

# CC: CLOUD COMPUTING IM BETRIEB

Dipl.-Medieninf. Hai Dang Le  
Software Engineer  
[hdang.88@gmail.com](mailto:hdang.88@gmail.com)

2018











# BE SP EL: AUTO SCAL NG BE AWS ( AAS)

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

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

BE SP EL: AUTO SCAL NG BE AWS ( AAS)







# BE SP EL: AUTO SCAL NG BE 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

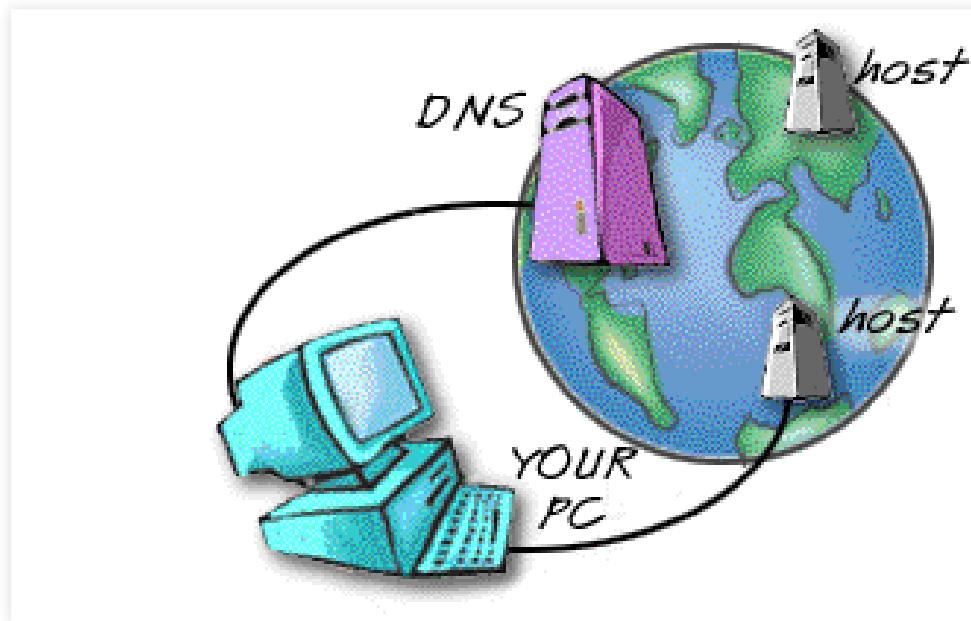
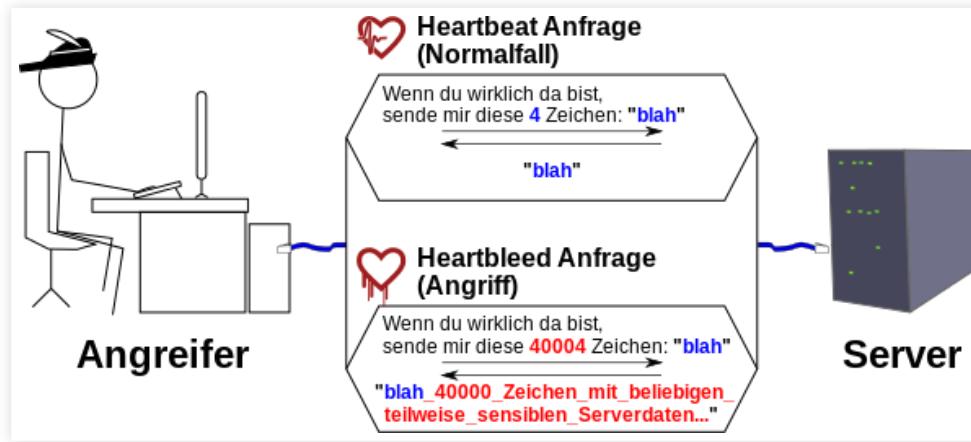
# **3. SECURITY**

