AVANTech-Day 2026

AVANTEC
Competence. Security. Trust.

IT-Security Deep Dive

AVANTech-Day 2026

AVANTEC
Competence. Security. Trust.

Disaster Recovery im Cloud-Zeitalter

Matthias Geiser
Principal Security Engineer, Content Security
AVANTEC

Über mich

Matthias Geiser – geiser@avantec.ch

AVANTEC
Competence. Security. Trust.

- Fan von offener Standards und dezentraler Infrastrukturen
- Seit 2002 bei AVANTEC
- Engineer im Content Security Team
  - Mail (xorlab, Cisco)
  - Verschlüsselung (SEPPmail)
  - Proxy / SASE (Netskope, Zscaler, Symantec)

Über Sie

AVANTEC
Competence. Security. Trust.

- Tätigkeitsbereiche
  - Produktion, Industrie, Handel, …
  - Banken, Versicherungen, …
  - anderes?

- Wie weit sind sie auf dem “Cloud Journey”?
  - Wir betreiben alle Server selber in unseren Datacenters
  - Wichtige Geschäftsprozesse laufen über SaaS Dienste
    - Z.B. Exchange Online, EntraID, ServiceNow, …
  - Unsere Server sind bei einem Hyperscaler/Hoster virtualisiert
  - Bin “cloud native”
  - Wir betreiben wichtige Server/Services wieder selber

Um was geht es heute?

Disaster Recovery im Cloud-Zeitalt

- Business Continuity Management
- Disaster Recovery Planning
- Risk Assessments / Business Im n
- RTO (Recovery Time Objective)
  - Maximal tolerierbare Ausf
- RPO (Recovery Point Objective)
  - Wieviele Daten dürfen verl

AVANTEC
Competence. Security. Trust.

Um was geht es heute wirklich?

