8. HANA Tech Night
27. Juni 2023
Mannheim - Baden

Tobias Hofmann

www.itsfullofstars.de

ABOUT ME

SAP Professional

1998 – ABAP

2004 – SAP Portal

2009 – SAP Mobile

2011 – UI5

2011 – SAP Cloud

2013 – Fiori

2016 – S/4HANA

Positionen

Entwickler

Berater

Architekt

Enterprise Architekt

Externer | SAP‘ler | Interner

Aktivitäten

Vorträge: DSAG, ASUG , TechEd, SAP Inside Tracks, HANA Tech Night, re>=CAP, Meetups
Veranstaltungen: SAP Inside Tracks, Meetup, ABAPConf
Länder: Deutschland, Brasilien, Americas
SAP „hacken“
Blog

DISCLAIMER

Ich bin kein Sicherheitsexperte
Die hier gezeigten Beispiele sind ein „Hobby“.

(aka: Ich war auch persönlich davon als Anwender betroffen)

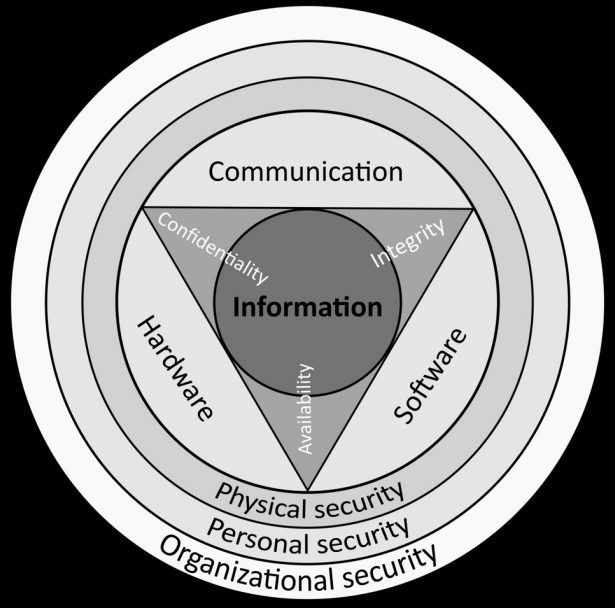
DISCLAIMER

Vieles hiervon ist auf meiner privaten Webseite: It‘s full of stars

SICHERHEIT ... IT'S COMPLICATED

Sicherheit ist einfach = **Sicherheit ist komplex**

INFORMATION SECURITY



CIA Dreiklang

Data **C**onfidentiality

Data **I**ntegrity

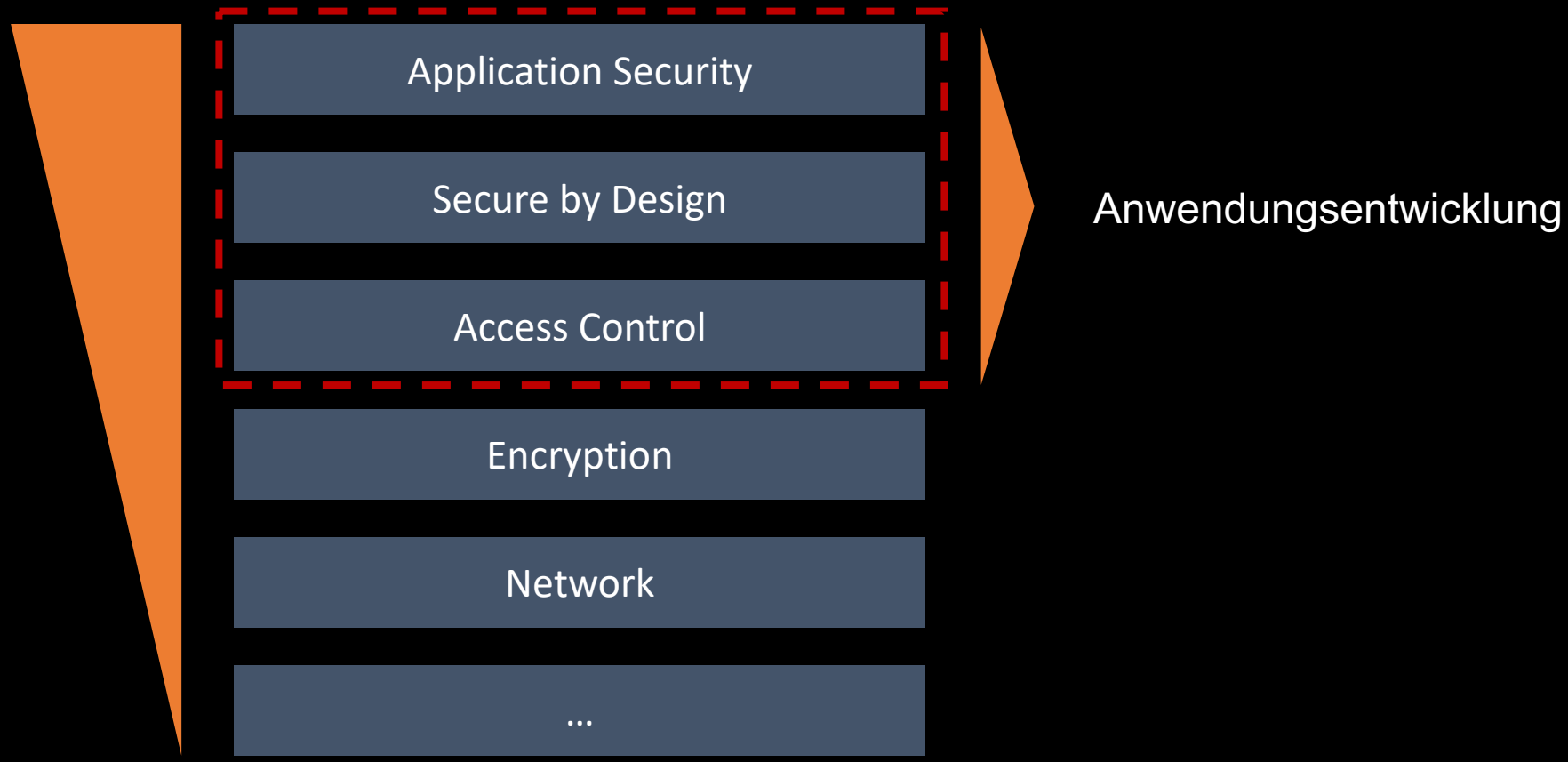
Data **A**vailability

[…] preventing or reducing the probability of unauthorized/inappropriate access to data, or the unlawful use, disclosure, disruption, deletion, corruption, modification, inspection, recording, or devaluation of information (Wikipedia)

