Projektdokumentation

Implementierung einer Virtualisierungsumgebung in eine Produktivumgebung mit veraltetem Server

Name	Paul Stephan
Ausbildungsberuf	Fachinformatiker für Systemintegration
Ausbildungsbetrieb	Mey-IT GmbH
Ausbilder	[redacted]
Prüfung	Sommer 2021

Erklärung

Oldenburgische Industrie- und Handelskammer

Eidesstattliche Erklärung

Bestätigung über die durchgeführte betriebliche Aufgabe[1]
(Diese Bestätigung ist als Deckblatt online einzureichen, gemeinsam mit dem Report/der Dokumentation.)

Prüfling (vollständige Anschrift und Telefonnummer)
Vorname, Name [redacted]
Straße, Hausnr.
PLZ, Ort
Tel.Nr.:

Ausbildungsbetrieb (vollständige Anschrift)
Firma [redacted]
Straße, Haus
PLZ, Ort
Tel.Nr.:

Hinweis vorab: Aus Gründen der besseren Lesbarkeit wird auf die gleichzeitige Verwendung männlicher und weiblicher Sprachformen verzichtet. Sämtliche Personenbezeichnungen gelten gleichermaßen für alle Geschlechter.

Ausbildungsberuf

Fachinformatiker für Systemintegration

Bezeichnung der betrieblichen Aufgabe

Implementierung einer Virtualisierungsumgebung in eine Produktionsumgebung mit veralteten Server

Eidesstattliche Erklärung des Prüflings

Hiermit versichere ich, dass ich die betriebliche Aufgabe unter der Betreuung von

Verantwortlicher im Unternehmen

[redacted]

selbstständig durchgeführt und die Unterlagen selbstständig zusammengestellt habe.

Dokumente und Textpassagen, die ich nicht selbstständig erstellt habe, sind von mir gekennzeichnet.

[redacted]

Ort, Datum Unterschrift des Prüflings

Bestätigung des Ausbildungsbetriebes

Wir bestätigen, dass die Angaben des Prüflings richtig sind.

[redacted]

Ort, Datum Unterschrift des Verantwortlichen, der die Aufgabe betreut hat.

[redacted]

Ort, Datum Unterschrift des Ausbilders

[1] Zur Vereinfachung wird einheitlich der Begriff „betriebliche Aufgabe" verwendet. Gemeint sind die Fachaufgabe/die Projektarbeit/der betrieblicher Auftrag. Die unterschiedlichen Bezeichnungen entstehen durch die verschiedenen Berufe, die eine Aufgabe online einstellen.

Inhaltsverzeichnis

Erklärung **2**

Inhaltsverzeichnis **3**

Tabellenverzeichnis **6**

Abkürzungsverzeichnis **7**

1 Einleitung **8**

1.1 Ausbildungsbetrieb 8

1.2 Auftraggeber 8

1.3 Änderungen gegenüber dem Projektantrag 8

1.4 Hintergründe des Projektauftrages 8

1.5 Ziel des Projektes 9

1.6 Zeitplanung des Projektes 9

2 Planung **10**

2.1 IST-Analyse 10

2.2 SOLL-Konzept 11

2.3 Erarbeitung von Lösungswegen 11

2.3.1 On Premise-Lösung 11

2.3.2 IaaS-/RZ-Lösung 11

2.3.3 Hinweis: 12

2.4 Angebotsvergleich/Gegenüberstellung 13

2.5 Kosten-Nutzen-Analyse 13

2.5.1 Nutzen 14

2.5.2 Ausfallsicherheit 14

2.5.3 Monatliche Kosten 14

2.5.4 Hinweis: 14

2.5.5 Wartung 14

2.5.6 Dynamik 15

2.5.7 Schutz vor Datenverlust 15

2.5.8 Schutz vor unbefugtem Datenzugriff 15

2.5.9 Nutzwertanalyse 16

2.6 Vertragsabschluss 16

3 Projektdurchführung **17**

3.1 Netzwerkumgebung 17

3.1.1 VPN 17

3.1.1.1 Einrichtung der IPSec Site To Site VPN-Verbindung 17
3.1.1.2 Einrichtung der SSL End To Site VPN-Verbindung 17
3.1.2 Portfilter 18
3.2 Serverkonfiguration 19
3.2.1 Installation 19
3.2.2 Konfiguration 19
3.2.2.1 Active Directory / Domänendienste 19
3.2.2.2 Druckserver und Drucker 19
3.2.2.3 Verzeichnisstruktur / Datei-Dienste 20
3.2.2.4 Gruppenrichtlinien 20
3.2.2.5 Konfiguration des Remotedesktop-Lizenzservers 21
3.2.3 Installation der Software 21
3.2.4 Einrichtung der Datensicherung 21
3.2.5 Migration der Daten 21
3.2.6 Einrichtung der Microsoft 365 Benutzer 22
3.2.7 Tests 22

4 Projektabschluss 23
4.1 Fazit 23

5 Anhang 25
5.1 Betriebsdokumentation 25
5.1.1 Einrichtung der IPSec Site To Site VPN-Verbindung 25
5.1.2 Einrichtung der SSL-VPN End To Site Verbindung 28
5.1.3 Einrichtung Zertifikatskette für SSL-VPN 29
5.1.4 Firewall AD-Anbindung 30
5.1.5 Einrichtung Benutzergruppe mit AD-Sync 32
5.1.6 Einrichtung der Domänen Gesamtstruktur 33
5.1.7 Erstellen von Verzeichnisfreigaben 35
5.1.8 Druckserver und Drucker 35
5.1.9 Erstellen der Gruppenrichtlinien 36
5.1.9.1 Drucker und Laufwerke 36
5.1.9.2 Startmenü und Taskleiste 37
5.1.9.3 Aufgabenplanung 37
5.1.9.4 Dateiexplorer 37

5.1.9.5 Remotedesktopverbindungs-Client 38
5.1.9.6 Desktop 38
5.1.9.7 Remotedesktop-Sitzungshost 38
5.1.10 Installation des RDP-Servers 38
5.1.11 Einrichtung des RDP-Lizenzierungsserver 39
5.1.12 Installation Microsoft 365 Apps 40
5.1.13 Wortmann Cloud Datensicherung 41
5.1.14 Abschließende Firewall Konfiguration 42
5.1.14.1 Netzwerkgruppen/Objekte 43
5.1.14.2 Portfilterregeln 43
5.1.14.3 Dienstgruppen 44

6 Quellenverzeichnis 45
6.1 Allgemeines 45
6.2 Securepoint Firewall 45
6.3 Microsoft 46
6.4 Wortmann Cloud 47

Tabellenverzeichnis

Tabelle 1 Zeitplanung 9
Tabelle 2 Gegenüberstellung der Kosten 13
Tabelle 3 Nutzwertanalyse 16
Tabelle 4 Server Rollen und Dienste 19

Abkürzungsverzeichnis

PDL	Pflegedienstleitung
MFG	Multifunktionsgerät
VPN	Virtual Private Network
IaaS	Infrastructure as a Service
RZ	Rechenzentrum
VDSL	Very High-Speed Digital Subscriber Line
NAS	Network Attached Storage
USV	Unterbrechungsfreie Stromversorgung
DNS	Domain Name Server
UNC	Uniform Naming Convention
URL	Uniform Resource Locator
IPSec	Internet Protocol Security
IKE	Internet Key Exchange
AES	Advanced Encryption Service
SHA	Secure Hash Algorith
SSL	Secure Socket Layer
UDP	User Datagram Protocol
ID	Identifier
AD	Active Directory
CA	Certificate Authority
RADIUS	Remote Authorization Dial in User Service
OU	Organization Unit
RDP	Remote Desktop Protocol
RGRP	Regelgruppe
NGRP	Netzwerkgruppe
DGRP	Dienstgruppe
XML	Extensible Markup Language
GPO	Group Policy Object
SMB	Server Message Block
ACL	Access Control List

1 Einleitung

1.1 Ausbildungsbetrieb

Die Mey-IT GmbH ist ein IT-Dienstleistungsunternehmen, das sich auf die Planung, Umsetzung und Betreuung der IT-Infrastruktur von Kunden spezialisiert. Im Fokus des Unternehmens steht dabei der respektvolle Umgang auf Augenhöhe mit dem Kunden und eine entsprechend angemessene Transparenz. Dies gilt insbesondere bei der Preisgestaltung von Projekten oder wiederkehrenden Dienstleistungen.
Das Team setzt sich derzeit noch aus dem Geschäftsführer/Gesellschafter und Ausbilder sowie einer Mitarbeiterin und mir als Azubi zusammen und erarbeitet seinen Kunden daher in enger Zusammenarbeit Konzepte rund um die IT-Infrastruktur. Wir begleiten unsere Kunden dabei sowohl vom Aufbau bis zur Inbetriebnahme als auch bei der Betreuung dieser.

1.2 Auftraggeber

Auftraggeber ist ein ambulanter Pflegedienst aus dem Landkreis Wesermarsch. Mit einer Filiale und einer dazugehörigen Tagespflege besteht das Team aus einem Geschäftsführer/Gesellschafter, einer Verwaltungskraft, einer PDL sowie einer stellv. PDL und mehreren Pflegekräften. Die Dienstleistungen werden dabei sowohl bei den Patienten vor Ort als auch in der Tagespflege durchgeführt. Die Dokumentation erfolgt dabei teils unterwegs und teils im Büro.
Der Auftraggeber möchte in diesem Projekt nicht namentlich genannt werden. Alle Hinweise auf den Auftraggeber, die direkte Rückschlüsse auf diesen ermöglichen werde ich entsprechend schwärzen oder durch Generalisierungen ersetzen (z.B. „kunde.local“ als Domäne).

1.3 Änderungen gegenüber dem Projektantrag

Im Projektantrag wurde die IPsec Verbindung nicht erwähnt. Diese hat sich erst im Laufe des Projektes ergeben und hing von der Entscheidung ab, welche Art der IT-Infrastruktur zur Realisierung des Projektes genutzt werden soll.

Außerdem fällt der Einsatz der ursprünglichen Anforderung von „Starmoney Business“ weg, da der Kunde sich entschieden hat diese Veränderung erst später in Angriff zu nehmen.

1.4 Hintergründe des Projektauftrages

Dem Auftraggeber ist es wichtig, dass der Zugriff auf die genutzten Dienste und Daten möglichst ausfallfrei gestaltet wird. Ohne, dass dabei ein großer Liquiditätsverlust für sein Unternehmen entsteht. Außerdem sollten die Daten unter Einhaltung der

geltenden Datenschutzverordnungen des Bundes und der EU geschützt werden, da es sich ja vor allem um personenbezogene Daten handelt. Der aktuell besonders schwierigen Pandemie Situation und gegebenen Verordnungen geschuldet sollte außerdem eine möglichst kontaktarme Durchführung des Auftrags erfolgen, um die Ansteckungsgefahr zu senken.

1.5 Ziel des Projektes

Ziel des Projektes ist es, die bisherige IT-Infrastruktur möglichst vollständig in das RZ zu übertragen, ohne dabei den betrieblichen Ablauf langfristig zu stören. Dabei sollen alle datenschutzrelevanten Aspekte erfüllt sein und ein standortunabhängiges Arbeiten ermöglicht werden. Bei der Übertragung soll die Struktur jedoch auch sinnvoll neugestaltet werden, um eine klarere Struktur der Server bereitzustellen. Eine neue Datensicherungslösung soll zudem den Schutz vor Datenverlust gewährleisten.

1.6 Zeitplanung des Projektes

Zeitplanung

ID	Aufgabenname	Start	Abschluss	Dauer
1	Planung	26.04.2021	26.04.2021	1T
2	Projektdurchführung	27.04.2021	29.04.2021	3T
3	Projektabschluss	30.04.2021	30.04.2021	,13T

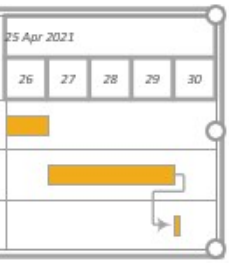


Tabelle 1 Zeitplanung

Die zeitliche Planung steht im Verhältnis 1T (1 Tag) gleich 8h (8 Stunden).

2 Planung

2.1 IST-Analyse

Der Pflegedienst besitzt einen Server mit „Microsoft Windows Server 2012 Foundation“, sowie 6 Arbeitsplätze mit Desktop-Computern und 5 Drucker bzw. Multifunktionsgeräte, davon eines mit aktiver Fax-Funktion. Der Server dient als Domaincontroller, DNS-Server, Fileserver, Datenbank-Server und Terminalserver. Die genannten Rollen und Dienste sind lokal installiert.

Die 6 Drucker/MFGs sind unterschiedlich positioniert. Es gibt jeweils 1 Einzelbüro für den Geschäftsführer, die PDL und die Verwaltung sowie ein Großraumbüro für die Mitarbeiter. Jedes Einzelbüro verfügt über ein eigenes MFG mit 2 Papierfächern. Ein Faxgerät steht auf dem Flur im OG. 2 weitere MFGs mit 2 Papierfächern stehen je an einem Ende des Großraumbüros für die Mitarbeiter.

Die 6 Arbeitsplätze sind unterschiedlich eingerichtet, halten den derzeitigen Anforderungen jedoch problemlos Stand. Die bereits erwähnten Drucker/MFG sind individuell an den Desktop-Computern per Netzwerk installiert und teils unterschiedlich benannt oder eingerichtet. Alle von den Desktop-Computern sind mit Windows 10 Pro als Betriebssystem ausgestattet, sowie der genutzten Software.

