

CC: CLOUD COMPUTING IM BETRIEB

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

WS 2018



AGENDA

3. SCALING, SECURITY

- a. Auto-Scaling
- b. Sicherheit bei Cloud Computing
- c. User Management

The background of the image is a dramatic, sunlit sky. Large, billowing white clouds are scattered across the frame, with bright sunlight streaming through them from behind. The overall atmosphere is one of vastness and power.

3. CLOUD COMPUTING FEATURE

A. AUTO-SCALING

AUTO-SCALING

- Essentieller Mechanismus im Cloud Computing um auf den Bedarf von Ressourcen zu reagieren
- dynamische Bereitstellung von VMs, Container, Speicher, Storage
- bidirektional: Scale-Up, Scale-Down
- Nutzen:
 - Elastizität: bessere Auslastung, Kostenoptimierung (Kosteneinsparung)
 - Verfügbarkeit und Zuverlässigkeit: durch Sicherstellung von min. Instanzen

AUTOSCALING STRATEGIEN

- Reaktiv: Cloud Umgebung beobachtet Kernmetriken (CPU, Memory, Traffic) und reagiert auf Last
- Proaktiv:
 - Scheduling (scheduled scaling): Zeitlich geplante Skalierung auf Basis von Erfahrungswerten
 - Prädiktiv (predictiv scaling): durch Vorhersage auf Basis von prädiktive Analyse

BEISPIEL: AUTO-SCALING BEI AWS (IAAS)

- CPU, Speicherauslastung, Netzwerk Traffic wird durch AWS EC2 überwacht
- alle Logs/Stdout werden an AWS Cloudwatch übermittelt (Logging/Monitoring-Service)

<http://docs.aws.amazon.com/autoscaling/latest/userguide/WhatIsAutoScaling.html>

- AMIs/VMs können zu Auto-Scaling Groups hinzugefügt werden, Konfiguration von Scaling-Plans:
 - Scaling Policies: reaktiv (standard), scheduled-scaling, dynamisch (auf Basis von Metriken aus Amazon SQS, Cloudwatch alarms)
 - min./max. und gewünschte Anzahl an Instanzen

<https://docs.aws.amazon.com/autoscaling/latest/userguide/as-using-sqs-queue.html>

BEISPIEL: AUTO-SCALING BEI AWS (IAAS)

- Ausführung: auf Basis von Scaling Plans werden AMI Instanzen hinzugefügt / terminiert
- hinzufügen von Instanzen (auf Basis von Launch-Configuration):
 - Instanziierung aus AMI
 - boot-up Phase, Initialisierung, Konfigurierung per Skript (siehe AMI Design Strategien)
 - Anbindung an Cloud-Storage
 - Registrierung ins Virtual Private Cloud (Netzwerk)
 - Registrierung beim Elastic Load-Balancer

BEISPIEL: AUTO-SCALING BEI AWS (IAAS)

- Status Überwachung: Health-Checking
 - über HTTP-Endpunkt: z.B. /heathcheck
 - healthy flag

BEISPIEL: AUTO-SCALING BEI CLOUD-FOUNDRY (PAAS)

- Monitoring / Überwachung von Basis-Metriken:
analog zu AWS EC2
- Skalierung auf Container / App-Ebene
- Skalierung über Einbinden eines "Auto-Scaler"-
Services an einer App
- Definition von Basis-Metriken:
 - min./max. Instanzen
 - CPU-, Traffic-, Speicher-Grenzen
- nur reaktiv

BEISPIEL: AUTO-SCALING BEI CLOUD-FOUNDRY (PAAS)

- Ausführung: auf Basis der Auto-Scaler Konfiguration werden Container-Intanzen hinzugefügt / terminiert
- hinzufügen von Instanzen:
 - Container Instanz wird aus dem gebautem Image instanziert
 - Einbinden der Container Instanz ins private virtual network
 - Container Prozess wird gestartet (run-Befehl)
 - Registrierung beim Load-Balancer

BEISPIEL: AUTO-SCALING BEI CLOUD-FOUNDRY (PAAS)

- Status Überwachung: Health-Checking
 - über HTTP-Endpunkt: z.B. /heathcheck, (http-response-Code: 200 bedeutet "OK", ansonsten "NOK")
 - Überwachung des Container Prozesses: terminiert der Container Prozess, stoppt der Container und crasht, es wird ein neuer Container gestartet

BEISPIEL: AUTO-SCALING BEI KUBERNETES (CAAS)

- Monitoring / Überwachung von Basis-Metriken: analog zu Cloud Foundry
- Skalierung auf Pod-Ebene (Kubernetes Konzept: Zusammenfassung von Containern)
- Skalierung über die Definition einer Auto-Scaling Konfiguration
- Konfiguration wird über Selektoren auf Kubernetes Bausteine (Pod, ReplicaSets, Deployments) angewendet
- Auto-Scaling ist reaktiv und basiert nur auf CPU-Last-Grenzen

BEISPIEL: AUTO-SCALING BEI KUBERNETES (CAAS)