Fokus liegt auf Daten

ABWEHRMASSNAHMEN

Ziel: Schutz der Daten

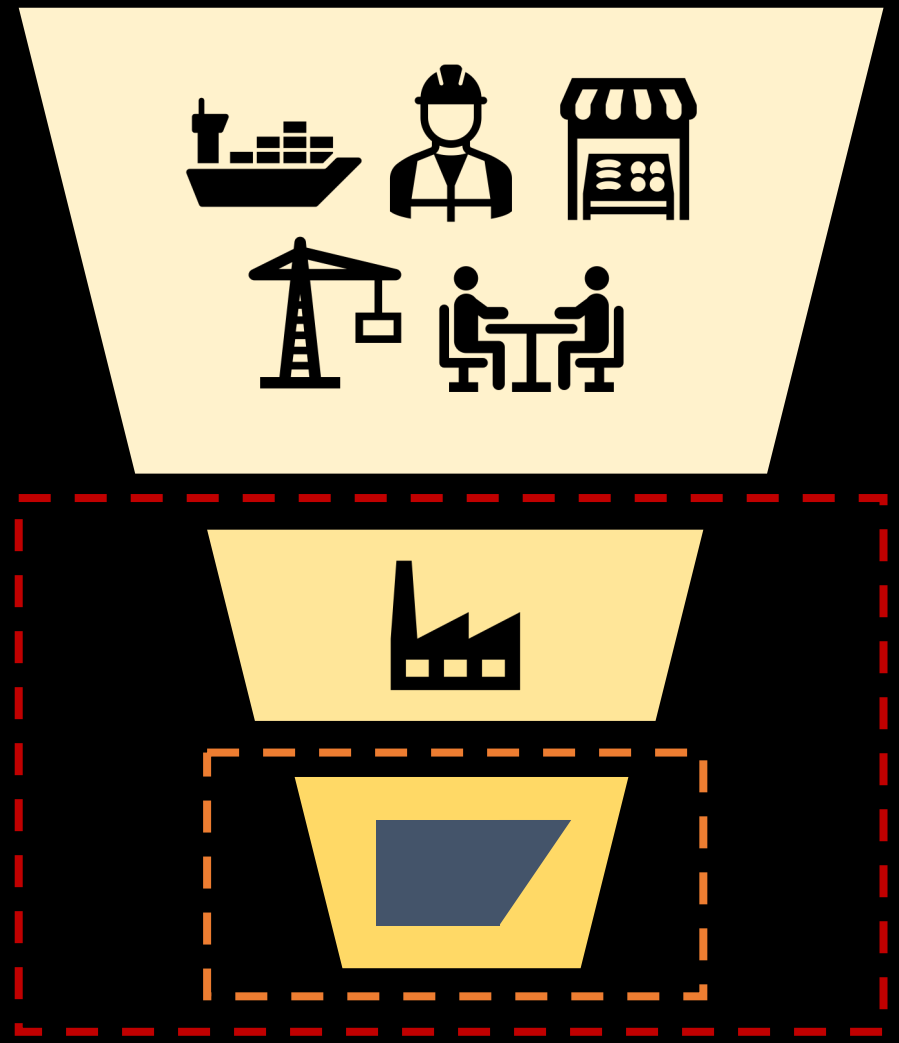


Sicherheit in der SAP Entwicklung

Prozesse

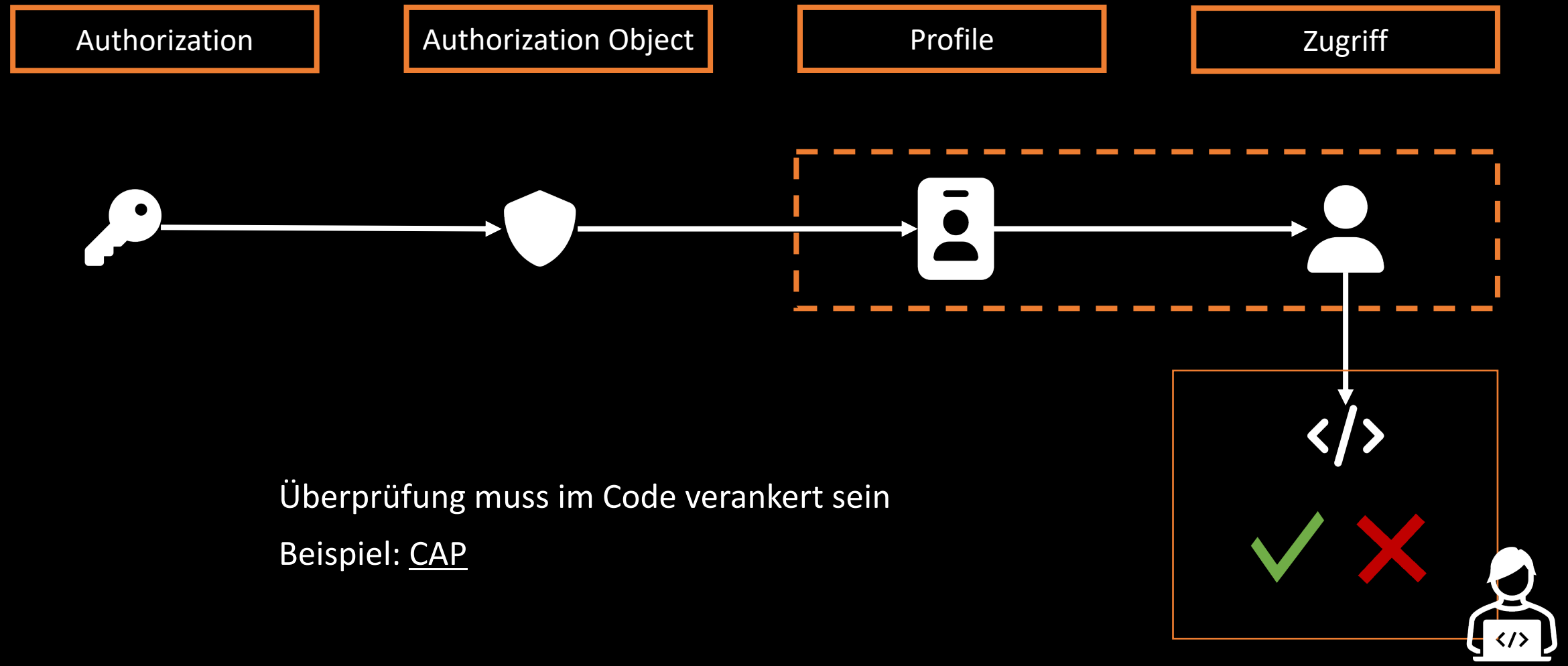
ERP

Integriertes ERP



SICHERHEIT IN DER SAP ENTWICKLUNG

Sichere Entwicklung in SAP: Berechtigungen

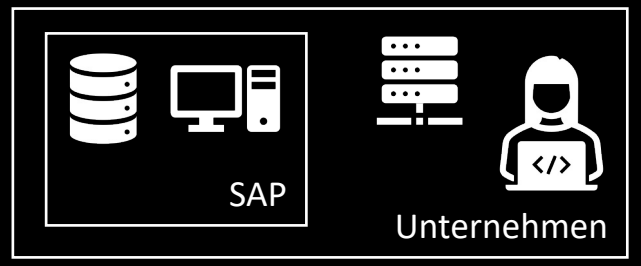


Überprüfung muss im Code verankert sein

Beispiel: CAP

Sicherheit in der SAP Entwicklung

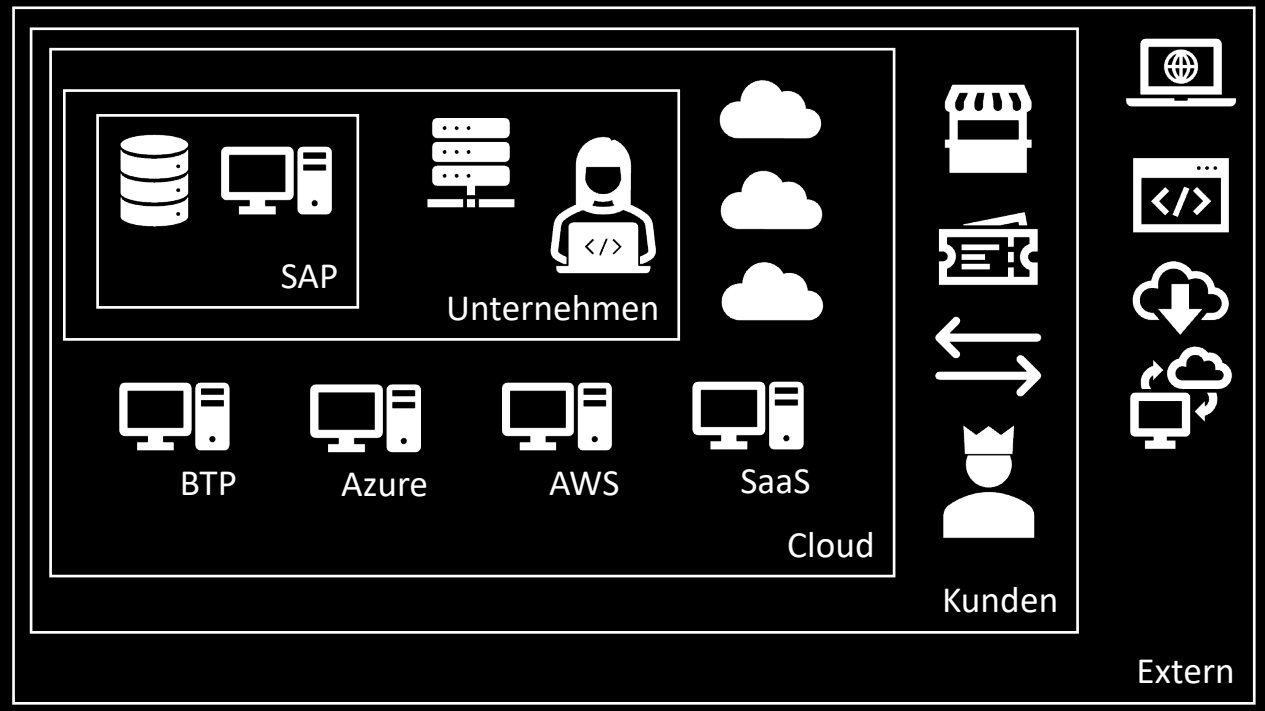
Damals



Monolithisch

Zugriff: LAN, VPN, Unternehmenslaptop

Heute



Offen

Cloud Native

Alptraum

Sicherheit in der SAP Entwicklung

Zugriff nur

mit SAPGui Client
mit Unternehmenslaptop
vom Unternehmensstandort
von Mitarbeitern

