ELLY

Der 'Plan B' - Aufrechterhaltung der Funktionsfähigkeit bei Ausfall der Cloud

Roman Leuprecht | Uniki GmbH

Übersicht

1. Über uns
2. Der Ausfall von OVH am 09.11.2017
3. Learnings & Umsetzung
4. Der Ausfall von OVH am 10.03.2021
5. Learnings
6. Single Points of Failure
7. Takeaways

Über uns

MIT ELLY DIE CLOUD VOR ORT

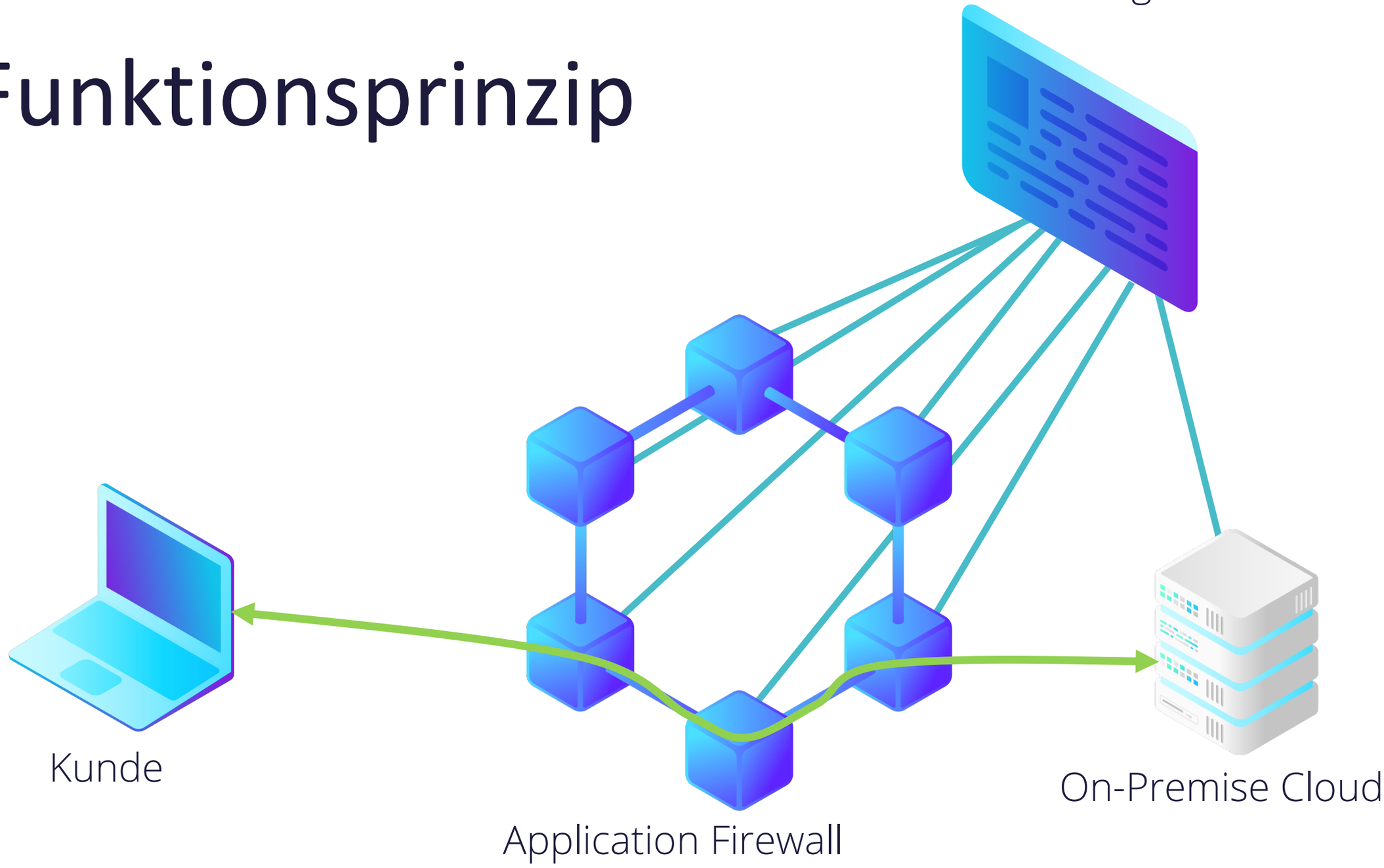
Uns gibt es seit 5 Jahren und wir betreuen über 300 Kunden im DACH Raum mit On-Premise Cloud Infrastrukturen. Dabei liegt der Fokus auf Datenhoheit, Open-Source und Hybrid-Cloud Lösungen.
Server beim Kunden vor Ort sind bei uns Standard, nicht die Ausnahme.

