HOCHSCHULE MITTWEIDA
UNIVERSITY OF APPLIED SCIENCES

BACHELORARBEIT

Herr

Abdo Frah

Vergleich von Grid-Computing und Cloud-Computing anhand Regeln und Ziele im IT-Governance Prozess

Mittweida, 2022

Fakultät:
Angewandte Computer- und Biowissenschaften

BACHELORARBEIT

Vergleich von Grid-Computing und Cloud-Computing anhand Regeln und Ziele im IT-Governance Prozess

Autor:
Herr Abdo Frah

Studiengang:
Angewandte Informatik

Seminargruppe:
IF19wl1-B

Erstprüfer:
Prof. Dr.-Ing. Christian Roschke

Zweitprüfer:
M. Sc. Manuel Heinzig

Einreichung:
Mittweida, 01.02.2023

Bibliografische Angaben

Frah, Abdo:

Vergleich von Grid-Computing und Cloud-Computing anhand von Regeln und Zielen im IT-Governance-Prozess.

Comparison of Grid-Computing and Cloud-Computing based on rules and goals of a standard IT governance process.

78 Seiten, Hochschule Mittweida, University of Applied Sciences,
Fakultät Angewandte Computer- und Biowissenschaften, Bachelorarbeit, 2022.

Abstract

Diese wissenschaftliche Arbeit leistet einen Beitrag zum Thema „Cloud-Computing“, welches unterschiedliche Möglichkeiten und Dienste bietet. Im Gegensatz dazu befasst sich dieser Forschungsbericht zusätzlich mit dem Konzept des Grid-Computing. Zu Beginn werden die IT-Governance-Regeln verglichen, die im Cloud- und Grid-Computing eines Unternehmens eine große Rolle spielen. Dabei werden zwei Varianten der der IT zur Verfügung stehenden Infrastrukturen für ausgewählte Dienste eingerichtet, welche den Regeln der IT-Governance folgen müssen. Die in dieser Arbeit ermittelten Informationen bieten einen guten Ausgangspunkt für die Umstellung der IT auf Cloud- bzw. Grid-Computing.

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungsverzeichnis

IT	Computer and Information Technology (Informationstechnik)
EAC	Exchange Admin Center
DHCP	Dynamic Host Configuration Protocol
TCP	Transmission Control Protocol
UPD	User Datagram Protocol
IP	Internet Protocol
AD	Active Directory
VPN	Virtual private network
IMAP	Internet Message Access Protocol
POP3	Post Office Protocol
SMTP	Simple Mail Transfer Protocol
VM	Virtual Machine
VPC	Virtual Privat Cloud
CVSS	Common Vulnerability Scoring System
HTTP	Hypertext Transfer Protocol
FTP	File Transfer Protocol
MS	Microsoft Server

1 Einführung und Motivation

Es stellt sich die Frage, ob die IT fähig ist, ein Unternehmen und dessen Kunden nachhaltig zu unterstützen und/oder ob eine Unterstützung ausschließlich mit der Leitung des Unternehmens ohne kooperative Interaktion mit allen im Laufe der Arbeitsprozesse beteiligten Abteilungen möglich ist. Mit den begrenzten Ressourcen eines Unternehmens steigen heutzutage auch die Voraussetzungen, diese vermehrten Leistungen zu gewährleisten (Johannsen & Kant, 2020, S. 1058). IT-Governance ist abhängig von der Unternehmensführung und -aufsicht. Auf der anderen Seite sind die Erwartungen an die IT, die neuen verfügbaren Dienstleistungen der Geschäftsentwicklung in einem zunehmend internationalen Umfeld zu fördern, sinkende Kosten in der IT und die Möglichkeit, ein Risikomanagement zu verwirklichen, welches die hochwertige Leistung garantiert und an die Nutzerbedürfnisse angepasst ist. Die Unternehmensleitung steuert die IT nach klaren Metriken durch die IT-Governance. Diese stellt sicher, dass die Bedürfnisse, Bedingungen und Möglichkeiten der Anspruchsberechtigten evaluiert werden. Auf diese Weise sollen ausgewogene, vereinbarte Unternehmensziele festgelegt, die Richtung durch Priorisierung und Entscheidungsfindung vorgegeben sowie die Performance und Compliance anhand der vereinbarten Richtung und Ziele überwacht werden. Mittels Cloud-Computing können nicht nur die Komponenten der IT-Infrastruktur, die für die Ausführung und Verwaltung unternehmensfähiger IT-Umgebungen benötigt werden, skaliert werden, sondern nach Bedarf auch die jeweilige Dienstleistung. Cloud-Services kommen demnach in unterschiedlichen Bereichen eines Unternehmens zum Einsatz. Dienste, die Grid-Systeme bereitstellen, um verteilte Rechenressourcen zu nutzen, konzentrieren sich auf den On-Demand-Zugriff auf Rechner, Daten und Dienste.