war einmal

Web Zugriff

OData

Integrierte, verteilte Systeme

Partnerzugriff

Single Sign-on

Hybride Landschaften

Verteilte Teams

Systeme stehen 24/7 im Internet

Weltweiter Zugriff

Abhängigkeit von vielen Komponenten

Komplexe Landschaften

Self-service Benutzererstellung

BOM: Updates / Patches

Komplexe Technologien

Nicht alle Features und Auswirkungen sind bekannt

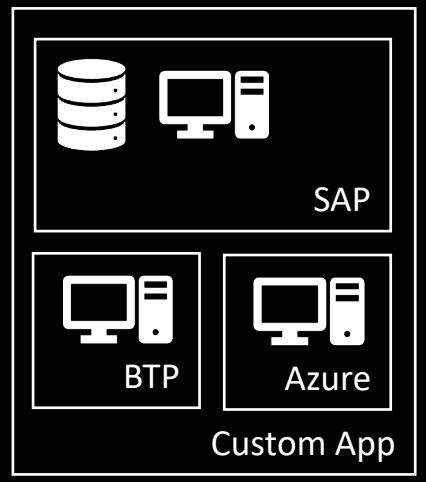
Druck: Zeit, Kosten, Projekte

Best of breed

Innovationen

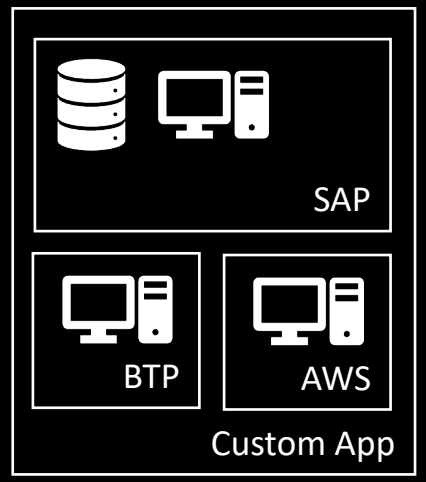
Sicherheit in der SAP Entwicklung

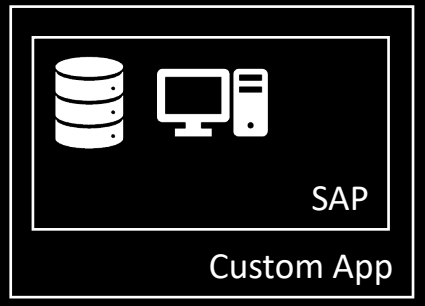
Meine App

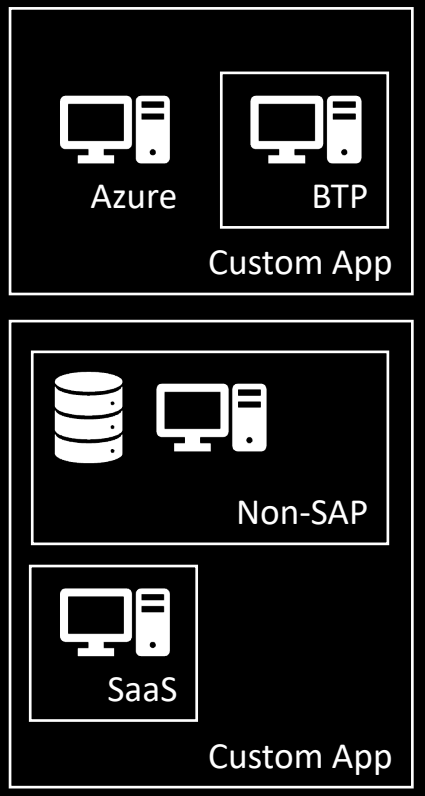


SAP Backend
BTP Services
Frontend Azure

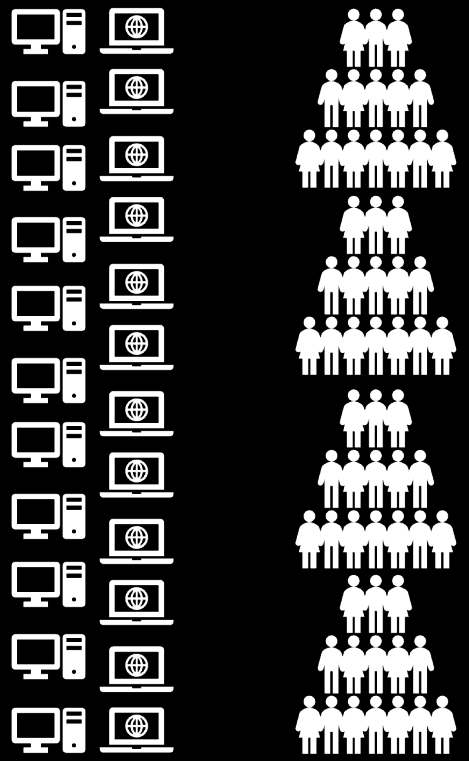