- Ausführung: auf Basis der Auto-Scaler Konfiguration werden Container-Instanzen hinzugefügt / terminiert
- hinzufügen von Instanzen:
 - Pod Instanz wird erstellt, alle Container Definitionen werden aus dem konfiguriertem Image instanziert
 - Einbinden der Pod/Container Instanz ins private virtual network
 - Container Prozess wird gestartet (run-Befehl)
 - Registrierung beim Service und Load-Balancer

BEISPIEL: AUTO-SCALING BEI KUBERNETES (CAAS)

- Status Überwachung: Health-Checking
 - über HTTP-Endpunkt: z.B. /heathcheck, (http-response-Code: 200 bedeutet "OK", ansonsten "NOK")
 - Überwachung der Pod/Container Prozesse: terminiert der Pod/Container Prozess, stoppt der Pod/Container, es wird ein neuer Pod/Container gestartet



3. SECURITY

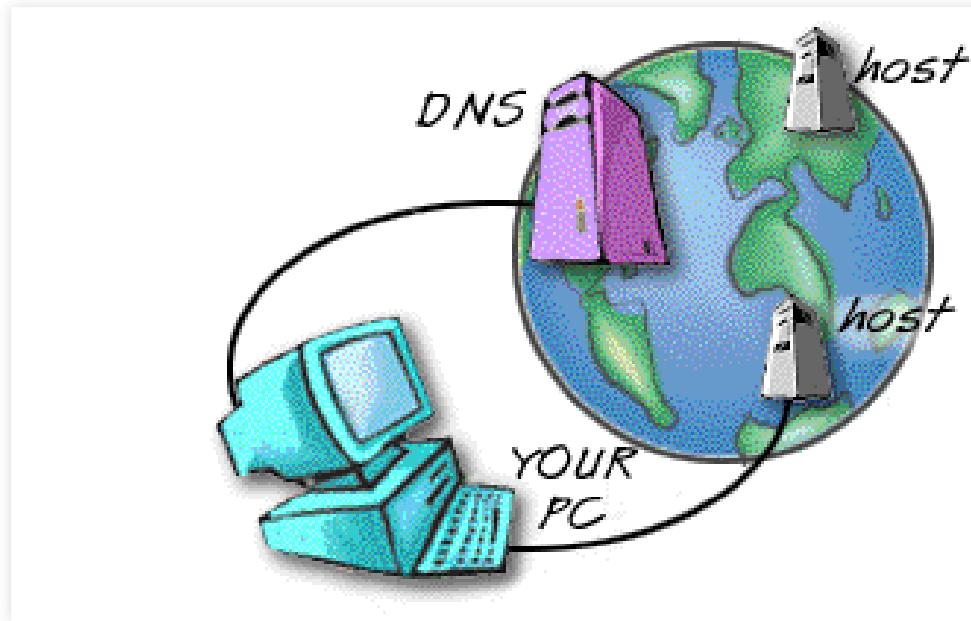
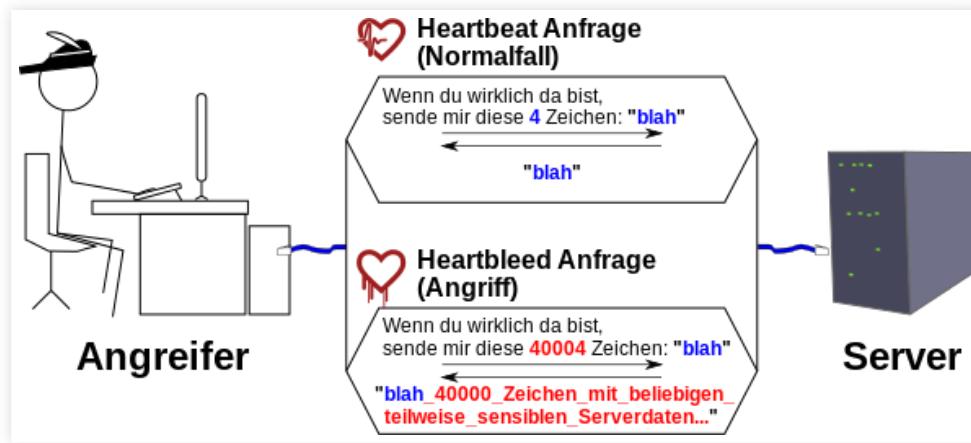
B. SECURITY BEI CLOUD COMPUTING