## **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 SICHERHEITSRISIKEN



# ALLGEMEINE SICHERHEITSRISIKEN

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



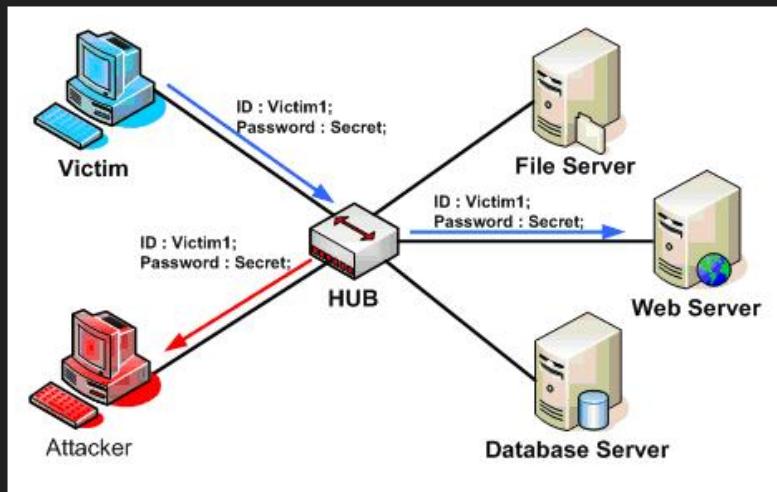
haveibeenpwnd

# ABWEHRSTRATEGIEN & MASSNAHMEN

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

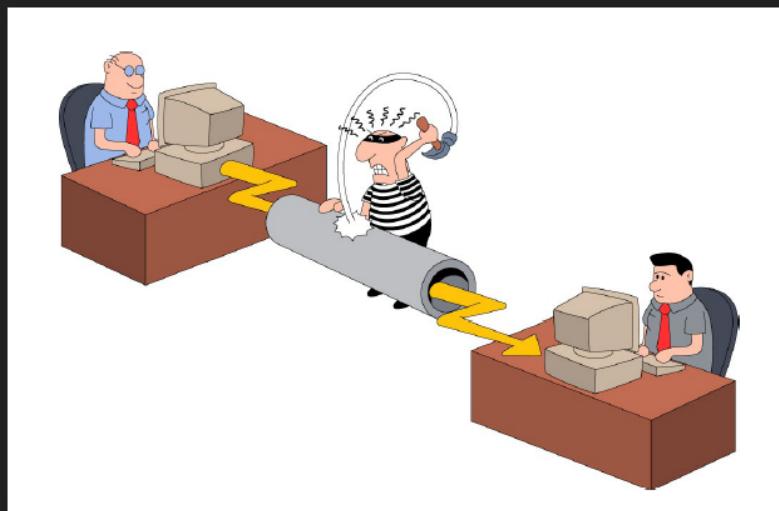
# BEISPIEL: ABHÖREN ÜBER HTTP-KOMMUNIKATION

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



# GEGENMASSNAHME: HTTPS-KOMMUNIKATION

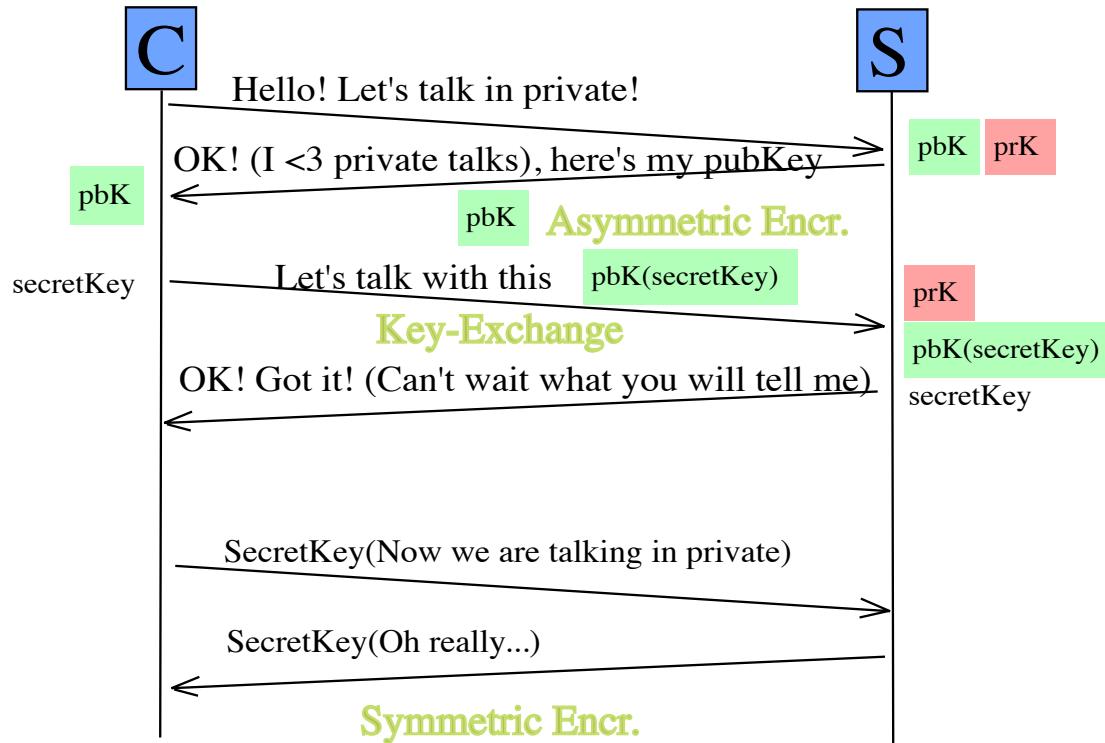
- Kommunikation über einen verschlüsselten Kanal  
(Klartext wird zu '%\$nO3s;M2d%W')
- SSL/TLS Protokoll
- Basis: symmetrische + asymmetrische  
Verschlüsselung