Meine Kollegen



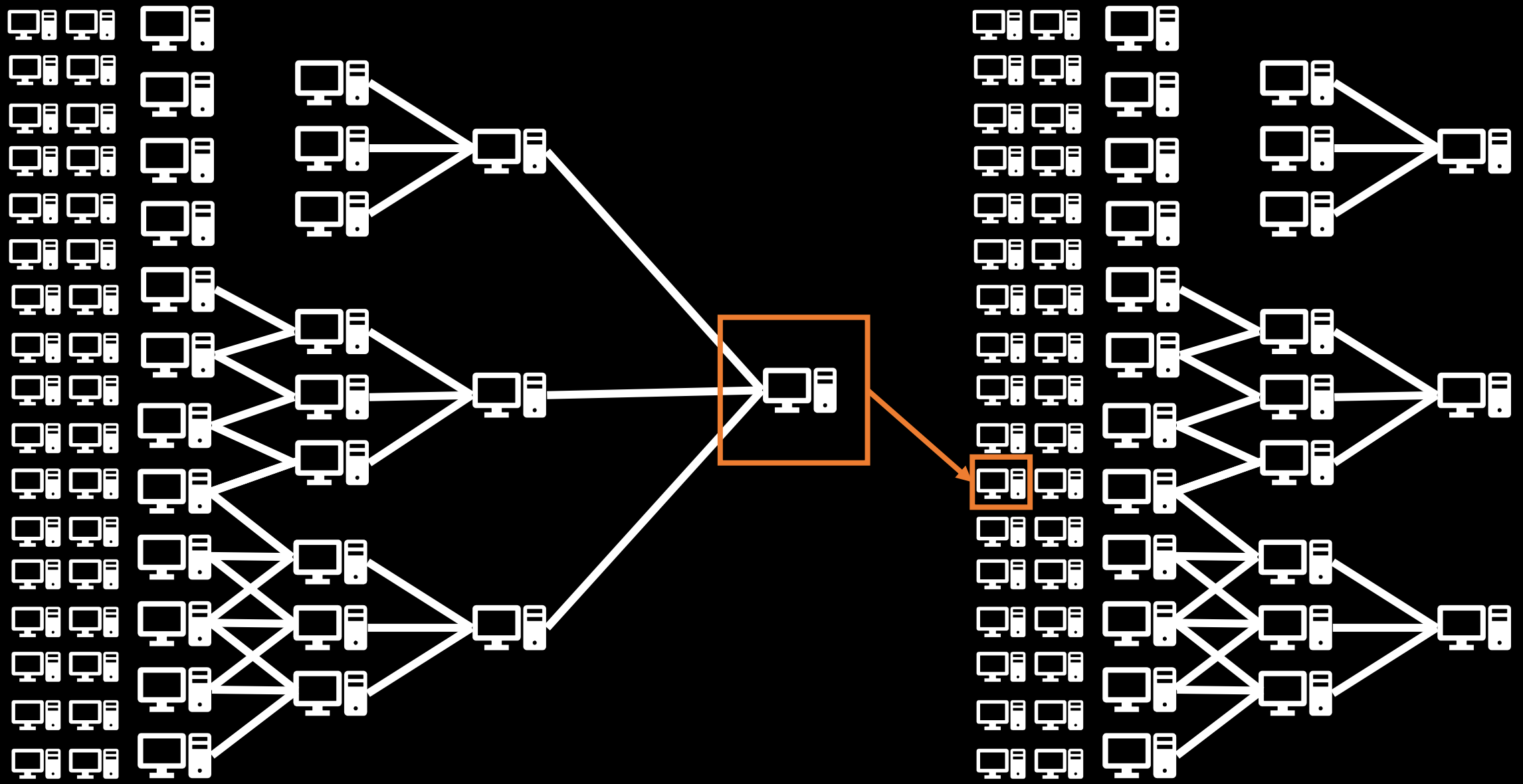




Ergebnis: Hunderte von App



SICHERHEIT IN DER SAP ENTWICKLUNG



Anzahl potentieller Angreifer – früher vs. heute

Anwender: 10.000

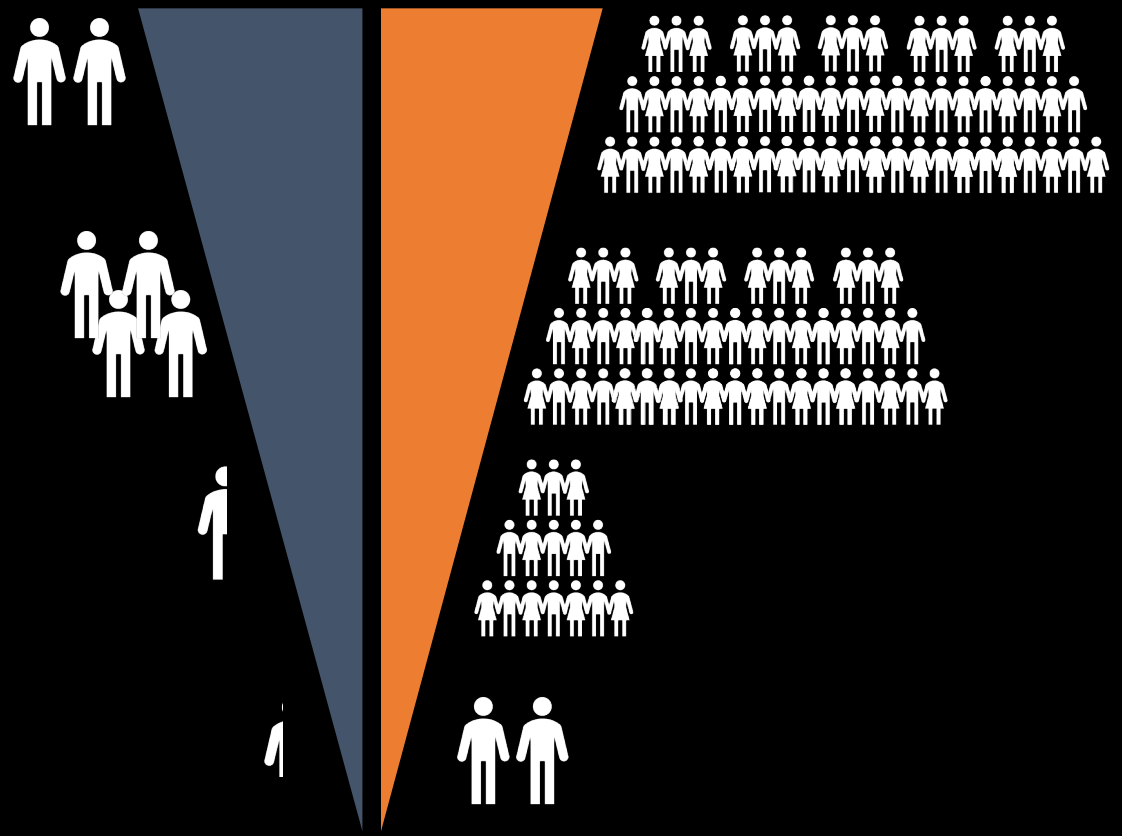
Zugriff auf die App (LAN/VPN)

Konzern: 300.000

Potentielle Angreifer

Innen/Außen/Hacker: 2.000

Echte Angreifer: 0,1% => 2



8 Milliarden Menschen

Menschen mit Internet-Zugang: 5,3 Milliarden

Anzahl Entwickler:
25 – 30 Millionen

0,1% => 25.000 – 30.000
0,01% => 2.500 – 3.000

(Beispiel)

SICHERHEIT IN DER SAP ENTWICKLUNG

Immer mehr Apps 

Immer mehr Anwender 

Immer mehr Bedrohungsszenarien 

Immer mehr Anforderungen 

Immer mehr Tools die einen Unterstützen ?