Die genutzte Software beläuft sich dabei auf Microsoft Office 2013/Microsoft Office 365 Apps, Adobe Acrobat Reader DC, Datev Unternehmen Online und die Branchen-Software „Heimbas“ als Variante für ambulante Pflegedienste. „Datev Unternehmen Online“ nutzt ein USB-Dongle zur Authentifizierung und benötigt zum direkten Hochladen von Scans einen lokal angeschlossenen Scanner. „Heimbas“ nutzt eine Datenbank zur Speicherung und Verwaltung der Datensätze. Da an 3 von 6 Arbeitsplätzen bereits Microsoft 365 genutzt wird werden unter Umständen weniger Lizenzen für die Nutzung von Microsoft 365 gebraucht.

Als Netzwerkkomponenten ist eine Securepoint RC100 Firewall, eine Telekom Digitalisierungsbox Premium (VDSL-Modem), ein 24-Port Gigabit Switch und ein Patchpanel mit CAT6A Verkabelung vorhanden. Die CAT6A Verkabelung bindet bereits alle Netzwerkkomponenten mit der RC100-Firewall, die wiederum hinter dem VDSL Modem angebunden ist. Die Verkabelung erfolgt dabei auf 2 Etagen, wobei im Obergeschoss das Büro und im Erdgeschoss die Tagespflege seinen Platz hat. Die Tagespflege besitzt lediglich einen Arbeitsplatz hinter dem der Wandschrank mit der TAE-Dose, dem VDSL-Modem, der RC100-Firewall, dem Switch und dem Patchpanel platziert ist. Von dort aus geht die CAT6A Verkabelung dann über einen Kabelkanal in das Obergeschoss und dort in die Büros.

Am benannten VDSL-Anschluss liegen zum Zeitpunkt der Durchführung etwa 100Mbit\s Download- und 40Mbit\s Uploadraten an.

Die Telefonie läuft separat über eine Telefonanlage, die direkt mit dem Modem verbunden ist und hier nicht näher erläutert wird.

Eine Datensicherung wird lediglich vom Server auf eine externe Festplatte gemacht. Überprüft wurde die Datensicherung bisher nicht bzw. unregelmäßig und wenn dann ausschließlich auf Durchführung der Sicherung.

2.2 SOLL-Konzept

Angestrebt wird eine Lösung, die den administrativen Aufwand durch Zentralisierung der Dienste verringert und erleichtert sowie die Sicherheit der Daten, in Bezug auf den Schutz vor Verlust und den berechtigten Zugriff, standortunabhängig und möglichst ausfallsicher bereitstellt. Die vernachlässigte Datensicherung und dessen Überprüfung sollen möglichst automatisiert werden.
Die Wartungskosten für das neue System sollen entsprechend sinken und die Flexibilität zur einfachen und schnellen Erweiterung, wie der Bereitstellung eines Arbeitsplatzes für neue Mitarbeiter, sollen gegeben sein.
Des Weiteren soll jeder Mitarbeiter seine Eigene Arbeitsumgebung (Desktop/Benutzer) nutzen können.

2.3 Erarbeitung von Lösungswegen

Nachdem im SOLL-Konzept die Anforderungen für die neue IT-Infrastruktur beschrieben wurden, entwickle ich 2 Lösungen, die den Anforderungen des Kunden entsprechen und stelle diese dem Kunden vor. Ich hole mir dafür bereits vorab Angebote ein, um diese direkt anbieten zu können. Wie bereits bekannt handelt es sich bei den 2 Lösungswegen um eine „On premise“-Lösung und eine IaaS-(RZ) Lösung.

2.3.1 On Premise-Lösung

Als einen ersten Lösungsvorschlag ist eine klassische lokale IT-Umgebung geplant. Dazu soll ein neuer Server mit Hypervisor Funktion die Serverumgebung virtualisieren und 3 weitere Server bereitstellen. Die 3 Server sollen mit Windows Server 2019 als Betriebssystem entsprechend den Rollen als „Domaincontroller“, „Terminalserver“ und „Datenbankserver“ installiert werden, wobei bei letzterem keine spezielle Rolle installiert wird, sondern vielmehr die Datenbank der Branchensoftware ausgelagert wird. Für die Mitarbeiter des Pflegedienstes werden Microsoft 365 Business Standard Lizenzen zur Lizenzierung auf dem Terminalserver vorgesehen. Die Datensicherung soll auf einer NAS im lokalen Netzwerk in Verbindung mit Veeam Backup and Replication Essentials Enterprise erfolgen. Um die Sicherung der Daten optimal zu gewährleisten, soll die NAS in einem anderen Brandabschnitt betrieben werden als der Server. Der Server soll über eine Online USV zusätzlich vor Stromausfall, Überspannung und/oder Frequenzschwankungen geschützt werden.

2.3.2 IaaS-/RZ-Lösung

Als Alternative ist eine IaaS-/RZ-Lösung für die neue IT-Umgebung angedacht. Dabei soll über unseren Partner Provider die Wortmann AG eine IaaS-Lösung bereitgestellt

werden, die vollständig von uns administriert werden kann. Auch hier sollen 3 Server mit den entsprechenden Rollen „Domänencontroller“, „Terminalserver“ und „Datenbankserver“ bereitgestellt werden. Die RZ-Umgebung wird per Site-To-Site VPN mit dem Büro-Netzwerk verbunden werden. Außerdem wird ein mobiler End-To-Site VPN Zugriff auf den Terminalserver ermöglicht. Die Datensicherung wird dann über eine Cloud-Lösung der Wortmann AG realisiert. Den Mitarbeitern wird hier ebenfalls Microsoft 365 Business Standard zur Verwendung auf dem Terminalserver bereitgestellt. Da in dieser Lizenz bereits Exchange Lizenzen enthalten sind bekommt hier auch jeder Mitarbeiter sein persönliches E-Mail-Postfach (gilt auch für die On Premise-Lösung).

2.3.3 Hinweis:

Sowohl für die On Premise- als auch die IaaS-Lösung kommen zusätzlich eine monatliche Dienstleistungspauschale für die Überprüfung des Backups und Wartungsarbeiten hinzu.

2.4 Angebotsvergleich/Gegenüberstellung

[redacted]		[redacted]	
[redacted] - Firewall VM - privates VLAN Segment - 1 öffentliche IP Adresse - 10 x Zugänge inkk. AV Paket & Conetentfilter	26 €	Server (Kosten 9533,76€) TERRA SERVER 7420 G3 - Netzteil REDUNDANT mit 750 Watt - Intel S2600STBR (2x 10 GbE) - Intel Remote Management Module V4 Lite 2 - 2 x CPU Intel Xeon Silver 4208 (8x 2.1 GHz) - 2 x DDR4 REG 32GB/PC2933/ECC (2Rx4) - Broadcom (LSI) MegaRAID 9361 8i SAS3 1GB 8x intern - TERRA Server 24H Vor Ort Service+ME+NFS 36 Monate - 2 x SSD 2.5" SATA3 3.8TB Seagate TLC (Nytro 1351) - 2 x MS WINDOWS SERVER 2019 Standard - 4 x MS Windows Server 2016/2019 5er Device CAL - MS Windows Server 2016/2019 10er User CAL (RDS) -USV VA 1500 Watt 1350	196,80 €
Server - DC (Rechteverwaltung / FileServer) - 2 Kern CPU - 4 GB RAM - 250 GB HDD Speicherplatz - Windows Server 2019	37,00 €		
Server - Terminalserver (wo die Mitarbeiter drauf arbeiten) - 4 Kern CPU - 24 GB RAM - 200 GB HDD Speicherplatz - Windows Server 2019 - 10 RDP CALS	161,00 €		
Server - App (Programme z.B. Heimbas) - 2 Kern CPU - 4 GB RAM - 250 GB HDD Speicherplatz - Windows Server 2019	37 €		
	261 €		196,80 €
10x Microsoft Business Premium inkl. Exchange - 50 GB Postfach	169,00 €	10x Microsoft Business Premium inkl. Exchange - 50 GB Postfach	169,00 €
terra Backup Standard 500 GB Max.	79,90 €	terra Backup Standard 500 GB Max.	79,90 €
Server Management Basic	44,97 €	Server Management Basic	44,97 €
Managed Antivirus	51,00 €	Managed Antivirus	51,00 €
Dienstleistungskontingent 3h	210,00 €	Dienstleistungskontingent 3h	210,00 €
	815,87 €		751,67 €

Tabelle 2 Gegenüberstellung der Kosten

Bei der Gegenüberstellung der Kosten wird darauf hingewiesen, dass anfallende Betriebskosten für z.B. Strom nicht enthalten sind! Diese Kosten sind für die RZ-Variante zu vernachlässigen, da sie bereits enthalten sind.

2.5 Kosten-Nutzen-Analyse

Nachfolgend werden die Kosten, die Implementierung der neuen IT-Infrastruktur anfallen, aufgeführt und gegenübergestellt.

2.5.1 Nutzen

Die Anschaffungskosten sind für den Auftraggeber wichtig. Zu hohe Anschaffungskosten bedeuten für ihn einen hohen Liquiditätsverlust. Der Auftraggeber tendiert deshalb dazu eine Lösung zu bevorzugen, die kaum Anschaffungskosten beinhaltet, um flexibel zu bleiben. Eine subjektive Favorisierung durch den Auftraggeber ist daher bereits ersichtlich. Eine Gegenüberstellung der beiden Lösungen führe ich trotzdem durch, um eine möglichst objektive Entscheidung zu gewinnen.

2.5.2 Ausfallsicherheit

Die Ausfallsicherheit ist wie bereits erwähnt wurde ein relevanter Aspekt, den der Kunde als Anforderung an uns gestellt hat. Der Zugriff auf die Daten und Dienste soll möglichst immer gegeben sein. Bei der On Premise-Lösung wäre eine Ausfallsicherheit nur in sehr begrenztem Maße vorhanden, da keine redundanten Systeme zur Absicherung des Betriebes vorhanden sind. Eine Wiederherstellung des Betriebes würde demnach bei einem Hardwaredefekt die Behebung dessen mit sich ziehen und unter Umständen länger als 24h dauern. Der Betrieb wäre dadurch maßgeblich für eine lange Zeit gestört.

Mit der IaaS-Lösung unseres Partners wären zwar genau wie bei der On Premise-Lösung keine redundanten Server vorhanden, die bei einem Ausfall den Betrieb gewährleisten können, jedoch verspricht die Wortmann AG die Bereitstellung der Systeme innerhalb von 4h nach Ausfall. Außerdem sind die Daten vor äußeren Einflüssen besser vor Verlust geschützt.

2.5.3 Monatliche Kosten

Im Vergleich zur „On Premise-Lösung“ fallen im Angebot mit der „IaaS-Lösung“ deutlich höhere monatliche Kosten für die Nutzung dieser an, sofern der Kunde sich entscheidet die „On Premise-Lösung“ stattdessen zu kaufen und nicht zu finanzieren.

2.5.4 Hinweis:

Die monatlichen Kosten für Die Microsoft 365 Dienste sowie die Dienstleistungspauschale gelten auch für die „On Premise-Lösung“.

2.5.5 Wartung

Der Wartungsaufwand beider Angebote muss ebenfalls berücksichtigt werden. Wartungen für die Hardware entfallen bei der „IaaS-Lösung“, da diese durch die Wortmann AG erfolgen. Updates für Betriebssystem und Software werden einerseits automatisch durch den Hersteller gemacht und andererseits durch uns über unsere Monitoring- und Patchmanagement-Lösung. Die Updates werden wir im Zuge der Backupüberprüfung einmal monatlich durchführen. Der gesamte Wartungsaufwand ist daher sehr gering.
Der Wartungsaufwand für die „On Premise-Lösung“ ist hingegen intensiv, da hierbei ebenfalls die Hardware gewartet werden muss. Das erfordert zudem immer einen Techniker, der mit der Hardware vertraut sein muss.

2.5.6 Dynamik

Auch die Dynamik ist ein wichtiger Aspekt des Kunden. Der Kunde möchte in Zukunft flexibel weitere Mitarbeiter einstellen können, ohne ständig überprüfen zu müssen, ob die IT-Infrastruktur dafür ausreichend skaliert und erweiterbar ist. Dies gilt sowohl für den Mitarbeiterzuwachs als auch bei Mitarbeiterentlassungen. Gerade im ambulanten Pflegedienst sie mit viel Dynamik im Personalbereich zu rechnen, da Fachkräfte rar sind.
Die „On Premise-Lösung“ bietet diese Flexibilität in Bezug auf den Mitarbeiterzuwachs und kann notfalls auch noch höher skaliert werden indem z.B. der Arbeitsspeicher erweitert wird. Jedoch wäre umgekehrt keine sinnvolle Möglichkeit gegeben die Skalierung wieder zu reduzieren. Das ist vor allem bei der Lizenzierung relevant.
Die „IaaS-Lösung“ bietet in beide Richtungen die volle Skalierbarkeit.

2.5.7 Schutz vor Datenverlust

Datenverlust ist für den Kunden ein sensibles Thema. Dem Kunden war zunächst gar nicht bewusst mit welchem Risiko er zunächst gearbeitet hat.
Der Schutz vor Datenverlust ist in beiden Varianten besser als im vorherigen Konzept. Jedoch schneidet das Datensicherungskonzept der IaaS-Lösung immer noch besser ab, da sich die Daten nicht nur in einem anderen Brandsicherheitsabschnitt, sondern an einer anderen Ortschaft befinden.