# SSL/TLS PROTOKOLL (VEREINFACHT)

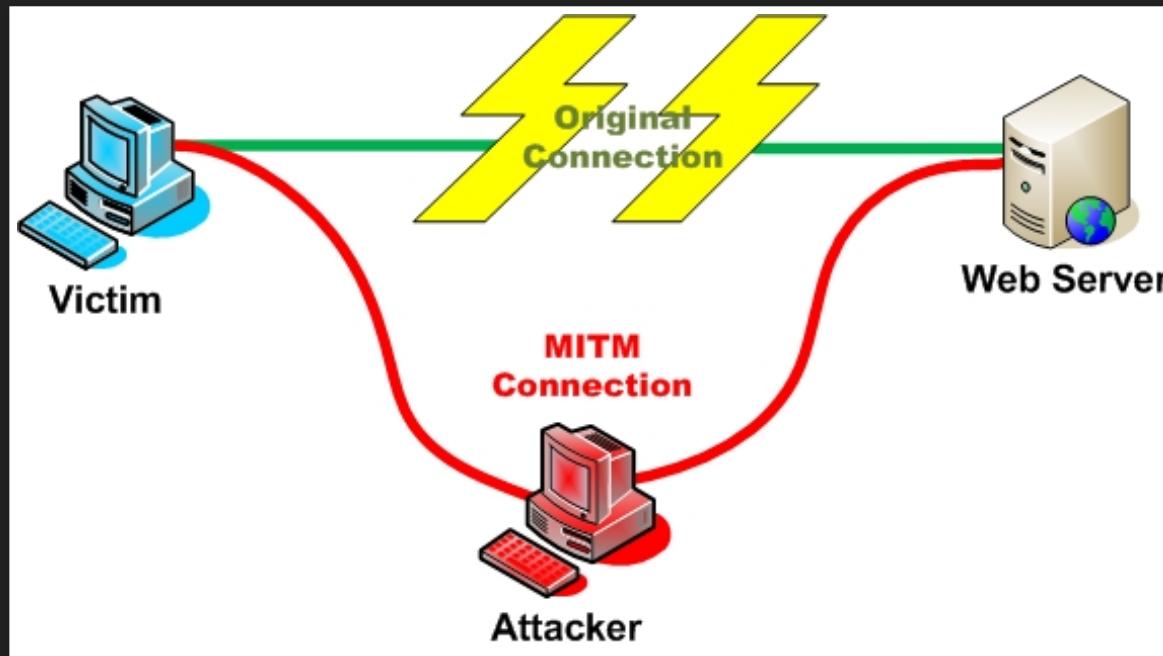
- 'Hello'
- Key-Exchange (über asymmetrische Verschlüsselung)
- Starte Verschlüsselungskanal (über symmetrische Verschlüsselung)