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 SICHERHEITSRISEN

- 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 SICHERHEITSRISIKEN

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



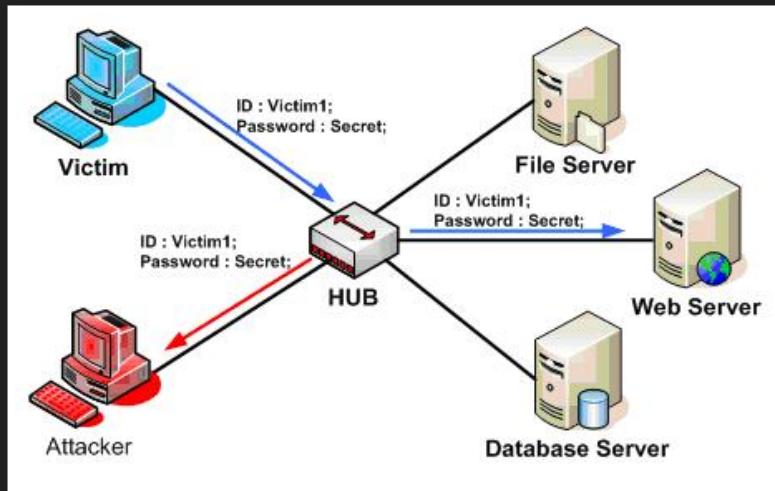
haveibeenpwnd

ABWEHRSTRATEGIEN & MASSNAHMEN

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

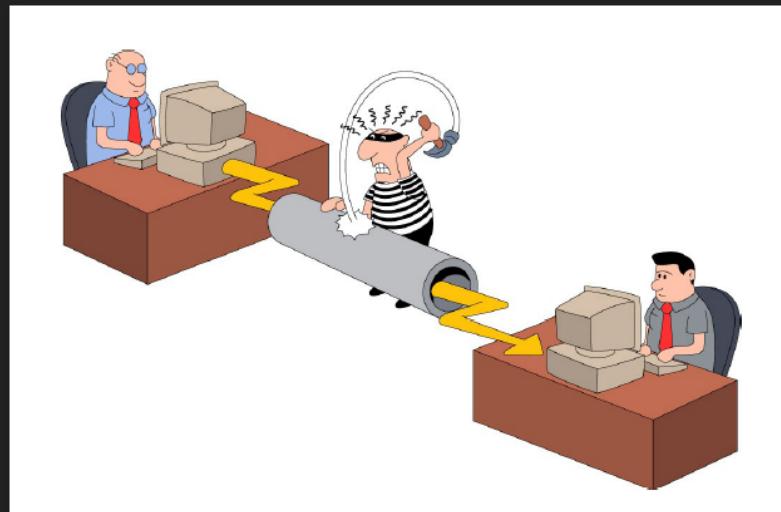
BEISPIEL: ABHÖREN ÜBER HTTP-KOMMUNIKATION

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



GEGENMASSNAHME: HTTPS-KOMMUNIKATION

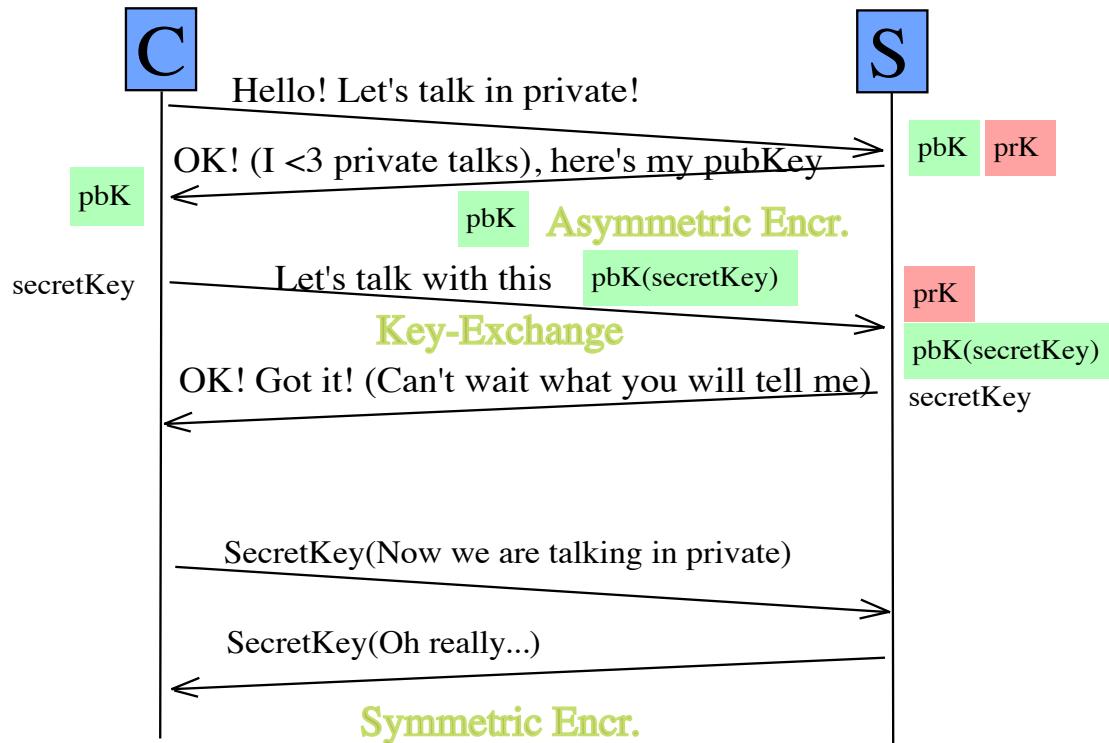
- Kommunikation über einen verschlüsselten Kanal
(Klartext wird zu '%\$nO3s;M2d%W')
- SSL/TLS Protokoll
- Basis: symmetrische + asymmetrische
Verschlüsselung