Sicherheit in der SAP Entwicklung

Ausreichend: Berechtigungsprüfung?

Was ist Sicherheit?

Aufruf: nur Befugte

Zugriff: so lange wie nötig

Verfügbarkeit: System

Rechtlich

Anwendung
Informationen
Identity & Access
Zero trust
Code obfuscation
Netzwerk
Cloud
Verschlüsselung
Scanner
Intrusion Detection
Firewall

Wissensaufbau Entwickler – Ziel: sichere Anwendungen

	IT Schulungen	Schulungen für Sicherheit
App Sicherheit	Coding, Entwicklung	?
Informationssicherheit	?	Pflichtschulung für Alle
Betrieb	Basis, DevOps	?
Rechtlich	?	?

SICHERHEIT IN DER SAP ENTWICKLUNG

Das Drucker-Syndrom

„Du kennst dich doch mit Computern aus. Mein Drucker spinnt. Fix das mal.“

Sicherheit in der SAP Entwicklung

Sicherheit in der Programmierung

„Du kannst doch programmieren!“

SICHERHEIT IN DER SAP ENTWICKLUNG

Sichere IT-Architektur

„Die App verwendet HTTPS“

„Wir verwenden ein Framework der SAP. Das langt.“

NEUE REALITAET IN DER ENTWICKLUNG

Alte Welt

1 Entwickler für alles

ABAP Full Stack

Konkreter Anwenderkreis

Sicherheit durch Zugriff

1 System für alles

Neue Welt

1 Team für alles

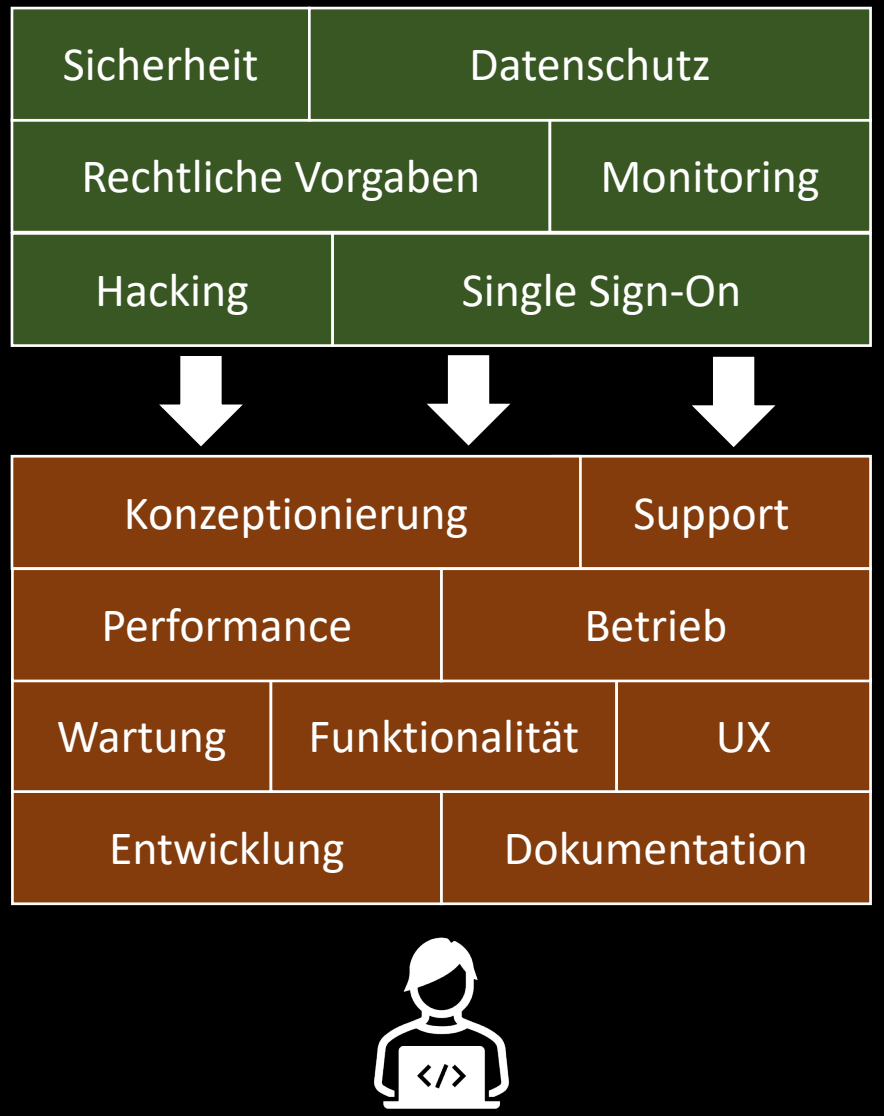
Entwickler

Gleicher Entwickler

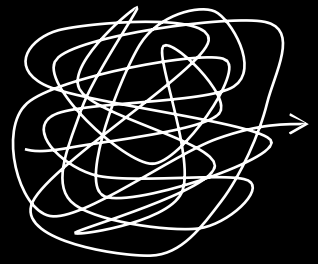
Mehr Aufgaben

Keine Schulung

NEUE REALITAET IN DER ENTWICKLUNG



UND JETZT?



UND JETZT?

Nichts tun ist auch keine Lösung

UND JETZT?

- Full-Stack Devs ist eine Utopie
- Übernehmt nicht zu viel Verantwortung
- Kein Sicherheitsexperte?
  - Macht nicht deren Job
  - Lasst die Sicherheitsexperten arbeiten
  - Auch mit Schulung: es dauert Jahre ein Experte zu werden
  - Die Experten sollen nicht nur einen Fragekatalog senden, sondern aktiv handeln
- Vertraut nicht zu sehr auf Prozesse
- Sagt NEIN

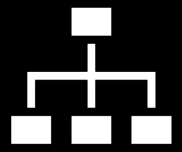
UND JETZT?

Nichts tun ist also doch eine Lösung?

UND JETZT?

Bereitet euch vor

Wo kann man was melden?
Intern / Extern



Wer ist für was zuständig?

Notfallplan vorhanden?
Regelmäßige Simulation?

