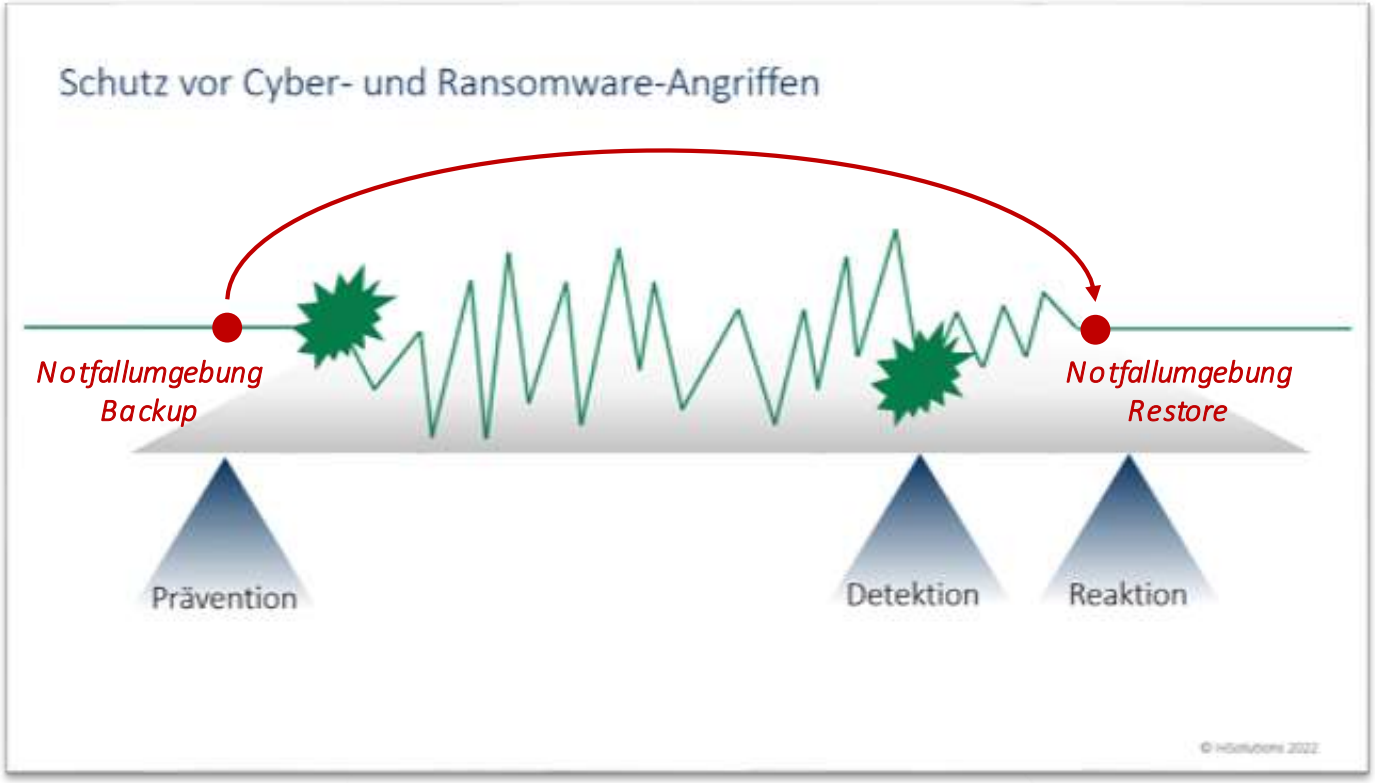
Präventive Notfallumgebung

Im Notfall schneller handlungsfähig sein…

Know-how to go

21. September 2022

Der Sprung "vor die Lage" durch die Notfallumgebung in der Cloud



Der Gedanke dazu ist eigentlich naheliegend, aber häufig nicht klar definiert und/oder umgesetzt

Situation

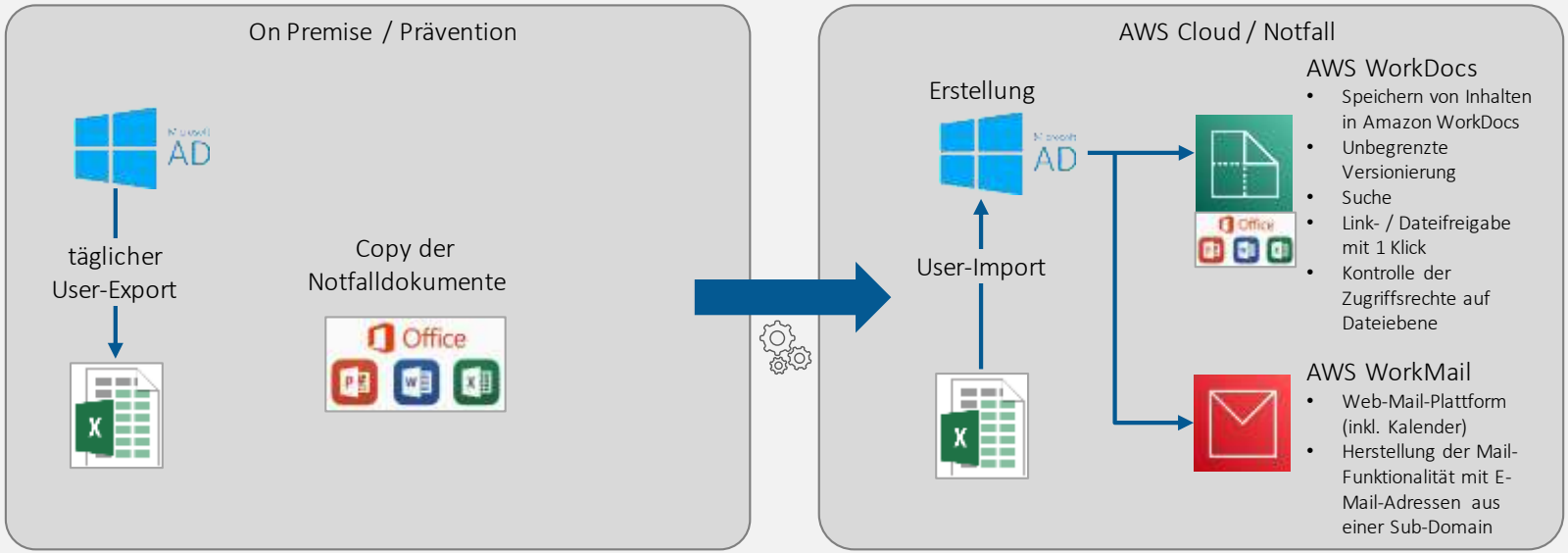
Viele Unternehmen wollen sich besser auf Krisensituationen vorbereiten, sind sich aber nicht sicher, welche Maßnahmen den größten Nutzen bei möglichst geringem Einsatz bieten und im Notfall schnell zur Verfügung stehen.