# SSL/TLS PROTOKOLL (VEREINFACHT)



# MIT WEM KOMMUNIZIERE ICH ?

Problem: Man-in-the-Middle



## AUTHENTIFIZIERUNG MIT ZERTIFIKATEN

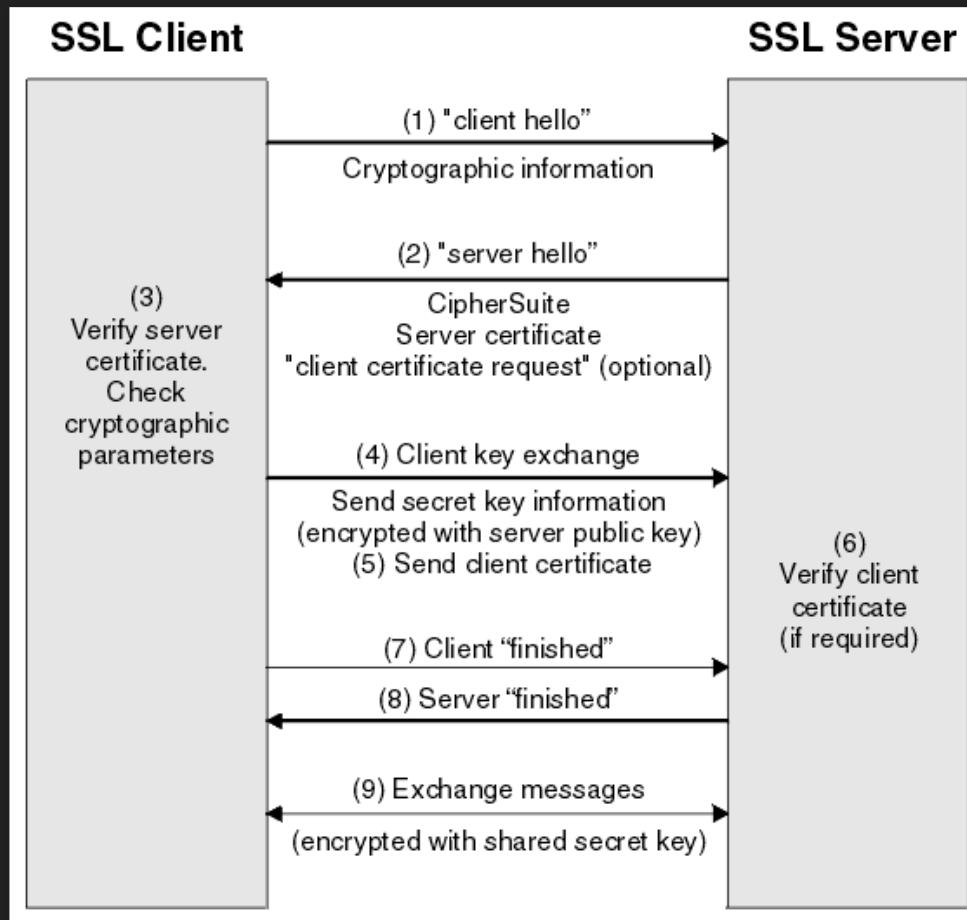
- Zertifikat enthält public Key
- Certificate Authority (Ausstellungsinstanz) bestätigt Echtheit des Zertifikats und den Kommunikationspartner
- Key-Exchange kann anschließend durchgeführt werden

# AUTHENTIFIZIERUNG MIT ZERTIFIKATEN

[https://www.youtube.com/embed/i-rtxrEz\\_E8](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](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](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

# 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](https://d0.awsstatic.com/whitepapers/Security/DDoS_White_Paper.pdf)
  - <https://docs.microsoft.com/de-de/azure/security/security-paas-deployments>
  - <https://azure.microsoft.com/en-us/blog/azure-ddos-protection-service-preview/>

# 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

# 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)
  - Ressourcen
    - ARN: Amazon Resource Name
    - Actions

# AWS IAM USER MANAGEMENT

- [https://www.youtube.com/embed/ySl1gdH\\_7bY](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