1.1 Aufgabenstellung

Der Fokus dieser Arbeit liegt auf den IT-Governance-Regeln, die zur Zielerreichung eines Unternehmens hinsichtlich Planung, Implementation, Evaluation und Verwaltung übereinstimmen. Hierfür ist es notwendig, zuerst den Windows Server 2019 sowie die VMware ESXi auf Hypervisor und anschließend die entsprechende Rolle für die Windows-Domain auf den Servern zu installieren. Zu den Ressourcen zählen Festplatten, ein Rechner, der Virtualisierung unterstützt, ein Layer-3-Switch, ein USB-Stick sowie ein LAN-Kabel als Hardware-Komponente. Zudem ist eine VPN-Verbindung sicherzustellen, die in diesem Fall von Securepoint Firewall stammt. Die möglichen Risken, die die Dienste in dieser Domain beeinträchtigen könnten, werden durch Wireshark Tools überwacht und evaluiert. Diese sind Domain Name Resolution (DNS), Dynamic Host Konfiguration Protocol (DHCP) als auch Mail Services Protocols (IMAP, POP3 und SMPT).

Im Grid-System findet der Datenaustauch zwischen zwei Nutzern in einer Domain in einem geographischen verteilten Unternehmen statt, oder in den zwei Domains eines Unternehmens und dessen Tochter-Unternehmen, die geographisch getrennt sind.

Der Datenaustauch in der Private-Cloud besteht zwischen zwei Nutzern in einer Domain in einem geographisch verteilten Unternehmen bzw. in zwei Domains eines Unternehmens und dessen Tochter-Unternehmen, die geographisch verteilt sind. Der Autor erbringt auch die Darstellung von Arten der Virtualisierung mit ihren Vor- und Nachteilen.

1.2 Aufbau der Arbeit

Der Fokus der vorliegenden Bachelorarbeit liegt verstärkt auf den IT-Governance-Regeln sowie Grid-Computing und Cloud-Computing. Der Grundlagenabschnitt (Kapital 2) bezieht sich auf die wesentlichen Begrifflichkeiten, die die Lesenden benötigen, um ein grundlegendes Verständnis zur Implementierung (Kapital 3) zu entwickeln. Der Autor wird zudem einige Arten des Cloud-Computing erläutern, welches auf Basis der Virtualisierung besteht. Darüber hinaus werden einige Sicherheitskriterien im Zusammenhang mit der Virtualisierung detailliert zusammengefasst. Unter anderem werden die Grundlagen von Domain- bzw. Netzwerkdiensten (DHCP, DNS, Mail Protokolle) erörtert und Risiken bzw. Angriffe auf diese erläutert. Hinzu kommt eine Zusammenfassung, inwiefern Grid-Computing den dynamischen, virtuellen und geographisch verteilten Organisationen bei direktem Zugriff auf Ressourcen helfen kann und ob bereits Grid-Computing unterstützte Technologien bzw. Projekte implementiert wurden. Das Grid-System birgt einige Risiken, durch welche es in einigen Fällen vorkommen kann, dass Grid-Computing nicht im IT-Feld umsetzbar ist und welche in diesem Abschnitt näher beschrieben werden. Das Kapital der praktischen Umsetzung bezieht sich auf die Implementation der einzelnen Szenen in der Organisation und den zugehörigen Strategien sowie die Verwaltung der Ressourcen. Eine Evaluation (Kapital 4) hinsichtlich positiver und negativer IT-Governance-Regeln gegen die Vorgehensweisen bezüglich der Umstellung auf Digitalisierung sowie während der Implementierung auftretender Probleme bildet den Abschluss dieser Arbeit.