Lösungsansatz

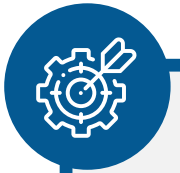
Wir glauben, dass es in einer Krisensituation besonders wichtig ist, möglichst schnell wieder kommunizieren und auf ein (Notfall-)Dokumenten-Set zugreifen zu können, bestenfalls bevor alle notwendigen Aktivitäten zu Vorbereitung und Start eines Notfall-Wiederanlaufs abgeschlossen sind.

Unser Lösungsansatz beinhaltet deshalb E-Mail, Office-Dokumente und ist weitgehend automatisiert

Lösungsüberblick (Elemente)



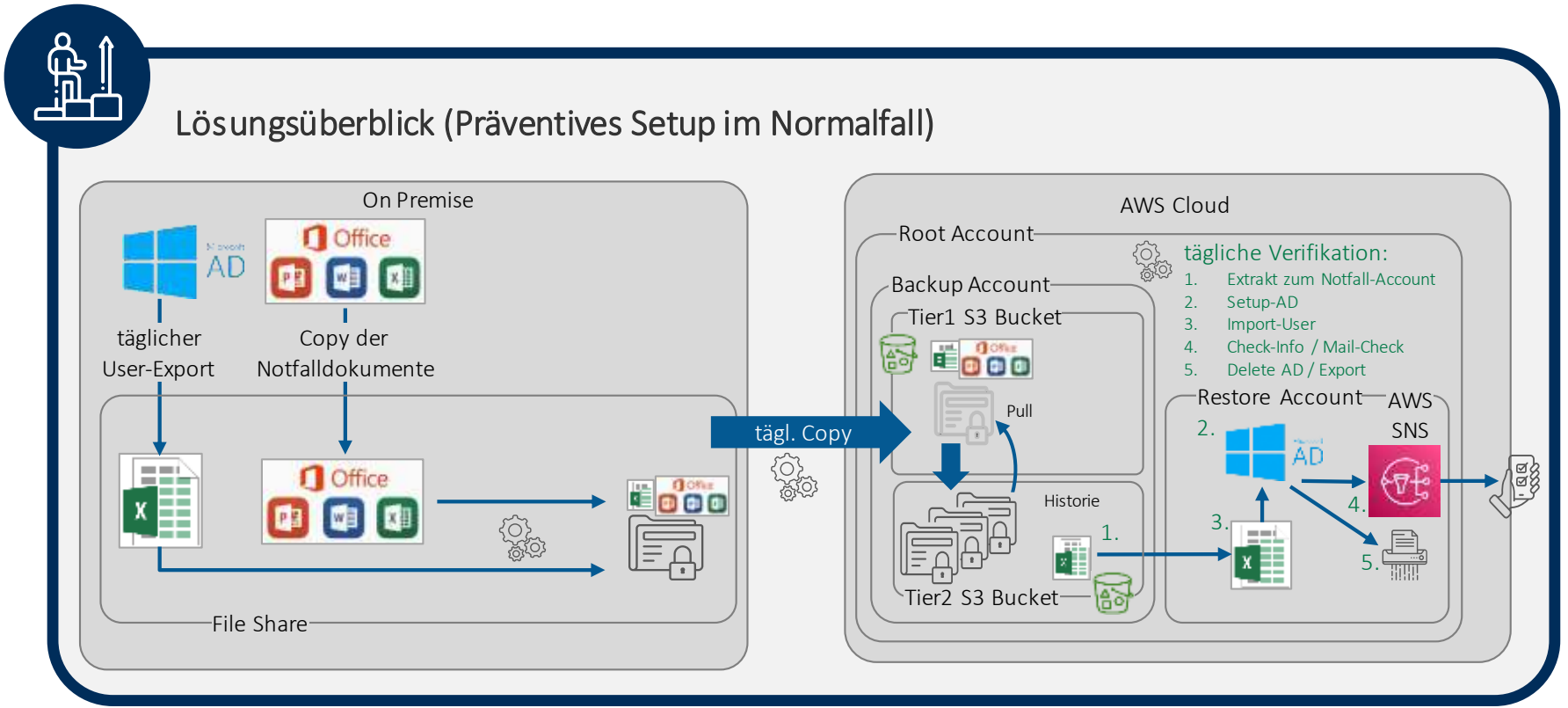
Die Implementierung in der Cloud bietet im Notfall viele Vorteile



