLÜCKEN, EXPLOITS

- Beispiel:
 - Heartbleed, "WannaCry"-Ransomware
- Maßnahmen:
 - IaaS/CaaS: automatische Security Patches für OS-Kernel, OS-Libraries
 - PaaS: automatische Container Patches und Runtime-Patches
 - SaaS: Patching in der Verantwortung des Cloud Solution Providers

CSA - MALICIOUS INSIDER

- Ursachen:
 - Mitarbeiter (und MA von Subunternehmern) haben ungeschützten Zugriff auf vertrauliche Daten
 - ungenügendes Access Management, physikalische Absicherung, MA Monitoring
- Beispiel:
 - Wikileaks, NSA - Leaks

CSA - MALICIOUS INSIDER

- Maßnahmen:
 - Security Awareness, Access Management
 - MA Screening
 - In Rechnenzentren (Cloud Provider):
Sicherheitszonen, Personenschleusen,
Biometrische Scanner, verschließbare Racks
 - Datenverschlüsselung

CSA - DENIAL OF SERVICE

- Ursachen:
 - böswillige Angriffe durch Konkurrenten, Spione, Hacker
 - "Kundenansturm" (Wie kann man DoS von Überlast unterscheiden ?)
- Angriffsvektor:
 - Infrastruktur: Loadbalancer, Netzwerk
 - Applikation: Functionsüberlastung, DB-Überlastung

CSA - DENIAL OF SERVICE

- Maßnahmen:
 - Infrastruktur Absicherung durch Cloud Provider
 - IP/App-based Rate-Limits/Blacklisting durch Cloud Provider / Service Betreiber
 - Microservices (decoupling of applications)
 - Verringerung der Service Qualität
- mehr:
 - https://d0.awsstatic.com/whitepapers/Security/DDoS_White_Paper.pdf

AUDITING: CLOUD ZERTIFIZIERUNGEN

- Motivation:
 - Kontrolle über Einhaltung von Sicherheitsregeln beim Cloud Provider
 - Vertrauen
- Problem:
 - sehr schwierig da geograph.-verteilt
 - nicht für jeden Kunden umsetzbar

CLOUD ZERTIFIZIERUNGEN

- Auditing durch eine Zertifizierungsstelle (3rd Party)
- Einhaltung von Compliance Regeln, Sicherheitspolicies, Sicherheitsstandards
- Technologie-Einsatz, Datenschutz, Organisation, Prozesse
- derzeit keine staatliche Zertifizierungsstelle
- unterschiedliche Standards und Bewertungskriterien mit unterschiedlicher Güte
- Beispiele: ISO 27001, Certified Cloud Service TÜV Rheinland, EuroCloud SaaS Star Audit

mehr: <https://digitalize-your-business.de/zertifizierte-cloud-services-in-deutschland-und-europa-qualitaet-mit-brief-und-siegel/>

SEARCHABLE ENCRYPTION

- Motivation:
 - Verschlüsselung von Daten in der Cloud
 - Ausführung von Suchen auf verschlüsselten Daten
- Ansätze:
 - Deterministic Encryption
 - Symetric Searchable Encryption
 - Asymmetric Searchable Encryption
 - Oblivious RAM
- <http://outsourcedbits.org/categories/encrypted-search/>