2.5.8 Schutz vor unbefugtem Datenzugriff

Der unbefugte Zugriff auf die Daten fällt ebenfalls in die Gewichtung. Der Kunde weist ausdrücklich darauf hin, dass er mit sensiblen personenbezogen Daten arbeitet und deshalb die Einhaltung der geltenden Datenschutzverordnungen des Bundes und der EU essenziell zu betrachten ist.
Die „On Premise-Lösung“ ist in diesem Fall beispiellos im Vorteil, da hier sämtliche Daten lokal gespeichert und gesichert werden. Es gibt also keine weiteren Schnittstellen, die einen Zugriff auf die Daten besitzen.
Für die „IaaS-Lösung“ besteht dieser Vorteil nicht unbedingt gänzlich. Zwar hat der Provider die Wortmann AG weder Einsicht auf die Daten der IT-Infrastruktur noch auf die Sicherungen, da diese verschlüsselt gelagert werden, jedoch wäre es prinzipiell mit höherer Wahrscheinlichkeit zu werten, dass mittels „Man-in-the-Middle“ oder anderen Attacken die Verbindung von der Filiale bis zum Rechenzentrum abgefangen wird. Der Datenverkehr an sich würde allerdings in jenem Fall verschlüsselt bleiben.

2.5.9 Nutzwertanalyse

Der deutliche Nutzen von der „IaaS-Lösung“ gegenüber der „On Premise-Lösung“

Kriterien	Gewichtung	On Premise-Lösung		IaaS-Lösung	
	Von 1 – 5	Punkte 1 - 3	Punkte x Gewicht	Punkte 1 - 3	Punkte x Gewicht
Anschaffungskosten	5	1	5	3	15
Wiederkehrende Kosten	4	3	12	1	4
Ausfallsicherheit	3	1	3	2	6
Wartung	1	1	1	2	2
Dynamik	2	2	4	3	6
Schutz vor Datenverlust	4	2	8	3	12
Schutz vor unbefugtem Datenzugriff	5	3	15	2	10
			48		55

Tabelle 3 Nutzwertanalyse

Die Nutzwertanalyse bietet nach der subjektiven Gewichtung der Kriterien als Entscheidungshilfe die Nutzung der „IaaS-Lösung“ an.
Für die Gewichtung wurden 1-5 Punkte vergeben, wobei 1 als eher weniger relevant und 5 als äußerst relevant aus Sicht des Kunden gilt. Die Punkte 1-3 entsprechen wiederum 1 für eher nicht erfüllt und 3 für in vollem Umfang erfüllt. Die Gesamtpunktezahl errechnet sich aus der Summe der Punkte, die zuvor für die einzelnen Kriterien vergeben und mit der Gewichtung multipliziert wurden.

2.6 Vertragsabschluss

Nach dem Gespräch und der Vorstellung beim Kunden bat dieser um einen Tag Bedenkzeit.
Am folgenden Tag hat sich der Kunde für das Angebot mit der „IaaS-Lösung“ entschieden und uns beauftragt dieses Projekt durchzuführen.

3 Projektdurchführung

3.1 Netzwerkumgebung

3.1.1 VPN

3.1.1.1 Einrichtung der IPSec Site To Site VPN-Verbindung

Zu Beginn der Durchführung wurde die IPsec Site To Site VPN-Verbindung zwischen der Filiale und der RZ-Umgebung eingerichtet. Die Firewall im RZ besitzt eine statische öffentliche IPv4-Adresse und erhält deshalb die Funktion des „Servers“. Das betrifft das „Startverhalten“ der Verbindung zwischen den Firewalls. Die Firewall im RZ antwortet in diesem Fall, während die in der Filiale des Pflegedienstes die Verbindung initiieren muss. Bei der Einrichtung muss das lokale und das remote Gateway/Interface angegeben werden, welches für die Verbindung verwendet werden darf. Als Methode wird IKE eingesetzt. Zusätzlich muss die IP-Adresse dieser Schnittstelle eingetragen werden. Im Falle des Remote-Gateways ist keine feste öffentliche IPv4-Adresse vorhanden gewesen weshalb stattdessen die unspezifische IPv4-Adresse 0.0.0.0/0 hier Anwendung findet. Die Authentifizierung findet mittels PSK statt. Eine Dead Peer Detection wird ebenfalls aktiviert, um die Verbindungsaktivität zu prüfen. Als Verschlüsselungsalgorithmus wähle ich den „AES-256-Standard“ der nach den aktuellen Sicherheitsbestimmungen als sicherer Standard gilt. Als Hashverfahren wähle ich „SHA2-256“. Auch dieses Verfahren gilt derzeit als sicher. Außerdem nutze ich die Diffie-Hellman Group 14 für einen 2048-bit key. Die Diffie-Hellman Group definiert die Schlüssel-Stärke während des Key-Exchange Prozesses. Die Key Lifetime wird auf 1h beschränkt.
Diese Einstellungen wurden nun auf der Firewall im RZ festgelegt. Die Gegenstelle in der Filiale benötigt zum Initiieren der Verbindung nun dieselben Einstellungen. Lediglich die Local/remote-Gateway ID muss entsprechend der Umgebung angepasst werden. Außerdem muss das Startverhalten von Antworten auf Initiieren umgeschaltet werden. Was ich zuvor nicht erwähnte, die gewünschten Netzwerke müssen bei der Konfiguration unter Freizugebene Netzwerke ebenfalls eingetragen werden (beide Seiten). Damit wäre die Phase1 der Ike/IPsec-Verbindung festgelegt. Die Einstellungen für Phase 2 sind entsprechend der Einstellungen in Phase 1 gewählt. Lediglich die Key-Lifetime beträgt in Phase 2 8 statt einer Stunde.

3.1.1.2 Einrichtung der SSL End To Site VPN-Verbindung

Für den mobilen Zugriff auf den Terminalserver habe ich zusätzlich eine SSL End To Site VPN-Verbindung auf der Firewall im RZ eingerichtet. Dazu habe ich zunächst die Firewall mit dem AD-Verzeichnisdienst des Domänencontrollers verbunden, um die Sicherheitsgruppen der AD für einen geringeren Administrationsaufwand zu nutzen. Dafür habe ich zunächst einen separaten Account in der AD erstellt, der zum Beitritt in die Domäne berechtigt ist. Anschließend habe ich die erforderlichen Zugangsdaten sowie die IPv4-Adresse des Domänencontrollers als Nameserver auf der Firewall

hinterlegt. Danach war die Verbindung bereits aktiv und der Verzeichnisdienst synchronisiert. Da alle Mitarbeiter einen VPN-Zugriff von unterwegs bekommen sollen habe ich auf der Firewall die Benutzergruppe „xnet-rw-user“ erstellt, die mit der AD-Sicherheitsgruppe „Domänen-Benutzer“ synchronisiert wird. Die Gruppe erhielt von mir die Berechtigung zur Nutzung von SSL-VPN und den Zugriff auf das Userinterface, welches ich unter dem Port 4331 bereitgestellt habe. Dann habe ich eine neue Zertifikatskette erstellt, die zur Authentifizierung der Clients an der Firewall genutzt wird. Dazu habe ich eine CA, ein Serverzertifikat mit Verweis auf die CA und ein Clientzertifikat mit Verweis auf die CA erstellt. Der zuvor erstellten Gruppe habe ich das Client-Zertifikat hinterlegt. Nun habe ich mit der eigentlichen Konfiguration der „SSL-VPN-RW“ Verbindung begonnen. Über den Assistenten habe ich in 5 Schritten die Konfiguration hinterlegt. Im ersten Schritt habe ich den Verbindungstyp festgelegt (Roadwarrior Server). Im 2. Schritt konnte festgelegt werden, ob IPv6 über IPv4 verwendet werden soll, hier habe ich die Funktion deaktiviert, da IPv6 beim Kunden keine Anwendung findet. Im 3. Schritt mussten die lokalen Einstellungen hinterlegt werden, die für die Verbindung relevant sind. Dazu gehört die Benennung der Konfiguration, das zu verwendende Transportprotokoll (UDP), der Port (1194) das zu hinterlegende Serverzertifikat und die freizugebenden lokalen Netzwerke (192.168.2.0/24). Im 4. Schritt habe ich das Tunnelnetzwerk bzw. Transfernetz angegeben, das für die Verbindung genutzt werden soll. Aufgrund der noch eher geringen Anzahl an aktiven Benutzern habe ich mich für das „172.16.0.0/27“ Transfernetz entschieden. Es bietet eine maximale Anzahl von 30 Hosts und bietet somit genügend IPv4-Adressen für alle Mitarbeiter und eine trotzdem kleinere Broadcastdomäne, was den Traffic verringert und die Performance erhöhen kann. Im 5. Schritt legte ich die Methode für die Benutzerauthentifizierung fest. Dazu gibt es 3 verschiedene Auswahlmöglichkeiten. Ich wählte die Methode „Local“ da „None“ und „Radius“ nicht möglich sind. „None“ ist für Authentifizierung über AD-Gruppen ungeeignet und für „Radius“ würde der zugehörige RADIUS-Server fehlen. Nachdem der Assistent dann erfolgreich abgeschlossen wurde, musste der SSL-VPN-Dienst der Firewall neugestartet werden, um die Verbindung zu aktivieren. In den „Impliziten Regeln“ der Firewall mussten dann nur noch die Funktionen „SSL-VPN über UDP erlauben“ und „Userinterface“ aktiviert werden.

3.1.2 Portfilter

Der Portfilter auf der Firewall im RZ musste um Netzwerkobjekte und Zugriffsbeschränkungen erweitert werden. Dafür habe ich die notwendigen Ports ermittelt, die für ausgehende Verbindungen der genutzten Anwendungen genutzt werden und diese explizit freigegeben, um den Bereich der freigegebenen Ports zu verringern und so die Sicherheit zu erhöhen. Dabei handelte ich nach dem Minimalprinzip. Die Ermittlung der notwendigen Ports erfolgte dabei durch die Dokumentationen der Hersteller und das Log der Firewall auf, der die Verbindungszugriffe mitprotokolliert werden. Für eine bessere Übersicht habe ich die Regeln in Regelgruppen unterteilt. So entstanden die Regelgruppen „rgrp int net > internet“, „rgrp internet > int net“, „rgrp xnet > int net“ und „rgrp int net > xnet“.

3.2 Serverkonfiguration

3.2.1 Installation

Die bereitgestellten Server erreiche ich wie auch die Firewall im RZ über den bereitgestellten VPN-Client. Die 3 Server sind bereits mit Microsoft Windows Server 2019 als Betriebssystem ausgestattet. Die Server besitzen statische IPv4-Adressen von 192.168.2.10 aufwärts. Vor der Installation der Rollen und Features stelle ich noch die Aktualität des Betriebssystems sicher und installierte über den Windows-Update Dienst fehlende Patches.
Die Installation der Server Rollen und Features erfolgt über den „Server-Manager“ weitestgehend automatisch. Dafür habe ich die erforderlichen Rollen und Dienste wie folgt ausgewählt und installiert:

System	SRV-DC-01	SRV-RDP-01	SRV-APP-01
Installierte Rollen/Dienste	- Active Directory / Domänendienste - DNS-Server - Druckserver - Remotedesktop-Lizenzserver	- Remotedesktop-Sitzungshost (sessionbasiert) - Remotedesktop-Verbindungsbroker	Keine

Tabelle 4 Server Rollen und Dienste

3.2.2 Konfiguration

3.2.2.1 Active Directory / Domänendienste

Die Active Directory / Domänendienste konfigurierte ich mit einer neuen Gesamtstruktur „kunde.local“. Der erstellten Gesamtstruktur füge ich 5 neue „OUs“ hinzu, „RDP-Server“, „Kunde“, „GF“ und „Mitarbeiter“ als untergeordnete „OU“ von „Kunde“ sowie „Test“ als dedizierte „OU“ zum Testen von Gruppenrichtlinien. Die neuen Benutzer erstelle ich entsprechend der erhaltenen Namensliste nach der Namenskonvention „m.mustermann“ (Max Mustermann). Zusätzlich erstellte ich die globalen Sicherheitsgruppen „Geschaeftsfuehrung“, „Verwaltung“ und „PDL“. Die Sicherheitsgruppe „Geschaeftsfuehrung“ wurde der OU „GF“ und die anderen der OU „Mitarbeiter“ zugeteilt.

3.2.2.2 Druckserver und Drucker

Im Anschluss installierte ich die Drucker aus der Filiale, die per IP-Adresse angebunden wurden mit den entsprechenden Treibern über die Druckerverwaltung des Druckservers. Dabei passte ich die Standardeinstellungen für die Drucker so an, dass stets das Papierfach mit dem A4 blanko Papier als Papierquelle zum Drucken gewählt

wird. Anschließend fügte ich die bereits installierten Drucker erneut über den bestehenden Port zu und passte dafür den Namen sowie die Standardeinstellungen des Drucks so an, dass diesmal das Papierfach mit dem Briefpapier als Papierquelle gewählt wird. Die Benennung erfolgte nach der Namenskonvention „Druckerstandort – Papierformat“ z.B. „Großraumbüro hinten – A4 Blanko“.

3.2.2.3 Verzeichnisstruktur / Datei-Dienste

Für die Benutzer wurden von mir Freigaben erstellt. Die Freigaben besitzen den physischen Pfad „E:\Shares\%Freigabename%“ wobei der Freigabename der Verzeichnisse „GF“, „PDL“, „Verwaltung“ und „Daten“ gemeint ist. Die Freigabeberechtigungen wurden entsprechend der Sicherheitsgruppen spezifiziert. Die Zugriffsberechtigungen werden vom Hauptverzeichnis (Freigabeverzeichnis) vererbt.

3.2.2.4 Gruppenrichtlinien

3.2.2.4.1 Drucker und Laufwerke

Die Drucker sowie die Freigabeverzeichnisse habe ich anhand mehrerer GPOs an die jeweiligen Empfangsberechtigten verteilt. Dazu erstellte ich insgesamt 5 Gruppenrichtlinienobjekte, „Laufwerke Jeder“, „Laufwerke GF“, „Laufwerke PDL“, „Laufwerke Verwaltung“ und „Drucker“. Die Gruppenrichtlinienobjekte beinhalten dem Namen entsprechend die Laufwerkszuordnung für die betroffenen OUs.