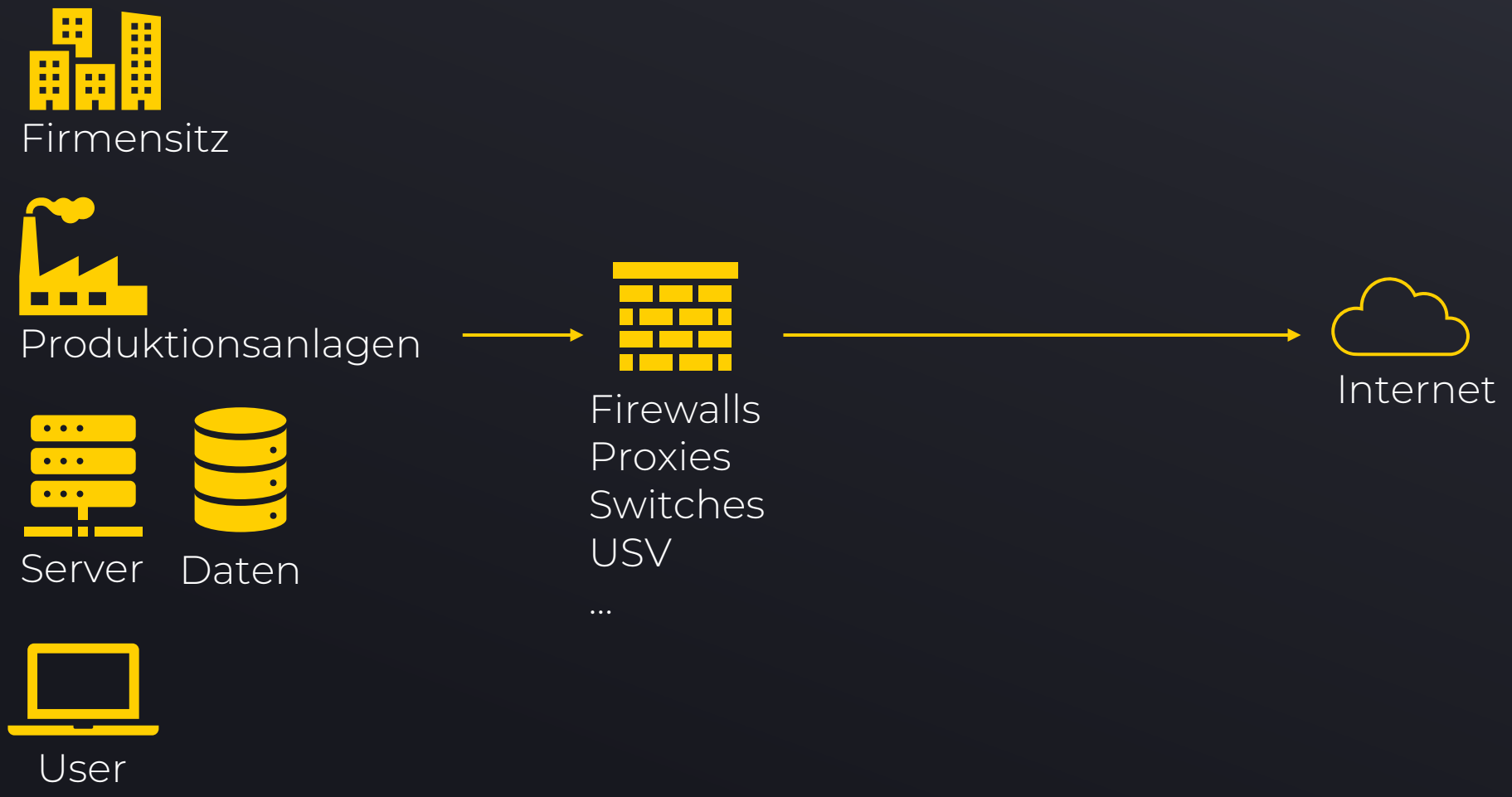
Disaster Recovery im Cloud-Zeitalter

AVANTEC
Competence. Security. Trust.

- Was hat sich in den letzen Jahren / Jahrzehnten in unserer IT Infrastruktur geändert?
- Welche neuen "Dinge" können dabei schief gehen?
- Was ist anders oder auch besser geworden?
- Was geht gerne vergessen?