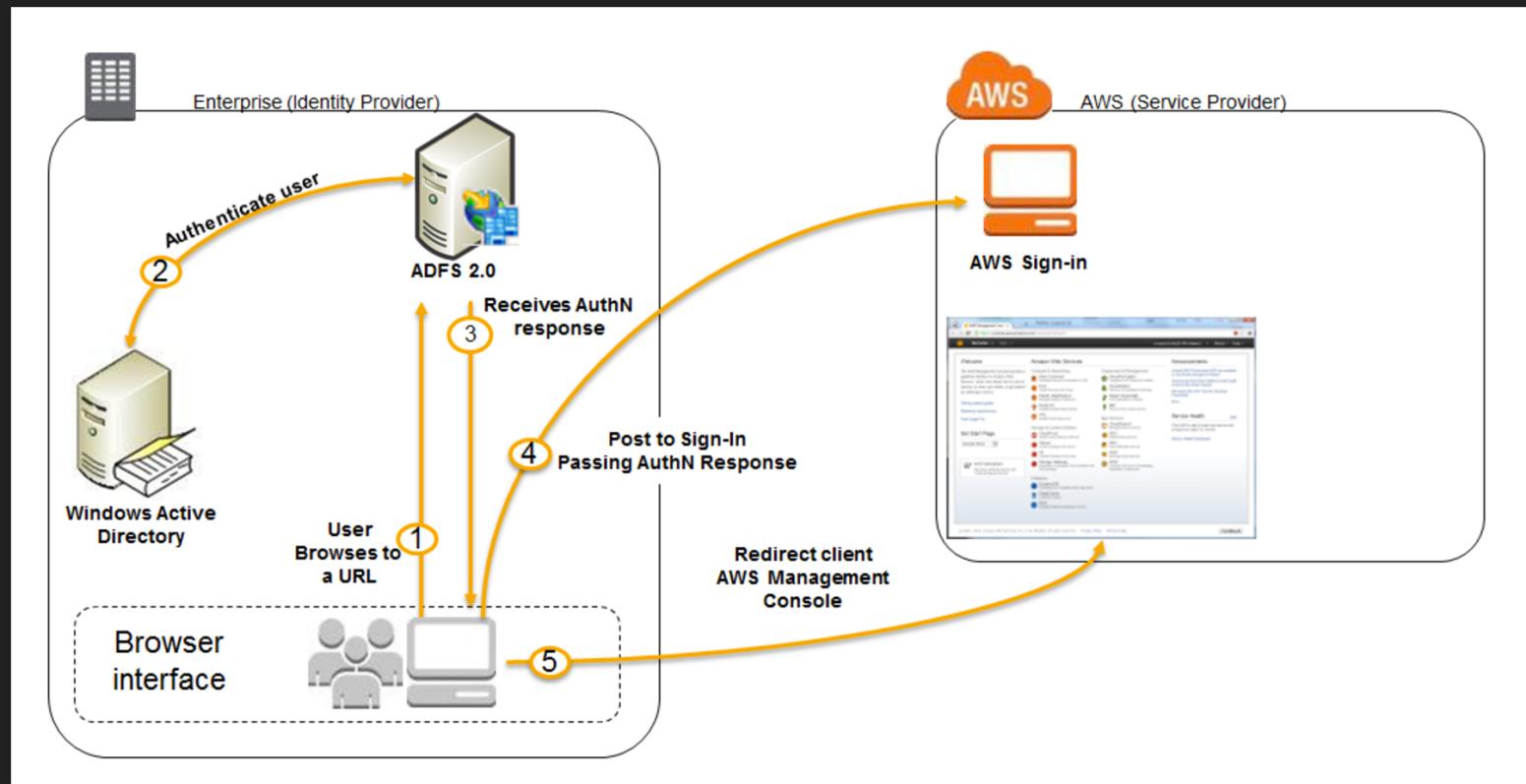
# MS AD FEDERATION SERVICE

- 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)

# INTEGRATION MIT MS ADFS + AWS IAM

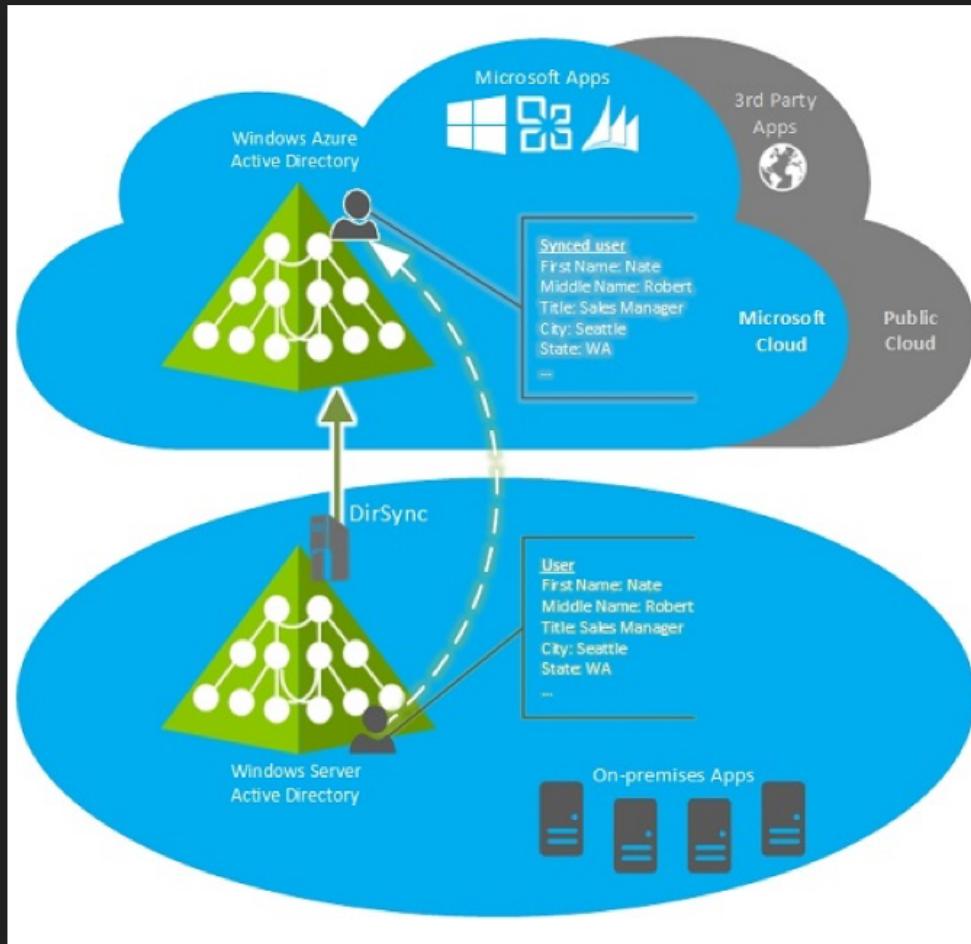
- Setup: two-way federated trust zwischen ADFS und AWS IAM
- ADFS authentifiziert und erstellt ein authentication ticket in Form eines signiertes SAML-Tokens
- ADFS Rules: überträgt AD Gruppen zu IAM Rollen und speichert diese im SAML Token
- AWS IAM empfängt signiertes SAML-Token und autorisiert Zugriff

