[1 Einführung 2](#_Toc499801411)

[1.1 Zweck des Dokuments 2](#_Toc499801412)

[1.2 Umfang und Abgrenzung des Dokuments 2](#_Toc499801413)

[1.3 Definitionen und Abkürzungen 2](#_Toc499801414)

[1.4 Referenzen 3](#_Toc499801415)

[2 Bestandsaufnahme 4](#_Toc499801416)

[2.1 Architektur 4](#_Toc499801417)

[2.2 Standorte und Netzinfrastruktur 5](#_Toc499801418)

[2.3 Anwender Profile 5](#_Toc499801419)

[3 Geschäftsanforderungen 6](#_Toc499801420)

[3.1 Herausforderung und Geschäftsabsicht 6](#_Toc499801421)

[3.2 Anforderungen 6](#_Toc499801422)

[4 Architektur der Infrastruktur 8](#_Toc499801423)

[4.1 Überblick 8](#_Toc499801424)

[4.2 Standort 9](#_Toc499801425)

[4.3 Azure Beschaffung 9](#_Toc499801426)

[4.4 Security-Konzept 9](#_Toc499801427)

[4.5 Azure IaaS 11](#_Toc499801428)

[4.6 WAN 13](#_Toc499801429)

[4.7 Azure PaaS 13](#_Toc499801430)

[4.8 Azure Controlling 13](#_Toc499801431)

[5 Betrieb 14](#_Toc499801432)

[6 Nachfolgende Planungstätigkeiten 15](#_Toc499801433)

1. Einführung
   1. Zweck des Dokuments

Die in diesem Dokument enthaltenen Informationen und Daten entsprechen dem Erkenntnisstand zum Zeitpunkt der Erstellung dieser Ausarbeitung. Sie sind nach bestem Wissen zusammengestellt.

Dieses Dokument darf nur seiner Zweckbestimmung entsprechend verwendet werden. Die darin enthaltenen Informationen sind vertraulich zu behandeln. Das Dokument selbst und die darin enthaltenen Informationen dürfen an außenstehende Dritte nicht weitergegeben werden, es sei denn, diese sind mit der Ausarbeitung oder Beurteilung ausdrücklich beauftragt.

Zweck dieses Dokumentes ist es ein Grobkonzept (Was wird benötigt) zu beschreiben, welches zur weiteren Planung und Umsetzung der Projekte genutzt werden kann. Ein Grobkonzept unterscheidet sich von einem Feinkonzept darin, dass hier nur das „Was“ beschrieben wird. Es wird keine konkrete Implementierung beschrieben wird, dies ist Teil eines Feinkonzeptes.

* 1. Umfang und Abgrenzung des Dokuments

Betrachtet wird das Fachverfahren MESAP des Umweltbundesamtes, welches für einen Betrieb in Azure vorgesehen ist. Dies soll in Azure auf IaaS betrieben werden.

* 1. Definitionen und Abkürzungen

Dieser Abschnitt listet die Bedeutungen aller Symbole, Terme, Akronyme und Abkürzungen auf, die für die korrekte Interpretation dieses Dokuments notwendig sind.

Design Entscheidungen werden mit einem Kasten gekennzeichnet.

Offene Abstimmungspunkte und Anforderungen sind grau hinterlegt.

|  |  |
| --- | --- |
| Begriffe und Beschreibungen | |
| AWS | Amazon Web Services |
| AD | Active Directory |
| ARM | Azure Resource Manager |
| BCDR | Business Continuity and Desaster Recovery |
| RPO | Recovery Point Objective |
| RTO | Recovery Time Objective |
| POC | Proof of Concept |
| IaaS | Infrastructure as a Service |
| PaaS | Platform as a Service |
| IT-Infrastruktur | Infrastruktur die zum Betrieb von Anwendungen notwendig ist. |
| Tenant | Verzeichnis für Benutzer |
| Forest | Microsoft Gesamtdomäne/Strukur |
| OMS | Operations Management Suite |
| SKU | Stock Keeping Unit |
| Cutover | Prozess der tatsächlichen technischen Migration |

* 1. Referenzen

Dieser Abschnitt führt alle Dokumente auf, die von diesem Dokument an irgendeiner Stelle referenziert wurden.