SSL/TLS PROTOKOLL (VEREINFACHT)

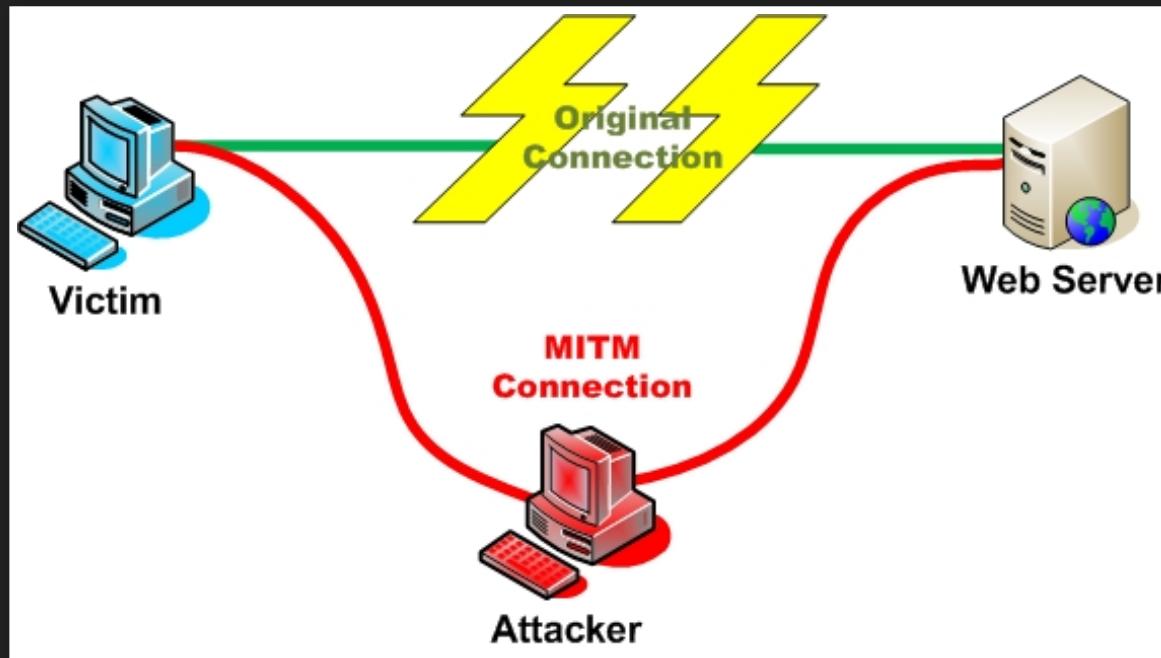
- 'Hello'
- Key-Exchange (über asymmetrische Verschlüsselung)
- Starte Verschlüsselungskanal (über symmetrische Verschlüsselung)

SSL/TLS PROTOKOLL (VEREINFACHT)



MIT WEM KOMMUNIZIERE ICH ?