3.2.2.4.2 Startmenü und Taskleiste

Um einen ungewollten Neustart oder das Herunterfahren des Systems zu unterbinden habe ich zusätzliche Richtlinien zur Verweigerung dieser erstellt.

3.2.2.4.3 Aufgabenplanung

Eine weitere GPO zur Aufgabenplanung habe ich erstellt um das Erstellen, Beenden und Löschen von Aufgaben zu unterbinden.

3.2.2.4.4 Dateiexplorer

Eine weitere GPO regelt das Verhalten des Dateiexplorers für die Benutzer. Um die Handhabung mit den Verzeichnissen zu erleichtern habe per Richtlinie alle irrelevanten Laufwerke des „Arbeitsplatzes“ ausblenden lassen.

3.2.2.4.5 Remotedesktopdienste

Ich habe weiter Richtlinien erstellt, die z.B. das Speichern der Kennwörter im Remotedesktop-Verbindungsclient unterbinden. Eine weitere Richtlinie diente wiederum dem Remotedesktop-Sitzungshost dazu den korrekten Lizenzierungsmodus und den entsprechenden Lizenzserver festzulegen.

3.2.2.5 Konfiguration des Remotedesktop-Lizenzservers

Die Konfiguration des Remotedesktop-Lizenzservers erfolgte über den Remotedesktop-Lizenzserver-Manager. Die Lizenz zur Registrierung des Lizenzservers habe ich bei der Wortmann AG per Mail angefragt und erhalten.

3.2.3 Installation der Software

Adobe Acrobat Reader DC und die Microsoft 365 Apps wurden von mir auf dem Terminalserver (SRV-RDP-01) installiert. Letztere wurde zuvor per XML-Datei vor der Installation angepasst und dann über das „OfficeDeploymentTool“ heruntergeladen und installiert. Dabei wurden einige Produktbestandteile von der Installation ausgenommen um Ressourcen zu schonen, da diese vom Kunden nicht genutzt werden sollen. Zudem wurden auf allen 3 Servern die ESET Filesecurity und der Client für unser Monitoring und Patchmanagement installiert.

Die Branchensoftware „Heimbas“ wurde vom Anbieter auf dem Server „SRV-APP-01“ installiert. Auf die Software kann per Client vom RDP-Server „SRV-RDP-01“ zugegriffen werden. Dieser ist als Verknüpfung auf dem Desktop für alle Benutzer hinterlegt.
Datev Unternehmen Online verbleibt als einziges auf dem Arbeitsplatz der Verwaltungskraft, da die Anwendung zum direkten Hochladen von eingescannten Dokumenten einen lokal angeschlossenen Drucker/Scanner benötigt.

3.2.4 Einrichtung der Datensicherung

Für die Sicherung der Daten vor Verlust habe ich die Wortmann Cloud Sicherung auf den 3 Servern eingerichtet. Die Sicherung erfolgt über einen Agenten, den man auf den ausgewählten Systemen installiert. Anschließend kann über das Webportal der Cloud die Einrichtung und Verwaltung der Systeme erfolgen. Dafür wird zunächst der Kunde im Portal mit der bereitgestellten Sicherungsumgebung verknüpft. Dann werden die Systeme dem Kunden zugeordnet. Im Anschluss können dann Sicherungspläne erstellt werden. Bei der verwendeten Sicherungsart handelt es sich um synthetische Vollbackups. Ich habe für die 3 Server einen täglichen und einen monatlichen Zeitplan erstellt. Beide Zeitpläne beinhalten jeweils den gesamten Server. Die täglichen Sicherungen werden 30 und die monatlichen 365 Tage lang aufbewahrt.

3.2.5 Migration der Daten

Die Daten und Verzeichnisse des alten Systems habe ich per SMB-Zugriff auf den Domaincontroller über die Anwendung „Total Commander“ kopiert bzw. übertragen. Die Zuordnung der Verzeichnisse zu den neuen Freigaben erfolgte nach Absprache mit dem Kunden. Die Daten wurden ohne ACL-Attribute übertragen. Die Übertragung diente hierbei gleichzeitig der Überprüfung der Verbindungsqualität.

3.2.6 Einrichtung der Microsoft 365 Benutzer

Während der Datenübertragung nutzte ich die Zeit zum Einrichten der Microsoft 365 Benutzer. Diese habe ich über das Microsoft 365 Admin Center zunächst erstellt und dann in den Microsoft 365 Apps auf dem RDP-Server für jeden Benutzer hinterlegt. So konnte ich ebenfalls die Exchange Konten im Outlook Mail Client einrichten.

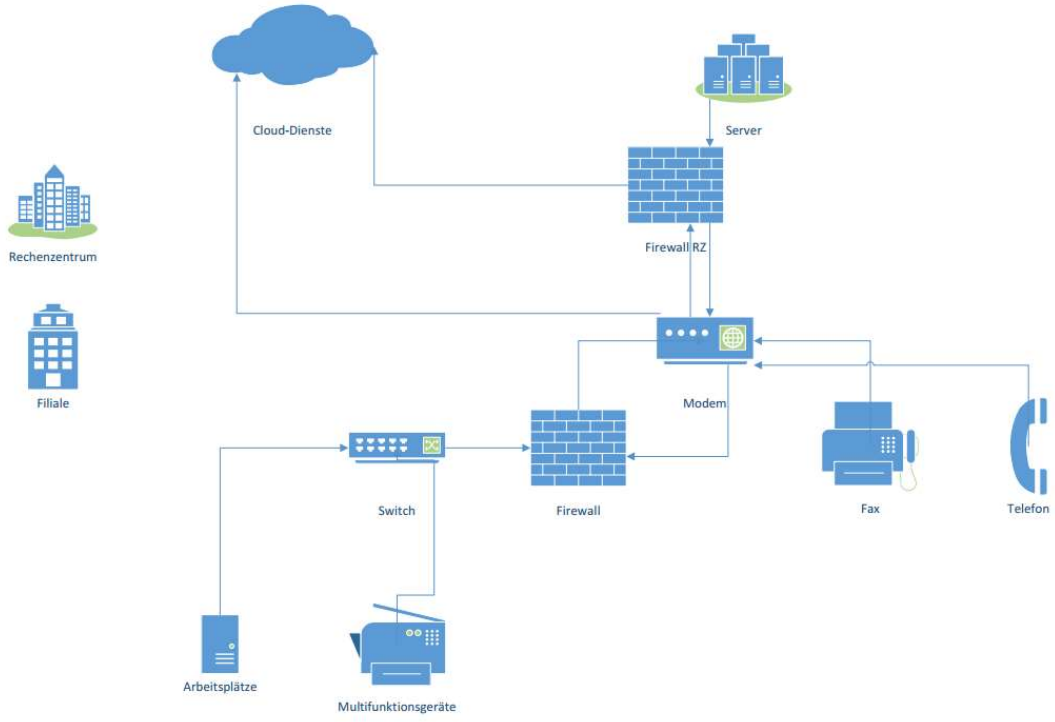
3.2.7 Tests

Bevor die finale Übergabe an den Kunden erfolgte, habe ich in enger Zusammenarbeit mit dem Kunden die neue IT-Infrastruktur getestet. Dafür wurde die neue Umgebung nach der Datenmigration vollständig in Betrieb genommen. Bei auftretenden Problemen habe ich in Bereitschaft schnell auf die Anfragen reagiert und diese bearbeitet. Die Bereitschaft für Anfragen bei Problemen habe ich während der der Erstellung der Dokumentationen eingeräumt.

Die Arbeit mit der neuen Umgebung erhielt zunächst viel positives Feedback in Bezug auf die viel performanteren Vorgänge, jedoch zeigten sich auch einige kleinere Probleme, die noch von mir bearbeitet wurden. Dabei handelte es sich vor allem um die Verwendung der Drucker. So wurden einigen Benutzern zusätzlich zu den freigegebenen Druckern auch die lokalen Drucker angezeigt, die für Verwirrung sorgten. Eine Anpassung der RDP-Verbindung-Clients schaffte hierbei Abhilfe. Die Umleitung der lokalen Ressourcen wie z.B. Drucker oder Laufwerke wurde deaktiviert. Das nächste war eine Problematik beim SMB Scan der Multifunktionsgeräte. Da die Benutzer zuvor in der Lage waren über ihre eigenen Laufwerke die Scans zu empfangen und zu verwalten, musste diese Konfiguration an allen Geräten angepasst werden. Dafür habe ich in den lokalen Adressbüchern der Multifunktionsgeräte einen einheitlichen Eintrag für einen SMB-Scan hinterlegt. Als Ziel habe ich ein Unterverzeichnis „Scans“ im Freigabeverzeichnis „Daten“ erstellt und freigegeben. Den UNC-Pfad habe ich im Adressbuch-Eintrag der MFGs hinterlegt sowie. Für den Zugriff habe ich einen extra Benutzer „Scans“ mit Zugriff auf das Unterverzeichnis angelegt und ebenfalls im Eintrag hinterlegt. Nach einem Test-Scan an jedem Gerät war für dieses Problem auch eine Lösung geschaffen. Diese Lösung habe ich den Mitarbeitern des Kunden kommuniziert.

4 Projektabschluss

In der Abbildung ist die neu geschaffene IT-Infrastruktur des Kunden skizziert dargestellt.



4.1 Fazit

Zum Abschluss des Projektes wurde überprüft welche Ziele technisch umgesetzt werden konnten und welche unerwarteten Probleme während des Projektes auftraten.

Tatsächlich konnten beinahe alle Ziele des Kunden umgesetzt werden. Die gewünschte Ausfallsicherheit konnte um ein Vielfaches verbessert werden. Statt einer durchschnittlichen Wiederherstellungszeit von ca. 24h bei einem hardwareseitigen Fehler, wird nun eine Wiederherstellungszeit von maximal 4h durch den Betreiber des RZs garantiert. Die Skalierbarkeit von Lizenzen und Ressourcen bietet zudem die größtmögliche Flexibilität in der finanziellen Gestaltung. Die Daten sind nach wie vor, vor unberechtigtem Zugriff durch Dritte abgesichert und zusätzlich besser vor Verlusten geschützt. Auch das standortunabhängige Arbeiten ist durch die mobilen VPN-Clients nun problemlos möglich.

Die Durchführung des Projektes verlief im Allgemeinen sehr gut. Es sind kaum Probleme aufgetreten und die Probleme, die auftraten konnten innerhalb der anvisierten Reaktionszeit bearbeitet und gelöst werden. Grund dafür dürfte vor allem die geplante Testphase sein. In dieser haben die Mitarbeiter, von sich aus, die

Funktionen des Systems auf ihre Korrektheit geprüft. Die Kommunikation verlief dabei ebenfalls sehr gut.

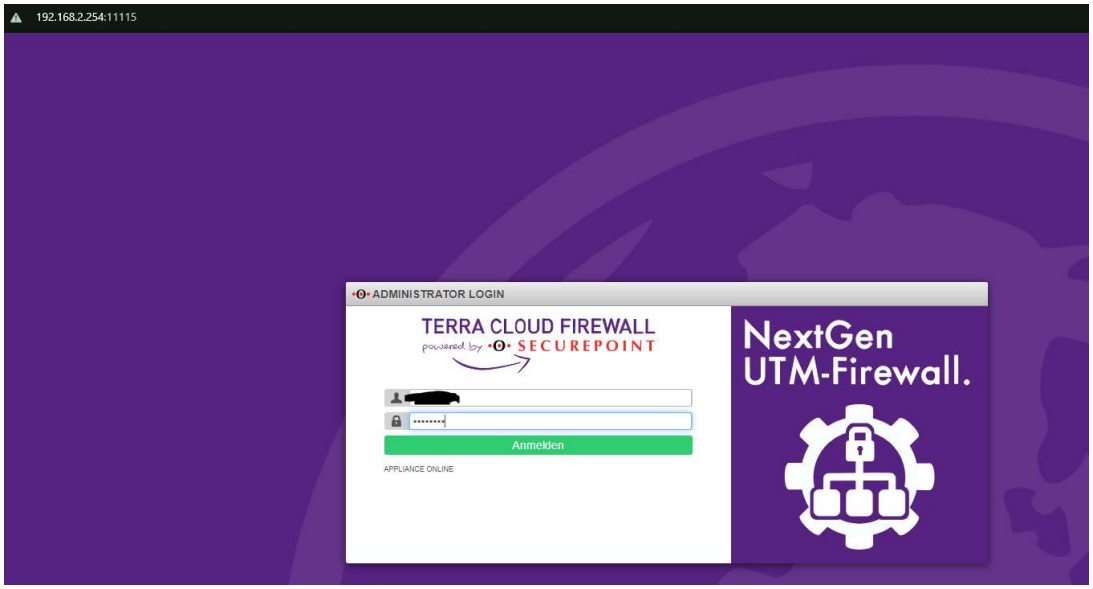
Der Kunde ist insofern sehr zufrieden mit der Projektdurchführung und dem Ergebnis. Gerade in Bezug auf die vorherigen Bedenken bezüglich der Datensicherheit ist der Kunde erleichtert. Ich bitte um Verständnis, dass entsprechende Vereinbarungen zum Datenschutz an dieser Stelle nicht näher dargestellt werden können. Die Vereinbarungen zum Datenschutz werden immer direkt zwischen uns und dem Auftraggeber individuell vereinbart. Wir haben zusätzlich zu der Vereinbarung mit dem Kunden eine Vereinbarung mit unseren Partnern, die die geltenden Datenschutzbestimmungen gewährleisten, jedoch dürfen auch diese hier nicht dargestellt werden.