Vorteile unseres Lösungsansatzes

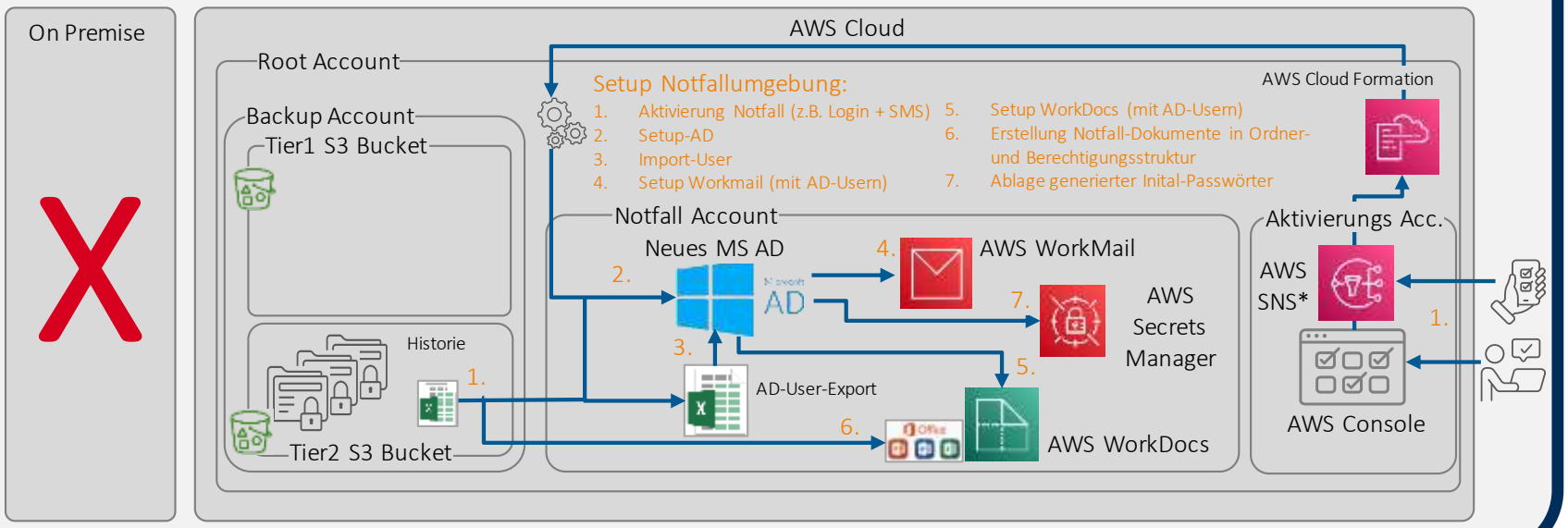
- Mit E-Mail und office-basierten Notfalldokumenten sind die wichtigsten Funktionen für den Notfall abgedeckt.
- Das Notfall-Setup lässt sich innerhalb von Minuten bis wenigen Stunden aktivieren (je nach Anzahl der User). Dazu ist nur ein Notfall-PC mit Internetzugang notwendig.
- Es entstehen im Normalbetrieb nur minimale Kosten für das S3-Bucket und ggf. für die Verifikationsfunktion (vermutlich < 100 EUR / Monat – je nach Datenaufkommen).
- Die Herstellung der Umgebung erfolgt nach der Aktivierung komplett automatisiert.
- Alle Dateien sind in mehrstufigen Accounts sicher in der Cloud abgelegt.
- E-Mail-Adressen aus einer Sub-Domain der bekannten Domain sind weiterhin im Einsatz (auf Wunsch können auch die Original-Adressen verwendet und die MX-Records umgeschaltet werden).
- Der Ansatz lässt sich flexibel erweitern, indem weitere Funktionen integriert werden (z.B. Chat und Telefonie (AWS Chime), Kanban-Board, wichtige (Applikations-) Server, Workflows etc.).
- Der Ansatz lässt sich flexibel auf andere (große) Cloud-Provider migrieren (z.B. Azure, Google etc.).
- Präventiver Einsatz im Projekt und reaktiver Einsatz im IR-Fall möglich

Im präventiven Setup (Normalfall) laufen alle Aktivitäten automatisiert ab.