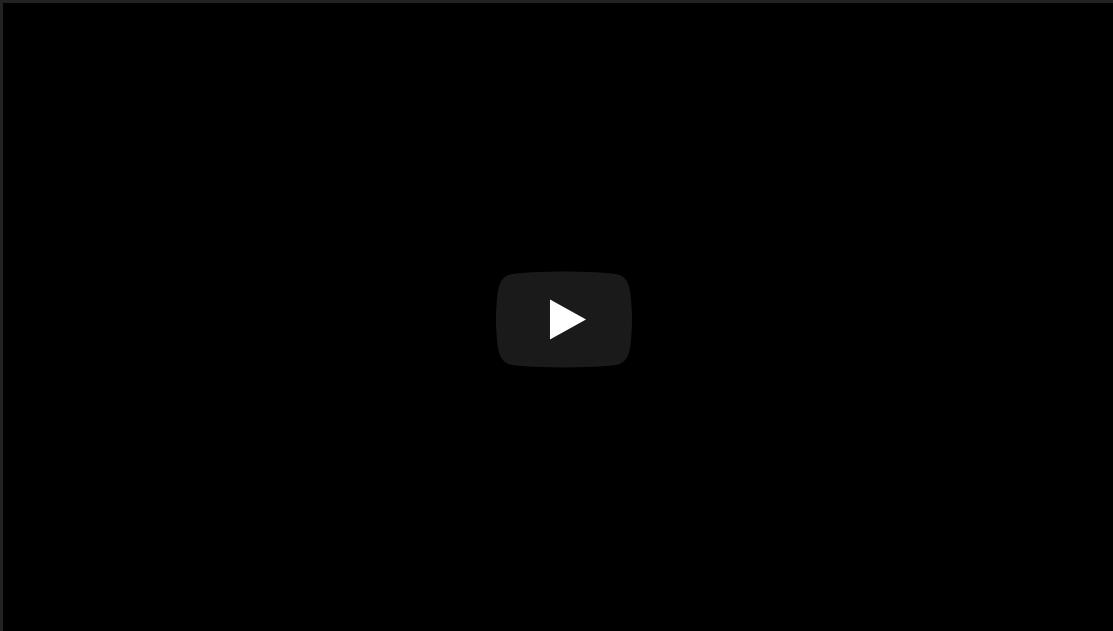
Problem: Man-in-the-Middle



AUTHENTIFIZIERUNG MIT ZERTIFIKATEN

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

AUTHENTIFIZIERUNG MIT ZERTIFIKATEN

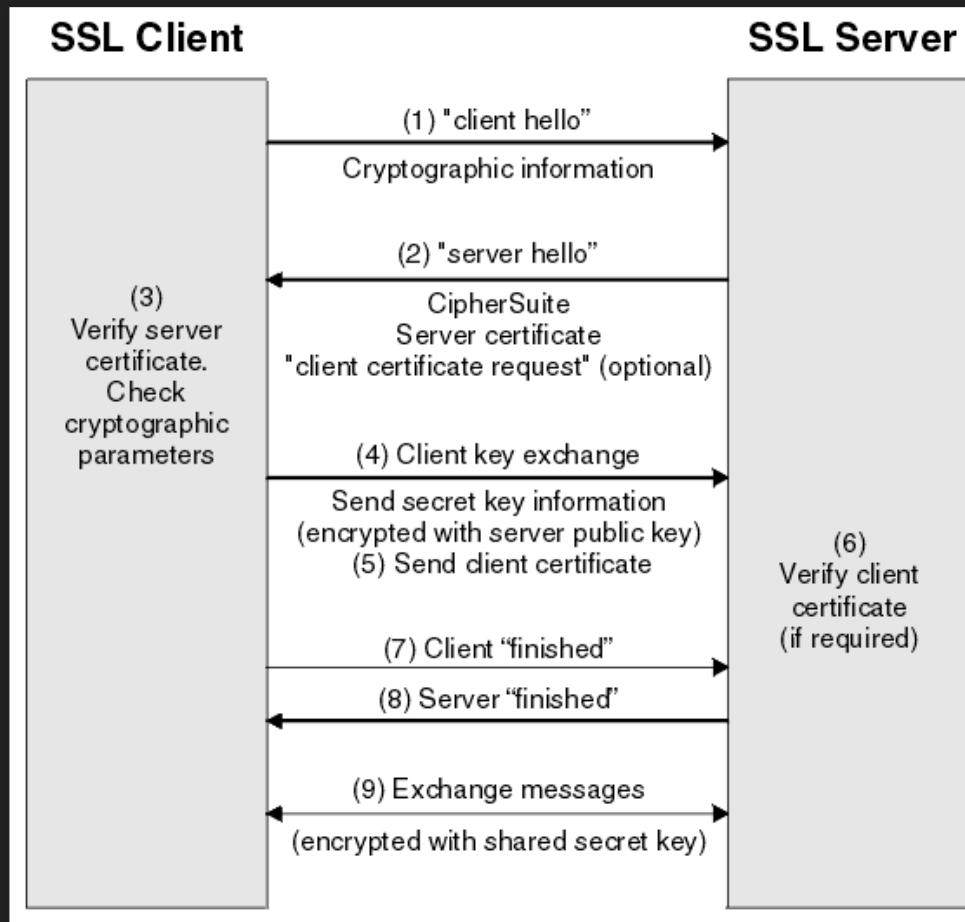


https://www.youtube.com/embed/i-rtxrEz_E8

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

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/>