2 Grundlagen

Nach der Einordnung der Aufgabenstellung und Festlegung der zu behandelnden Themenschwerpunkte soll das nun folgende Kapital ein grundlegendes Verständnis vermitteln.

2.1 Server-Virtualisierung

In diesem Kapitel soll ein Überblick über die Server-Virtualisierung gegeben werden. Im Besonderen werden die verschiedenen Typen von Virtualisierung betrachtet sowie die Vor- und Nachteile genauer erläutert.

2.1.1 Abstrakt

Vielen technologieabhängige Unternehmen stellen ihre Server bereit, die nur mit einem Bruchteil ihres Aufwands ausgeführt werden, da sie über ihren physischen Server oftmals eine bestimmte Anwendung bzw. einen bestimmten Service laufen lassen. Dies ist insofern eine ineffiziente Vorgehensweise, da die untere Grenze des Mindest-Hardwareverbrauchs nicht erreicht wird, was wiederum zu höheren Betriebs- und IT-Kosten führt. Die Lösung dafür bietet eine virtuelle Maschine (VM), d. h. eine virtuelle Darstellung oder Emulation eines physischen Rechners (Siegert & Baumgarten, 2010, S. 26). Sie werden oft als VM-Gast bezeichnet, während die physische, ausführende Maschine, als Host bezeichnet wird. Die Virtualisierung ermöglicht die Erstellung mehrerer virtueller Maschinen mit jeweils eigenem Betriebssystem (BS DE, OS EN) und eigenen Anwendungen auf einer einzigen physischen Maschine. Eine VM kann nicht direkt mit einem physischen Computer interagieren. Stattdessen benötigt es eine leichtgewichtige Softwareschicht namens Hypervisor, um die ihr zugrunde liegende physische Hardware anzupassen. Der Hypervisor weist jeder VM physische Rechenressourcen wie Prozessoren, Arbeitsspeicher und Speicher zu. Zudem hält er jegliche VMs voneinander getrennt, damit sie sich nicht gegenseitig stören.

2.1.2 Hypervisor

Der Hypervisor ist eine Software, welcher als Umgebung virtueller Hardware dient und den VMs Hardware-Ressourcen zu Verfügung stellt.

Hypervisor Type

Bare-metal Virtualization Hypervisor (Hypervisor Type 1):

Hypervisoren werden direkt auf der physischen Hardware ausgeführt und ersetzen das Betriebssystem. Sie verwenden ein separates Softwareprodukt, um VMs auf dem Hypervisor zu erstellen und zu bearbeiten. Mithilfe einiger Verwaltungstools wie vSphere von VMware können Nutzer ein Gastbetriebssystem auswählen, das in der VM installiert werden soll. Es kann eine VM als Vorlage für andere verwendet werden, welche dupliziert bzw. geklont werden können, um neue zu erstellen. Abhängig von Anforderungen können mehrere VM-Vorlagen für unterschiedliche Zwecke erstellt werden, z. B. Softwaretests, Produktionsdatenbanken und Entwicklungsumgebungen (siehe Abbildung 1 (SUMIT. SINGH, 2021)).