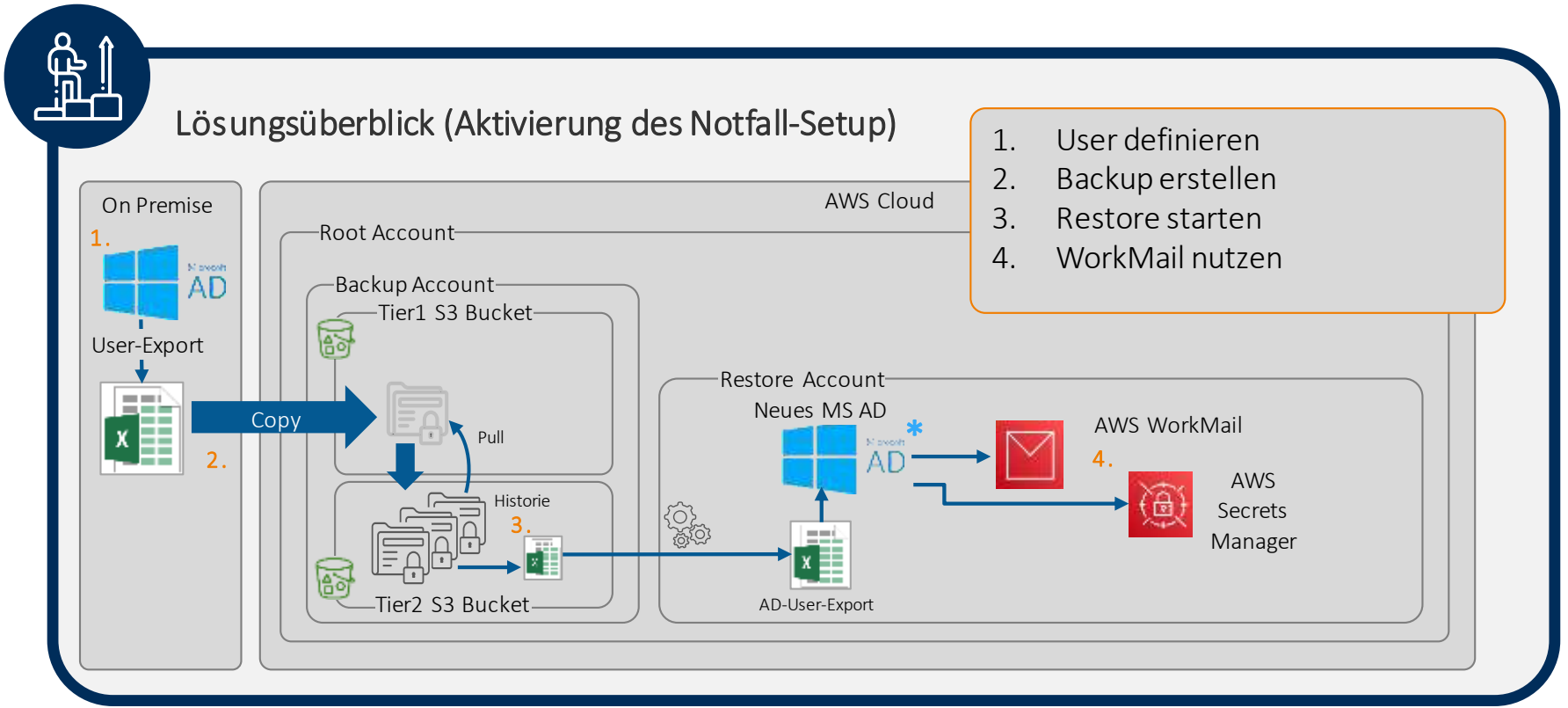
Für die Aktivierung der Notfall-Umgebung können unterschiedliche Mechanismen (parallel) verwendet werden.

Lösungsüberblick (Aktivierung des Notfall-Setup)



* Future Iteration

Scope der Live-Demo: Schwerpunkt AWS WorkMail



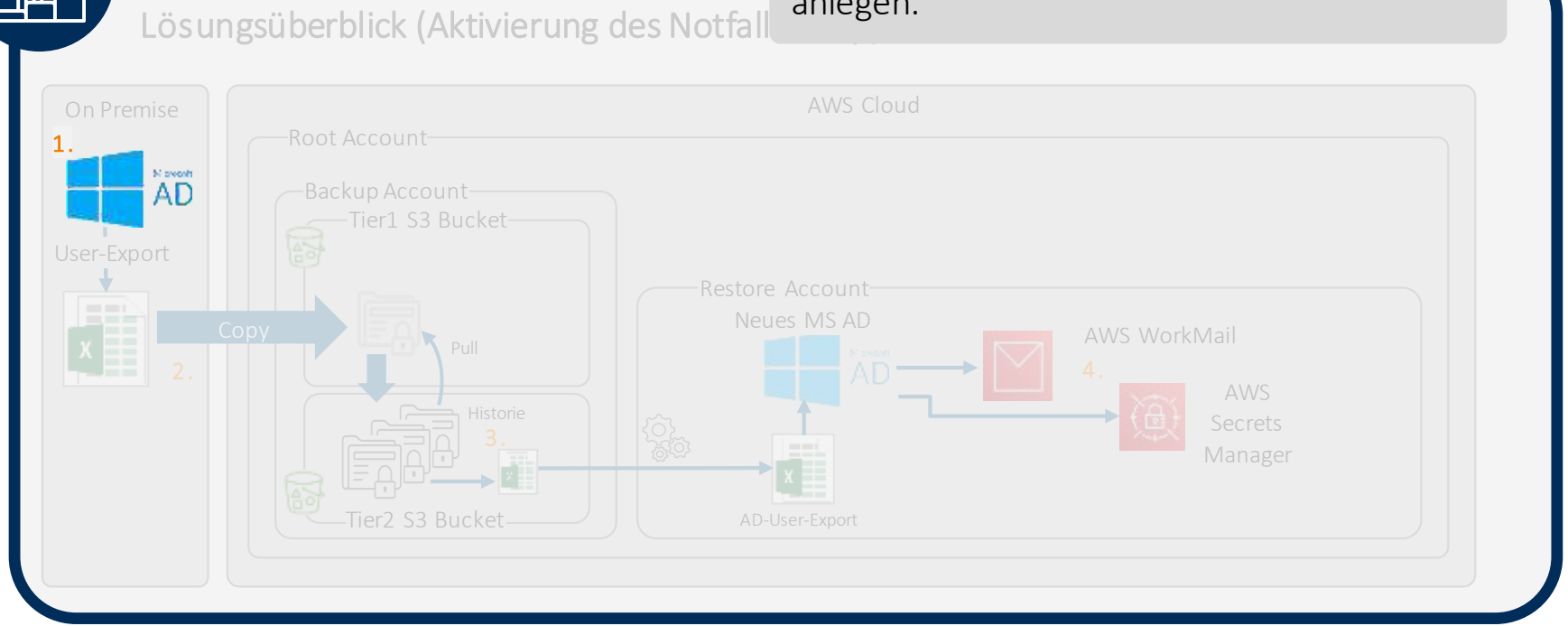
*) In der Demo wird das AWS Simple AD genutzt, um die Zeit für die Provisionierung zu reduzieren