5 Anhang

5.1 Betriebsdokumentation

5.1.1 Einrichtung der IPSec Site To Site VPN-Verbindung

Die Einrichtung der IPSec Site To Site Verbindung habe ich mithilfe der von Securepoint bereitgestellten Dokumentation eingerichtet (s.). Bevor mit der Konfiguration gestartet werden konnte musste zunächst eine SSL-VPN Verbindung mit der Firewall im RZ hergestellt werden. Die Daten dafür wurden von Wortmann bereitgestellt. Anschließend konnte über das Webinterface der Firewall die Konfiguration vorgenommen werden. Diese erreichte man über die interne IPv4-Adresse (192.168.2.254) per https unter Verwendung des Ports 11115.



Nach der Anmeldung wird unter VPN>IPSec>IPSec Verbindung hinzufügen der Assistent für die Einrichtung der Konfiguration aufgerufen.

In 4 Schritten wird dann die grundsätzliche Konfiguration der VPN-Verbindung erstellt.

Im ersten Schritt wählt man den Verbindungstyp aus. In diesem Fall wurde „Site To Site“ ausgewählt.

Im zweiten Schritt trägt man dann den Namen, die Authentifizierungsmethode und die zu verwendende IKE Version aus.

Für die Konfiguration wurde die PSK Authentifizierung und IKEv2 gewählt.

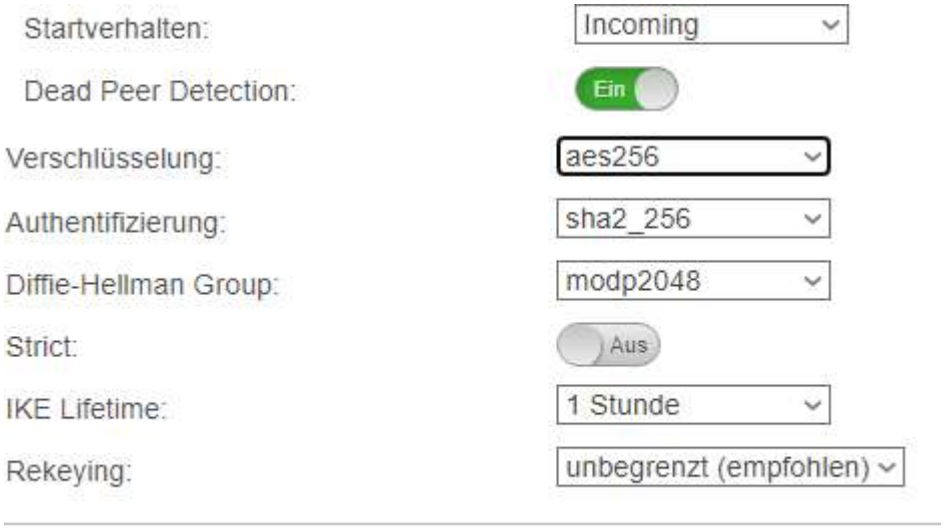
In Schritt 3 des Assistenten werden die Local Gateway ID und das freizugebende Netzwerk festgelegt. Die Local Gateway ID beschreibt die Schnittstelle der Firewall, an dem die Verbindung anliegt.

Hier wurde entsprechend die WAN-Schnittstelle (eth0) als Local Gateway ID und das interne Netzwerk (192.168.2.10) festgelegt.

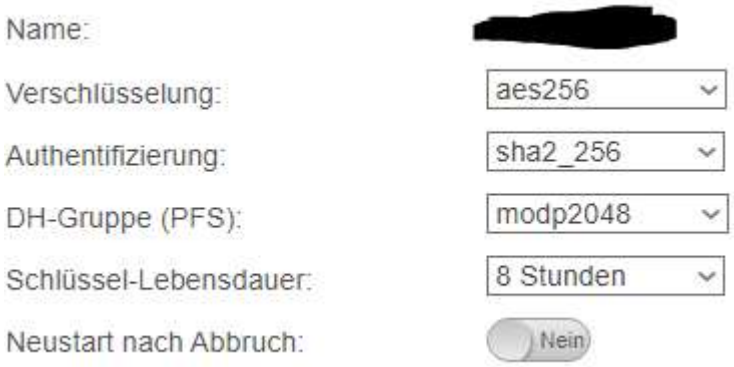
Im letzten Schritt werden dann die Werte für das Remote Gateway, die Remotegateway ID und das dort freigegebene Netzwerk festgelegt.

Da das Remote Gateway nicht über eine statische IP-Adresse verfügt musste an dieser stelle die unspezifische Adresse „0.0.0.0“ hinterlegt werden. Als freigegebenes Netzwerk der Gegenstelle wurde zudem entsprechend das Netzwerk 192.168.200.0/24 eingetragen.

Nach Abschluss des Assistenten wurden noch die Parameter für die 2 IKE Phasen angepasst und das Startverhalten der Verbindung für dieses Gateway festgelegt. Außerdem wurde die Dead Perr Protection aktiviert, die für eine korrekten Verbindungsstatus von Vorteil sein kann.



Für IKE Phase 2 wurden entsprechend diese Werte festgelegt.



Damit ist die Konfiguration der IPSec Verbindung auf der Firewall im RZ abgeschlossen. Lediglich die entsprechenden Portfilterregeln müssen hier noch angelegt werden (s.Portfilter). Die Portfilterregeln wurden zu beginn durch die

„Impliziten Regeln“ ausgelassen. Die weitere Konfiguration erfolgt dann auf der Firewall des Kunden (RC100 Securepoint). Da diese dieselbe Konfigurationsoberfläche besitzt erspare ich hierbei die Dokumentation der Konfiguration und weise lediglich darauf hin, dass die Konfiguration entsprechend dieser zu wiederholen ist und lediglich das Startverhalten auf „Initiate“ gestellt wird.

5.1.2 Einrichtung der SSL-VPN End To Site Verbindung

Für die Einrichtung einer End To Site VPN-Verbindung gibt es zwei Möglichkeiten. Hier wurde die SSL-VPN Roadwarrior Server Variante genutzt. Für die Einrichtung wurde auf der Firewall im RZ mittels Assistenten eine Konfiguration erstellt. In 5 Schritten wurde der Assistent durchgeführt.

Im ersten Schritt musste unter VPN>SSL-VPN>SSL-VPN Verbindung hinzufügen der Verbindungstyp (Roadwarrior Server) festgelegt werden.

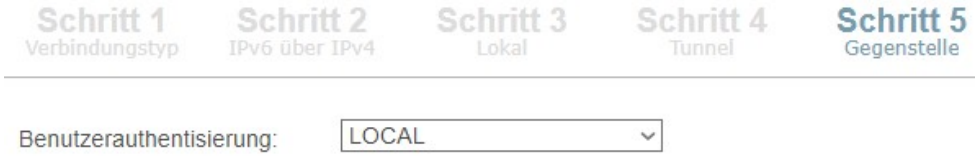
In Schritt 2 wird festgelegt, ob die Funktion IPv6 über IPv4 verwenden aktiv sein soll. Das wurde hier nicht verwendet, da nicht benötigt.

In Schritt 3 werden dann die lokalen Einstellungen für den Roadwarrior Server hinterlegt.

Die Werte entsprechen der Abbildung. Hier gilt es zusätzlich zu erwähnen, dass das Serverzertifikat zu einer Zertifikatskette gehört, die für die Verwendung von SSL-VPN notwendig ist und erstellt werden muss (s. Zertifikatskette erstellen). Im vierten Schritt muss das zu verwendende Transfernetzwerk festgelegt werden, welches der Vermittlung zwischen dem Roadwarrior Server und dem Client dient.

Das Transfernetz 172.16.0.0/27 wurde entsprechend der doppelten Anzahl der aktiven Nutzer gewählt und sollte im Idealfall mit keinem anderen Netzwerk auf der Server oder Client Seite übereinstimmen.

Im letzten Schritt wurde dann noch die Benutzerauthentisierung festgelegt.



Da beim Kunden die Domänen-Benutzer automatisch auch die SSL-VPN Benutzer darstellen sollen wurde hierfür bereits die Firewall an die AD angebunden und eine entsprechende lokale Benutzergruppe mit der AD-Sicherheitsgruppe „Domänen-Mitglieder“ verknüpft. Die Einrichtung der Konfiguration für SSL-VPN Raodwarrior Server ist damit grundsätzlich abgeschlossen.

5.1.3 Einrichtung Zertifikatskette für SSL-VPN

Die Einrichtung der Zertifikatskette für die SSL-VPN Roadwarrior Server Konfiguration kann direkt auf der Firewall erstellt und verwaltet werden. Dazu findet man unter Authentifizierung>Zertifikate eine Verwaltung. Zuerst erstellt man eine CA in der man die Unternehmensinformationen (obligatorisch) hinterlegt.

CA | ZERTIFIKATE | WIDERRUFEN | CRLS

Name	Gültig bis	Status	Algorithmus	
CA-sslvpn	31. Dez. 2037 23:59 Uhr	OK KEY	sha256 mit RSA Verschlüsselung	
CA-Xnet-[redacted]	31. Dez. 2037 23:59 Uhr	OK KEY	sha256 mit RSA Verschlüsselung	

Anschließend können im Reiter Zertifikate Server und Client Zertifikate erstellt werden, die auf einer der erstellten CAs basieren.

CA | ZERTIFIKATE | WIDERRUFEN | CRLS

Cert ID	Name	CA	Gültig bis	Status	Algorithmus	
163	sslvpn-server	CA-sslvpn	31. Dez. 2037 23:59 Uhr	OK KEY	sha256 mit RSA Verschlüsselung	
164	sslcert-admin	CA-sslvpn	31. Dez. 2037 23:59 Uhr	OK KEY	sha256 mit RSA Verschlüsselung	
214	Xnet-RW-Server	CA-Xnet-[redacted]	31. Dez. 2037 23:59 Uhr	OK KEY	sha256 mit RSA Verschlüsselung	
215	Xnet-RW-Group-[redacted]	CA-Xnet-[redacted]	31. Dez. 2037 23:59 Uhr	OK KEY	sha256 mit RSA Verschlüsselung	

Beim Erstellen des Serverzertifikats muss der Schalter „Serverzertifikat“ aktiviert werden. Die hinterlegten Cas und Zertifikate können an dieser Stelle auch widerrufen oder wiederhergestellt werden. Ein Import bzw. Export einer CA oder eines Zertifikats ist ebenfalls möglich.

5.1.4 Firewall AD-Anbindung

Die Firewall wurde an die AD angebunden, um dessen Verzeichnisdienst nutzen zu können. Um die Firewall anzubinden, wurde zunächst ein weiterer Domänen-Administrator erstellt, der für die Firewall AD Anbindung genutzt wird. Unter Authentifizierung>AD/LDAP-Anbindung kann über einen Assistenten wahlweise eine Anbindung an einen AD bzw. LDAP Verzeichnisdienst erfolgen. Dafür muss im ersten Schritt der Verbindungstyp, hier „AD – Active Directory“, festgelegt werden.

AD/LDAP AUTHENTIFIZIERUNGS ASSISTENT

Schritt 1 Verzeichnistyp | Schritt 2 Einstellungen | Schritt 3 Nameserver | Schritt 4 Beitreten

Verzeichnistyp: AD - Active Directory

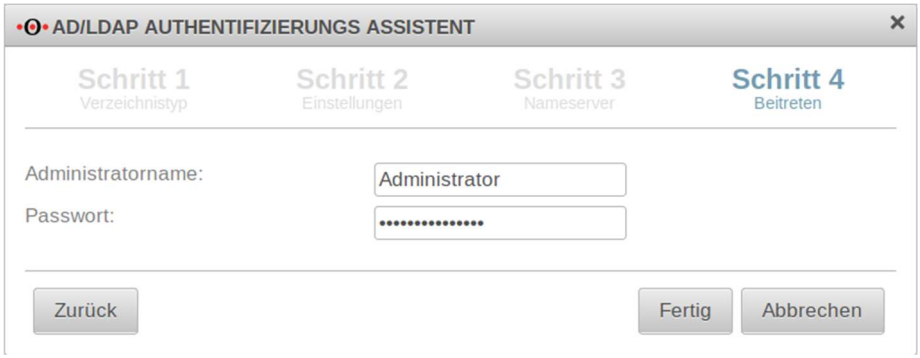
Weiter | Abbrechen

Im nächsten Schritt wurde dann die IPv4-Adresse des Domaincontrollers, die Domain, die Arbeitsgruppe und der Appliance Account festgelegt.

Die Werte sind durch „192.168.2.10“, „kunde.local“, „kunde“ und „Firewall“ zu ersetzen.

In Schritt 3 müssen die Nameserver der Domain (Domaincontroller) angegeben werden.

Hier wurde ebenfalls die IP-Adresse des Domaincontrollers hinterlegt. Im letzten Schritt wird der Benutzer für den Domänenbeitritt festgelegt.



Dafür wurde statt „Administrator“ der erstellte Benutzer „fw“ hinterlegt.

Mit einem Klick auf „Fertig“ werden die Einstellungen gespeichert und die Verbindung versucht herzustellen. Bei korrekter Konfiguration findet man folgendes Menü vor.

In den Reitern können die Einstellungen gelesen und verändert werden.

5.1.5 Einrichtung Benutzergruppe mit AD-Sync

Unter Authentifizierung>Benutzer im Reiter Gruppen können die lokalen Gruppen der Firewall verwaltet werden. Beim Hinzufügen der Gruppe wurden zunächst die Berechtigungen für die Gruppe gesetzt und der Gruppenname eingetragen. Die Gruppe benötigt für die Nutzung von SSL-VPN entsprechend die Berechtigung SSL-VPN und zum Downlaod der benötigten Konfigurationsdatei und Zertifikate die Berechtigung Userinterface.