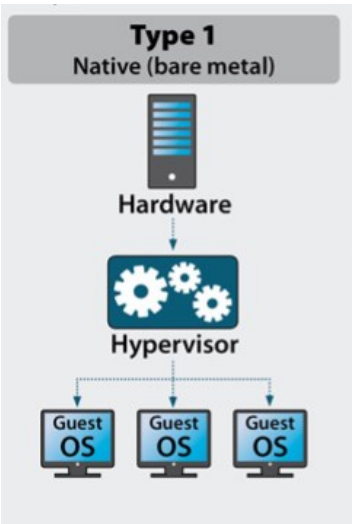


Abbildung 1: Hypervisor Typ 1

Hosted Virtualisierung Hypervisor (Hypervisor Type 2):

Hypervisoren werden als Anwendung innerhalb eines Host-Betriebssystems ausgeführt und zielen auf Einzelbenutzer-Desktop- oder Notebook-Plattformen ab. Bei einem Typ-2-Hypervisor (siehe Abbildung 2 Hypervisor Typ 2 (SUMIT. SINGH, 2021)[1]) wird manuell eine VM erstellt und anschließend ein Gastbetriebssystem darin installiert. Der Hypervisor kann verwendet werden, um der VM physische Ressourcen zuzuweisen, indem die Menge an Prozessorkernen und Speicher, die sie verwenden kann, manuell festlegt wird. Abhängig von den Fähigkeiten des Hypervisors können auch Optionen wie 3D-Beschleunigung für Grafiken festgelegt werden.

[1] https://k21academy.com/oracle-ebs-r12-on-cloud/e-business-suite-r12-on-oracle-cloud-question-answers-day-1-live-session-review/

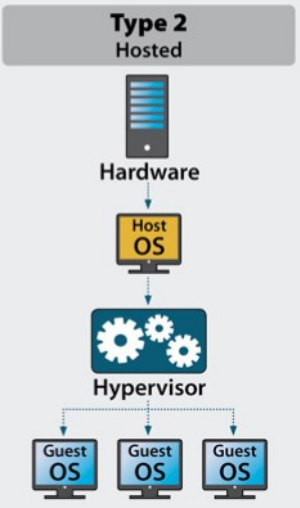


Abbildung 2: Hypervisor Typ 2

Vorteile beim Einsatz von Hypervisor

Mehrere Server-Betriebssysteme, die besondere Aufgaben erfüllen müssen, als Gast-Betriebssystem auf einen physischen Rechner zu virtualisieren, kann viele Vorteile mit sich bringen:

Serverkonsoliderung: Die Server-Virtualisierung maximiert die Hardwareauslastung, indem mehrere Anwendungen und Dienste auf weniger Hardware aggregiert werden, wodurch Anwendungen und Dienste sicher auf derselben Serverhardware koexistieren können. Auf diese Weise können mehrere Betriebssysteme gleichzeitig in der Cloud-Umgebung betrieben werden(Zimmer, 2006, K. 1–2) .

Einsparung bei Hardwarewartung: Die Ausstattung vor Ausfällen in den virtuellen Maschinen ist deutlich geringer als in Maschinen, die ohne Virtualisierung im Betrieb sind (Zimmer, 2006, S. 1–2).

Geringere Ausfallzeiten: Die Maßnahmen, die zum Einsatz kommen, um die Ausfall-zeiten zu reduzieren, sind bei Einrichtung eines Hypervisors wesentlich verwaltbar und halten länger als in non-virtuelle Systeme. Durch Snapshot (VMWARE, 2016)[2]ist das gesamten BS auf einen alten gesicherten Zustand wiederherzustellen.

Vorgehensweise bei kritischem System-Update in produktiver Umgebung: Durch Klon-Funktion sind kritische Update auf einem geklonten System zu installieren und weiter zu überprüfen. Diese Methode in einem Cluster (*Erstellen eines Clusters*, 2020) (siehe Abbildung 3)(ODGERS, 2015)[3] könnte eine geringere Ausfallzeit gewährleistet.

---

[2] https://kb.vmware.com/s/article/1015180?lang=de

[3] https://www.joshodgers.com/2015/06/09/whats-next-scale-storage-separately-to-compute-on-nutanix/