TRIFFT MICH JA NIE, WAS SOLL DAS GANZE ALSO

Beispiele

OData

- Metadata: Datenmodell liegt komplett vor
- Protokoll: Mögliche Operationen sind bekannt

Diskussion

- OData Scanner
- Metadata nicht ausliefern
  - UI5 App: metadata.xml ist in der App vorhanden
- Nur Ausliefern was notwendig ist
  - odata.metadata=none [ui5, odata]

DIE ANDEREN MACHEN SCHON IHREN JOB

- https://www.itsfullofstars.de/2023/02/stretching-access-to-training-material-in-sap-learning-hub/
- https://www.itsfullofstars.de/2023/02/access-to-learning-hub-excercise-documents/
- https://www.itsfullofstars.de/2022/05/mind-the-protocol/

- Kundenspezifisches Workshopmaterial war öffentlich zugänglich

- Massendownload von SAP Education PDFs
  - 75+ GB
  - Keine Firewall, keine Echtzeitanalyse, keine KI oder ML
  - Keine Abfrage ob Authentifiziert

DSGVO

Komplexes Thema

- Persönliche Daten, z.B. IP
- Archivierung, Export, Reports, Löschen
- Cookie Consent

Eine App DSGVO konform zu gestalten ist nicht primär Job eines Entwicklers
Lasst die DSGVO Abteilung hier aktiv arbeiten

Diskussion

- YouTube Videos einbinden: https://www.youtube-nocookie.com/
- Links für Datenschutz: Inhalt muss korrekt sein
- Cookie Consent: Widerruf
- Hirn einschalten

DSGVO

Kleine Liste

- https://www.itsfullofstars.de/2023/05/sap-apphaus-website/
- https://www.itsfullofstars.de/2023/03/take-care-of-your-templates/
- https://www.itsfullofstars.de/2023/02/legal-requirements/
- https://www.itsfullofstars.de/2023/01/yes-were-open/
- https://www.itsfullofstars.de/2022/10/unsee-juice-for-sap-connect/
- https://www.itsfullofstars.de/2022/10/sap-universal-id-and-gdpr/
- https://www.itsfullofstars.de/2022/05/wie-man-mit-einer-meldung-zu-einem-dsgvo-verstos-richtig-umgeht/
- https://www.itsfullofstars.de/2022/05/mind-the-protocol/

SINGLE SIGN-ON

Single Sign-on ist toll

Alle lieben Single Sign-on

Die korrekte Konfiguration ist schwierig

Viel Liebe geht raus an SAP Universal ID

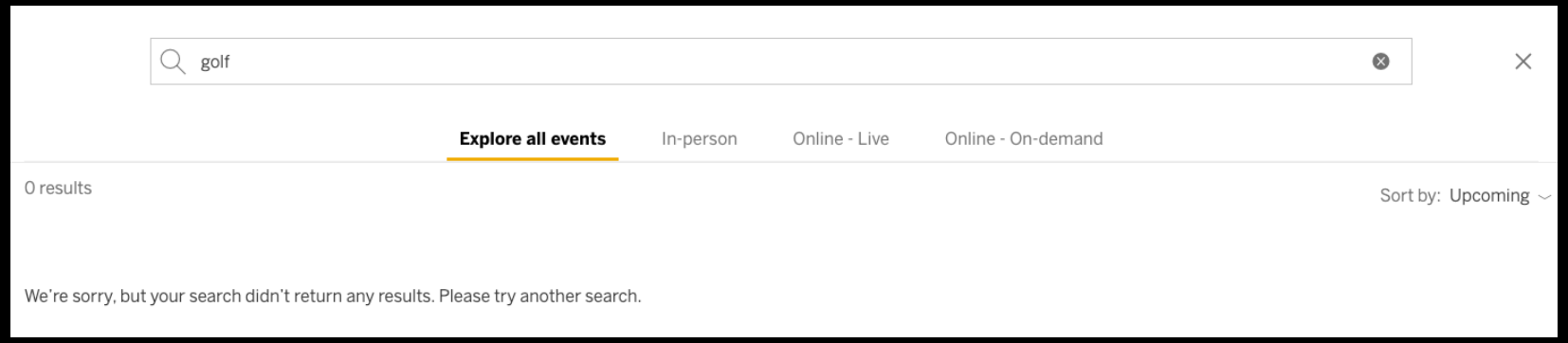
SINGLE SIGN-ON

Beispiele

- SAML SSO für alle authentifizierten Benutzer https://www.itsfullofstars.de/2023/01/yes-were-open/
- Authentifiziert über einen Cookie Wert auslesen
- Code Beispiele aus Tutorials sterben langsam
  - neo-app.json: "authenticationMethod": "saml" | "none"
  - xs-app.json: "authenticationType": "ias" | "xsuaa"(default) | "basic" | "none“
  - SAML: Mapping Benutzer -> Gruppe notwendig. Viele Beispiele für WebIDE gaben Zugriff auf alle angemeldete Benutzer oder none
  - Beispiele für CF verwenden oft auch none
- Problem: Bad Practices aus Tutorials werden 1:1 übernommen und sterben nur langsam

VERSTECKTE INFORMATIONEN

- SAP Events
- Liste an Veranstaltungen wird aktiv kommuniziert



VERSTECKTE INFORMATIONEN

Basis Wissen Internet

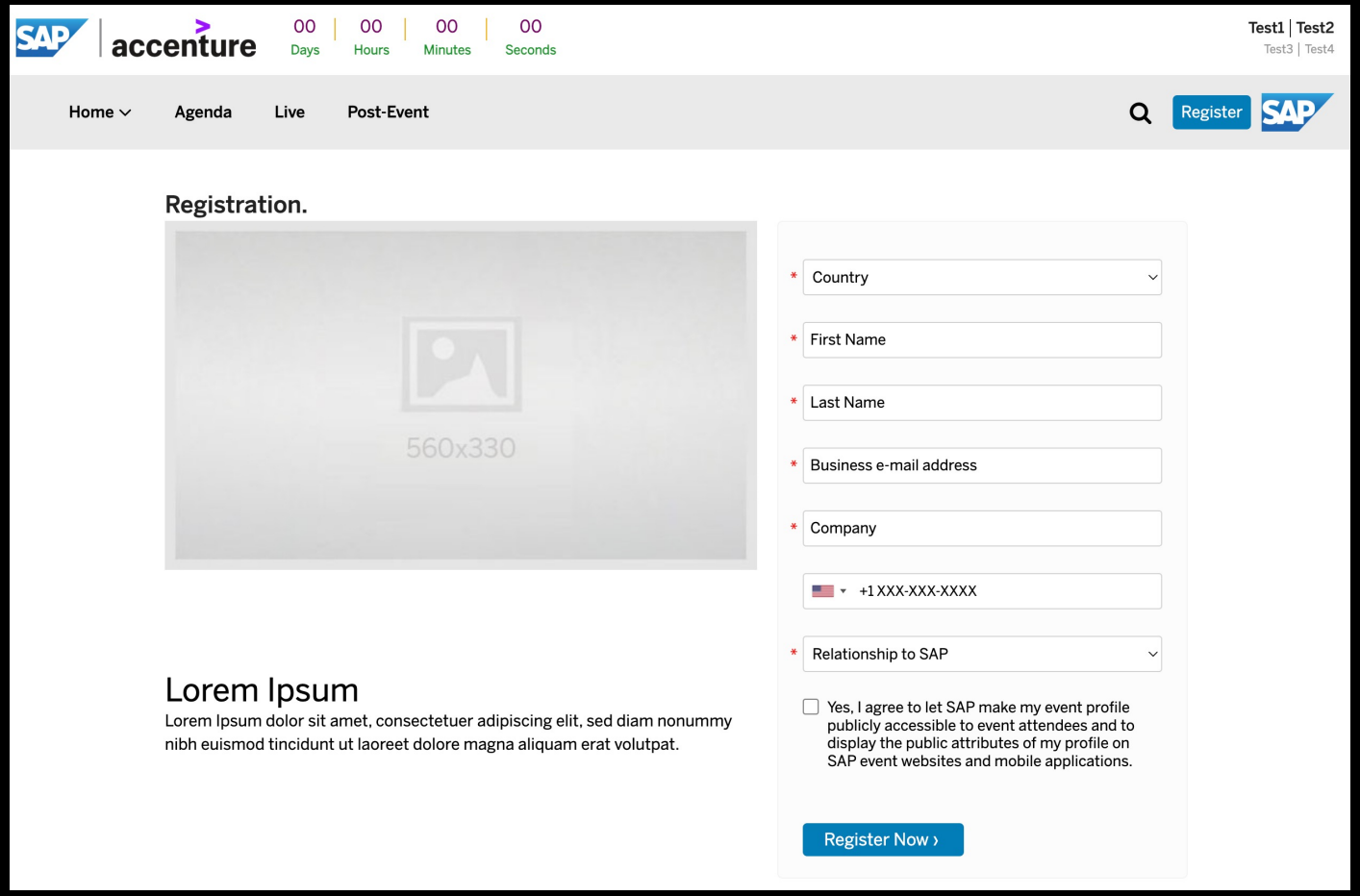
- Standard für Webcrawler: robots.txt
- Frei zugängliche Datei