Vorbereitende Schritte (nicht in Demo)

1. AWS Accounts (Backup & Restore) erstellen
2. CloudFormation Stack in Backup-Account provisionieren:
   - Berechtigung des Restore Accounts auf den Backup-Account
   - Erstellung der S3 Buckets in den Accounts
   - Config-Block für OnPrem-AD erzeugen
3. Über CloudFormation Stack Restore-Account-DNS-Setup erstellen
4. Notfall-SubDomain anlegen, an AWS delegieren
5. OnPrem Windows Server VM und AD provisionieren
6. Binary für Backup auf Windows Server VM hinterlegen und über Config-Block konfigurieren

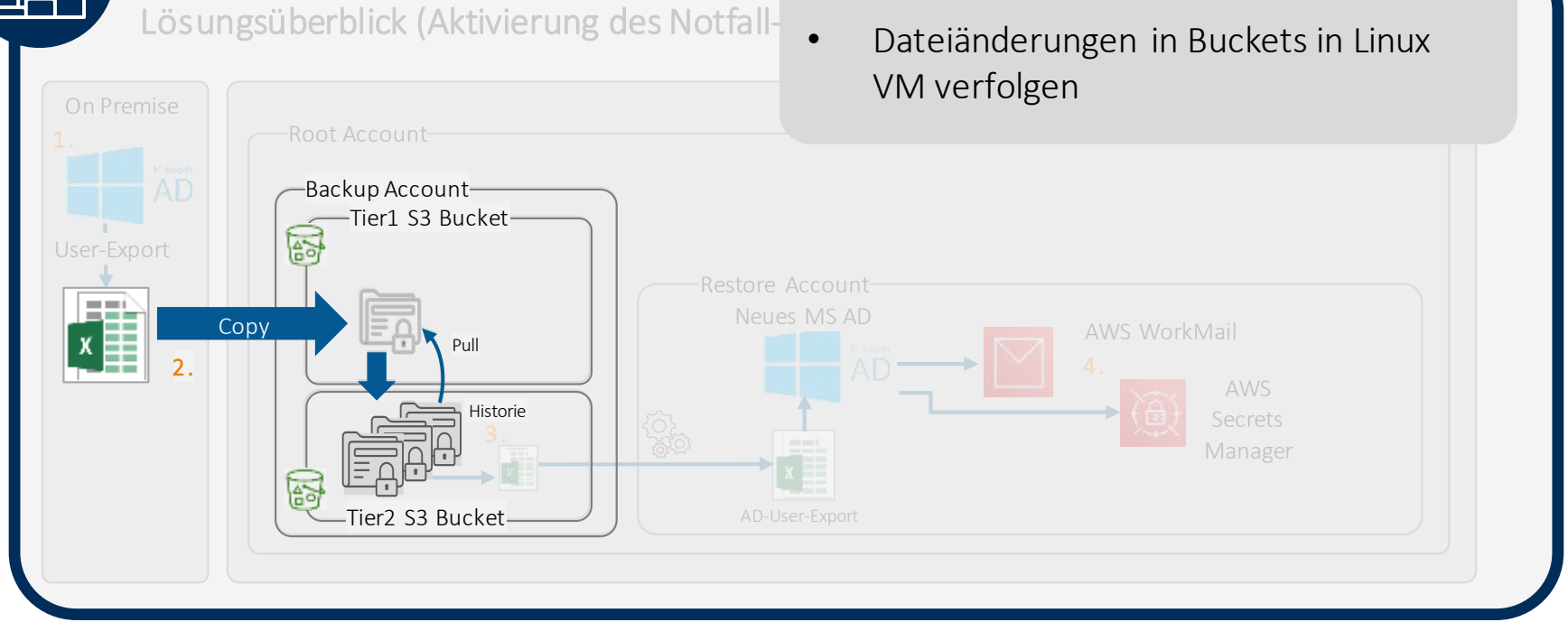
Live-Demo: 1. User definieren

User, die später WorkMail-Zugriff erhalten sollen, in OnPremise AD (Win Server VM) anlegen.