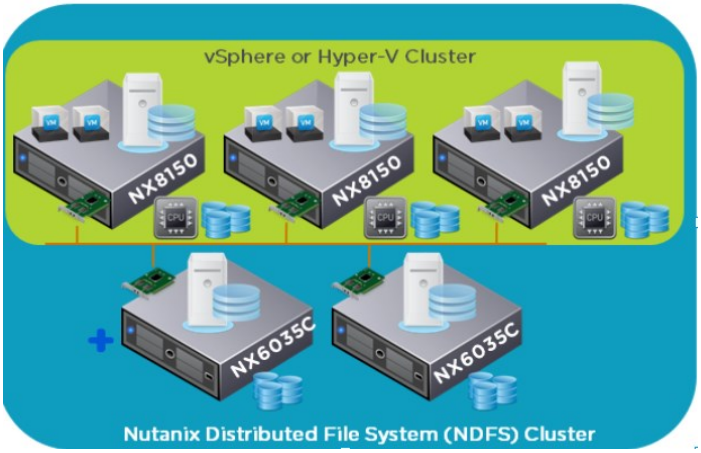


Abbildung 3: Cluster Darstellung

Nachteile beim Einsatz von Hypervisor

Selbstverständlich entstehen durch die Umsetzung von Virtualisierung, wie bei anderen Technologien auch, einige Risiken, die im Folgenden als wesentliche Nachteile dargestellt werden.

1. Eine der Säulen der Virtualisierung sollte das Gastisolationskonzept sein: Eine VM kann nicht direkt mit dem Host oder den anderen VMs interagieren. Durch die Zuweisung von Ressourcen kann ein Hypervisor die Gäste isolieren. Hierdurch wird der Hypervisor vor den Gästen geschützt und ein direkter Hardwarezugriff der Gäste, denen der Hypervisor nicht vertrauen kann, unterbunden. Gäste benötigen Isolation, da eine virtuelle Maschine (Gast) ohne Autorisation kompromittiert wurde oder betrieben wird. Ein Verlust von logischer Isolation bzgl. der Virtualisierung hätte zur Folge, dass zwei Subjekte unerwünschten Zugriff auf ein Objekt erhalten, den sie ohne den Einsatz von Virtualisierung nicht hätten. Daher führt ein Verlust von Isolation zu einer Bedrohung bzgl. der Informationssicherheit(Xiao, Bin u. a., 2007, Kap. 5).

2. Die Speicherverwaltung betrifft nicht nur den physischen Arbeitsspeicher, sondern auch die Virtualisierung. Diese hat zur Folge, dass der Zugriff auf den Arbeitsspeicher in der Virtualisierung unmittelbar erfolgt. Die softwareseitige Virtualisierung zur Speicherverwaltung „Extended Page Tables “ (EPT) ist eine x86-Virtualisierungstechnologie der zweiten Generation von Intel für die Memory Management Unit (MMU)(VMware Inc., 2008, S. 2)[4]. Die EPT-Verletzung (siehe Abbildung 4) (VMware Inc., 2008, Abb. 2) tritt ein, wenn auf eine Seite zugegriffen wird und dieser Zugriff nicht gleichgeordnet mit den gesetzten Bits des jeweiligen EPT-Eintrages ist. Es ist also vergleichbar mit einem „Page fault“.

[4] https://www.vmware.com/pdf/Perf_ESX_Intel-EPT-eval.pdf

3. Hohe Leistung nötig: Um viele Gastsysteme auf einem Wirt laufen zu lassen, muss dieser eine ausreichende Leistung bereitstellen.

4. Gesamtausfall möglich: Wenn das physische Wirtssystem ausfällt, fallen alle VMs aus. Daher ist eine entsprechende Absicherung notwendig.