Klassisch

Alles in der Firma



Klassisch

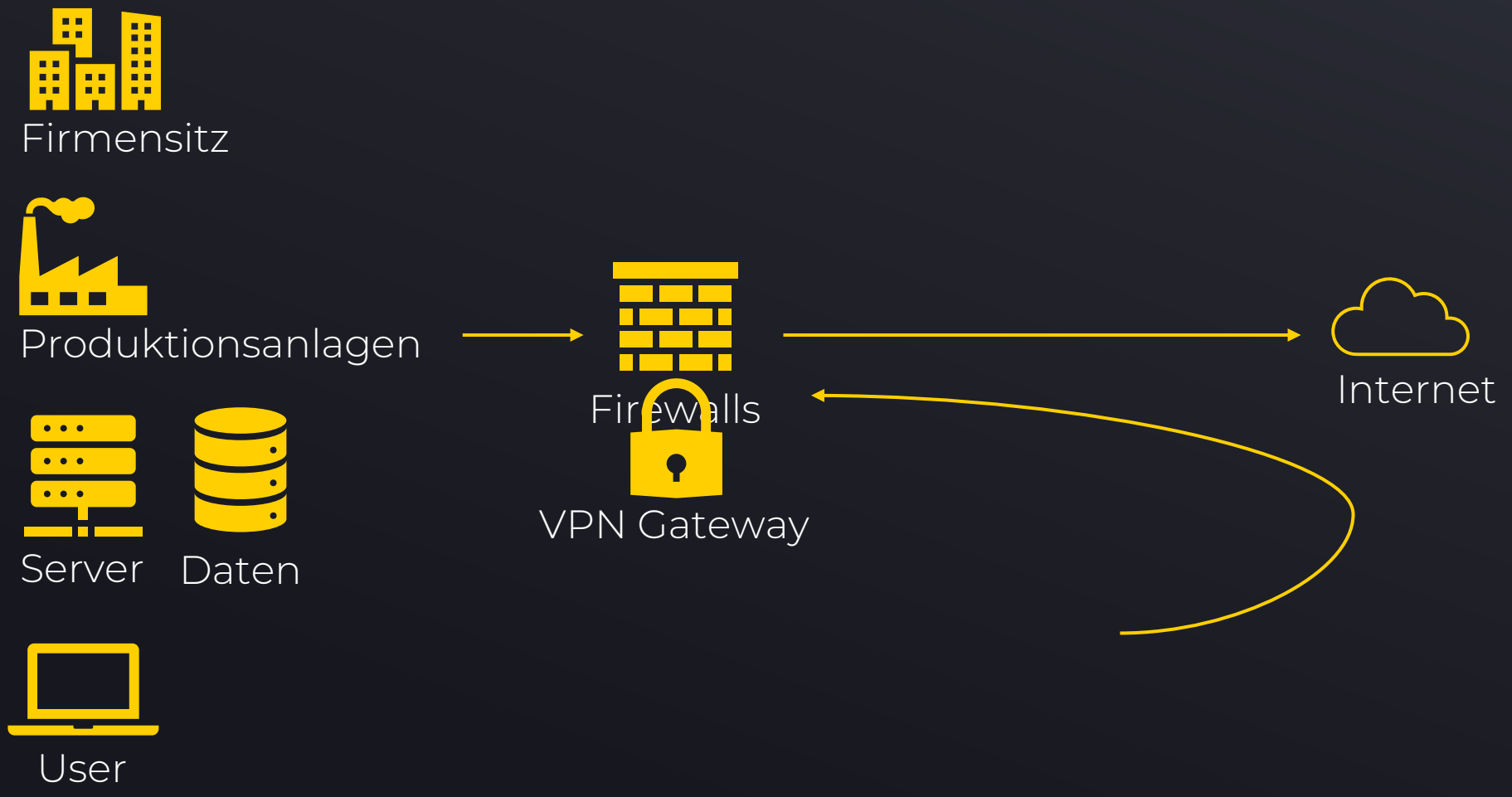
Alles in der Firma

AVANTEC
Competence. Security. Trust.

- Redundanz
- Mehrere Standorte
- Mehrere ISP
- Cold Standby
- Backup
- ...

Home Office / Roaming User

User unterwegs



Home Office / Roaming User

User unterwegs