# 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

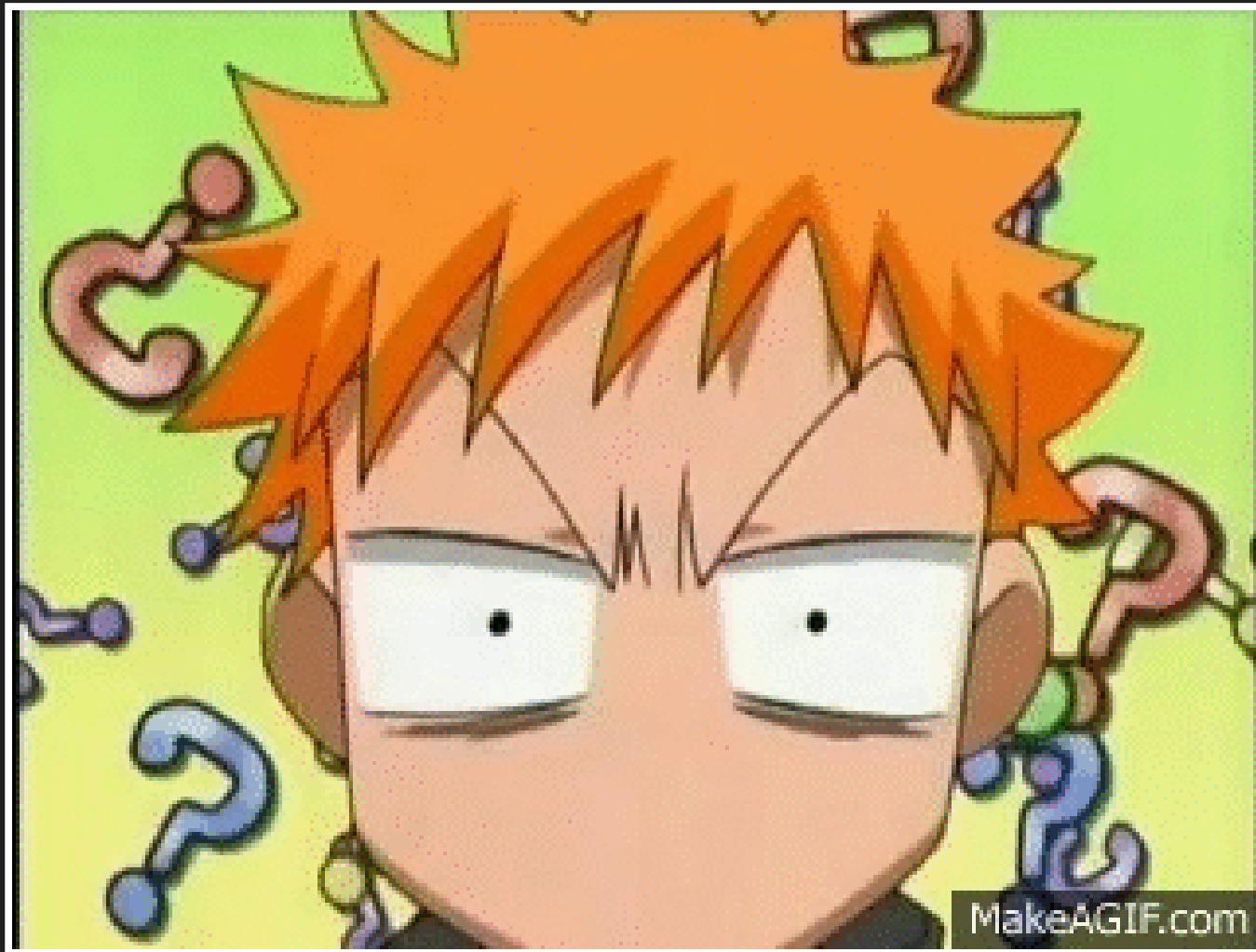


- <https://youtu.be/lcSATObaQZE?t=6m6s>

# IDENTITY-AS-A-SERVICE (IDAAS)

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

# FRAGEN ?



# 3. DATA PRIVACY

## C. DATENSCHUTZ

# DATENSCHUTZ

Darf ich Daten erheben und bei einem Cloud-Provider speichern der nicht in D (oder EU) ansässig ist?