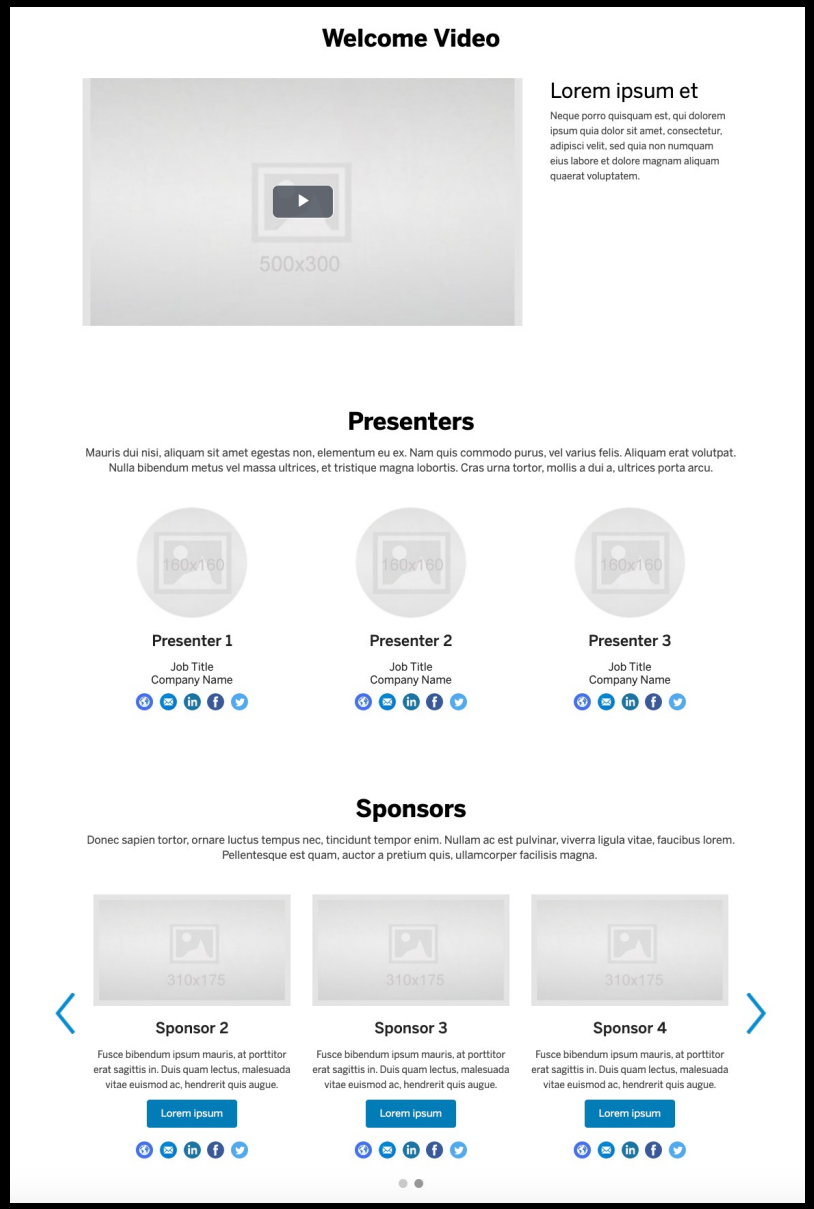
7.397 Veranstaltungen

- Suche nach Golf: 18 Ergebnisse
- Disallow: /us-customer-appreciation-golf-outing-at-sap-for-utilities-conference/
- Disallow: /us-an-evening-at-top-golf-with-sap-and-cognitus/
  Disallow: /us-2023-sap-successfactors-isv-mixer-at-topgolf-lv/

VERSTECKTE INFORMATIONEN

- Suche nach Test: 481 Ergebnisse
- https://events.sap.com/test-epam-smoke-0908/en/home