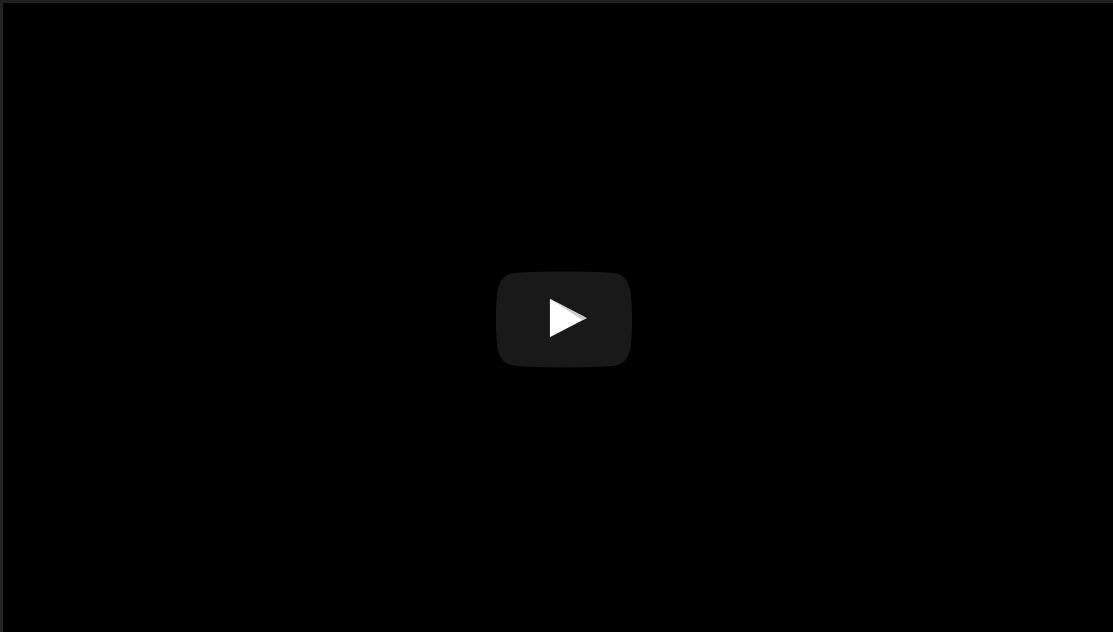
IDENTITY MANAGEMENT IN DER CLOUD

- Authentifizierung
 - Logins für verschiedene Personen Gruppen:
Anwender, Entwickler, Administratoren, Product Owner
- Autorisierung
 - Accessmanagement für SaaS-Applicationen, VMs
für Infrastruktur

BEISPIELE

- AWS IAM
 - Gruppen, User, support für Multi-Factor-Authentication
 - Access Management über Security Policies (JSON-Files)
 - Resourcen
 - ARN: Amazon Resource Name
 - Actions

AWS IAM USER MANAGEMENT



- https://www.youtube.com/embed/ySl1gdH_7bY

PROBLEME MIT CLOUD IDM

- Unternehmen haben meist schon ein zentrales IDM, Ersatz meist unerwünscht
- Yet-another-Username-Password (YAUP) für SaaS-Anwendungen (aus verschiedenen Clouds)
- kein Single-Sign-On
- Gefahr von Vendor Lock-in, wenn ausschließlich IDM des Cloud Providers genutzt wird
- Login Daten liegen in der Cloud

ON-PREMISE IDM-INTEGRATION

- Motivation:
 - IDM soll in der Enterprise IT bleiben
 - keine redundanten user-accounts
 - Kosten Einsparung
 - erhöhte Sicherheit: SSO, 1 Account pro MA, Daten bleiben on-premise

ENTERPRISE IDM: WINDOWS ACTIVE DIRECTORY

- Active Directory Protocol
- Identitäten und Rollen: Groups, Users
- Baumstruktur
- SSO im Intranet z.B. durch **Kerberos**, Session Cookies

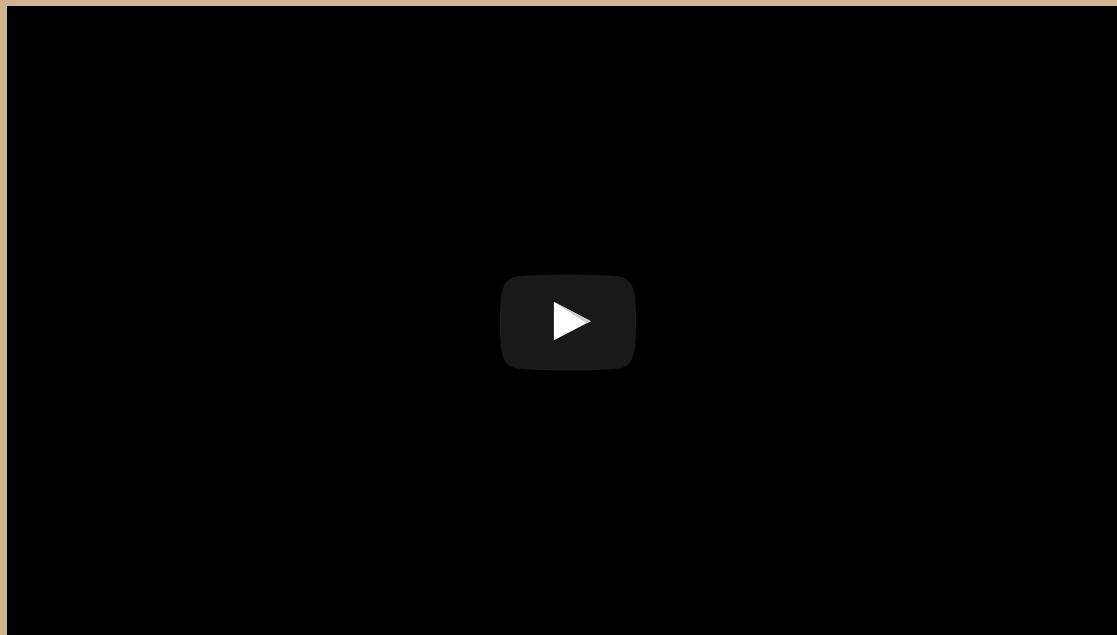
WIE KANN MAN SAAS-ANWENDUNGEN
BEIBRINGEN ENTERPRISE AD-USERN ZU
AUTHENTIFIZIEREN UND ZU
AUTORISIEREN ?