* Microsoft Technet Knowledgebase

<http://technet.microsoft.com>

* Microsoft Produktseite

[www.microsoft.de](http://www.microsoft.de)

* Microsoft Azure Dokumentation

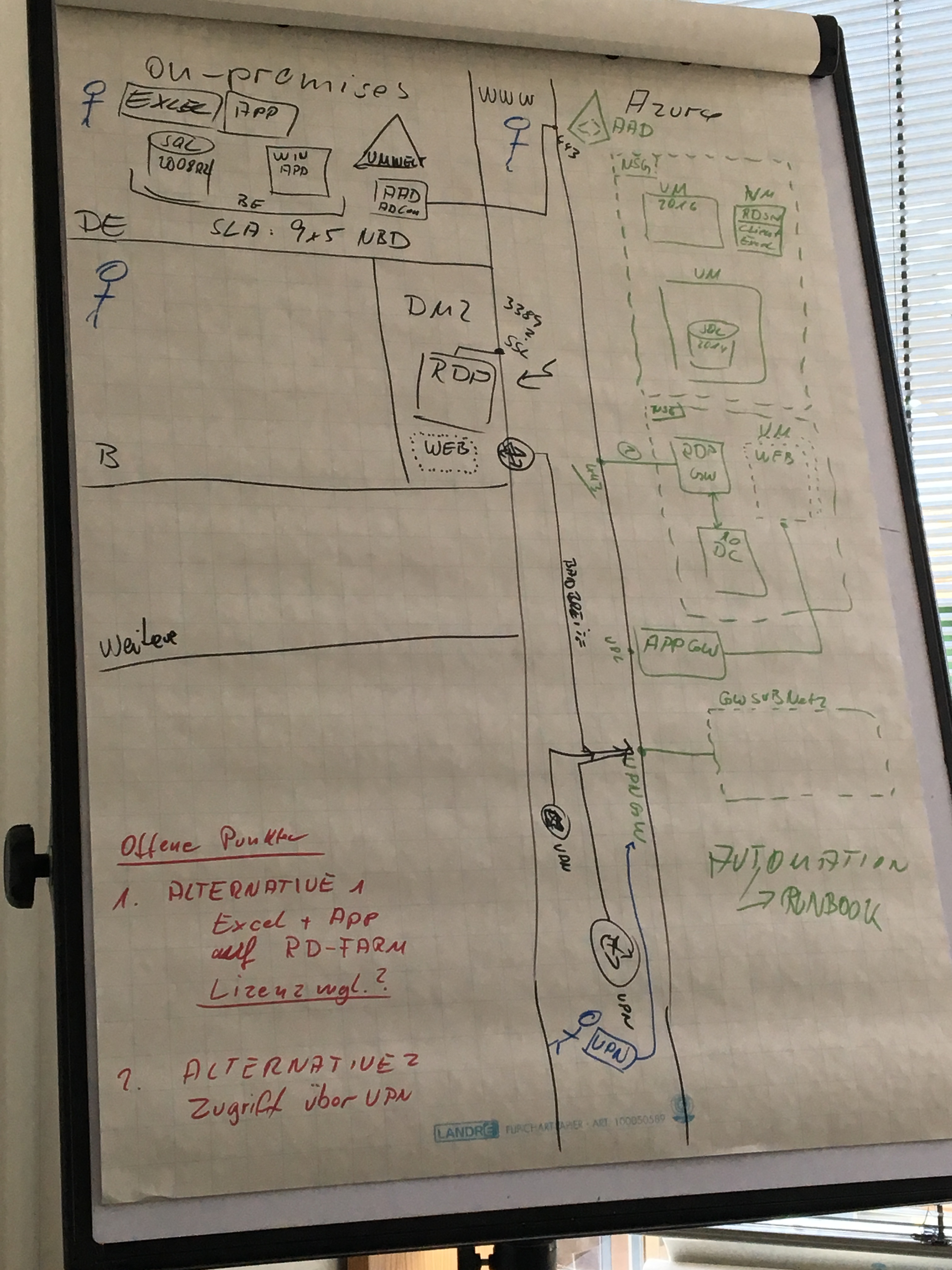
<https://azure.microsoft.com/de-de/documentation>