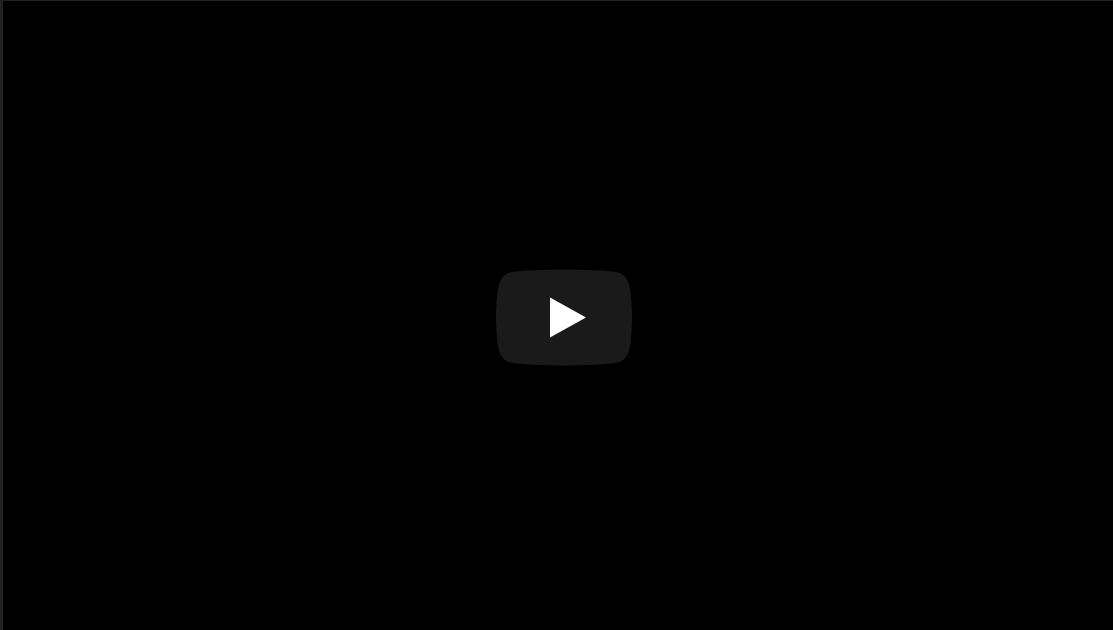
IDENTITY MANAGEMENT IN DER CLOUD

- 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

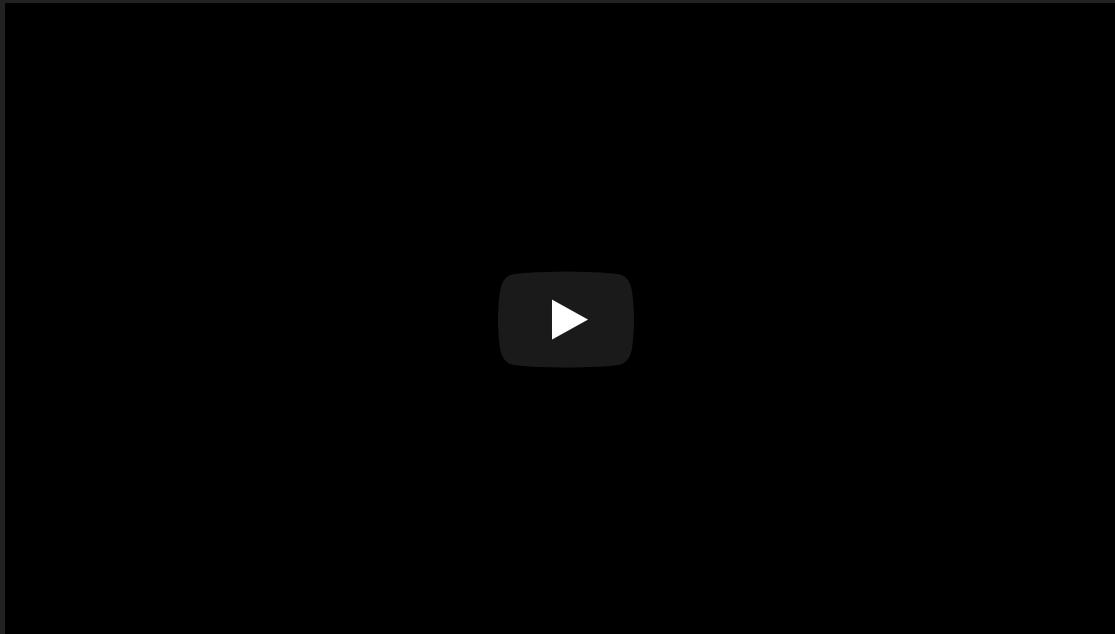
WIE KANN MAN SAAS-ANWENDUNGEN
BEIBRINGEN ENTERPRISE AD-USERN ZU
AUTHENTIFIZIEREN UND ZU
AUTORISIEREN ?

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



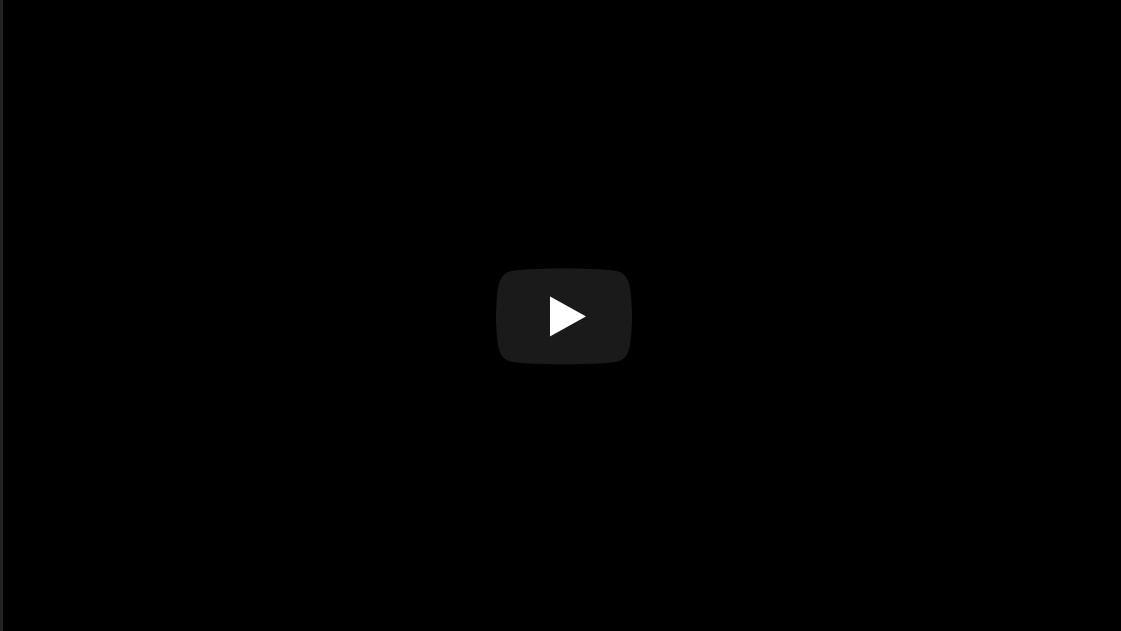
- <https://www.youtube.com/embed/i8wFExDSZv0>