# DATENSCHUTZ

- Recap: Besonderheiten bei Cloud Computing
  - keine technische Beschränkung durch natürliche Grenzen
  - Undurchsichtigkeit der Datenverarbeitung
  - Geographische Verteilung, Grenzüberschreitender Datenverkehr
  - Kosteneinsparung durch Übertragung von Verantwortung

# RECAP: WELCHE DATEN SIND SCHUTZBEDÜRFIG ?

- Beispiele:
  - Steuerlich relevante Daten (§146 Abs. 2 S1 AO)
    - müssen im Inland oder in einem Mitgliedstaat der EU/EWR (durch Einwilligung der zust. Finanzbehörde) gespeichert werden (§146 Abs. 2a AO)

- Handelsdaten z.B. Buchungsbelege, Handelsbriefe (§257 Abs.4 HGB)
  - müssen im Inland für 6 bzw. 10 Jahre aufbewahrt werden
- Personenbezogene Daten (§3 Abs.1 BDSG)
  - Vertraulichkeit und Integrität muss bewahrt sein
- Quelle:

<https://www.datenschutzzentrum.de/cloud-computing/20100617-cloud-computing-und-datenschutz.html>

# RECAP: WAS SIND PERSONENBEZOGENE DATEN ?

- §3 Abs. 1 BDSG:
  - "(1) Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmmbaren natürlichen Person (Betroffener)"
  - Daten die eindeutig einer Person zugeordnet werden können

# RECAP: WAS SIND PERSONENBEZOGENE DATEN ?

- die Identität einer Person aus dem Inhalt des Datums oder mit Zusatzwissen sich herstellen lässt
  - Quellen:
- [https://www.gesetze-im-internet.de/bdsg\\_1990/\\_\\_3.html](https://www.gesetze-im-internet.de/bdsg_1990/__3.html)
- [https://www.ldi.nrw.de/mainmenu\\_Datenschutz/Inhalt/FAQ/PersonenbezogeneDaten.php](https://www.ldi.nrw.de/mainmenu_Datenschutz/Inhalt/FAQ/PersonenbezogeneDaten.php)

# RECAP: WAS SIND PERSONENBEZOGENE DATEN ?

- Beispiele:
  - Alter, Augenfarbe, Geburtsort
  - Telefonnummer, E-Mail Adresse
  - KFZ-Kennzeichen

## RECAP: BESONDERS SCHUTZWÜRDIGE PERSONENBEZOGENE DATEN

- "(9) Besondere Arten personenbezogener Daten sind Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben"
- Verlust kann erhebliche Konsequenzen für die betroffene Person haben
- es gelten erhöhte Schutzmaßnahmen

# RECAP: ANWENDBARKEIT

- anonymisierte Daten
  - BDSG findet keine Anwendung wenn die Daten so anonymisiert sind dass nur mit unverhältnismäßigem Aufwand die Daten einer Person zugeordnet werden können
- pseudonymisierte Daten
  - schließen die Anwendbarkeit des BDSG nicht aus

# RECAP: ANWENDBARKEIT

- zentrale Bedeutung hat die "verantwortliche Stelle" (Person die Daten für sich selbst erhebt und verarbeitet bzw. für sich verarbeiten lässt)
- befindet sich diese in der EU/EWR oder Deutschland findet das jeweilige Nationale Recht bzw. deutsches Datenschutzrecht Anwendung
- befindet sich die verantwortliche Stelle außerhalb der EU/EWR, aber werden Daten innerhalb der EU (Server) verarbeitet gilt das "Territorialprinzip"

# RECAP: ANWENDBARKEIT

- Sitzlandprinzip (europäisches Recht)
  - Europ. Datenschutzrichtlinie (EU-DSRL) Art. 4 Abs. 1a), b): kommt es für die Anwendbarkeit einzelstaatlichen Rechts darauf an, in welchem Mitgliedstaat die Daten verarbeitende Niederlassung ihren Sitz hat.