Im Reiter SSL-VPN musste anschließend festgelegt werden, dass der OpenVPN-Client im Userinterface herunterladbar ist, welche SSL-VPN Verbindung, welches Client-Zertifikat und welches Remote Gateway verwendet werden soll.

Im Reiter Verzeichnis Dienst musste dann noch die entsprechende AD-Sicherheitsgruppe für die Verknüpfung mit der lokalen Gruppe festgelegt werden.

Da alle Mitarbeiter diesen Zugriff benötigten wurde entsprechend die Gruppe „Domänen-Benutzer“ zugeordnet.

Das Userinterface, über dass der Installer oder weitere Dienste z.B. bezüglich SSL-VPN genutzt werden können wurde von mir auf dem Port 4431 per https verfügbar gemacht. Dafür habe ich in den Servereinstellungen der Firewall den Port des Userinterface angepasst. Damit ist die Gruppenzuordnung bzw. Erstellung abgeschlossen.

5.1.6 Einrichtung der Domänen Gesamtstruktur

Für die neue Gesamtstruktur der Domäne müssen zunächst die erforderlichen Rollen und Features installiert werden. Beim Kunden wurden dem Server „SRV-DC-01“ die auf der Abbildung befindlichen Rollen und Features zugeordnet bzw. installiert.

Die Installation des DNS-Servers erforderte zudem die Konfiguration einer statischen IP-Adresse.

Eigenschaften von Internetprotokoll, Version 4 (TCP/IPv4)

Allgemein

IP-Einstellungen können automatisch zugewiesen werden, wenn das Netzwerk diese Funktion unterstützt. Wenden Sie sich andernfalls an den Netzwerkadministrator, um die geeigneten IP-Einstellungen zu beziehen.

○ IP-Adresse automatisch beziehen
◉ Folgende IP-Adresse verwenden:

IP-Adresse:	192 . 168 . 2 . 10
Subnetzmaske:	255 . 255 . 255 . 0
Standardgateway:	192 . 168 . 2 . 254

○ DNS-Serveradresse automatisch beziehen
◉ Folgende DNS-Serveradressen verwenden:

Bevorzugter DNS-Server:	127 . 0 . 0 . 1
Alternativer DNS-Server:	185 . 35 . 12 . 73

Nach Abschluss der Installation musste der Server zum Domaincontroller heraufgestuft werden. Dabei wurde die Gesamtstruktur der Domäne festgelegt.

Konfiguriert diesen Server als ersten Active Directory-Domänencontroller in einer neuen Gesamtstruktur.

Name der neuen Domäne: [redacted] Dies ist auch der Name der neuen Gesamtstruktur.

NetBIOS-Name der Domäne: [redacted]

Gesamtstrukturfunktionsebene: Windows Server 2016

Domänenfunktionsebene: Windows Server 2016

Zusätzliche Optionen:

Globaler Katalog: Ja

DNS-Server: Ja

DNS-Delegierung erstellen: Nein

Datenbankordner: C:\Windows\NTDS

Protokolldateiordner: C:\Windows\NTDS

Ordner "SYSVOL": C:\Windows\SYSVOL

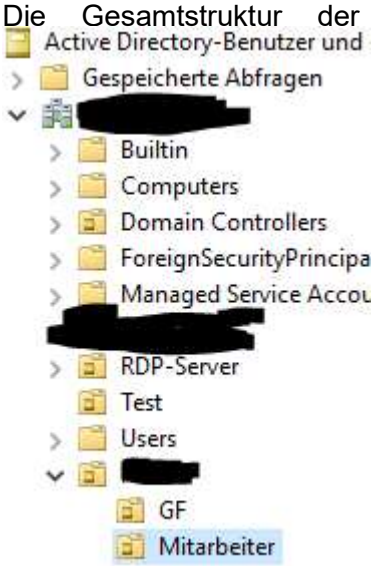
Der DNS-Serverdienst wird auf diesem Computer konfiguriert.

Der Computer wird so konfiguriert, dass dieser DNS-Server als bevorzugter DNS-Server verwendet wird.

Das Kennwort des neuen Domänenadministrators entspricht dem Kennwort des lokalen Administrators dieses Computers.

Hier wurde grundsätzlich mit den standardmäßigen Einstellungen von Microsoft gearbeitet.

Die Gesamtstruktur der Domäne konnte nun weiter angepasst werden.



Über die Verwaltungsanwendung „Active Directory-Benutzer und Computer“ wurden 5 OUs erstellt -wie dargestellt. Anschließend wurden die globalen Sicherheitsgruppen „PDL“, „Verwaltung“ und „Geschaeftsfuehrung“ erstellt. Die beiden erstgenannten wurden in der OU „Mitarbeiter“ und die Gruppe „Geschaeftsfuehrung“ in der OU „GF“ erstellt. Anschließend wurden nach diesem Schema die Benutzer erstellt und zugeordnet.

5.1.7 Erstellen von Verzeichnisfreigaben

Für die Benutzer wurden Freigaben erstellt. Die Freigaben besitzen den physischen Pfad „E:\Shares\%Freigabename%“ wobei der Freigabename der Verzeichnisse „GF“, „PDL“, „Verwaltung“ und „Daten“ gemeint ist. Die Freigabeberechtigungen wurden entsprechend der Sicherheitsgruppen spezifiziert. Die Zugriffsberechtigungen werden vom Hauptverzeichnis (Freigabeverzeichnis) vererbt. Mitglieder der Sicherheitsgruppe „Geschaeftsfuehrung“ haben Vollzugriff auf alle Verzeichnisse. Mitglieder der Sicherheitsgruppe „PDL“ besitzen Vollzugriff auf das Verzeichnis „PDL“ sowie „Daten“. Mitglieder der Sicherheitsgruppe „Verwaltung“ besitzen Vollzugriff auf das Verzeichnis „Verwaltung“ und „Daten“. Alle anderen Benutzer und Gruppen (Ausnahme von Administratoren oder System) besitzen Lese/Schreib/Änder-Berechtigungen auf das „Daten“ Verzeichnis.

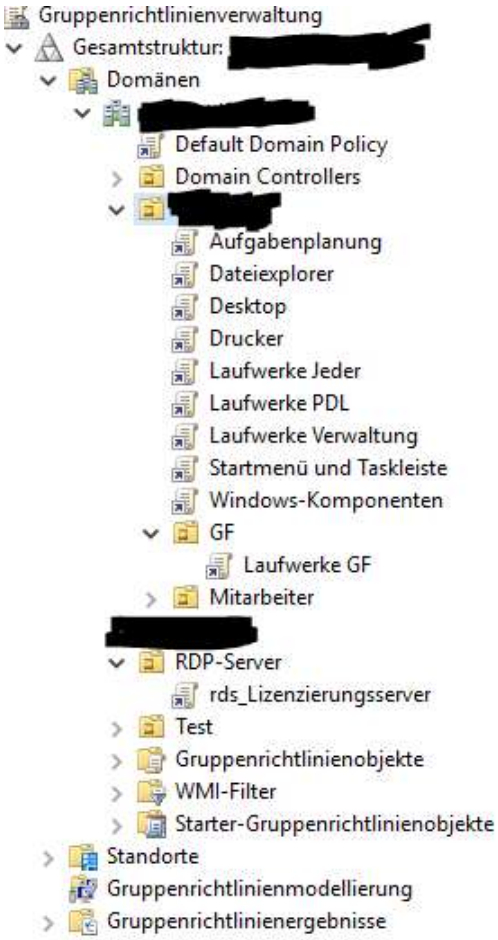
5.1.8 Druckserver und Drucker

Im Anschluss installierte ich die Drucker aus der Filiale, die per IP-Adresse angebunden wurden mit den entsprechenden Treibern über die Druckerverwaltung des Druckservers. Dabei passte ich die Standardeinstellungen für die Drucker so an, dass stets das Papierfach mit dem A4 blanko Papier als Papierquelle zum Drucken gewählt wird. Anschließend fügte ich die bereits installierten Drucker erneut über den bestehenden Port zu und passte dafür den Namen sowie die Standardeinstellungen des Drucks so an, dass diesmal das Papierfach mit dem Briefpapier als Papierquelle

gewählt wird. Die Benennung erfolgte nach der Namenskonvention „Druckerstandort – Papierformat“ z.B. „Großraumbüro hinten – A4 Blanko“.

5.1.9 Erstellen der Gruppenrichtlinien

Für die erstellten OUs wurden Gruppenrichtlinienobjekte erstellt.



Die Benennung der Objekte orientiert sich an der jeweiligen Funktion bzw. Anpassung die von ihm vorgenommen wird.

5.1.9.1 Drucker und Laufwerke

Die Drucker sowie die Freigabeverzeichnisse habe ich anhand mehrerer GPOs an die jeweiligen Empfangsberechtigten verteilt. Dazu erstellte ich insgesamt 5 Gruppenrichtlinienobjekte, „Laufwerke Jeder“, „Laufwerke GF“, „Laufwerke PDL“, „Laufwerke Verwaltung“ und „Drucker“. Die Gruppenrichtlinienobjekte beinhalten dem Namen entsprechend die Laufwerkszuordnung für die betroffenen OUs. Die Laufwerke wurden mit der Option „Ersetzen“ und dem Freigabepfad unter Benutzerkonfiguration>Einstellungen>Windows-Einstellungen>Laufwerkszuordnungen erstellt. Für die Laufwerke wurden Laufwerksbuchstaben vergeben und die Option Laufwerk einblenden aktiviert. Die Buchstaben „O“, „G“, „P“ und „V“ wurden entsprechend dieser Reihenfolge für die Verzeichnisse „Daten“, „GF“, „PDL“ und „Verwaltung“ vergeben. Für die Gruppenrichtlinienobjekte, die sich auf „PDL“ und „Verwaltung“ beziehen habe ich außerdem im Reiter „Gemeinsame Optionen“ den

Punkt „Zielgruppenadressierung auf Elementebene“ aktiviert. Dazu musste ich Kriterien Festlegen anhand derer die Zielgruppenadressierung stattfinden soll. Für die „PDL“ nutze ich die Kriterien „Ist Mitglied der Sicherheitsgruppe <SID PDL> oder ist Mitglied der Sicherheitsgruppe <SID GF>“. Für die „Verwaltung“ nutzte ich entsprechend „Ist Mitglied der Sicherheitsgruppe <SID Verwaltung> oder Ist Mitglied der Sicherheitsgruppe <SID GF>“. Die Kriterien sichern die korrekte Zuweisung der Laufwerke. Für die Drucker habe ich eine GPO „Drucker“ erstellt, die jedem Benutzer der Domäne alle Drucker der Filiale zuteilt. Unter dem Zweig Benutzerkonfiguration>Einstellungen>Systemsteuerungseinstellungen>Drucker habe ich 10 Objekte (Drucker) hinterlegt, die mit der Aktion „Ersetzen“ verbunden werden. Dafür habe ich lediglich den Freigabepfad des Druckers hinterlegt und keine weitere Zielgruppenadressierung vorgenommen. Die GPO habe ich dann mit der OU „Kunde“ verknüpft. Diese GPO wird somit bei aktiver Vererbung an Unterverzeichnisse jeglicher Art vererbt. Über einen Benutzer „Testuser“ habe ich die Übernahme der Gruppenrichtlinien getestet. Zusätzlich habe ich weitere Benutzer „Testgf“, „Testpdl“ und „Testvw“ zur Überprüfung der Gruppenrichtlinienobjekte genutzt.

5.1.9.2 Startmenü und Taskleiste

Um einen ungewollten Neustart oder das Herunterfahren des Systems zu unterbinden habe ich zusätzlich im Zweig Benutzerkonfiguration>Richtlinien>Administrative Vorlagen>Startmenü und Taskleiste die Einstellungen „Befehle Herunterfahren, Neustarten, Energiesparen und Ruhezustand ausblenden und Zugriff verweigern“ sowie „Option Abmelden dem Startmenü hinzufügen“ aktiviert. Diese Einstellungen verhindern das Herunterfahren oder Neustarten des Systems und bieten zudem die Funktion Abmelden für die RDP-Sitzung im Startmenü an. Diese GPO habe ich ebenfalls der OU „Kunde“ zugeordnet.

5.1.9.3 Aufgabenplanung

Eine weitere GPO zur Aufgabenplanung habe ich erstellt um das Erstellen, Beenden und Löschen von Aufgaben zu unterbinden. Unter Benutzerkonfiguration>Richtlinien>Administrative Vorlagen>Windows-Komponenten>Aufgabenplanung habe ich deshalb die Richtlinien „Erstellen von neuen Aufgaben nicht zulassen“, „löschen von Aufgaben nicht zulassen“ und „Ausführen oder Beenden einer Aufgabe verhindern“ aktiviert. Die GPO habe ich anschließend mit der OU „Kunde“ verknüpft.

5.1.9.4 Dateiexplorer

Eine weitere GPO regelt das Verhalten des Dateiexplorers für die Benutzer. Um die Handhabung mit den Verzeichnissen zu erleichtern habe per Richtlinie alle irrelevanten Laufwerke des „Arbeitsplatzes“ ausblenden lassen. Zusätzlich habe ich die folgenden Richtlinien aktiviert, „Benachbarte Computer nicht unter Netzwerkumgebung anzeigen“, „CD-Brennfunktion entfernen“, „Den Menüeintrag Verwalten im Kontextmenü des Datei-Explorers ausblenden“, „Gemeinsame Dokumente vom Arbeitsplatz entfernen“,

„Optionen Netzlaufwerk verbinden und Netzlaufwerk trennen entfernen“, „Registerkarte Hardware entfernen“, „Registerkarte Sicherheit entfernen“ und „Symbol Gesamtes Netzwerk nicht in Netzwerkumgebung anzeigen“. Die Richtlinien sollen den Benutzern helfen die richtigen Verzeichnisse beim Speichern zu wählen, indem die Möglichkeiten zur Auswahl ganz einfach beschränkt werden. Diese GPO habe ich ebenfalls der OU „Kunde“ zugewiesen.