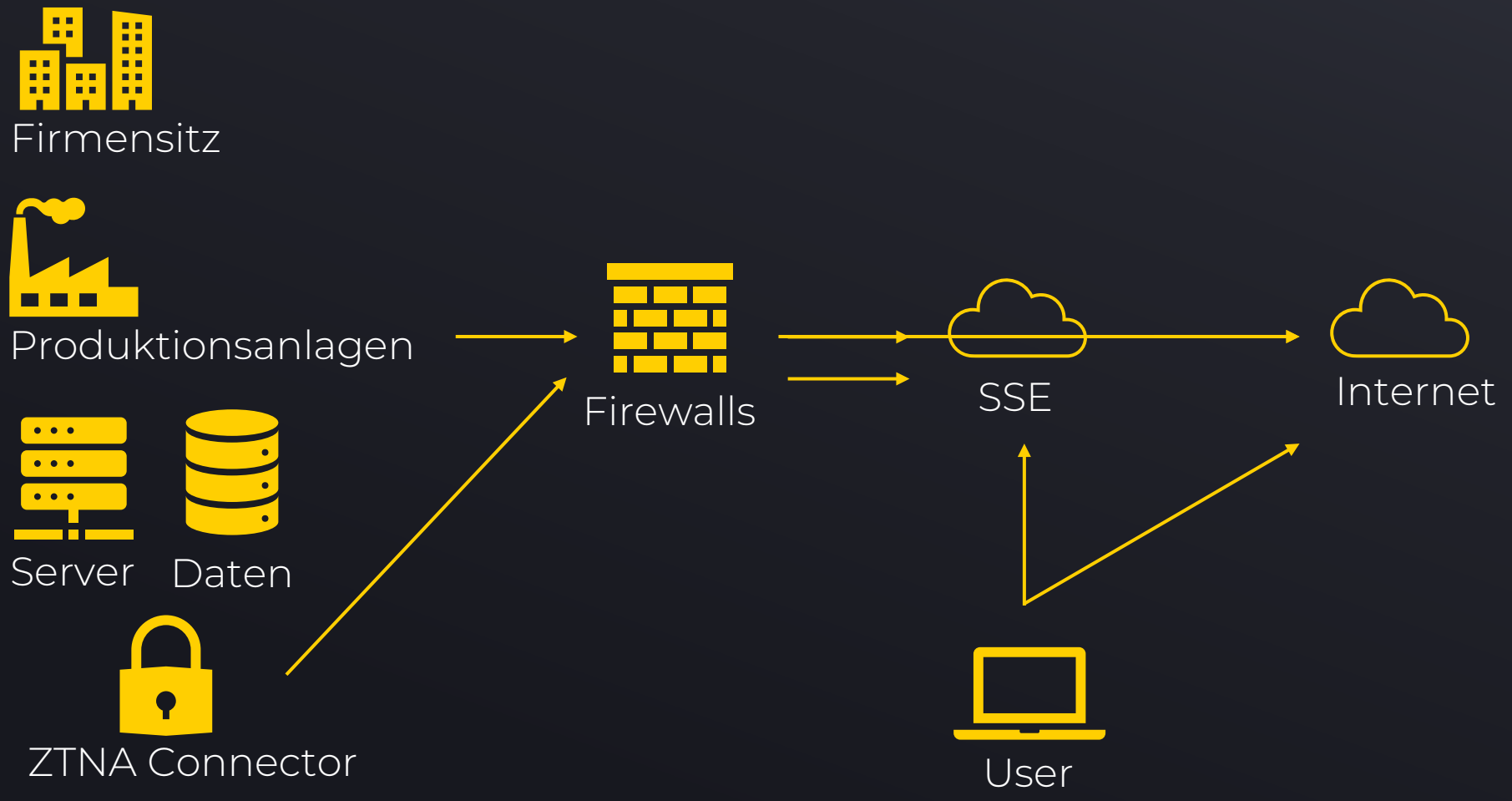
- VPN Gateway
- Infrastruktur beim User kann ausfallen
- “WLAN schlecht”
- Endkunden ISP-Vertrag ohne SLA

- Auswirkungen
  - Mehr Debug Aufwand von fremder Infrastruktur
  - User kommt halt ins Büro

SASE

Security in der Cloud

AVANTEC
Competence. Security. Trust.