- findet Anwendung bei grenzüberschreitenden Datenverkehr, regelt welches Nationale Recht Anwendung findet
- befindet sich eine Niederlassung eines Unternehmens/verantwortliche Stelle in Deutschland (und der Hauptsitz in der EU), in dem die Datenerhebung/-Verarbeitung stattfindet, dann findet das BDSG Anwendung
- Relevant ist das Land in dem sich die Niederlassung der verantwortlichen Stelle befindet, das jeweilige Nationale Recht gilt

# RECAP: ANWENDBARKEIT

- Territorialprinzip
  - das jeweilige Nationale Recht findet Anwendung in der die Datenerhebung, -verarbeitung, -nutzung stattfindet, d.h. in dem Land an dem sich die Server befinden
- Quelle: <https://www.datenschutzbeauftragter-info.de/ist-das-bundesdatenschutzgesetz-bdsg-im-internationalen-datenschutz-anwendbar/>

# RECAP: AUFTRAGSDATENVERARBEITUNG

Welche Regelungen gibt es damit Daten zur Verarbeitung in eine Cloud transferiert werden können  
?

# RECAP: AUFTAGSDATENVERARBEITUNG (§11 BDSG)

- betrifft das Outsourcing von Datenverarbeitung
- regelt die Verantwortlichkeit im Sinne des Datenschutzes, zwischen dem Auftraggeber und Auftragsnehmer
- Verantwortlich ist der Auftragsgeber der die Datenverarbeitung für sich durchführen lässt
- der Auftragsgeber ist die verantwortliche Stelle, hat Kontrollpflichten ggü. dem Auftragsnehmer
- bei Datenverlust/Leck hat die verantwortliche Stelle eine Meldepflicht

# RECAP: BEISPIEL CLOUD COMPUTING: SAAS

- Rollen: Cloud-Nutzer (Person o. Firma), Cloud Anbieter, Rechenzentrumsbetreiber
- Verantwortliche Stelle ist der Cloud Nutzer, dieser lässt über Auftragsdatenverarbeitung personenbezogene Daten durch den Cloud Anbieter und Rechenzentrumsbetreiber (Subbeauftragung) verarbeiten
- der Cloud Nutzer ist verantwortlich für den Schutz der Daten
- der Cloud Nutzer hat die Pflicht den Cloud Provider sorgfältig auszuwählen

# RECAP: MINDESTANFORDERUNGEN FÜR DIE AUFTAGSDATENVERARBEITUNG

1. Gegenstand und Dauer des Auftrags
2. Umfang, Art und Zweck der Verarbeitung, Art der Daten und Kreis der Betroffenen
3. die Datensicherungsmaßnahmen nach § 9 BDSG
4. Berichtigung, Löschung und Sperrung der Daten
5. die (Kontroll-)Pflichten der Auftragnehmer (AN)
6. Unterauftragsverhältnisse
7. Kontrollrechte der Auftraggeber (AG)
8. Mitteilungspflichten der AN bei Verstößen
9. Weisungsbefugnisse
10. Datenlöschung beim AN. Nach § 11 Abs. 2 S. 4, 5 BDSG muss sich der AG regelmäßig über die Beachtung der Datensicherungsmaßnahmen überzeugen

# RECAP: VERARBEITUNG VON PERSONENBEZOGENEN DATEN AUSSERHALB DER EU

- nach BDSG nur erlaubt wenn die Einwilligung aller Betroffenen eingeholt wurde oder ein angemessenes Datenschutzniveau im Drittland sichergestellt ist (§ 4b Abs. 2, 3 BDSG)
- angemessenes Datenschutzniveau besteht nach Attestierung der Europ. Kommission in Andorra, Argentinien, Australien, Faroer Inseln, Guernsey, Israel, Isle of Man, Jersey, Kanada, Schweiz, Uruquay und Neuseeland
- für die Nutzung in Staaten außerhalb der EU muss ein angemessenes Datenschutzniveau gewährleistet werden, z.B. durch gesonderte Abkommen:
  - Bsp.: Safe-Harbor (nicht ausreichend), Binding Corporate Rules (muss durch die Datenschutzaufsichtsbehörden genehmigt werden)

# FAZIT

- Es ist am sichersten dass Daten die innerhalb der EU erhoben/verarbeitet werden, die EU Grenzen nicht verlassen
- als Maßnahmen zur Erfüllung der Kontrollpflicht als verantwortliche Stelle können Zertifizierungen des Cloud Providers herangezogen werden (ISO 27001, Trusted Cloud)
- neben des Standorts, sollte der Cloud Provider sorgfältig nach folgenden Kriterien ausgesucht werden:
  - Verschlüsselungsmöglichkeiten, Anonymisierung von Daten
  - werden Daten in ein Drittland repliziert ?
  - Verbindliche Zusagen in Sachen Transparenz, SLAs, Vertragliche Zusagen ausreichend? (z.B. Mindestanforderungen für ADV)