Prinzipiell sind wir ein Rechenzentrum, nur der Server steht beim Kunden vor Ort.

Unsere Strukturen in der Cloud

- Hinter „On-Premise aber sorglos“ steckt viel Cloud-Magie
- Alle Kundendeployments sind über eine Application Firewall erreichbar, ohne diese kein Zugriff von außerhalb des Firmennetzes
- Server melden sind an Cloud-Diensten an
  - Beziehen Updates
  - Melden sich an der Firewall an
  - Melden Diagnosedaten

Funktionsprinzip

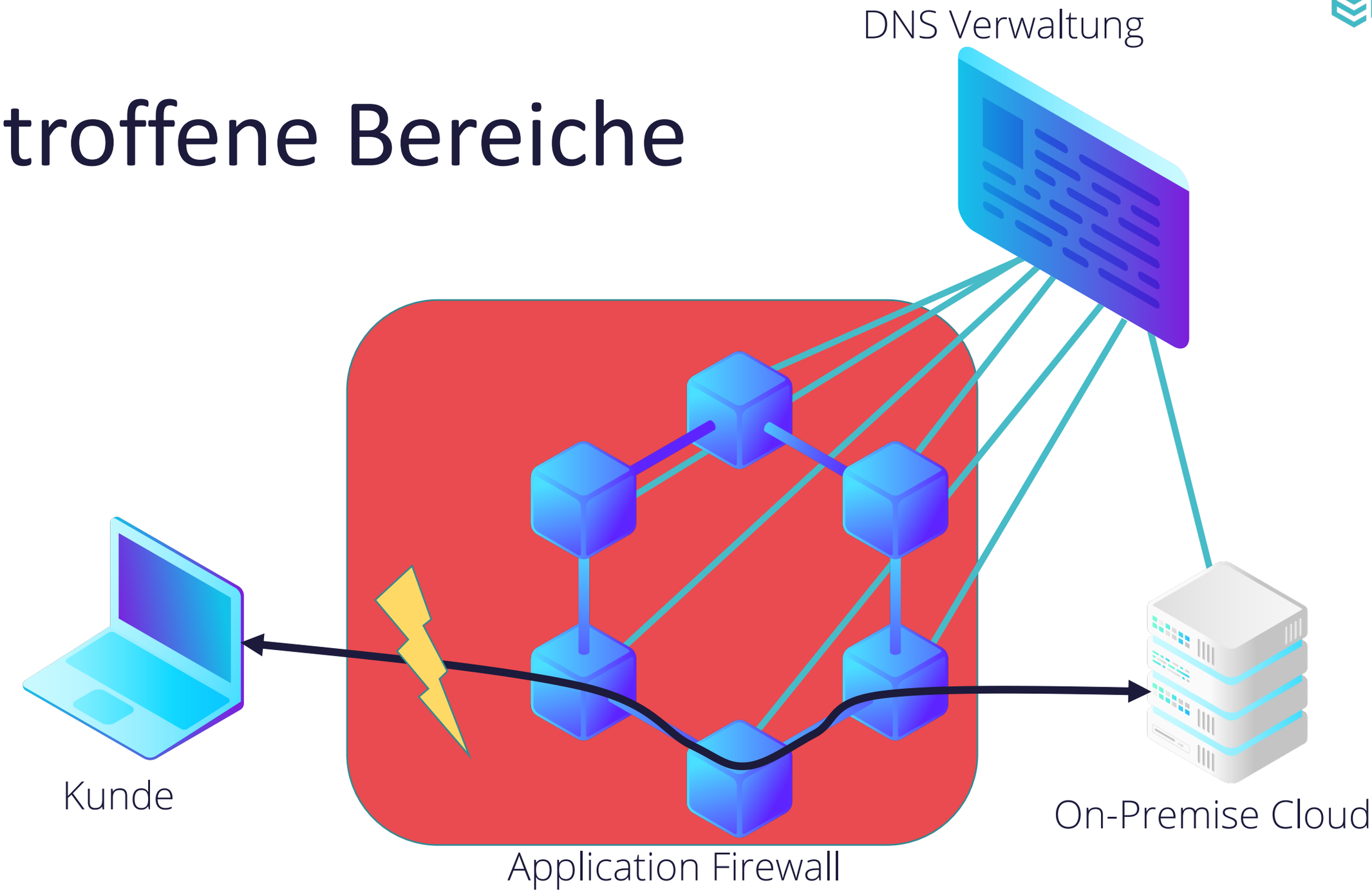


09.11.2017

STROMAUSFALL IM RECHENZENTRUM SBG

- Ausfall findet in der Hauptarbeitszeit um 11 Uhr Vormittags statt
- Komplettes RZ ohne Strom