SASE

Security in der Cloud

AVANTEC
Competence. Security. Trust.

Im folgenden müssen wir uns immer fragen, was passiert, wenn ein Cloud Anbieter ausfällt

- Teilausfall
  - SaaS Dienst in sich (hoffentlich) hoch redundant
  - Ausfallwahrscheinlichkeit einer einzelnen Teikomponente hoch
    - Per Design
    - Merkt man nicht
  - Ausfall eines POP
  - Performance Degregation (Brown out)
    - Wird vom Provider nicht immer proaktiv angeganen, zuwenig gut gemonitored
    - ➔ Eigene Messung vom Client aus
      - Automatisches / manuelles Failover
  - SLAs
    - Verfügbarkeit 99.999% (26s Ausfall / Monat)
    - Meist bloss Erstattung von Abokosten, kein Schadenersatz

SASE

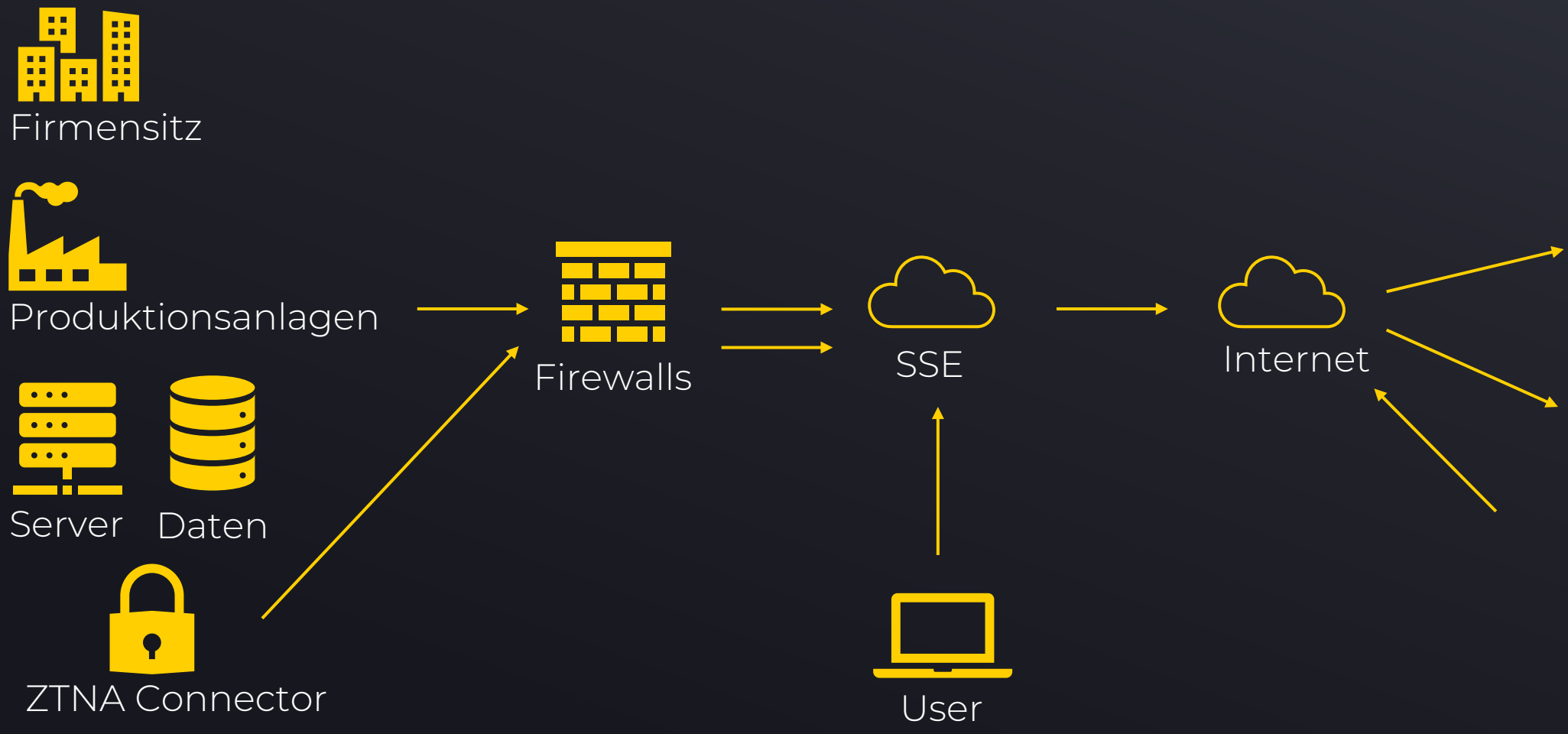
Security in der Cloud

Im folgenden müssen wir uns immer fragen, was passiert, wenn ein Cloud Anbieter ausfällt

- Totalausfall
  - Temporär
  - ➔ Brauche Umgehungslösung
    - Beispiel Cloud SWG
      - ➔ Fail-open
        - No Protection
        - Verlassen auf Endpoint Protection
      - ➔ Fail-close
        - Kein Surfen, kein Email, …
        - Nur direkter Zugriff auf trusted sites
      - ➔ Alternativer Proxy
        - Fall-back auf private service edge / on-premises Proxy
        - Sekundärere Cloud SWG Anbieter
    - Beispiel ZTNA
      - ➔ Zugriff geht nicht / User kommt ins Office
      - ➔ Fall-back auf private service edge / klassisches VPN
      - ➔ Sekundäre ZTNA Lösung

?aaS

Server / Daten in der Cloud



?aaS

Server / Daten in der Cloud

- Daten in der Cloud
  - Mails nicht abrufbar
  - Sharepoint / OneDrive / … nicht verfügbar
  - S3 Buckets nicht verfügbar
- Server/Applikationen in der Cloud
  - Zugriff auf einzelne SaaS Applications gestört
    - Welche Geschäftsprozesse sind davon abhängig?
    - Kein Einfluss auf Recovery Zeit
  - Funktionieren Produktionsanlagen auch autonom ohne Cloud-Anbindung/Internet?

- Services in der Cloud
  - SSO
    - IDP / EntraID geht nicht, MFA geht nicht (Duo, MS Authenticator, …)
    - nichts geht mehr!
    - Beispiel
      - 29.10.2025, 8h Ausfall
    - ➔ Break-Glass Accounts für Admins
    - ➔ Redundanter IDP
      - Alle Applications müssen enrolled werden!

Unterschiede Cloud ⇔ on-premises

Vorteile Cloud

- Skalierbarkeit
- Kann schnell Ressourcen zur Verfügung stellen
- Weltweite Redundanz
- Kosten?

Unterschiede Cloud ⇔ on-premises

Nachteile Cloud

- Keinen Einfluss auf Verfügbarkeit
  - Krankenkasse: Change Freeze im Herbst
- Keinen Einfluss auf Recovery-Geschwindigkeit und Priorisierung
- Versteckte Abhängigkeiten, von denen ich nichts weiss
  - Beispiel:
    - Onlineshop ➔ SaaS: Zahlungsdienstleiter ➔ läuft in AWS
- Shared Responsibility Model
  - Cloud Provider: security **of** the cloud
  - Kunde: security **in** the cloud
    - Daten Backup
    - ➔ Kann ich meine Daten überhaupt exportieren?
- Kosten?
- Abhängigkeit / Vendor Lock in
  - durch proprietäre Schnittstellen, Datenformate, …

Komplettausfall

Gründe (1/2)

- Menschliches Versagen, fehlerhaftes Software Update / Konfigurationsänderung
  - Cloudflare 5.12.2025, 28% des Cloudflare HTTP WAF Traffics (“nur” 25 Minuten Unterbruch)
  - Cloudflare 18.11.2025, 5h Unterbruch
- Katastrophen
  - März 2021, Brand bei OVH (Strassburg)
  - März 2026 Iran greift AWS Datacenter in den Vereinigten Arabischen Emiraten und Bahrain an
- Anbieter pleite oder stellt Geschäftsbereich ein
  - Insolvenz von UKCloud: spezialisiert auf Services für den öffentlichen Sektor in UK
- Preissteigerungen
  - Preise für E5 (laut MS Copilot)
    - 2015: Office 365 E5: 35$ /User/Monat
    - 2022: +63%
    - 2026: Microsoft 365 E5: 60$ /User/Monat
    - Total +71%
    - +5% /Jahr