5. Lizenzierung: Es kann Probleme mit Software-Lizenzen geben, denn rechtlich zählen VM als eigenständige Rechner.

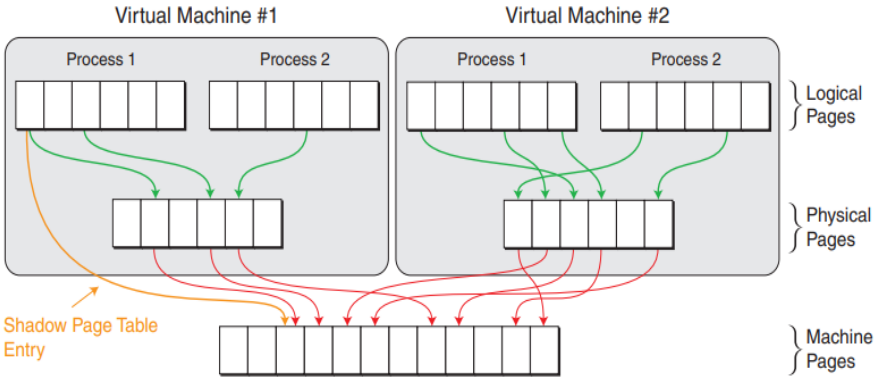


Abbildung 4: MMU-Diagramm

2.2 Cloud-Computing

Dieser Abschnitt vermittelt einen Überblick über Cloud-Computing, wobei im Besonderen die Typen des Cloud-Computing und deren Betriebsmodelle betrachtet werden.

2.2.1 Abstrakt

Schon seit einigen Jahren werden durch Data-Mining, Simulation von wissenschaftlichen Arbeiten oder webbasierten Anwendungen mehrere Terabyte an Daten erzeugt. Diese auf einzelnen Rechnern zu analysieren und zu verarbeiten, ist mit einem zusätzlichen Zeitaufwand verbunden. Eine potenzielle Lösung für dieses Problem ist die verteilte Verarbeitung der Daten mithilfe speziell entwickelter Software-Anwendungen. Zur Ausführung einer Anwendung, deren Einsatz in Verbindung mit Cloud-Computing steht, werden Ressourcen benötigt, auf denen sich diese Software installieren lässt. Zu diesem Zweck steht die Cloud-Computing-Software zur Verfügung, welche solch einen Infrastrukturdienst bietet.

2.2.2 Definition

Cloud-Computing (Baun u. a., 2011, S. 4)ist die Bereitstellung von Technologie, die es Kunden ermöglicht, Informationen, Daten und Anwendungen über das Internet auszutauschen – ohne durch ihren physischen Standort eingeschränkt zu sein(VAQUERO

u. a., 2009). Der Begriff Cloud-Computing-Technologie wird verwendet, um ein globales Netzwerk von Remote-Servern zu beschreiben, das als ein einziges Ökosystem fungiert. Jedes einzelne verfügt über einzigartige Funktionen für die Datenspeicherung und -verwaltung, das Ausführen von Anwendungen und mehr.
Diese Möglichkeiten eröffnen schnellere Innovationen, flexiblere Ressourcen und eine skalierbarere Arbeitsweise für Unternehmen.

Wesentliche Vorteile des Cloud-Computing im Überblick:

- Niedrigere Betriebskosten.
- Effizientere Gestaltung der Infrastruktur der Organisation.
- Die Änderung von geschäftlichen Anforderungen ist skalierbar:
- Die Konsolidierung der angebotenen Dienste erfolgt aufseiten der Dienstleister durch Virtualisierung. Durch die Virtualisierung ergibt sich für den Kunden eine dynamische IT-Struktur, die er exakt an seine Bedürfnisse anpassen kann. Der Anbieter hat den Vorteil, dass er seine eigene IT-Infrastruktur effizienter auslasten kann.

2.2.3 Cloud-Service Typen

Im Folgenden werden verschiedene Cloud-Dienste auf Basis von Rechendiensten erläutert.

Infrastructure-as-a-Service (IaaS):
Dieser Typ, bei dem die Infrastruktur für das Outsourcing bereitgestellt werden muss, um den Betrieb innerhalb des Unternehmens zu unterstützen, wird als IaaS bezeichnet. In diesem Service werden Hardware, Software und Speicher für Rechenzentren, Server und Netzwerkraum bereitgestellt (siehe Abbildung 5 IaaS(Baun u. a., 2011, S. 30)). IaaS wird zu Recht als Hardware as a Service (HaaS) bezeichnet. Ein Beispiel für IaaS ist in den Amazon Web-Services enthalten (Amazon Web Services Inc., 2023aa).