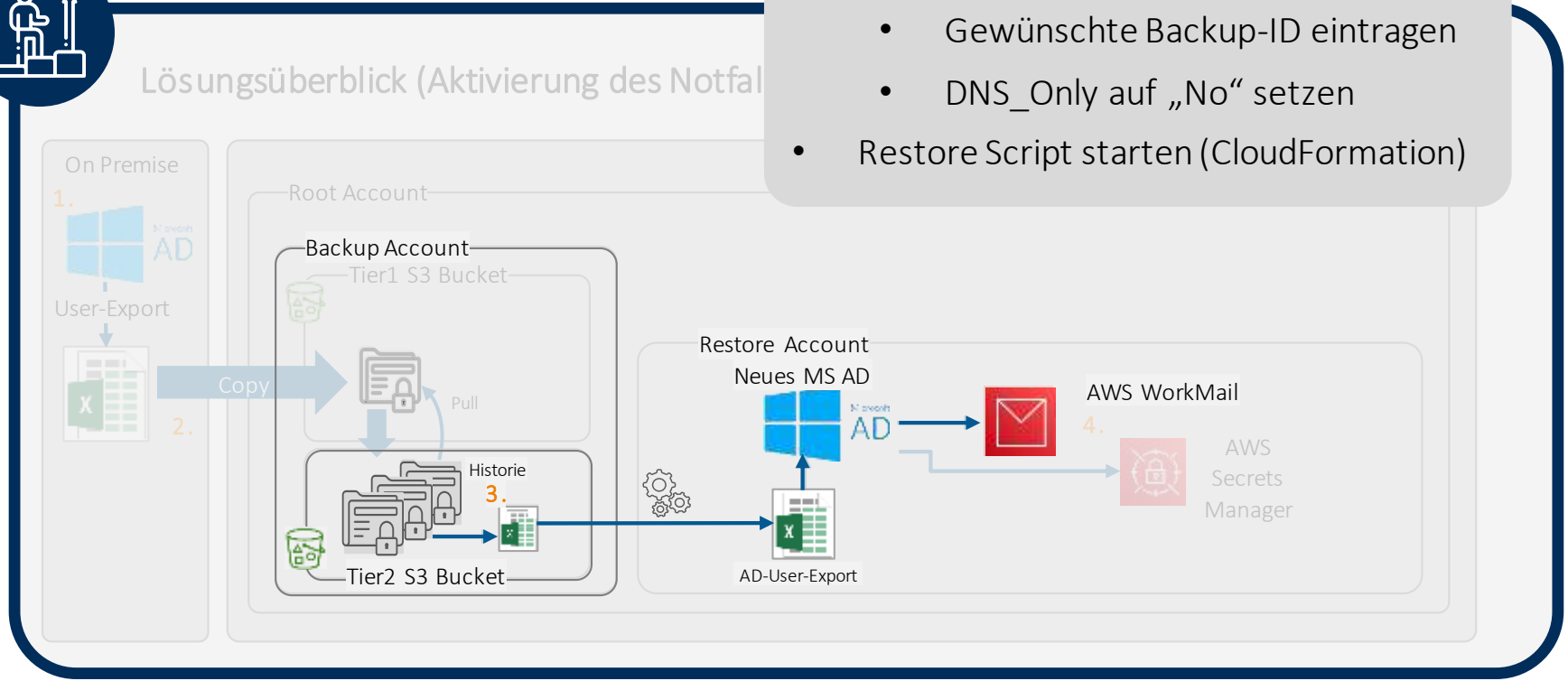
Live-Demo: 2. Backup erstellen

- Backup.exe in Windows Server VM ausführen (ggf. mehrfach zur Erzeugung einer Historie)
- Dateiänderungen in Buckets in Linux VM verfolgen