* Azure Preiskalulator https://azure.microsoft.com/de-de/pricing/calculator/

1. Bestandsaufnahme
   1. Architektur

IST-Architektur in SCHWARZ gezeichnet.

Es sind im Wesentlichen interne Standorte und externe Standort an das Fachverfahren angebunden. Interne Benutzer greifen direkt auf die Daten zu indem der Client eine TCP-Verbindung zur Datenbank aufbaut. Externe Benutzer (www) greifen per RDP-Protokoll auf die Anwendung zu.



* 1. Standorte und Netzinfrastruktur

Die lokale Infrastruktur wird in Dessau und Berlin gehostet. In Berlin findet der Übergang zum Internet statt. In Berlin werden die VPN-Router gehostet.

* 1. Anwender Profile

**Lokale Anwender des Umweltbundesamtes**

Lokale Anwender haben ein Plugin in Excel und einen Fat-Client installiert. Diese bauen eine direkte TCP-Verbindung zur Datenbank auf. Die Benutzer-IDs befinden sich in der Windowsdomäne „UMWELT“

**Remote Anwender Dienstleister**

Dienstleister greifen per RDP-Session auf einen RDP-Host in der DMZ zu, der in Berlin gehostet wird. Dort ist sind alle Anwendungsbestandteile installiert. Es wird ein Funktions-Account soweit wie möglich verwendet.

1. Geschäftsanforderungen
   1. Herausforderung und Geschäftsabsicht

Die Motivation liegt zum einen im unabhängigen Betrieb des Fachverfahren, welches ein flexibleres Reagieren auf Anforderungen ermöglicht. Zudem ist Azure in der IT-konsolidierung des Bundes aller Voraussicht nach als Cloudplattform (Bundescloud) gesetzt. Eine Migration des Fachverfahren mit Standard-Tools von Microsoft Azure ermöglich zudem eine einfache Lift-and-Shift-Migration, falls sich die aktuell angestrebte Umgebung im Zuge der Konsolidierungsbestrebungen ändern sollte.

* 1. Anforderungen
     1. Funktionale Anforderungen

Im Grundsatz ist die Plattform auf dem die Anwendung betrieben wird stabil und unterlag in der Vergangenheit nur sehr wenigen Veränderungen. Besondere Anforderungen hinsichtlich der Skalierbarkeit können somit nicht abgeleitet werden.

**Anbindung von Remote-Arbeitsplätze**

Externe Anwender sollen flexibel über das Internet weiterhin auf die Anwendung zugreifen können.

* + 1. Nicht-funktionale Anforderungen

**SLA des Fachverfahren**

Anwendungen unterliegen üblicherweise einem Zeitraum, in denen Sie dem Anwender zur Verfügung stehen müssen. Diese wird in einem Service Level Agreement (SLA) definiert.

Zudem sind im Falle eines Desasters technische Vorkehrungen zu treffen, um eine Anwendung dem Anwender wieder nutzbar zu machen. Die Anforderung wird mit den Kennziffern RTO/RPO beschrieben. RTO (Recovery Time Objective) bezeichnet die Zeitspanne nach der eine Anwendung den Anwendern wieder nutzbar gemacht werden muss. RPO (Recovery Point Objective) bezeichnet einen maximal verkraftbaren Datenverlust der eintreten würde, wenn Daten, die in einer bestimmten Zeitspanne erzeugt wurden, nach dem Recovery verloren würden.