Betroffene Bereiche



Folgen

STROMAUSFALL IM RECHENZENTRUM SBG

- Hauptserver nicht erreichbar
- Kein automatischer Failover eingerichtet
- Kein Kunde erreichbar für ca. 3h
- Währenddessen komplett neue, parallele Infrastruktur installiert
- DNS funktioniert und erlaubt Umstellung auf neue Infrastruktur in anderen RZs

Learnings

STROMAUSFALL IM RECHENZENTRUM SBG

- Systeme müssen automatisiert provisionierbar sein
- Provisionierung nach Rollen ist wichtig
- Konfiguration nicht festgelegt, sondern mit zentralem Dienst
- Einfache Lösung = bessere Lösung
- DNS ist enorm robust
  - Aber Achtung: TTL einplanen!
- Failover nützt nur etwas, wenn er automatisch abläuft

Umsetzung

STROMAUSFALL IM RECHENZENTRUM SBG

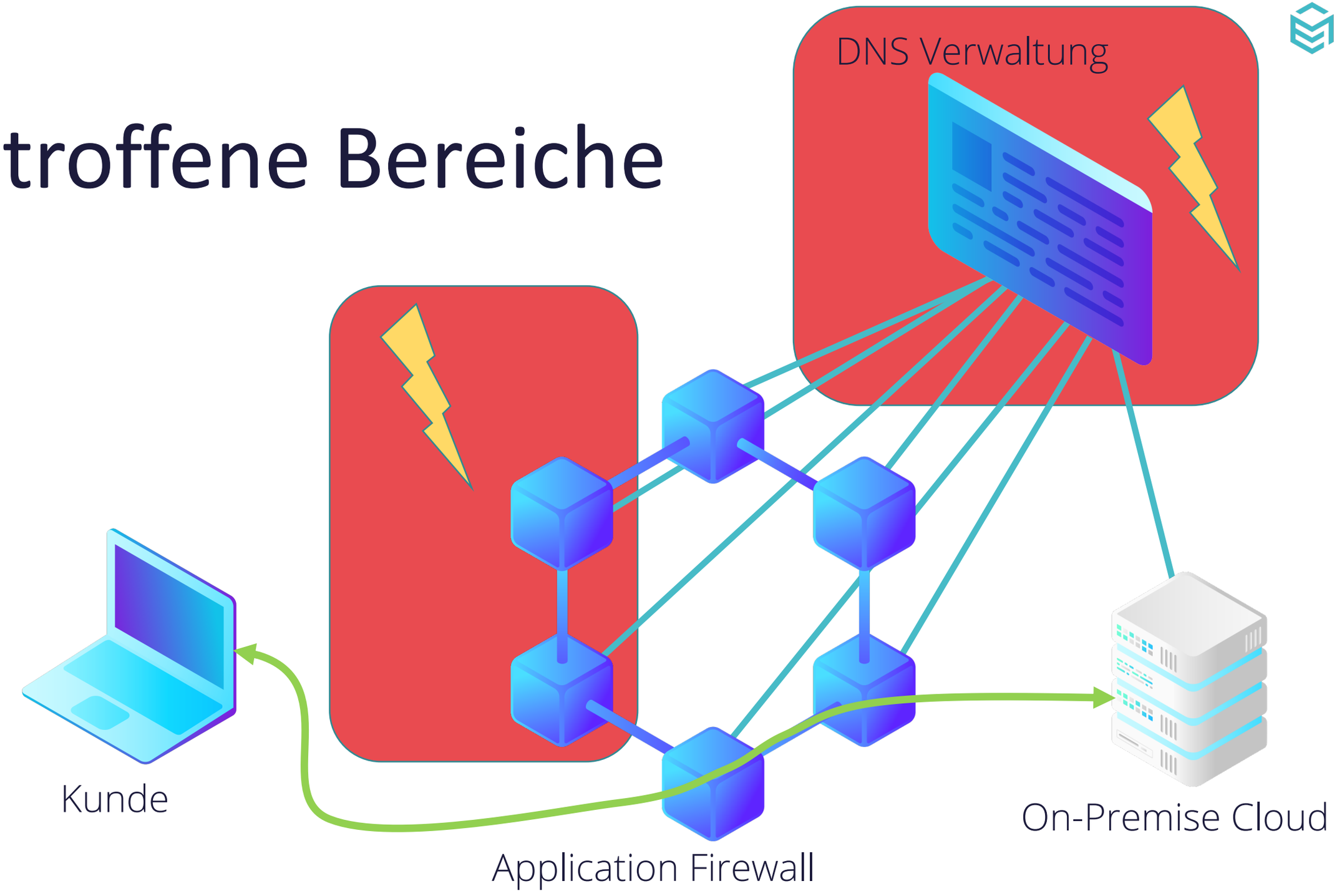
- Provisionsskripte für jede Art von Server
- Dopplung der Dienste: Fast jeder Server bietet jeden Dienst
- Buchung weiterer Hardware in anderen RZs bei anderen Dienstleistern
  - Vorgabe: 1 Maschine pro Standort und Dienstleister
  - Mind. 6 Maschinen vorhalten
- Automatischer Failover via Monitoring