Teuerung: ~+8%

Komplettausfall

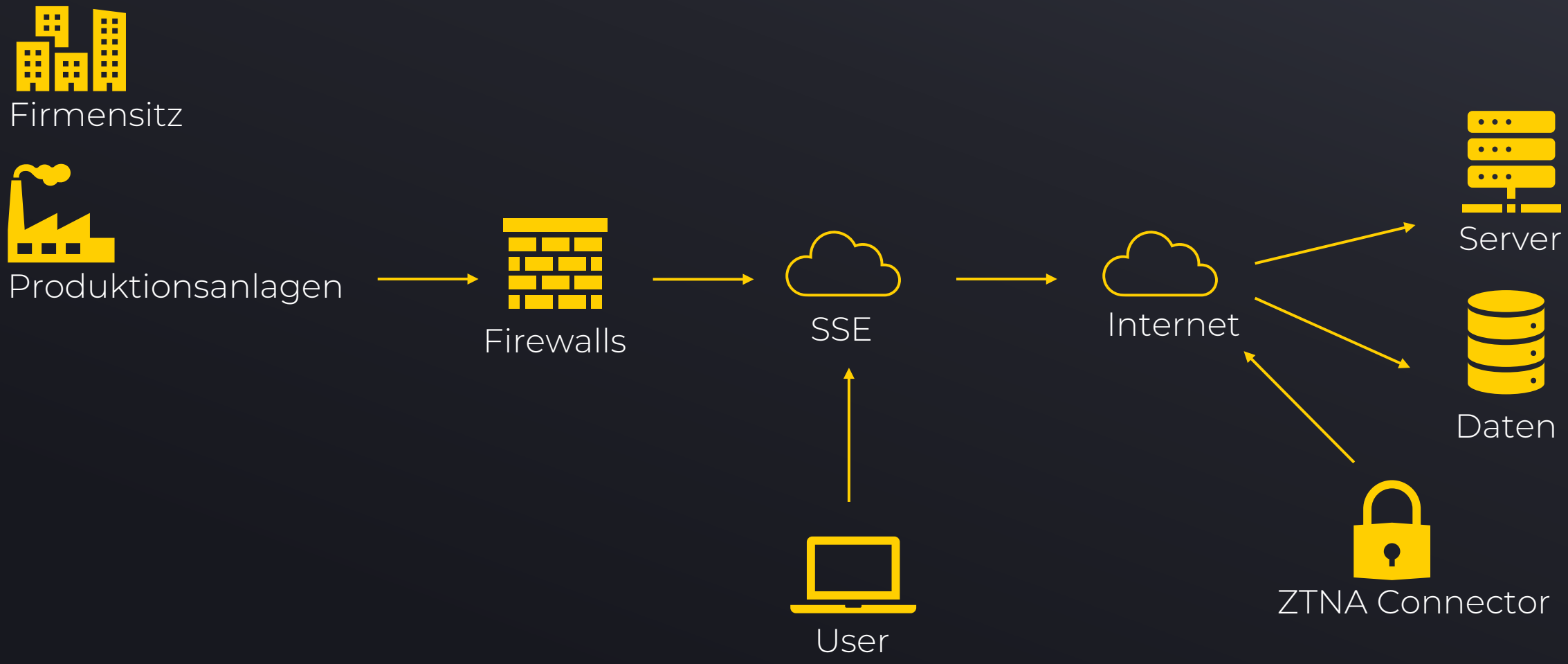
Gründe (2/2)

- Will / kann / darf Service nicht mehr anbieten
  - Privacy Shield bietet kein angemessenes Datenschutzniveau gemäss DSG ➔ keine unverschlüsselten Personendaten der Behörden in US Clouds
    - Wegen Cloud Act, FISA 702 (Foreign Intelligence Surveilance Act)
  - Broadcom kündigt "Vmware Cloud Service Provider"-Programm (VCSP) in Europa
    - Viele Europäsche Cloud Anbieter, welche Vmware einsetzen, können ihre Services nicht mehr erbringen, bzw. müssen auf einen anderen Hypervisor migrieren
  - IStGH Internationaler Strafgerichtshof in Den Haag
    - Behandelt Völkermord, Verbrechen gegen die Menschlichkeit und Kriegsverbrechen
    - Sanktionen der US-Regierung u.a. gegen Chefankläger Karim Khan
    - MS sperrte Zugriff auf Exchange Online Postfach
    - ➔ Migration zu OpenDesk
    - ➔ Sovereign Cloud
      - Achtung: Angebote der grossen US Hyperscaler sind Augenwischerei
        - Auch wenn die Daten auf europäischen/Schweizer Servern liegen kann die US Regierung trotzdem Einfluss nehmen
      - ➔ Wir brauchen echte lokale Anbieter

Shift to the Cloud

“alles” in der Cloud

AVANTEC
Competence. Security. Trust.