Desaster

Zeit die vergeht, die Anwendung

wieder nutzbar zu machen

Daten die verloren gehen, die in dieser

Zeitspanne erzeugt wurden.

RTO

RPO

t

t

Definition der SLA für die Fachverfahren

|  |  |  |  |
| --- | --- | --- | --- |
| Anwendung | Anwendergruppe | SLA | RTO/RPO |
| MESAP | Alle Benutzer | 9h x 5 Werktage | 1 Tag /1 Tag |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Datensicherheit**

Das Betreiben einer IT-Infrastruktur in der Public Cloud erfordert besondere Maßnahmen in Bezug auf die Datensicherheit zu treffen. Die Exponiertheit einer Public Cloud erfordert es technische Vorkehrungen, um ein Risiko des Datenverlustes zu minimieren. Diese werden im folgenden Konzept weiter beschrieben.

**Berechtigungskonzept**

Mit der Nutzung von zentralisierten IT Ressourcen kommt einher, dass IT-Administratoren immer mehr Zugriff auf sensible Daten erhalten. Dies ist untrennbar mit dem Tätigkeitsfeld verbunden. Daher besteht die Anforderung ein detailliertes Berechtigungskonzept zu entwerfen, um Risiken so weit wie möglich einzugrenzen.

Führend ist der Grundschutzkatalog nach BSI und der besondere Kriterienkatalog C5. Dieser sollte im Nachgang ausgewertet werden.

**IT-Konsolidierung des Bundes**

Die IT-konsolidierung des Bundes sieht eine Beschaffungs-, Betriebs- und Dienstkonsolidierung vor. Das Grobkonzept muss diese Anforderungen abdecken.

Führend ist hier das „Grobkonzept zur IT-Konsolidierung Bund“, welches im Detail ausgewertete werden muss.

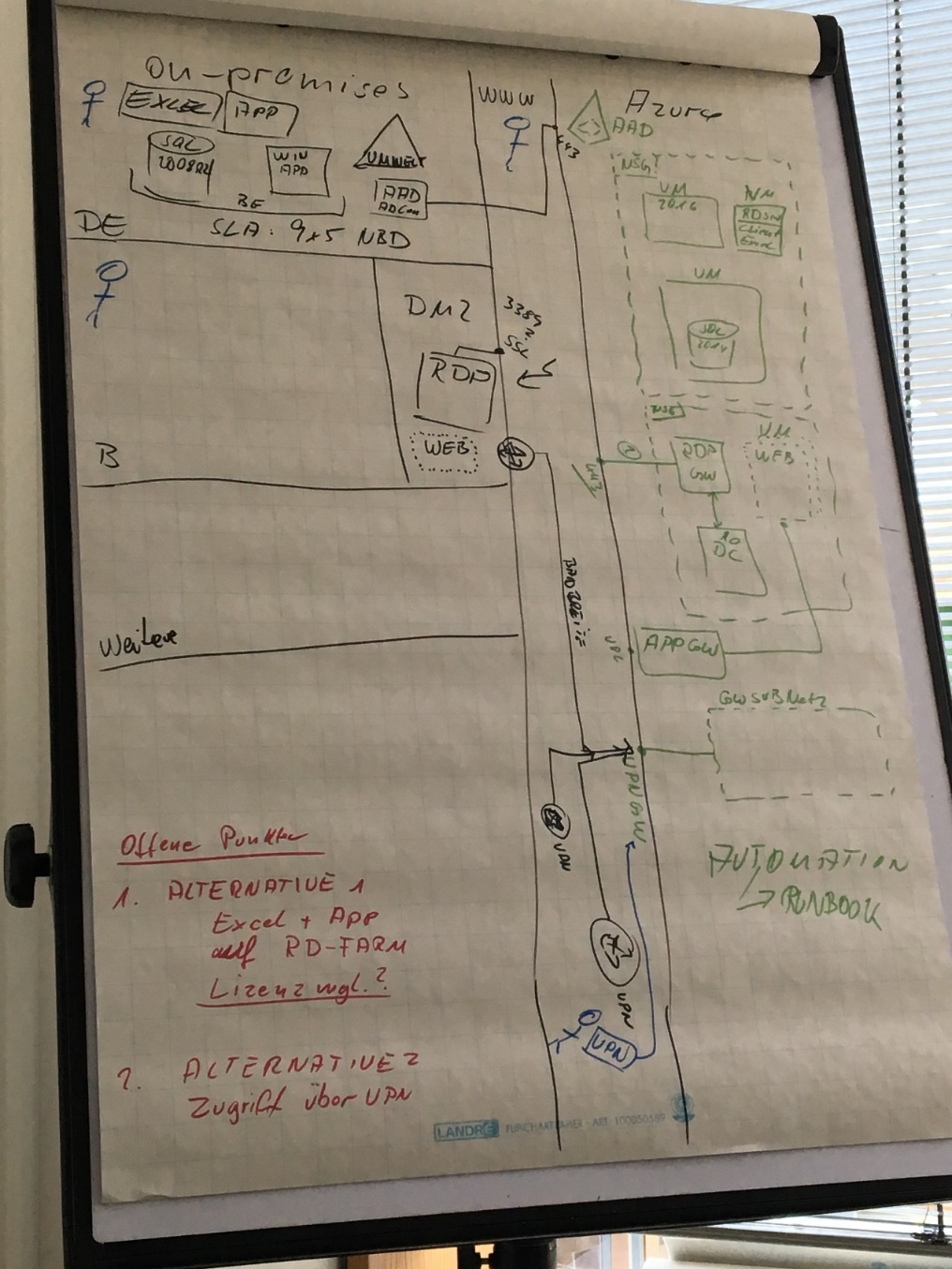
Nach einem ersten Überblick werden Anforderungen abgedeckt und nachfolgend beschrieben.