Versteckte Informationen

Fiori App als Launchapd

- https://www.itsfullofstars.de/2023/01/part-ii-sap-help-status-page/

Nicht unüblich

VERSTECKTE INFORMATIONEN

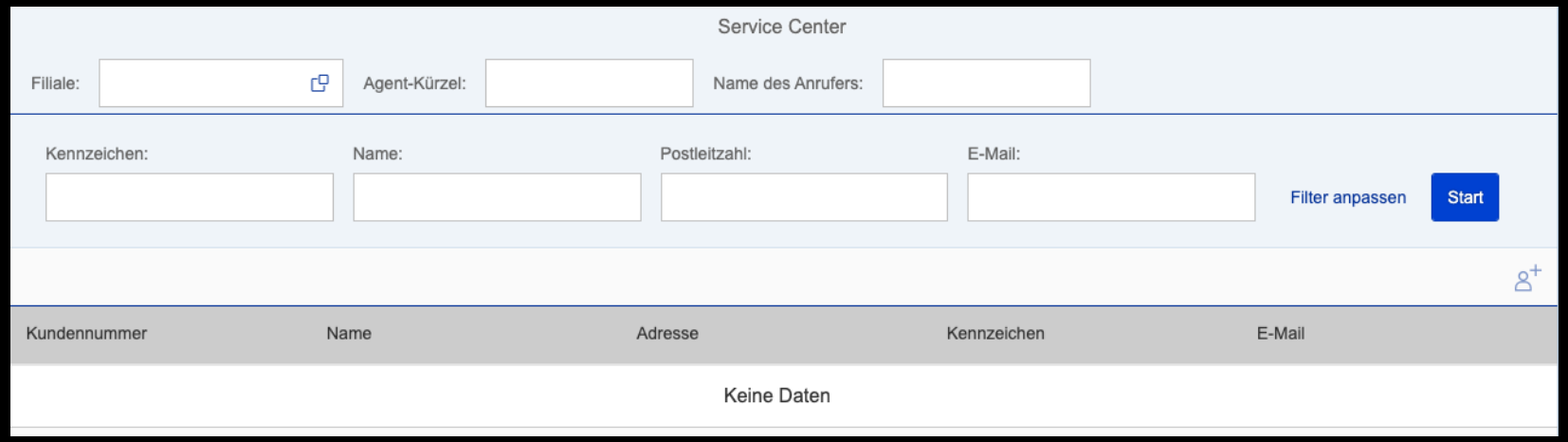
Terminbuch

https://pneuhage-management-gmbh---co--kg-pneuhage-cf-prd-bvnhz5cbddf42.cfapps.eu10.hana.ondemand.com/pneutborderbook-1.0.0/index.html

```
"CallCenter": {
    "viewType": "XML",
    "viewName": "CallCenter"
},
"CallCenterAfterCustomerCreate": {
    "viewType": "XML",
    "viewName": "CallCenter"
},
```

```
{
    "name": "CallCenter",
    "pattern": "callcenter/start",
    "target": "CallCenter"
},
```

https://pneuhage-management-gmbh---co--kg-pneuhage-cf-prd-bvnhz5cbddf42.cfapps.eu10.hana.ondemand.com/pneutborderbook-1.0.0/index.html#/callcenter/start



VERSTECKTE INFORMATIONEN

Alles was zwischen keinem Datenzugriff und Datenleck liegt ist die Berechtigungsprüfung im Backend OData Service

Zur Erinnerung:

- 1 Fall < - > 1 App
- Fiori Launchpad

OFFENE INFORMATIONEN

Eigene Domäne

- Andere bieten das aus einer Hand **SAP: Nö**
- Andere bieten dies kostenlos an **SAP: Nö**
- Andere: out of the box **SAP: Nö**

Ergebnis
Wichtige Informationen sind öffentlich zugänglich

OFFENE INFORMATIONEN

Globus E-Mail Werbung

Link:
https://approuter-kunden-prod.cfapps.eu10.hana.ondemand.com/data-buffer/sap/public/cuan/link/200/A6...1ERQ&_K13_=282&_K14_=eeee5a

Logon
https://ajwbnx4o8.accounts.ondemand.com/saml2/idp/sso/ajwbnx4o8.accounts.ondemand.com?SAMLRequest=nZJdb

Keine eigene Domäne verwendet

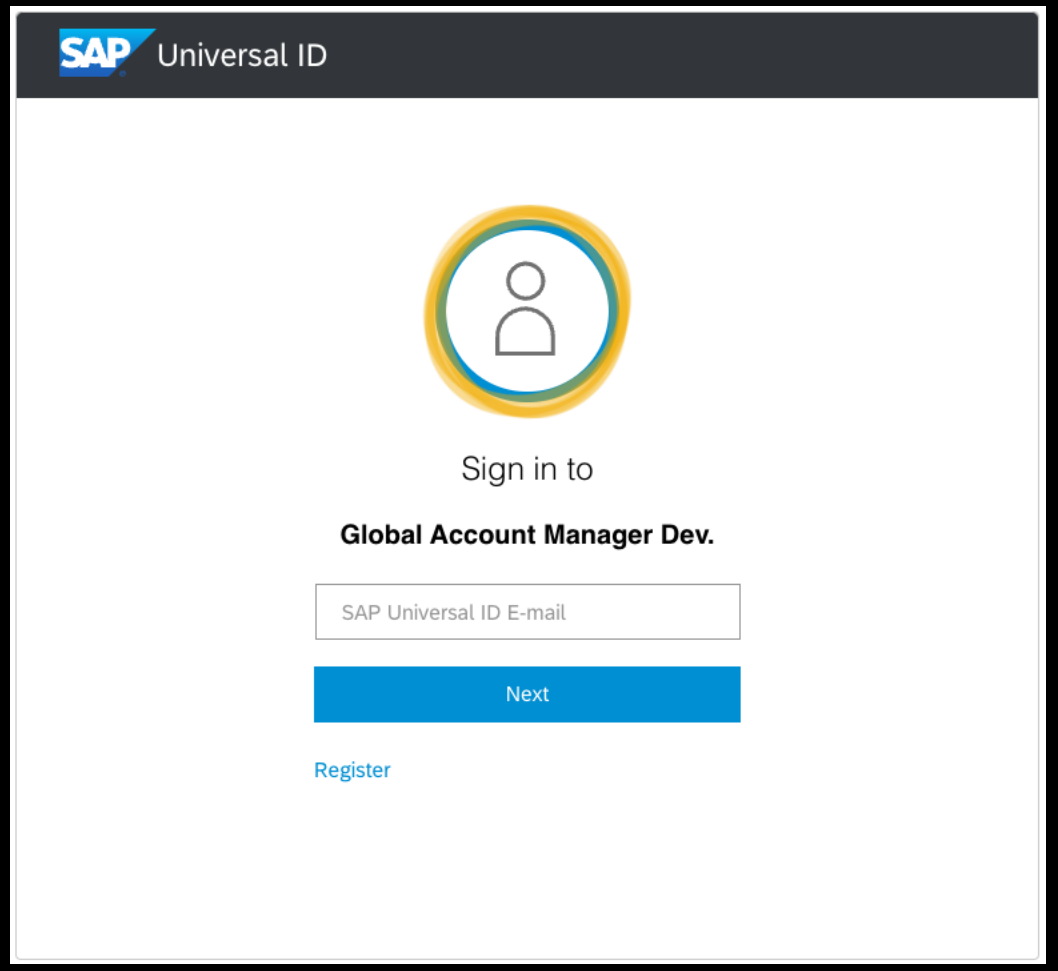
- SAP Kunde
- SAP BTP
- Cloud Foundry
- Lokation (eu10)
- Account ID
- SAML 2.0

CLOUD NATIVE

Wenn schon Cloud, dann richtig

Landschaft: 100% Cloud

- https://account-dev.sap.com/
- https://account-qa.sap.com/
- https://accounts.sap.com/



CLOUD NATIVE

Links zu DEV/QA Seiten

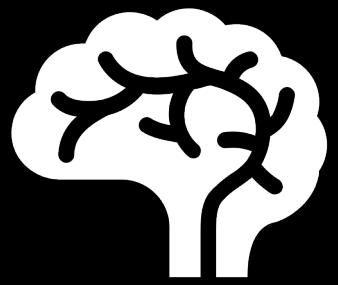
- https://www-qa.sap.com/products/free-trials.html
- https://community-qa.sap.com/
- https://learning-preview.sap.com/
- https://support-qa.sap.com/
- https://newssap2.wpengine.com/

Zugriff ist geschützt

A) Warten. Es braucht nur eine Fehlkonfiguration

B) Die Links sind für QA. Man kann auch einen QA Benutzer beantragen

IHR, DIE IHR HIER EINTRETET, LASST ALLE HOFFNUNG FAHREN?



Hirn einschalten