5.1.9.5 Remotedesktopverbindungs-Client

Das Speichern von Kennwörtern für die Remotedesktopverbindungs-Clients habe ich unterbunden, indem ich eine GPO erstellt habe, die die Richtlinie „Speichern von Kennwörtern nicht zulassen“, im Zweig Benutzerkonfiguration>Richtlinien>Administrative Vorlagen>Windows-Komponenten>Remotedesktopdienste>Remotedesktopverbindungs-Client, aktiviert.

5.1.9.6 Desktop

Unter Benutzerkonfiguration>Richtlinien>Administrative Vorlagen>Desktop habe ich zuletzt dann noch die Richtlinien „Eintrag Eigenschaften aus dem Kontextmenü des Arbeitsplatzes“, „Internet Explorer-Symbol auf dem Desktop ausblenden“, „Symbol Netzwerkumgebung auf dem Desktop ausblenden“, „Freigaben von zuletzt geöffneten Dateien nicht in Netzwerkumgebung hinzufügen“ und „Manuelle Umleitung der Profilordner durch Benutzer verhindern“ aktiviert. Auch diese Einstellungen sollen den Benutzern dienen, um die Handhabung mit dem Speichern von Dateien zu vereinheitlichen und zu erleichtern. Die GPO wurde ebenfalls mit der OU „Kunde“ verknüpft.

5.1.9.7 Remotedesktop-Sitzungshost

Für den Remotedesktop-Sitzungshost habe ich ebenfalls eine GPO erstellt. Die erstellte GPO beinhaltet die Richtlinien zur Konfiguration des Lizenzierungsmodus sowie des Remotedesktop-Lizenzservers. Die Richtlinien sind hier in der Computerkonfiguration im Zweig Richtlinien>Administrative Vorlagen>Windows-Komponenten>Remotedesktopdienste>Remotedesktop-Sitzungshost>Lizenzierung zu finden. Als Lizenzierungsmodus habe ich „Pro Benutzer“ und als Lizenzserver „192.168.2.10“ bzw. „SRV-DC-01“ gewählt. Diese GPO habe ich dann mit der erstellten OU „RDP-Server“ verknüpft.

5.1.10 Installation des RDP-Servers

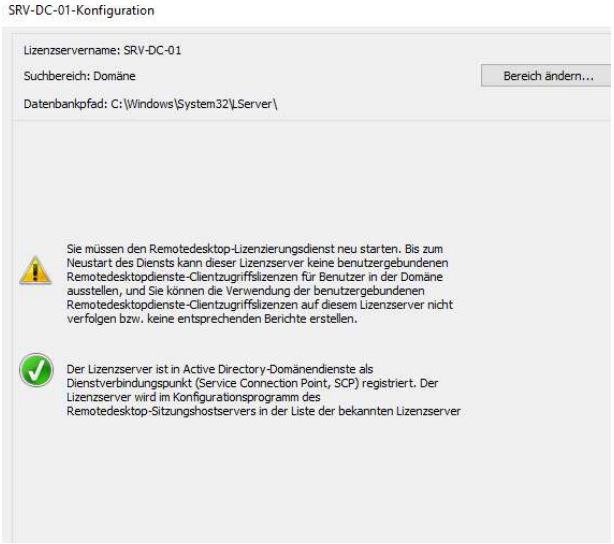
Die Installation des RDP-Servers erfolgte über den Server Manager weitestgehend automatisch. Die Rollen und Dienste wurden auf den Servern „SRV-DC-01“ und „SRV-

RDP-01“ entsprechend folgender Abbildung aufgeteilt.

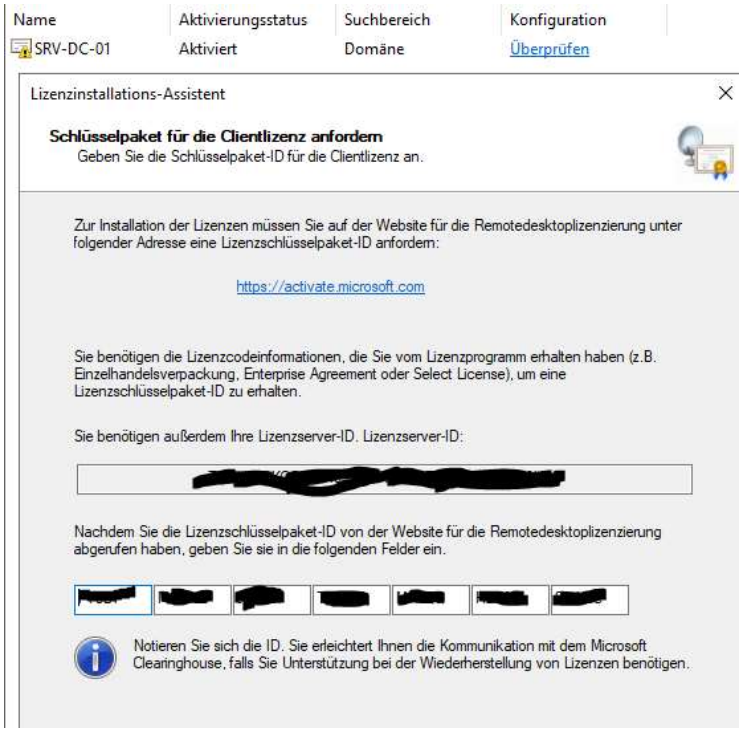
Vollqualifizierter Domänenname des Servers	Installierter Rollendienst
SRV-DC-01.[redacted]	RD-Lizenzierung
SRV-RDP-01.[redacted]	RD-Verbindungsbroker
SRV-RDP-01.[redacted]	RD-Sitzungshost

5.1.11 Einrichtung des RDP-Lizenzierungsserver

Die Konfiguration des Remotedesktop-Lizenzservers erfolgte über den Remotedesktop-Lizenzserver-Manager. Dafür habe ich zunächst über den Assistenten den Lizenzserver aktiviert, indem ich die Methode zur Aktivierung ausgewählt und die Unternehmensinformationen des Lizenznehmers hinterlegt habe (Diese Informationen sind obligatorisch).



Im Anschluss habe ich direkt die Lizenz aktiviert, die ich von der Wortmann AG dazu bereitgestellt bekommen habe.



Anschließend habe ich den Server (SRV-DC-01) zum Mitglied der Gruppe „Terminal Server License Servers“ gemacht. Nachdem ich dann den Dienst „TermServiceLicensing“ neugestartet habe,

TermService	1060	Remotedesktopdienste	Wird ausgeführt
TermServLicensing	3888	Remotedesktoplizenzierung	Wird ausgeführt

wurde der Lizenzserver im Remotedesktoplizenzierungsmanage auch korrekt angezeigt.

SRV-DC-01	Aktiviert	Domäne	OK

5.1.12 Installation Microsoft 365 Apps

Um die Microsoft 365 Apps auf einem Terminalserver bereitstellen zu können müssen einige Anpassungen vor der Installation vorgenommen werden. Dazu stellt Microsoft einen XML-Editor im Web bereit über den man die erforderlichen Anpassungen in der Konfiguration des Installationssetups vornehmen kann.

Produkte

Architektur	32-Bit
Microsoft 365-Apps für Unternehmen	×
Updatekanal	Aktueller Kanal
Bereitzustellende Version	Neueste
Ausgeschlossene Anwendungen:	
Access	×
OneDrive (Groove)	×
Skype for Business	×
OneDrive Desktop	×
Publisher	×
Teams	×
Ausgeschlossene Funktionen:	
Bing	×

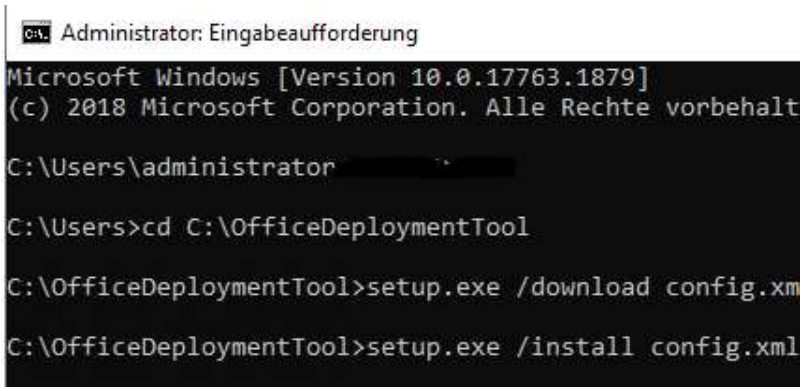
Sprachen

Deutsch (Deutschland) --Primär	Vollständig

Lizenzierung und Aktivierung

Product Key	Benutzeraktivierung
Lizenzbedingungen akzeptieren	Ein
Aktivierung gemeinsam genutzter Computer	Ein
Lizenzierungstoken mit Roaming	Aus

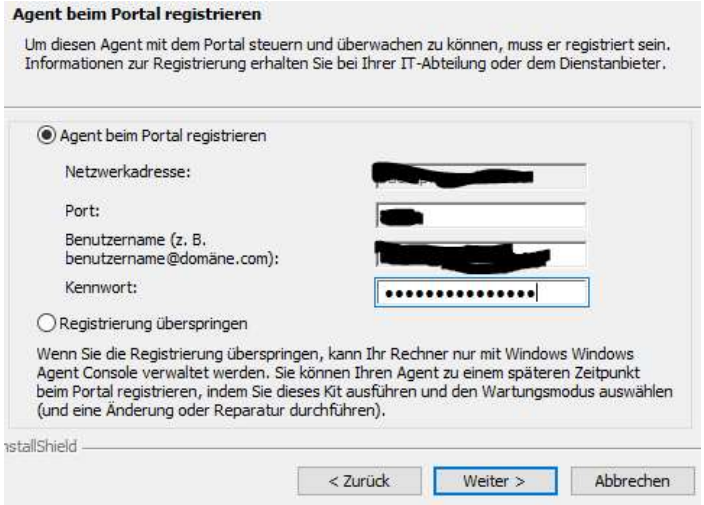
Unter dem Punkt Lizenzierung und Aktivierung musste ich den Punkt „Aktivierung gemeinsam genutzter Computer“ aktivieren. Das ist die einzige Vorgabe von Microsoft vor der Installation über das „OfficeDeploymentTool“. Ich habe allerdings weitere Anpassungen vorgenommen, die das Installationssetup betreffen. Die Softwarearchitektur habe ich von 64- auf 32-Bit umgestellt. Um Ressourcen zu schonen habe ich zudem einige Anwendungen von der Installation ausgeschlossen, da der Kunde diese nicht verwenden möchte. Zu den ausgeschlossenen Anwendungen zählen „Microsoft Access“, „OneDrive (Groove)“, „Skype for Business“, „OneDrive Desktop“, „Publisher“ und „Teams“. Die dabei entwickelte XML-Datei habe ich auf dem Terminalserver (SRV-RDP-01) heruntergeladen und zusammen mit dem „OfficeDeploymentTool“ in einem Verzeichnis gespeichert. Anschließend führte ich das „OfficeDeploymentTool“ über die Kommandozeile unter Angabe der XML-Datei aus. Die Befehle dazu lauten „setup.exe /download downloadconfig.xml“ zum Herunterladen der Microsoft 365 Apps und „setup.exe /configure installconfig.xml“ zum Installieren der Microsoft 365 Apps.



Danach beginnt der gewohnte Installationsassistent von Microsoft 365 mit der Installation der Produkte. Die Produktaktivierung erfolgt dann später über die Benutzerlizenzen für Microsoft 365 Business Standard.

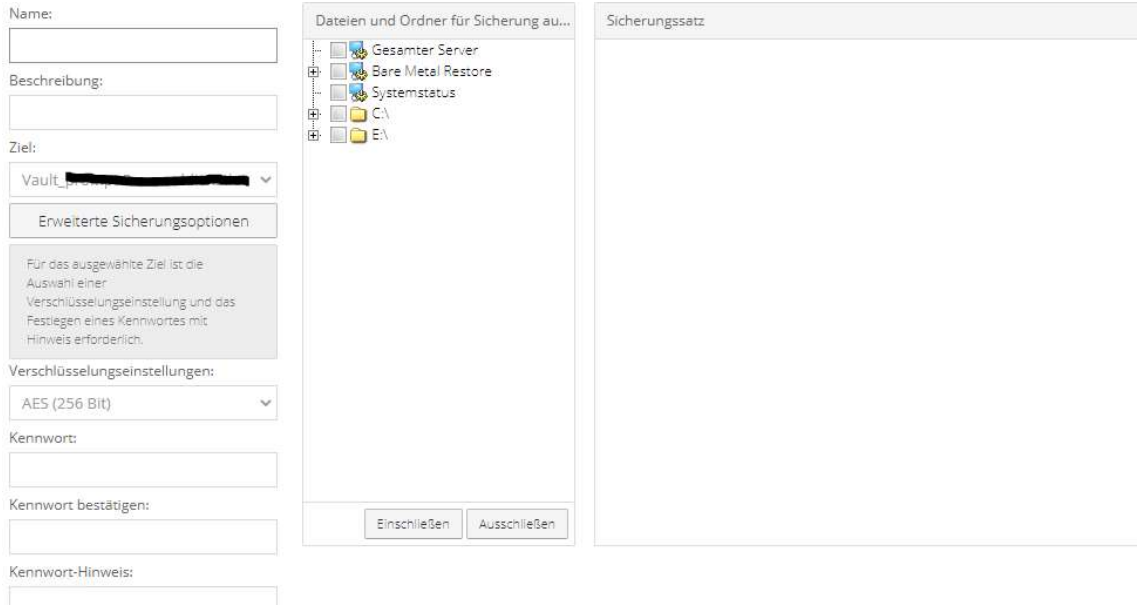
5.1.13 Wortmann Cloud Datensicherung

Alle 3 Server wurden standardmäßig über den Agenten installiert und registriert.