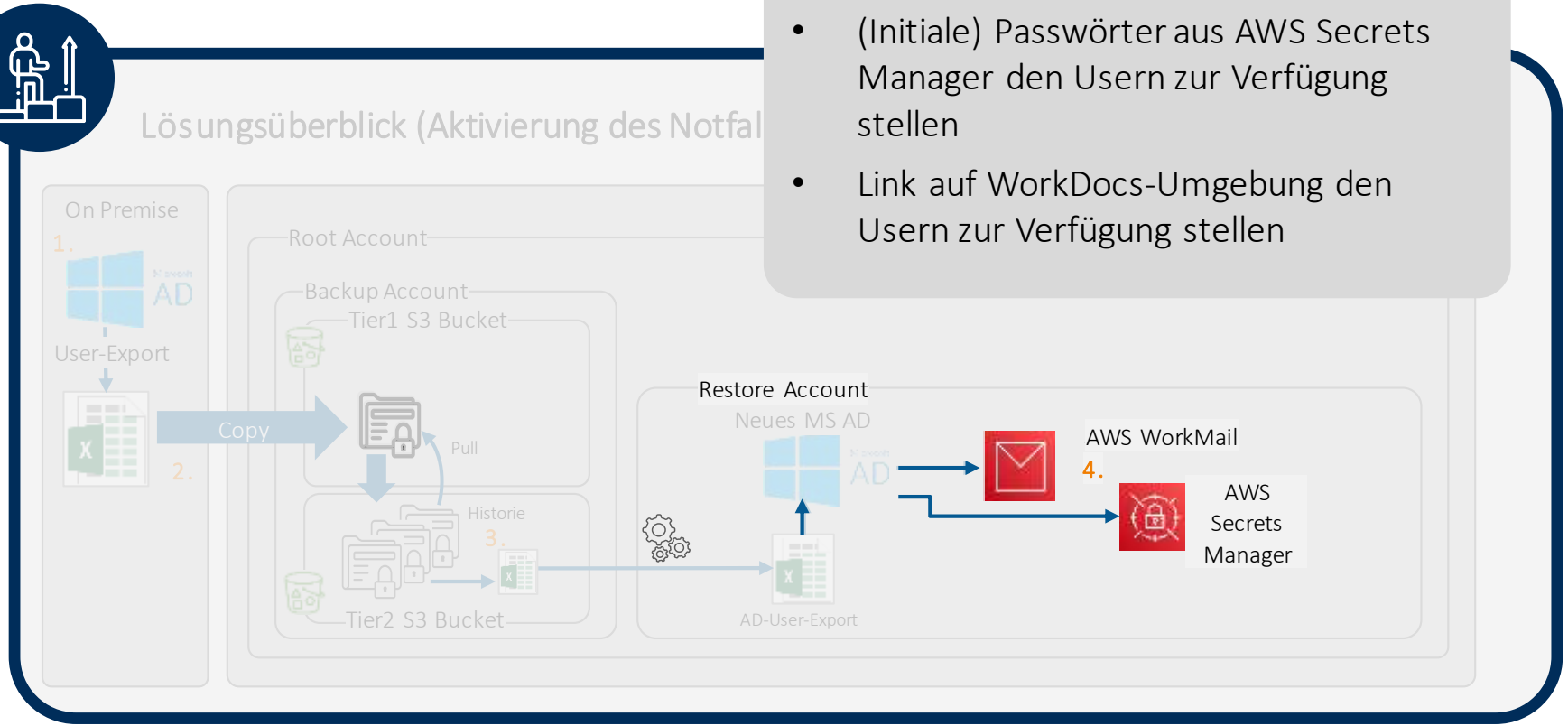
Live-Demo: 3. Restore starten

- Änderungen an Restore-Konfigurationsdatei vornehmen:
  - Gewünschte Backup-ID eintragen
  - DNS_Only auf „No“ setzen
- Restore Script starten (CloudFormation)



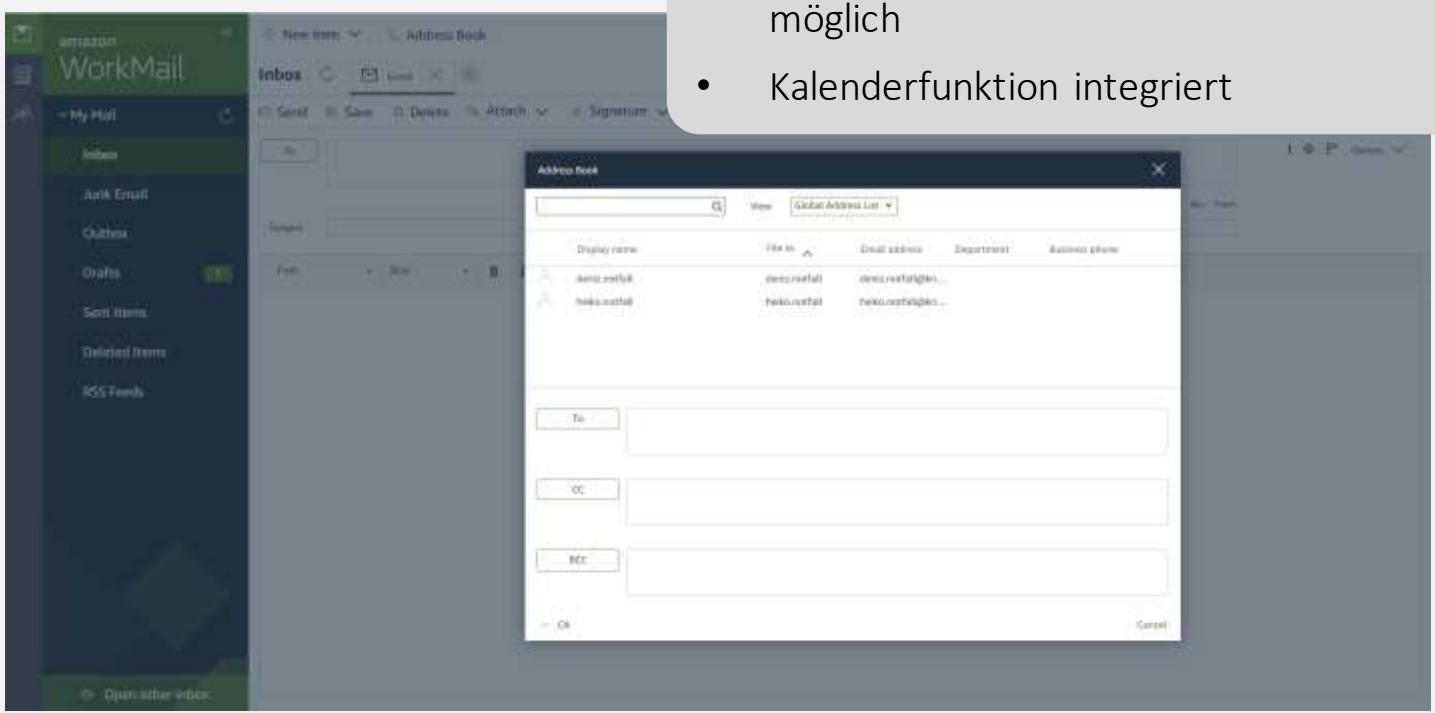
Live-Demo: 4. Workmail verwenden

- (Initiale) Passwörter aus AWS Secrets Manager den Usern zur Verfügung stellen
- Link auf WorkDocs-Umgebung den Usern zur Verfügung stellen