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)

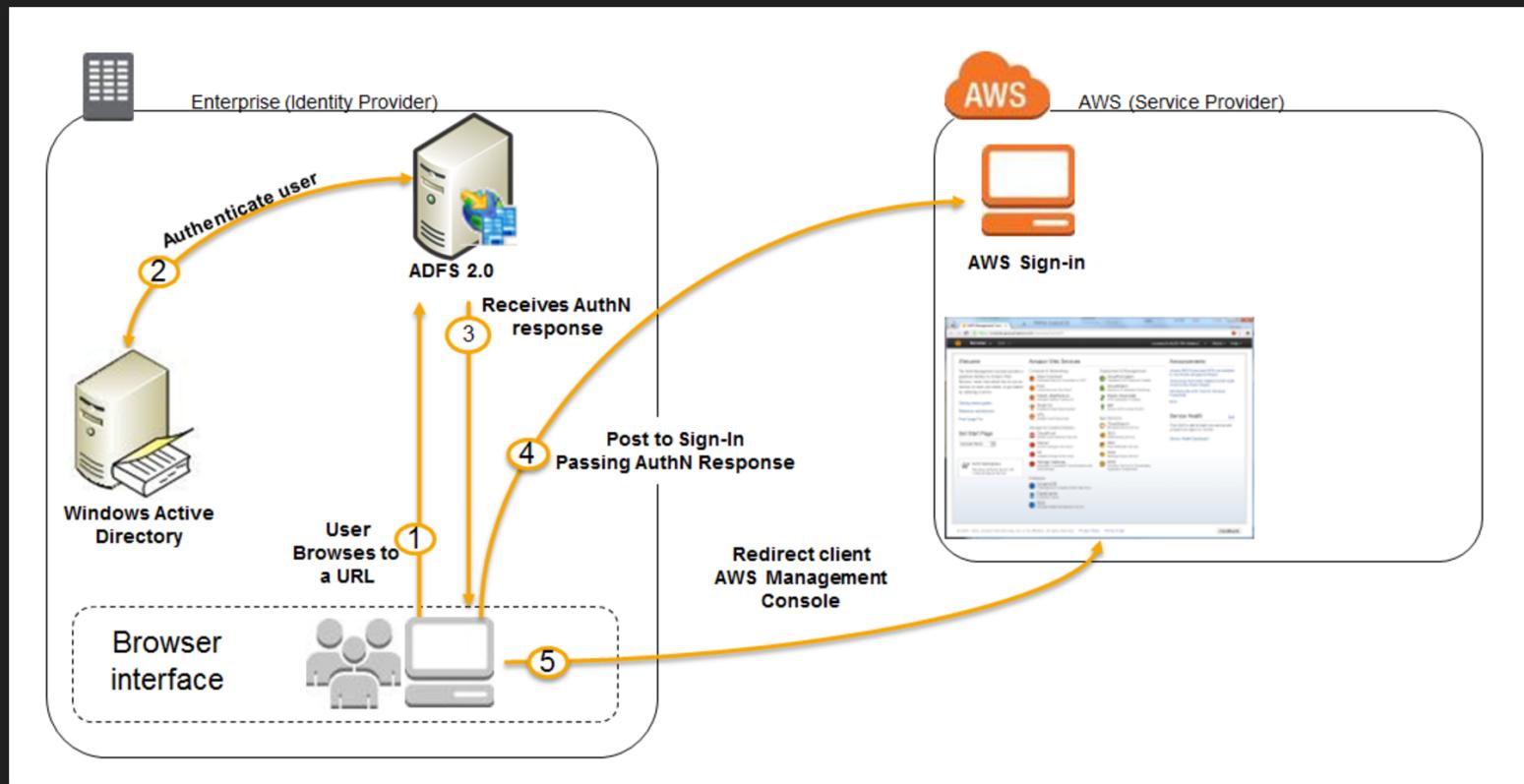


- <https://www.youtube.com/embed/8xNuPhDVbHU>

INTEGRATION MIT MS ADFS + AWS IAM

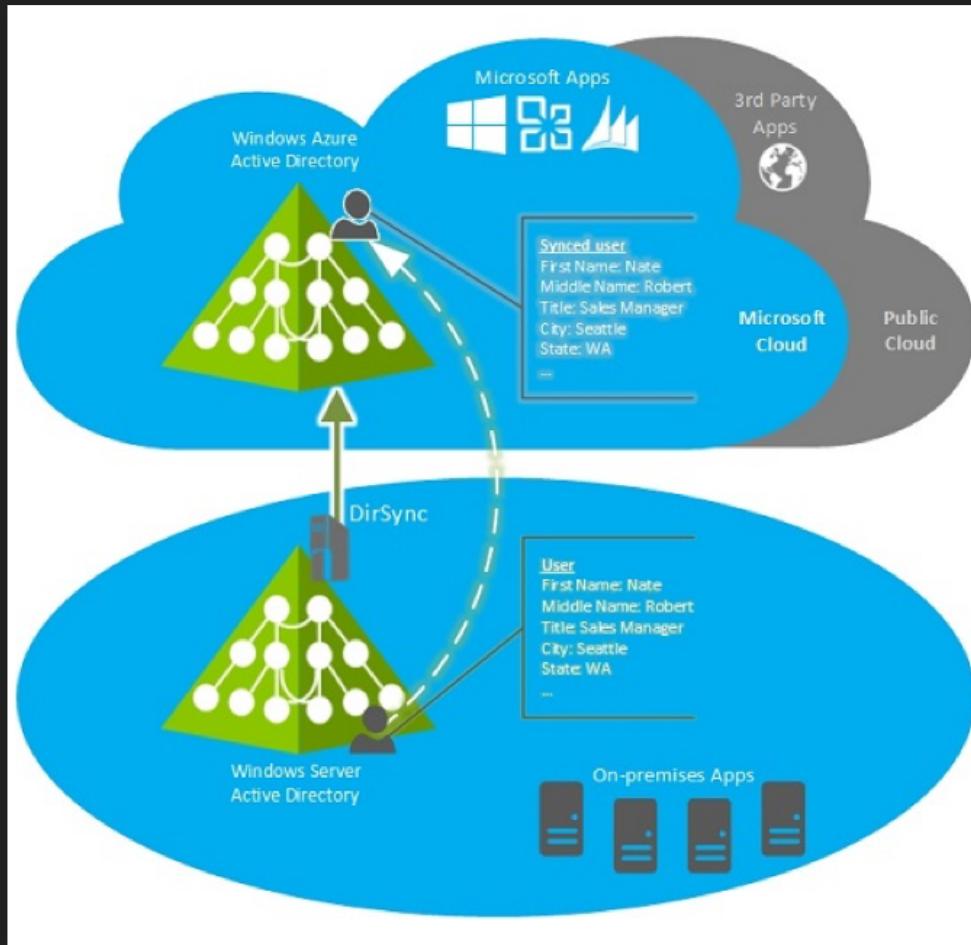
- Setup: two-way federated trust zwischen ADFS und AWS IAM
- ADFS authentifiziert und erstellt ein authentication ticket in Form eines signiertes SAML-Tokens