Shift to the Cloud

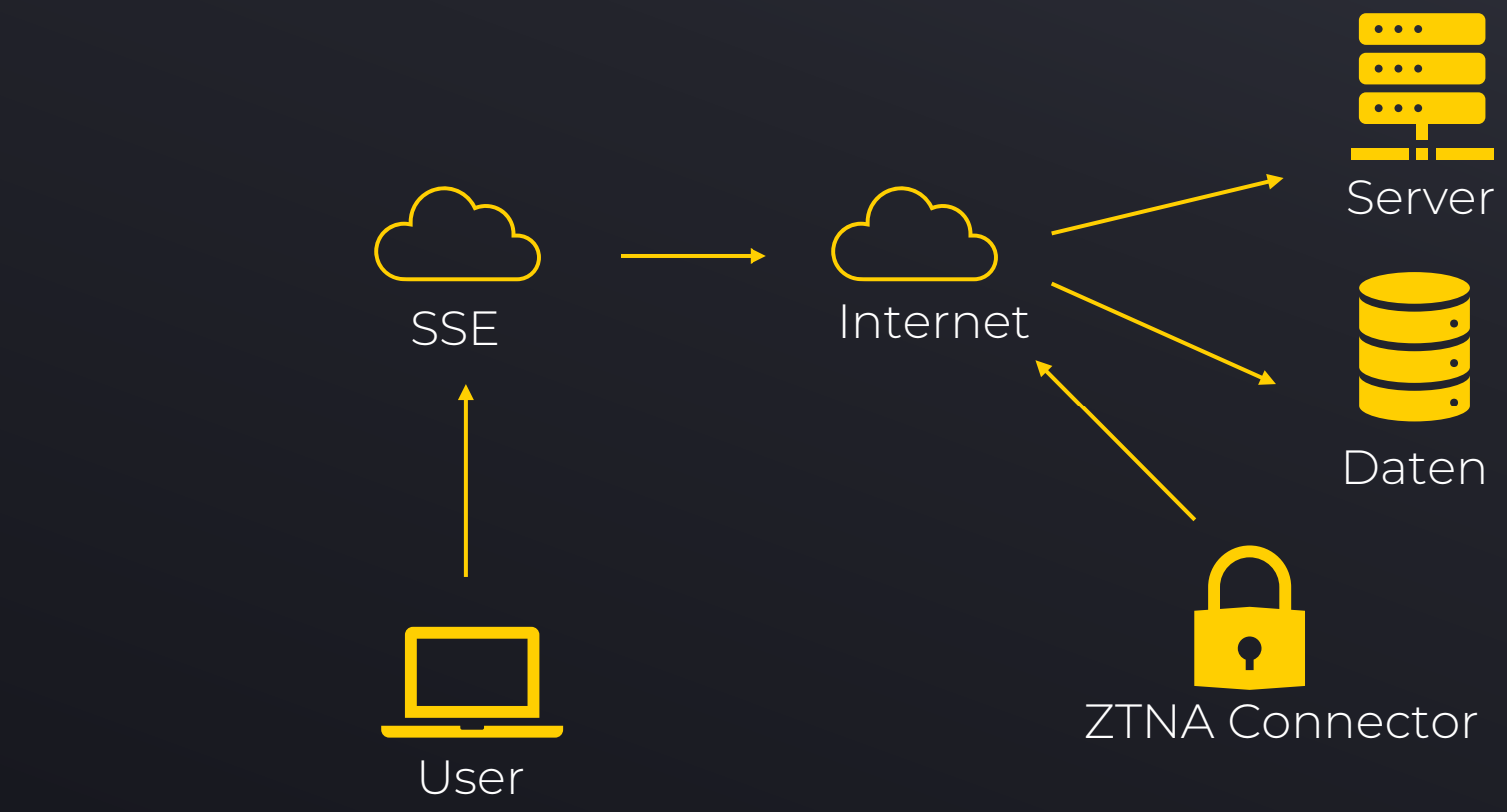
“alles” in der Cloud

AVANTEC
Competence. Security. Trust.

- Ein Cloud Anbieter
  - Verschiedene availability zones / weltweite Redundanz
    - ➔ Kosten!
    - ➔ Daten dauernd replizieren
- Mehrere Cloud Anbieter
  - Virtuelle Maschinen lassen sich relativ einfach bei einem anderen Provider hochfahren
    - ➔ Infrastructure as code
    - ➔ Planung / Vorbereitung / Basis Infrastruktur muss vorhanden sein
    - ➔ VMs bei Bedarf hochfahren
    - ➔ Daten dauernd replizieren
  - Cloud native / serverless Applikationen
    - Man muss schon bei der Entwicklung darauf achten, dass die entsprechenden Schnittstellen / Funktionen der verschiedenen Anbieter unterstützt werden
    - Vorteil: ➔ Pay per use, kostet nur, wenn die Funktion ausgeführt wird

Was haben wir alles vergessen?