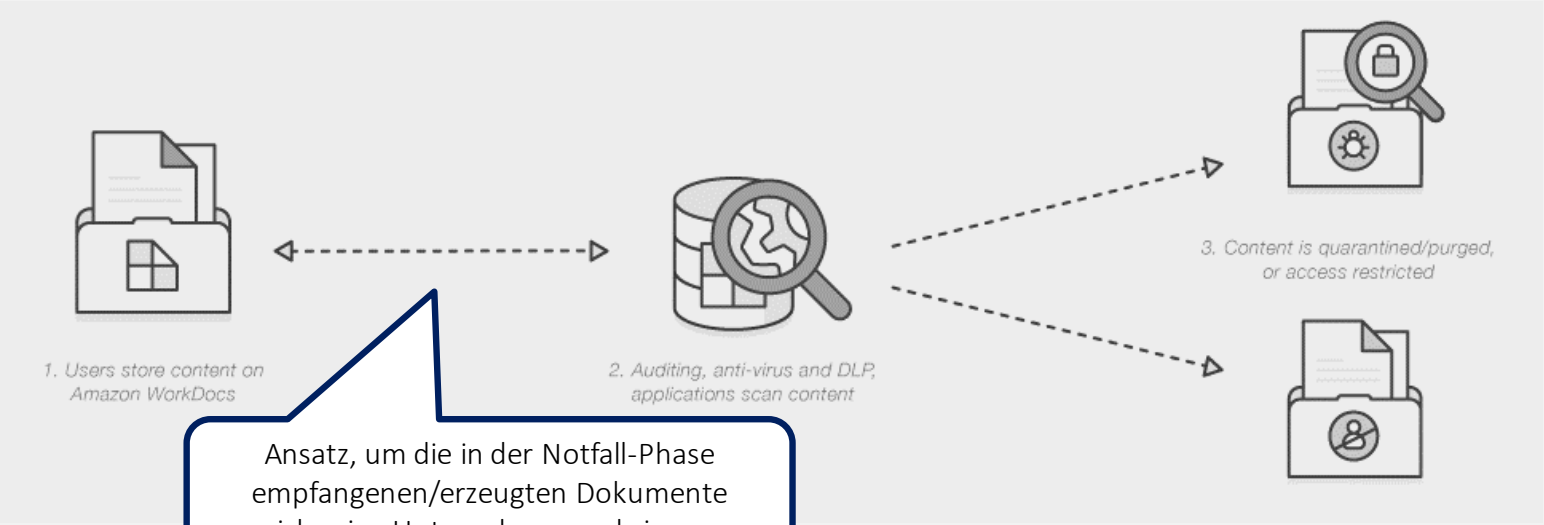
Live-Demo: 4. Workmail verwenden

- Alle provisionierten User sind im Adressbuch sichtbar
- (Externer) Mail-Versand und –Empfang möglich
- Kalenderfunktion integriert



Auf Basis von AWS WorkDocs lassen sich weitere Use Cases in der Notfall-Umgebung verwirklichen.

Integration von Amazon WorkDocs mit Ihren Anwendungen für Sicherheitsprüfungen, Antivirenschutz und zur Vermeidung von Datenverlusten



Ansatz, um die in der Notfall-Phase empfangenen/erzeugten Dokumente sicher ins Unternehmen zu bringen

Auf Basis von AWS WorkDocs lassen sich weitere Use Cases in der Notfall-Umgebung verwirklichen.

Integrieren von Kooperationsfunktionen in Ihr bestehendes Content Management-System

Nutzung eines bestehenden Content-Management-Systems (welches im Cloud-Backup hinterlegt wurde oder in der Cloud läuft; z.B. auch Confluence)

Auf Basis von AWS WorkDocs lassen sich weitere Use Cases in der Notfall-Umgebung verwirklichen.

Mit Amazon WorkDocs eine Prozessmanagement-Anwendung erstellen

Einfache (vor dem Notfall) hinterlegte Workflows die im Notfall genutzt werden können

Zur Überprüfung der Eignung des Ansatzes kann vor die eigentliche Implementierung ein PoC geschaltet werden.

PoC

- Einrichtung von Sub-Accounts innerhalb des HiSolutions AWS-Accounts
- Erzeugung des AD
- Definition und Import von Test-Usern
- Einrichtung von WorkMail & WorkDocs
- Erzeugung einer Demo-Mail-Domain und Umschaltung der Domain auf WorkMail (MX Records)
- Erzeugung von Demo-Dokumenten für die WorkDocs-Umgebung
- Gemeinsamer Workshop zur Nutzung von WorkDocs / WorkMail
- (zum Ende des PoC-Zeitraums) Feedback-Workshop & Entscheidung weiteres Vorgehen

Implementierung im Projekt

- Anlegen und Sichern des AWS-Accounts (Initial-Setup inkl. Subaccounts, SSO, Control-Tower-Aktivierung etc.)
- Gemeinsame Erstellung/Konfiguration der Skripte für Backup, Verschlüsselung und Transport des Exports
- Gemeinsame Erstellung/Konfiguration der Skripte für die Verifikation
- Gemeinsame Erstellung/Konfiguration der Skripte für die Aktivierung der Notfallumgebung
- Gemeinsame Konzeption regelmäßiger Tests
- Gemeinsame Konzeption des Rückbaus der Notfallumgebung
- Aktivierung und Test der Backup-Funktion inkl. Verifikation
- Aktivierung und Test der Notfallumgebung (mit angepasstem Backup)

Team DevOps & Cloud Transformation
(Hansgeorg Langhorst / Heiko Müller)

Schloßstraße 1 | 12163 Berlin

info@hisolutions.com | +49 30 533 289 0

www.hisolutions.com