1. Architektur der Infrastruktur

Dieses Kapital beschreibt die SOLL-Architektur der Infrastruktur speziell für dieses Fachverfahren. Es wurde dabei keine Rücksicht auf die Migration von weiteren Fachverfahren genommen. Insbesondere das Subnetz-Design kann nur unter verhältnismäßig großem Aufwand verändert werden, daher sind bereits ab Start (aus Erfahrung) relativ große Subnetz-Bereiche für die Azure-Umgebung vorzusehen, um weitere Migrationen zu ermöglichen. Zudem ist die Tool-Auswahl für das Management der Ressourcen nicht darauf ausgelegt.

* 1. Überblick

Die SOLL-Infrastruktur ist in GRÜN dargestellt. In den nachfolgenden Kapiteln werden die einzelnen Building-Blocks beschrieben.



* 1. Standort

Standort der Ressourcen ist Azure Germany Northeast sein, da dies den kürzesten Leitungsweg zu den Standorten des Unternehmens hat. Zudem ist der Datenstandort Deutschland gesetzt.

* 1. Azure Beschaffung

Azure kann über verschiedene Wege beschafft werden. Allen voran ist das Cloud Solution Provider (CSP) Programm zunächst hier die richtige Wahl, da das Umweltbundesamt auch Betriebsleistungen an einen Provider abgeben möchte. Zudem kann der Kunde selbstverständlich auch selbst im Rahmen eines EAs oder MPSAs für die Beschaffung von Azure Ressourcen sorgen.

Die Azure Nutzung wird über Azure-Subscriptions gesteuert. Eine Azure-Subscription beschreibt eine konkrete Möglichkeit Azure Ressourcen an Microsoft zu bezahlen. Die Azure Cloud bieten unterschiedliche Möglichkeiten im Nachhinein die Bezahlung in eine andere Vertragsart zu überführen.

Im Grundsatz muss dafür die Azure-Subscription im kaufmännischen System der Microsoft per Support-Ticket auf einen anderen Vertrag umgebucht werden. Im engen Rahmen kann dies der Kunde auch selbst umbuchen.