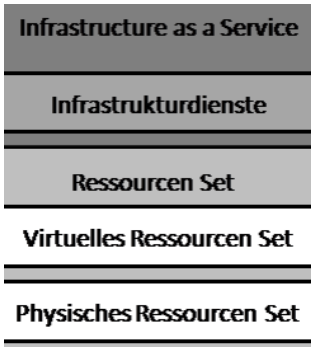


Abbildung 5: Cloud Architektur IaaS

Platform-as-a-Service (PaaS):
Der Cloud-Dienst PaaS (siehe Abbildung 6 PaaS(Baun u. a., 2011, S. 30)) stellt dem Nutzer Hardware- und Softwaretools für die Anwendungsentwicklung zur Verfügung (Baun u. a., 2011, S. 35). Mithilfe dieses Dienstes werden verschiedene Komponenten in die zugrunde liegende Infrastruktur der Organisation integriert. Neben Datenbankverwaltungssystemen und Programmiersprachenbibliotheken bietet der Dienst auch das Bearbeiten, Kompilieren und Testen sowie Versionsverwaltung an. Die Integration von Webdiensten ist ein Vorteil von PaaS. Dieser Service ist einfach und leicht zu bedienen. (Microsoft Azure(MICROSOFT, 2023bb)).

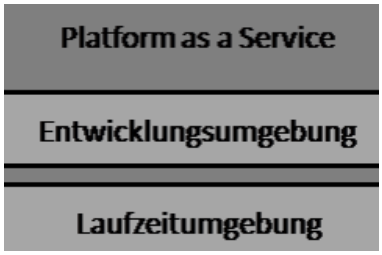


Abbildung 6: Cloud Architektur PaaS

Software-as-a-Service (SaaS):

Bei diesem Service wird verteilte Software zentral gehostet und lizenziert. SaaS ähnelt dem Applikation Service Provider (ASP). Der Anbieter erstellt eine einzige Kopie einer Anwendung, die allen Benutzern zur Verfügung gestellt wird. Benutzer können nach Vereinbarung mit dem Anbieter neue, auf der Software basierende Features oder Funktionalitäten hinzufügen, die auf ihre Nutzung angepasst sind (siehe Abbildung 7 SaaS (Baun u. a., 2011, S. 30)). APIs können in unternehmenseigene Tools integriert werden. Die Verwaltung der Infrastruktur wird durch den Anbieter übernommen (Höllwarth, 2013, Kap. 2.6.3). Ein Beispiel für Software as a Service ist Microsoft 365(MICROSOFT, 2023aa).

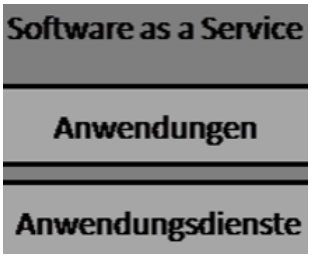


Abbildung 7: Cloud Architektur SaaS

2.2.4 Cloud-Betriebsmodelle

Modelle wie SaaS (Software as a Service), PaaS (Platform as a Service) und IaaS (Infrastructure as a Service) finden vielfältig Verwendung, je nachdem, welches Format

bzw. welche Bedürfnisse ein Unternehmen aufweist. Im Folgenden wird der Unterschied zwischen Public, Private und Hybrid-Cloud erfasst.

Private-Cloud:

Die Cloud-Infrastruktur befindet sich innerhalb der Organisation und wird ohne die Erlaubnis der Organisation nicht mit anderen geteilt, was als private-Cloud bezeichnet wird. Die Private-Cloud ist unter allen Cloud-Bereitstellungen am sichersten. Anpassung, Skalierung und Flexibilitätskontrolle sind in der Private-Cloud höher. Hard- und Software werden nur für den Eigentümer gebaut (Baun u. a., 2011, S. 28) (siehe: Abbildung 8).

Public-Cloud:

Kunden aus dem Internet nutzen Cloud-Dienste, bei denen die Infrastruktur auf dem Cloud-Computing-Unternehmen basiert. Die Public-Cloud ist jedoch nicht sicher und Organisationen mit sensiblen Informationen sollten diese nicht verwenden. Die Informationen stehen allen zur Verfügung, die die Cloud nutzen (Baun u. a., 2011, S. 28) (siehe Abbildung 8)(D'ANTONI, 2022)[5].