AVANTEC
Competence. Security. Trust.



Was haben wir alles vergessen?

AVANTEC
Competence. Security. Trust.

- DNS
  - Wo sind die DNS Server meiner eigenen Zonen?
  - Im Desaster Fall muss ich DNS Einträge ändern können
  - Oder die DNS Zonen zu einem anderen Anbieter umbiegen
    - Dazu brauche ich den Registrar
    - Ist oft identisch mit dem DNS Server Betreiber
  - Beispiel: Webland
    - Hoster für KMU, 75’000 Domains
    - Ende November 2025: Ausfall für ~3 Wochen wegen defektem Storage
- Intune
  - Client Management
  - Das einzige, was nicht in der Cloud ist, sind die Endgeräte
  - Ohne Intune kann ich diese nicht managen, updaten, Compliance Checks

Was haben wir alles vergessen?

AVANTEC
Competence. Security. Trust.

- Indirekte Abhängigkeiten
  - Auch meine Cloud Anbieter nutzen weitere Cloud Services
    - Rund 70% des Webtraffics läuft über einen CDN Anbieter
      - Cloudflare: 30% der fortune 1'000 Unternehmen, 25Mio Websites
      - Fastly
      - Amazon Cloudfront
      - Akamai
    - Beispiele:
      - Github, ChatGPT, Confluence, Trello, … bei AWS
      - Zahlungsanbieter Stripe bei AWS
      - Transport
        - DHL bei Azure
        - Post bei AWS/Azure

Fazit

Abhängig von der eigenen Situation

AVANTEC
Competence. Security. Trust.

- Analog zu “klassischen” Desaster Szenarien
  - Redundanz
    - SaaS
      - ➔ Option zum Umzug zu alternativem Anbieter
        - Agilität
      - ➔ mehrere IDP, “ohne EntraID geht gar nichts”
    - IaaS
      - ➔ mehrere Availability Zones
  - Cold Standby
    - ➔ Infrastruktur bei zweitem Cloud Anbieter (IaaS, PaaS, SaaS)
    - ➔ Oder on-premises
  - Multi Vendor Strategie ➔ weitere Anbieter, in unabhängiger Jurisdiktion?
  - Getestetes Backup/Restore!
    - Ein RAID ist kein Backup
    - Ein S3 Bucket ist kein Backup
    - Nicht nur für Daten der “eigenen” Cloud Infrastruktur sichern!
    - Auch für Daten in SaaS Diensten (Exchange Online, SharePoint, ServiceNow, …)

Fragen / Diskussion

AVANTech-Day 2026

AVANTEC
Competence. Security. Trust.

DANKE

BeyondTrust · CHECK POINT · CROWDSTRIKE · digicert · netskope · THALES · tenable · xorlab · zscaler

AVANTEC
Competence. Security. Trust.

Nächste Session 14:45

Session 3

Zero Trust Branch (ZTB) mit Airgap – wozu ist das gut? — **Holdener, 5. OG**
Produkt: zscaler
Referenten: René von Arx, Raffael Späni

Thread Huntig Deep Dive: Von Hypothese zu Detection Engineering — **Frei, 4. OG**
Produkt: CROWDSTRIKE
Referent: Alessandro Salucci

Disaster Recovery im Cloud-Zeitalter — **Lehmann Steingruber, 5. OG**
Produkte: zscaler netskope
Referent: Matthias Geiser

Authentication – passwordless, strong, secure — **Odermatt, 4. OG**
Produkt: THALES
Referent: Dirk Gluch

Zscaler Automatisierung — **Cancellara, 4. OG**
Produkt: zscaler
Referent: Christian Schnittert

AVANTEC
Competence. Security. Trust.

Nächste Session 16:00

Session 4

Was ist PAM mit Zero Standing Privileges (ZSP)? — **Frei, 4. OG**

Produkt: BeyondTrust
Referenten: Michael Scherzinger, Jessica Warland

Kontrolle und Schutz im Zeitalter von KI – Der Zscaler-Ansatz für GenAI Security — **Cancellara, 4. OG**

Produkt: zscaler
Referent: Jonas Kugler

How to deploy Check Ponit SASE in 30 minutes — **Holdener, 5. OG**

Produkt: CHECK POINT
Referent: Tobias Wälchli

Einblick ins Cyber Defence CenterPRA — **Odermatt, 4. OG**

Referent: Tobias Balschun