* 1. Security-Konzept
     1. Azure Active Directory

Azure Active Directory (Azure AD) ist der mehrinstanzenfähige cloudbasierte Verzeichnis- und Identitätsverwaltungsdienst von Microsoft. Azure AD kombiniert grundlegende Verwaltungsdienste mit Identitäts-Governance und Zugriffsverwaltung für Anwendungen. Azure AD bietet außerdem eine umfassende, auf Standards basierende Plattform, mit der Entwickler ihre Anwendungen mit einer Zugriffssteuerung ausstatten können, die auf zentralisierten Richtlinien und Regeln basiert.

Es wird ein neuer Tenant erstellt. Dieser Tenant wird mit einer neuen noch zu schaffenden Gesamtstruktur verbunden.

Es ist eine neue unabhängige Domäne eingeplant, die die Benutzerprofile für das Fachverfahren hält. Mittels „Azure-Active-Directory-Connect“ werden die Benutzerprofile in das Azure Active Directory synchronisiert.

Die Administration der Cloud wird per Multi-Faktor-Authentifizierung zusätzlich gesichert.

Alternativ kann die vorhandene Domäne „UMWELT“ weiter genutzt werden. Dann ist ein Azure Active Directory Connect Server on-premises aufzubauen, der die gewünschten Benutzer-IDs und Gruppen in den AAD-Tenant synchronisiert. Dies ist mit der internen-IT abzustimmen

* + 1. Domänenstruktur

Es ist geplant einen Domänencontroller in das Azure VNET zu platzieren, welcher eine eigene neue Gesamtstruktur enthält.

* + 1. Berechtigungskonzept

Rollen dienen dazu einem Benutzer (IT-Administrator) oder einer Benutzergruppe Zugriff auf Ressourcen zu geben.

Es werden die mit Azure gelieferten Rollen verwendet.

Benutzerdefinierte Rollen können mit PowerShell erstellt werden. Dies ist bei einem überschaubaren Kreis von Administratoren zunächst nicht notwendig. Benutzerdefinierte Rollen ermöglichen den granularen Zugriff auf bestimmte Ressourcen (Ressource Group, VNET, etc.)

Sollen später dienstleistende Unternehmen in die Administration eingebunden werden, so lassen sich hiermit granulare Berechtigungsstruktur entwickeln lassen.

Es bieten sie zunächst die folgenden Gruppen an.

|  |  |  |
| --- | --- | --- |
| Gruppe | Zweck | Berechtigung |
| Azure Admins | 100 % Zugriff auf Azure Ressourcen und Domäne | Alles |
| Externe Admins | Dienstleister mit Zugriff auf Azure | Azure Ressourcen |
| Interne Anwender | Anwender mit Zugriff auf das Fachverfahren, ohne RDP | Kein Zugriff über RDP |
| Externe Benutzer | Benutzer mit Zugriff auf das Fachverfahren per RDP | Ausschließlich Zugriff per RDP |

Gruppen können entweder in Azure direkt angelegt werden oder werden durch die Synchronisation eines ADs erstellt.

* + 1. Policies

Azure Policies ermöglichen das Einschränken von Administrator-Rechten. Damit kann ein Überprovisionieren von teuren Ressourcen eingeschränkt werden.

Die ist zunächst nicht Teil dieses Konzeptes, sollte dennoch nachfolgend betrachtet werden.

* + 1. Locks

Azure Locks verhindern das Löschen und/oder das Verändern vorhandener Ressourcen. Damit kann bei der Administration von kritischen Ressourcen ein Vier-Augen-Prinzip durchgesetzt werden.

Die ist zunächst nicht Teil dieses Konzeptes, sollte dennoch nachfolgend betrachtet werden.

* 1. Azure IaaS
     1. LAN

Ein VNET bildet den netzwerktechnischen Rahmen. Es ist ein Adressbereich zu wählen, der im Netz des Umweltbundesamtes gerouted werden kann. D. h. der Netzbereich muss mit den internen IT-Bereich abgestimmt werden.