10.03.2021

BRAND IM RECHENZENTRUM SBG

- Brand bricht um 0.40 Uhr aus und zerstört den gesamten Block SBG-2
- Alle Server in SBG-2 -> Totalverlust
- Monitoring schlägt um 1.29 Uhr an und detektiert Hauptserver als offline.
- Automatischer Failover springt an und ist ab 1.44 Uhr aktiv
- Kunden ohne Spezialsetup bemerken den Ausfall nicht
- Nur Hintergrundarbeiten sind zu erledigen

Betroffene Bereiche



Folgen

BRAND IM RECHENZENTRUM SBG

- Für 80% aller Kunden… keine
- Für die restlichen 20%:
  - Alle Anwendungen funktionstüchtig
  - Keine Erreichbarkeit der Adminoberfläche bis zur Umstellung der IP-Adressen im Kunden-DNS
- Datenbank-Cluster musste im Hintergrund neu initialisiert werden

Ein voller Erfolg

Learnings

BRAND IM RECHENZENTRUM SBG

- Automatischer Failover hat funktioniert
- DNS Einstellung des Providers (OVH) war überlastet und hat sich als Single Point of Failure herausgestellt
- Datenbank-Cluster war viel manueller Aufwand, hier ist eine bessere Lösung notwendig
- Kein Datenverlust dank Multi-Cloud Strategie

Single Point Of Failure

VERTEILTE SYSTEME IN DER PRAXIS

- Echter „Multi-Master“ ist selten
- Oft ein Master oder „versteckter Master“
- Oft ist BGP und eigenes ASN keine Option
- Provider bieten nur interne Failover-IP
- Multi-Cloud-Multi-Master ist eine Herausforderung die nur selten gemeistert wird

Single Point Of Respon-sibility

DAS 1x1 DER CLOUD PROVIDER

- SPOF lässt sich oft nicht vermeiden
- Verteilung der SPOF auf verschiedene Provider notwendig
- Pidgeonhole Principle: Mehr Provider als SPOF notwendig
- Jeder Provider erhält einen SPOF im System

Provider als SPOF

WENN SICH DER SPOF VERSTECKT

- Auch Provider betreiben komplexe Systeme
- Wechselwirkungen im Fehlerfall oft nicht mit einberechnet
- Beispiel: Ein Fehler im Directory Service eines großen Provides verhinderte im März die Anmeldung an vielen Diensten, inkl. Der Admin-Konsole und der Bürosoftware
- Failover-Systeme müssen so gut es geht von Provider SPOF unabhängig sein

Menschen als SPOF

BEREITSCHAFT? DIE SCHLÄFT SCHON

- Jeder Zwischenfall benötigt Intervention oder zumindest Monitoring
- Ist eine Person evtl. ein SPOF?
- Wissen und Verhalten im Notfall müssen mehrere Mitarbeiter kennen
- Was wenn der Admin krank ist?
- Redundanz & Fallbacks sind hier genauso wichtig

Takeaways

REDUNDANZ SCHAFFEN IN DER SOFTWARE

- Einfachste Lösung: Mehrere Instanzen eines Dienstes bei mehreren Providern
- Kommunikation über Standardkanäle wie z.B. TLS ist Pflicht
- ASN & BGP werden selten unterstützt
- Software sollte bei Ausfall einzelner Dienste weiterlaufen (Stichwort Circuit-Breaker)
- Wenn SPOF, dann 1 SPOF = 1 Provider

Takeaways

REDUNDANZ SCHAFFEN IN DER ORGANISATION

- Mehrere Mitarbeiter schulen
- Risikoanalyse bzgl. der Provider betreiben
- Abhängigkeitsanalyse bzgl. der Provider betreiben
- Maschinen arbeiten, Menschen prüfen. Der Failover sollte auch ohne Menschen funktionieren.

Takeaways

TESTEN SIE IHRE STRATEGIE

- Mitarbeiter müssen Wissen abrufbar haben
- Sanitäter müssen trainieren, IT-ler auch!
- Erstellen Sie unterschiedliche Tests, z.B. ohne Nutzung der Cloud-Administration

Egal wie wichtig Ihr Service ist, diese Strategie ist wichtiger, daher:

Ziehen Sie den Stecker und prüfen Sie, ob alles im Fehlerfall funktioniert.

KONTAKT

Uniki GmbH
Freisinger Landstr. 28
80939 München
Deutschland

info@uniki.de

+49 89 215 36 46 70

www.uniki.de

Vielen Dank