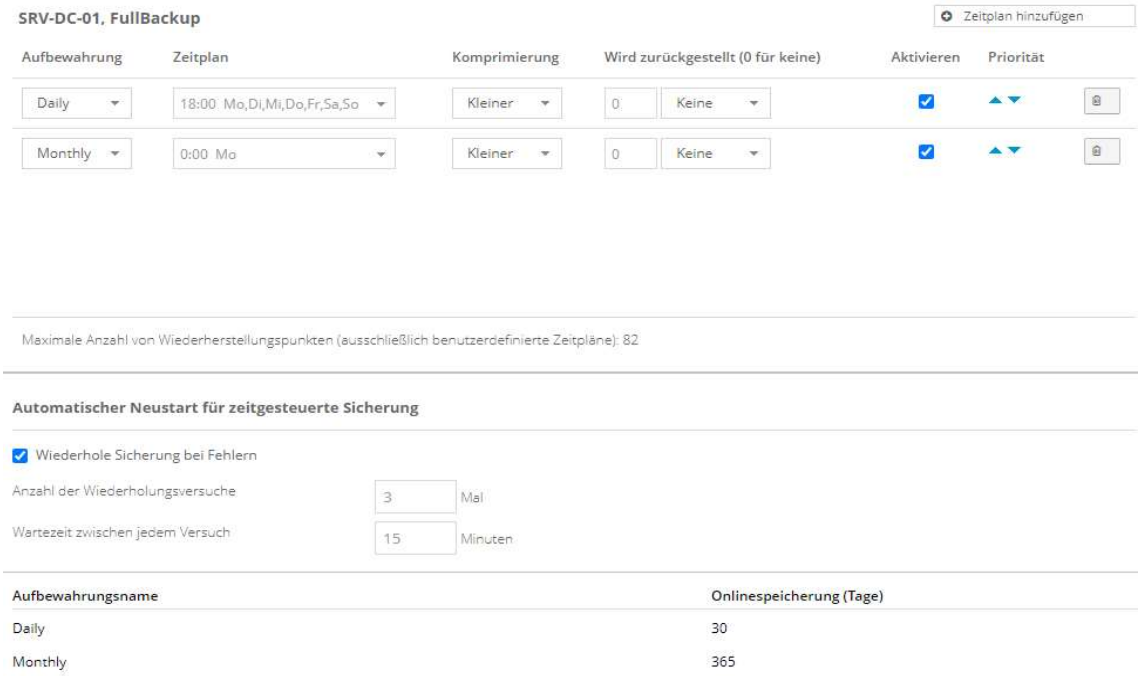


Eine „Sub-Site“ wurde angelegt und das Vault-Profil hinterlegt. Als Sicherungsquelle wählte ich in allen 3 Fällen den Gesamten Server aus, um eine einfache und schnelle

Wiederherstellung der Umgebung sowie die granulare Rücksicherung einzelner Dateien oder Verzeichnisse zu gewährleisten.



Als Zeitplan habe ich für jede Maschine eine tägliche Sicherung zwischen 0-6Uhr in 2-stündigen Abständen sowie eine monatliche Sicherung immer am ersten Montag des Monats definiert. Letztere erfolgt im Zeitraum zwischen 18-24 Uhr ebenfalls in 2-stündigen Abständen. Bei der Sicherungsart handelt es sich um eine inkrementelle Datensicherung. Für den Fall eines Fehlers während des Sicherungsprozesses habe ich zudem eine dreimalige Wiederholung im Abstand von 15 Minuten definiert.

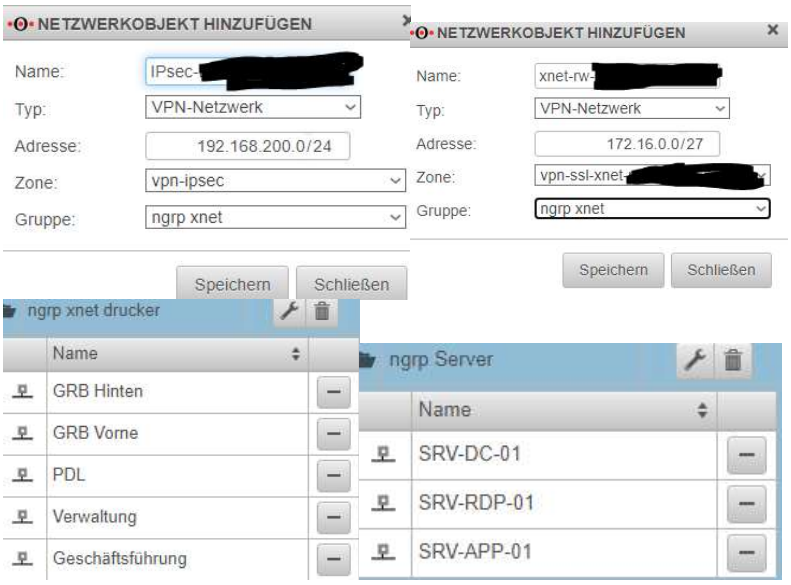


5.1.14 Abschließende Firewall Konfiguration

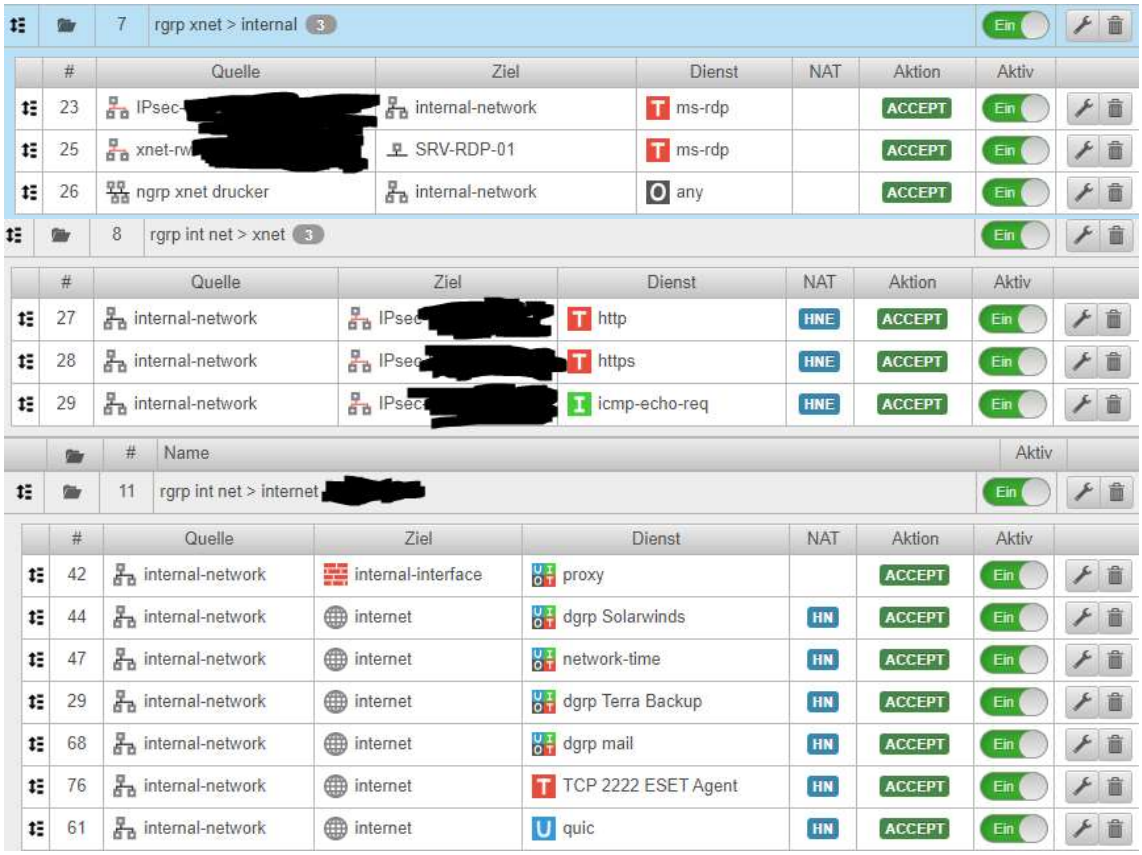
Der Portfilter auf der Firewall im RZ musste um Netzwerkobjekte und Zugriffsbeschränkungen erweitert werden. Dafür habe ich die notwendigen Ports ermittelt, die für ausgehende Verbindungen der genutzten Anwendungen genutzt werden und diese explizit freigegeben, um den Bereich der freigegebenen Ports zu

verringern und so die Sicherheit zu erhöhen. Dabei handelte ich nach dem Minimalprinzip. Die Ermittlung der notwendigen Ports erfolgte dabei durch die Dokumentationen der Hersteller und das Log der Firewall auf, der die Verbindungszugriffe mitprotokolliert werden. Für eine bessere Übersicht habe ich die Regeln in Regelgruppen unterteilt. So entstanden die Regelgruppen „rgrp int net > internet“, „rgrp internet > int net“, „rgrp xnet > int net“ und „rgrp int net > xnet“.

5.1.14.1 Netzwerkgruppen/Objekte



5.1.14.2 Portfilterregeln



5.1.14.3 Dienstgruppen

dgrp mail

	Name
T	imap
T	imap-ssl
T	pop3
T	smtp
T	smtps
T	submission
T	pop3s

dgrp Solarwinds

	Name
T	TCP3377
U	UDP1234
U	UDP1235

dgrp Terra Backup

	Name
T	terra.backup
T	Terra Backup
T	Agent-Vault_Com

network-time

	Name
T	ntp-tcp
U	ntp-udp

proxy

	Name
T	domain-tcp
U	domain-udp
T	webcache
T	http-transparent
I	icmp-echo-req
T	pop3proxy
T	proxy-urlshortener
T	https-transparent

Die Ports für die entsprechenden Dienste sind den Hersteller Dokumentationen zu entnehmen.

6 Quellenverzeichnis

6.1 Allgemeines

IPSec Allgemein
https://www.elektronik-kompendium.de/sites/net/0906191.htm
IKE Allgemein
https://m.heise.de/security/artikel/Einfacher-VPN-Tunnelbau-dank-IKEv2-270056.html?seite=all

AES-Verschlüsselung
https://de.wikipedia.org/wiki/Advanced_Encryption_Standard

SSL-VPN Allgemein
https://www.elektronik-kompendium.de/sites/net/1410151.htm#:~:text=Funktionsweise%20von%20SSL%2DVPN,eingebaut%20und%20funktioniert%20praktisch%20%C3%BCberall.

6.2 Securepoint Firewall

Zonenkonzept
https://wiki.securepoint.de/UTM/NET/Zoneneinstellungen

Firewallregeln
https://wiki.securepoint.de/UTM/RULE/Portfilter
https://wiki.securepoint.de/UTM/RULE/Hidenat_Exclude
https://wiki.securepoint.de/UTM/RULE/Implizite_Regeln

VPN
https://wiki.securepoint.de/UTM/VPN/SSL_VPN-Roadwarrior
https://wiki.securepoint.de/UTM/VPN/SSL_VPN-Roadwarrior#Herunterladen_des_SSL-VPN_Clients_im_Userinterface

https://wiki.securepoint.de/UTM/VPN/IPSec-S2S

Benutzerverwaltung

https://wiki.securepoint.de/UTM/AUTH/Benutzerverwaltung

Verzeichnisdienstanbindung

https://wiki.securepoint.de/UTM/AUTH/AD_Anbindung

Zertifikatsverwaltung

https://wiki.securepoint.de/UTM/AUTH/Zertifikate

Verschlüsselung

https://wiki.securepoint.de/UTM/AUTH/Verschl%C3%BCsselung

Servereinstellungen

https://wiki.securepoint.de/UTM/NET/Servereinstellungen

Datenschutz

https://wiki.securepoint.de/UTM/AUTH/Datenschutz

6.3 Microsoft

Remotedesktop Lizenzserver

https://docs.microsoft.com/de-de/windows-server/remote/remote-desktop-services/rds-activate-license-server

Remotedesktop Server Einrichtung

https://kosilov.de/windows-server-2019-terminalserver-einrichten-anleitung

Einrichtung des Domaincontrollers

https://www.bmsoft.de/anleitung/windows-server-2019-domaenencontroller-installieren/

Einrichtung des Druckservers

https://www.windowspro.de/philip-lorenz/print-server-windows-server-2019-installieren

Einrichtung der Gruppenrichtlinien

https://www.group24.de/blog/2019/06/27/gruppenrichtlinien-in-einer-windows-server-umgebung/

https://lost-in-it.de/netzlaufwerk-per-gruppenrichtlinien-verteilen/

https://www.tech-faq.net/drucker-per-gruppenrichtlinien-installieren/

Einrichtung von Verzeichnisfreigaben

https://lost-in-it.de/ordner-freigeben-unter-windows-server/

Microsoft 365 Einrichtung

https://docs.microsoft.com/de-de/microsoft-365/admin/setup/setup-business-standard?view=o365-worldwide

Microsoft 365 Trust Center

https://www.microsoft.com/de-de/trust-center

6.4 Wortmann Cloud

IaaS

https://wiki.terracloud.de/index.php/IaaS

Datensicherung

https://wiki.terracloud.de/index.php/Backup