Im VNET werden zunächst 4 Subnetze gebildet.

|  |  |  |
| --- | --- | --- |
| Subnetz | Zweck | VMs |
| Prod-Netz | Backend-Server | MESAP-Datenbank, MESAP-App-Backend,  RDS-Host,  Domänencontroller |
| DMZ-Netz | Frontend-Server | RDS-Gateway, Webportal (später) |
| App-Gateway-Netz | Wird von Microsoft vorgeschrieben | App-Gateway |
| Gateway-Netz | Wird von Microsoft vorgeschrieben | VPN-Gateway |

Die Subnetze Prod-Netz und DMZ-Netz sind zusätzlich auf IP-Ebene mit Network Security Groups abzusichern. Dadrin sind explizierte Portfreigaben zu konfigurieren.

* + 1. Virtuelle Maschinen

Die Festplatten der VMs sind zu verschlüsseln. Dafür ist ein Key-Vault in Azure anzulegen, um das Schlüsselmaterial sicher abzulegen. Dafür sind ausschließlich Standard-VMs zu nutzen.

Es ist ein Patch-Management einzurichten. Aufgrund der Übersichtlichkeit der Umgebung kann auf das eingebaute Patch-Management der einzelnen Windows Server zurückgegriffen werden. Eine Alternative ist das herkömmliche WSUS, SCCM oder Azure OMS.

Azure Monitoring ist im ersten Schritt ausreichend, um ein grundsätzliche Monitoring zu gewährleisten.

Mit dem internen IT-Bereich ist nachfolgend eine Abstimmung zu den Anforderungen notwendig.

Der derzeitige Lizenzbestand für Betriebssysteme und weitere Software ist derzeit nicht bekannt. Dies sollte mit der internen IT abgestimmt werden, um den richtigen VM-Typ auszuwählen.

Es wird für Auslieferung des Fachverfahrens ein RDP-Host und ein RDP-Gateway installiert. Dies ist mit einem öffentlichen Zertifikat ausgestattet, welches die geforderte Sicherheit sicherstellt. Die RDP-Infrastruktur ist entweder an die neue AD-Gesamtstruktur angebunden oder an der vorhandenen angeschlossen.

Die interne IT, muss dafür ein Zertifikat zur Verfügung stellen.

* + 1. Backup-Recovery

Die Virtuellen Maschinen werden in einem Recovery-Services-Vault registriert. Eine Backup-Policy sorgt für die regelmäßige Sicherung und das Management der vorhandenen Backups.

* + 1. Automation

Es ist ein Automation Account anzulegen, der die VMs bei Bedarf stoppt und startet. Dafür sind zwei Scripte zu schreiben. Die Compute-Kosten einer VM fallen nur an, wenn die VM gestartet ist. Daher soll das Fachverfahren in den Nicht-Nutzungs-Zeiten gestoppt werden. Siehe auch SLA Anforderungen Kap. 2.2.2. Storage Kosten fallen dennoch weiterhin an, auch wenn die VM gestoppt ist.

* + 1. Infrastruktur Verwaltung

Mittels wiederverwendbarer Scripte ist es mögliche die grundlegenden Azure Ressourcen anzulegen und zu konfigurieren. Diese Scripte sind in JSON notiert und können automatisiert in einer Azure Umgebung ausgerollt werden. Die Azure Grundeinrichtung (Onboarding, Anlegen Azure AD, Konfiguration der VMs, etc.) bleibt hiervon unberührt.

Skripte werden in einem zentralen Repository verwaltet.

In JSON Scripten ist es möglich die folgenden Ressourcen mit relativ wenig Aufwand automatisiert bereitzustellen.

* VNET
* Subnetze
* VPN-Gateway
* Firewallfreigaben (NSG)
* VM Hüllen
* Application Gateway
* Loadbalancer
* Routing-Einträge
* Backup-Recovery
* Policies
* Locks
* Automation Account (Runbooks)

Es wird empfohlen die folgenden Konfigurationsarbeiten händisch auszuführen.