- ADFS Rules: überträgt AD Gruppen zu IAM Rollen und speichert diese im SAML Token
- AWS IAM empfängt signiertes SAML-Token und autorisiert Zugriff

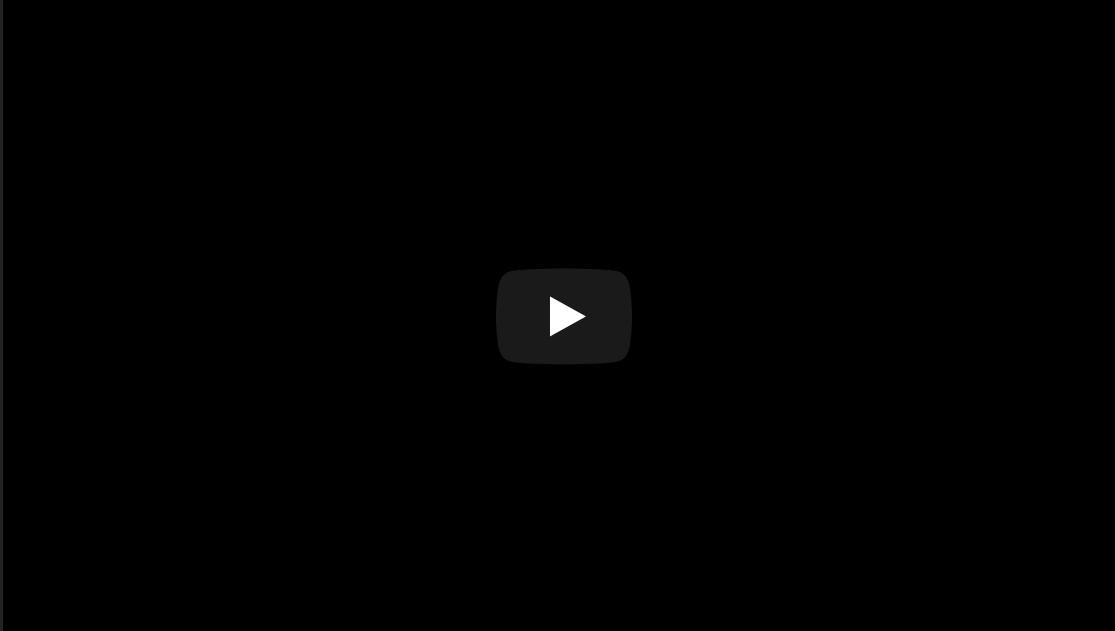
INTEGRATION MIT MS ADFS + AWS IAM



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 ?

