Merkblatt:
Geteilte Swiss Cloud Umgebung

Mehrere Organisationen teilen ein System

Benutzerverwaltung, Datenspeicher und Störungen
- Eine gemeinsame Benutzer-, Gruppen- und Rechteverwaltung (gleiches Active Directory).
- Jede Organisation hat einen eigenen Datenspeicher, jedoch befindet er sich auf dem gleichen geteilten System.
- Störungen können sich auf alle Organisationen auf einem geteilten System ausbreiten (auch wenn dies nur von einer Organisation verursacht wurde), dies betrifft auch Ransomware.

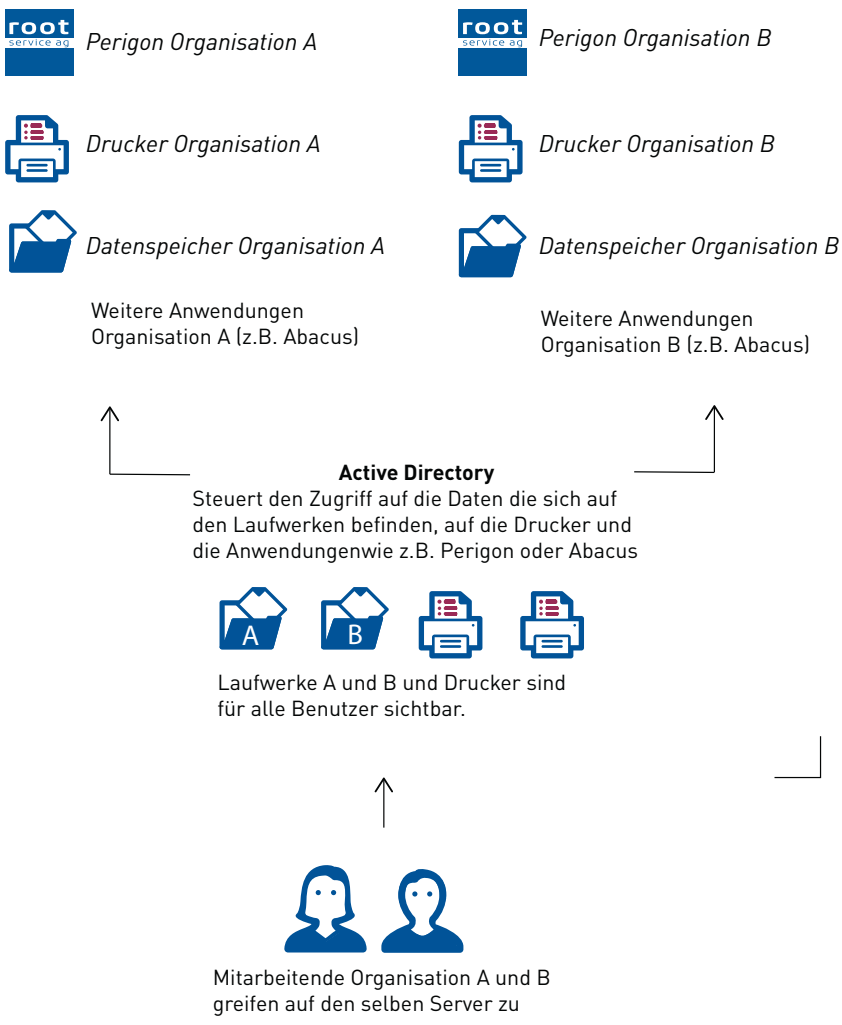
gesteuerter Schutz von:
- Datenablage
- Drucker
- Perigon o.a. Anwendungen

Wartungsaufgaben
- Können nur gemeinsam erfolgen wie bspw. Server-Neustart.
- Programm- und Windowsupdates müssen gemeinsam gemacht werden. Betrifft bspw. Abacus.

Erweiterte Schutzvorkehrungen
- Eine MFA-Lösung für die Windows Anmeldung kann nur umgesetzt werden, wenn die Organisation einen eigenen Terminal-Server innerhalb des geteilten Systems besitzt.

Mit Berechtigungen und Gruppenrichtlinien

Mehrere Organisationen teilen ein System



Ro-ot Service AG
UID: CHE-104.695.341
Wydenstrasse 29
8575 Bürglen
+41 (0)71 634 80 40

info@root.ch
web.root.ch

Stand 01.08.2023 | Version [01]

Merkblatt:
Geteilte Swiss Cloud Umgebung

Risiken

Konfigurationsfehler
- Durch Konfigurationsfehler im Berechtigungssystem, gibt es keine weitere Schutzvorkehrung gegen die Dateneinsicht der anderen Organisationen auf dem geteilten System.

Störungen
- Störungen (sowie auch Ransomware) verursacht durch andere Organisationen können sich auf das gesamte geteilte System ausweiten.

Datenzugriff
- Logon Scripts sind für alle Teilnehmer grundsätzlich lesbar.
- Alle Active Directory User sind lesbar für die User innerhalb dieser Umgebung.

Interne Bedrohungen
- Obwohl die gemeinsame Benutzer-, Gruppen- und Rechteverwaltung effizient sein kann, besteht das Risiko, dass ein Benutzer innerhalb einer Organisation bösartige Handlungen ausführt und dadurch Zugriff auf die Daten anderer Organisationen in der geteilten Umgebung erhält.

Compliance Risiken
- In einer geteilten Swiss Cloud Umgebung müssen alle Organisationen sicherstellen, dass sie die geltenden gesetzlichen und regulatorischen Anforderungen einhalten, insbesondere in Bezug auf den Datenschutz und die Vertraulichkeit der Daten. Es besteht das Risiko, dass eine Organisation versehentlich gegen Compliance-Vorschriften verstößt und dadurch die gesamte geteilte Umgebung gefährdet.

Empfehlung zur Risikominimierung

Eigener Terminal Server
- Drucker können individuell konfiguriert werden.
- Programmupdates können unabhängig von den anderen Organisationen durchgeführt werden.
- Terminal-Server Neustarts können ohne Einfluss auf die anderen Organisationen durchgeführt werden.

Datenverschlüsselung
- Störungen (sowie auch Ransomware) verursacht durch andere Organisationen können sich auf das gesamte geteilte System ausweiten.

Regelmässige Schulungen
- Logon Scripts sind für alle Teilnehmer grundsätzlich lesbar
- Terminal-Server Neustarts können ohne Einfluss auf die anderen Organisationen durchgeführt werden.

Ro-ot Service AG
UID: CHE-104.695.341
Wydenstrasse 29
8575 Bürglen
+41 (0)71 634 80 40

info@root.ch
web.root.ch

Stand 01.08.2023 | Version [01]