TRUST FEDERATION

- Idee:
 - zentraler Identity Provider (IP), authentifiziert User und erstellt ein Auth-Token
 - Services / Apps (Service Providers) sind so konfiguriert dass sie den Identity Provider vertrauen (Federated Trust)
 - Jeder unauthorisierter Zugriff auf einen Service wird an den IP weitergeleitet
 - IP leitet Auth-Token an den Service Provider
- Beispiele: SAML, OpenId

PROTOKOLL SAML

- Security Assertion Markup Language (SAML)
- Single-Sign-On für die Cloud Integration



- <https://www.youtube.com/embed/i8wFExDSZv0>

IDENTITY FEDERATION

- Idee:
 - die Rollen und Zugriffsberechtigungen sind im Netzwerk / Services verteilt
 - jeder Service verwaltet nur die Berechtigungen die es braucht
 - Authentifizierung geschieht per Trust Federation über den Identity Provider
 - Mapping der Identität des Users auf seine Berechtigungen erfolgt im Service

MS AD FEDERATION SERVICE

- MS Service für Identity Federation
- kann als Identity Provider für eine Cloud-Integration dienen
- ADFS authentifiziert User gegen On-Premise Enterprise AD
- ADFS generiert SAML Tokens für konfigurierte Trusts (Cloud Services)