* Aufsetzen einer Domäne
* Konfiguration der Betriebssysteme
* Domänenjoin
* Installation der Backup-Clients
* Installation des Fachverafahrens
* Planen von Automation-Jobs

Für alle Tätigkeiten bietet Microsoft eine Form der Automatisierung an, dies empfiehlt sich hinsichtlich des zukünftigen Bedarfes aufgrund des zu erwartenden Aufwands nicht.

* 1. WAN

Das Azure VPN Gateway bietet bis zu 1 Gbits Durchsatz. VPN ist ein Internetprotokoll, welches KEINE QoS bietet. Eine Alternative dazu bildet Azure Expess Route. Dies ist eine dedizierte redundante Verbindung in das physikalische Azure Rechenzentrum.

Alle Standorte werden über ein Gateway an das VNET in Azure angebunden.

Voraussetzung ist, dass das Netzwerkgateway auf Seiten des Umweltbundesamtes Azure Cloud unterstützt. In Abhängigkeit davon wird die konkrete Konfiguration definiert.

Nachfolgen sind die Anforderungen mit der internen IT abzustimmen.

* 1. Azure PaaS
     1. Application-Gateway

Das Webportal für das Fachverfahren wird in einem DMZ-Netz platziert. Es wird dringend davon abgeraten die entsprechende VM mitteln öffentlicher IP direkt ins Internet zu stellen. Es bietet sich hier ein der Plattform-Dienst Azure Application Gateway an. Der die Benutzer-Requests entgegennimmt und an die Webanwendung weitergibt. Die stellt die geforderte Sicherheit sicher.

Mit der internen IT ist die Verwendung eines öffentlichen Zertifikates abzustimmen.

* + 1. Load-balancer

Es wird empfohlen das RD-Gateway hinter einem Loadbalancer zu platzieren, um so wenig Angrifffläche wie möglich zu bieten. Siehe auch vorheriges Kapitel.

* 1. Azure Controlling

Die anfallenden Kosten für Azure Ressourcen können detailliert ausgewertet werden.

Dies ist zunächst nicht Inhalt dieses Konzeptes und sollte nachfolgend abgestimmt werden.

1. Betrieb

Im nachfolgenden werden die Betriebstätigkeiten der skizzierten kundenindividuellen Umgebung in Form einer RACI Matrix skizziert.

Die tatsächliche Abstimmung der Tätigkeiten ist noch durchzuführen. Es ist ein individueller Leistungsschein zu erstellen.

|  |  |  |  |
| --- | --- | --- | --- |
|  | UBA Fachbereich | UBA interne IT | Provider |
| Azure Grundadministration   * Subscription-Management * Benutzeradministration * Kostenmanagement * Sicherheit mit MFA |  |  |  |
| Administration VMs   * Überwachung Kapazität * Antimalware * Patch-Management * Überwachung der Verfügbarkeit * Changerequests |  |  |  |
| Administration Application Delivery   * Einrichten neuer Anwendungen auf RDP-Hosts * Benutzerverwaltung |  |  |  |
| Administration der Datenbanken   * Backup&Recovery * Changerequests |  |  |  |
| Administration WAN   * Überwachung der Stecken * Änderungen IP-Netze * Pflege Firewalls * Einrichtung Zugänge |  |  |  |
| DesasterRecovery   * Regelmäßiges Backup * Wiederherstellung im Desaster-Fall |  |  |  |

R=Responsible (Durchführungsverantwortung)

A=Accounatble (Rechenschaftspflichtig)

C=Consultet (Muß befragt werden)

I=Informed (Muß informiert werden)

1. Nachfolgende Planungstätigkeiten

Die nachfolgenden Planungstätigkeiten sind noch durchzuführen.

* Feinkonzept
* Auswertung BSI Testat und Anforderungen an die Nachweispflicht
* Auswertung des Grobkonzept IT-Konsolidierung des Bundes
* Leistungsschein Betriebstätigkeiten