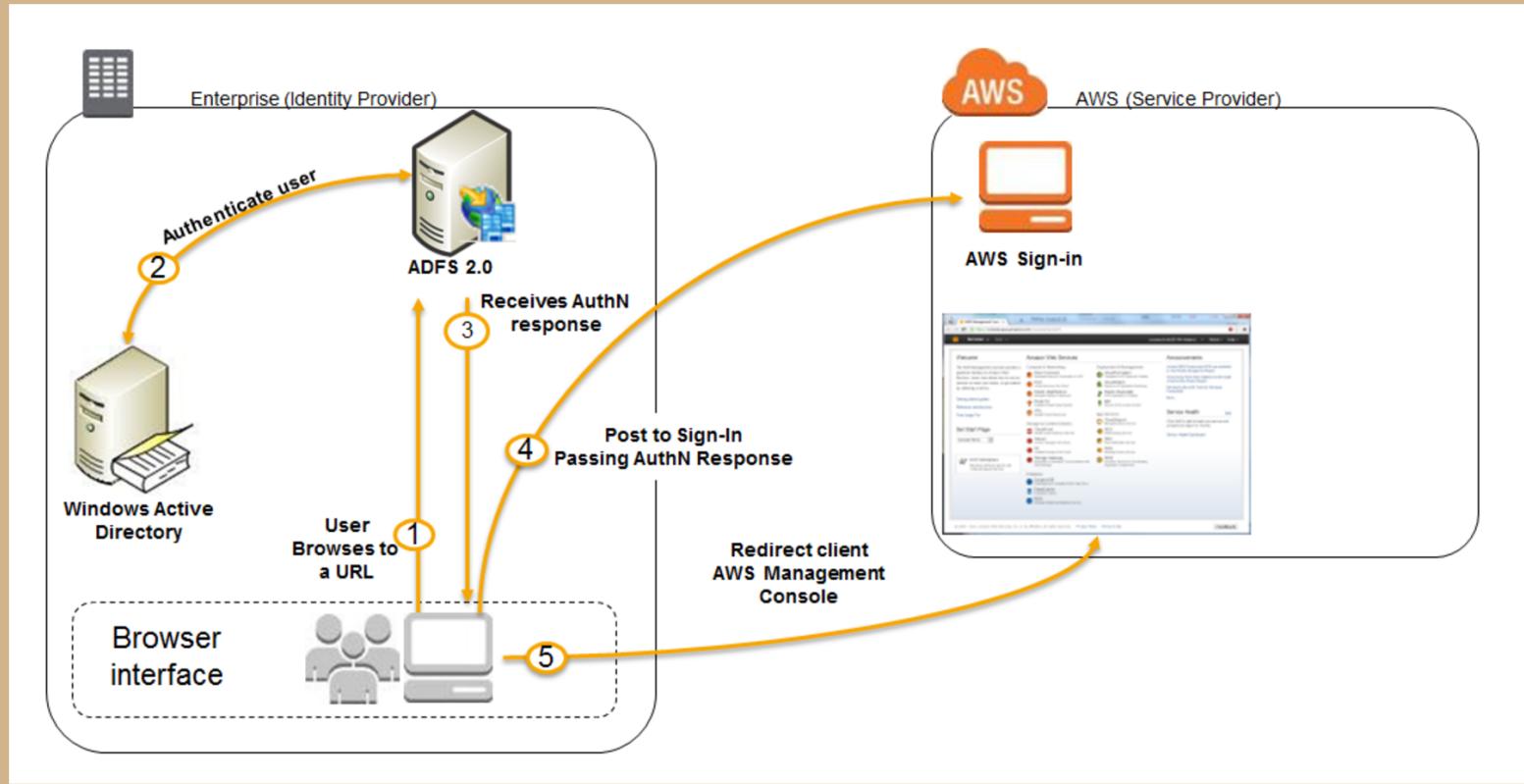


- <https://www.youtube.com/embed/8xNuPhDVbHU>

INTEGRATION MIT MS ADFS + AWS IAM

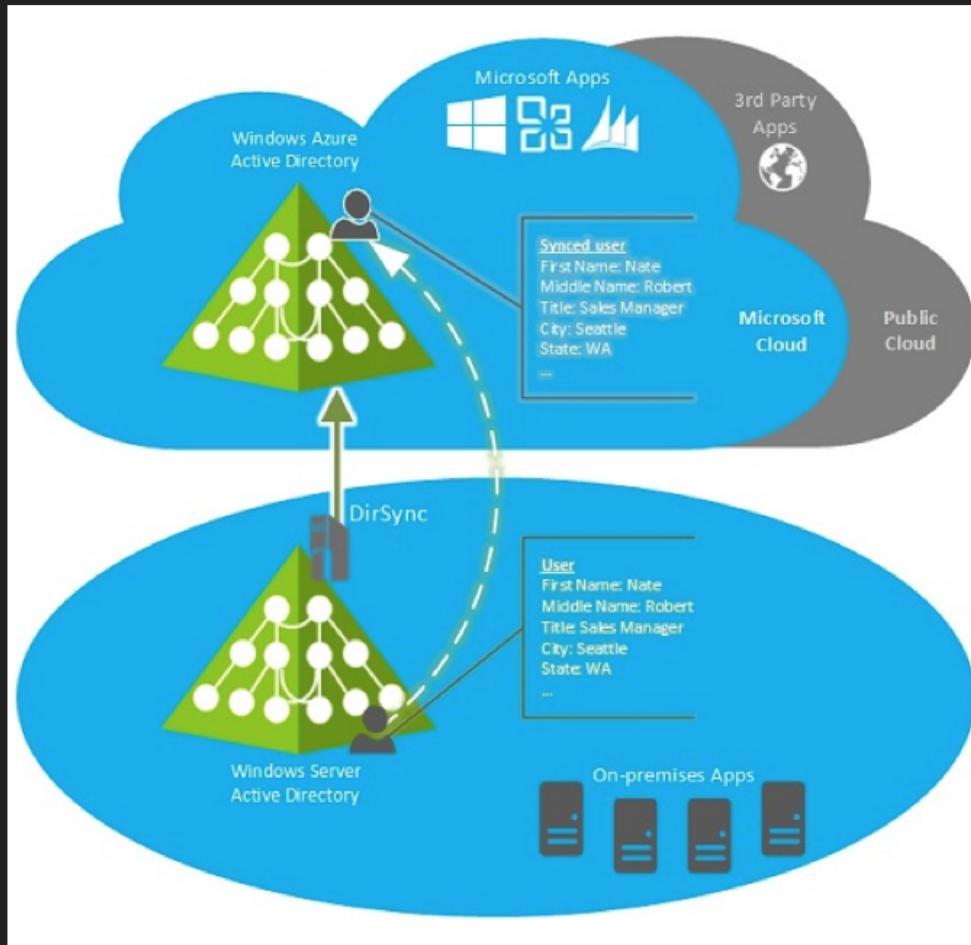
- Setup: two-way federated trust zwischen ADFS und AWS IAM
- ADFS authentifiziert und erstellt ein authentication ticket in Form eines signiertes SAML-Tokens
- ADFS Rules: überträgt AD Gruppen zu IAM Rollen und speichert diese im SAML Token
- AWS IAM empfängt signiertes SAML-Token und autorisiert Zugriff

INTEGRATION MIT MS ADFS + AWS IAM



INTEGRATION MIT MS ADFS + AZURE AD

- Lösungen:
 - Azure AD ist selber ein Identity Provider für Azure mit Unterstützung für Web-IDM Protokolle e.g. SAML, OpenId
 - Azure SaaS Apps können Azure AD als Identity Provider nutzen
 - SSO für Azure SaaS-Apps (auch externe SaaS-Apps: Salesforce)
 - ADFS + AD Connect (ehem. "DirSync") synchronisiert Ids mit Azure AD
 - Azure AD + ADFS authorisieren User





- <https://youtu.be/lcSATObaQZE?t=6m6s>

IDENTITY-AS-A-SERVICE (IDAAS)

- Identity Provider für die Cloud
- keine On-Premise Lösung mehr nötig
- Ersatz für Enterprise AD
- SSO für Cloud

FRAGEN ?