Hybrid Cloud:

Die Kombination aus privaten und öffentlichen Cloud-Services basiert (siehe Abbildung 8 und 9)(D'ANTONI, 2022)[3-a] auf den Cloud-Betriebsmodellen und wird als Hybrid-Cloud bezeichnet. Organisationen haben den Vorteil der öffentlichen-Cloud – während sie hohe Arbeitslasten bewältigen, bleiben die Informationen trotzdem sicher, da die private-Cloud darin integriert ist (Baun u. a., 2011, S. 30).

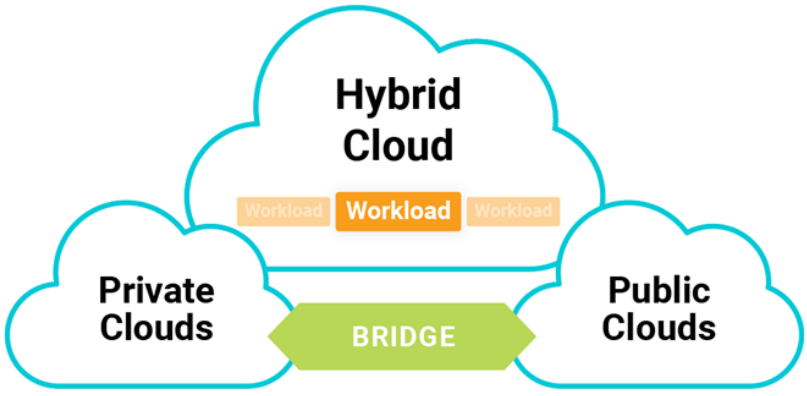


Abbildung 8: Cloud- Betriebsmodellen

[5] https://orangematter.solarwinds.com/2022/10/24/hybrid-cloud-benefits/

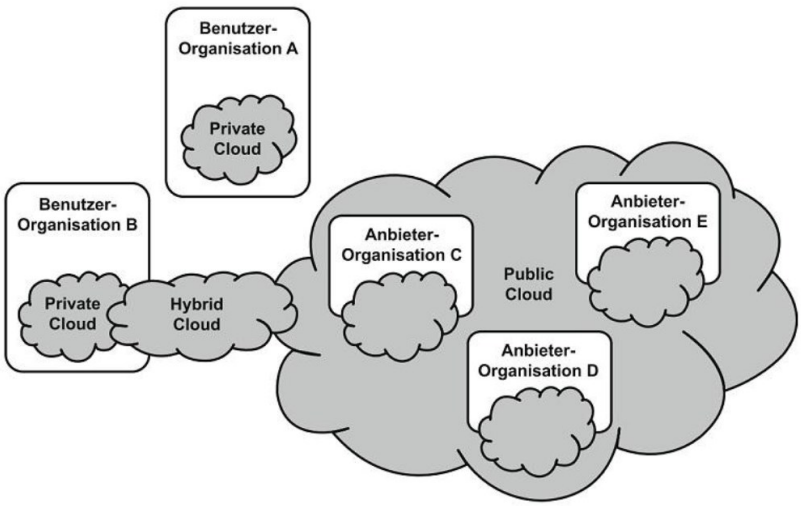


Abbildung 9: Nutzungsmodelle (Bedner, 2012, Abb. 2, S. 35)

Virtual Private-Cloud(Bedner, 2012, S. 35)**:**

Kunden, die Ressourcen gemeinsam nutzen, werden isoliert. Diese Isolationsebene wird durch ein privates IP-Subnetz oder ein virtuelles lokales Netzwerk (VLAN) erreicht.

So bietet Amazon zum Beispiel die Amazon Virtual Private-Cloud (AMAZON WEB SERVICES INC., 2023bb) [6](Amazon VPC), bei der dem Nutzer ein isolierter Bereich der Amazon Web Services Cloud zur Verfügung gestellt wird, welches auf einem vom Nutzer frei gewählten, virtuellen Netzwerk ausgeführt wird.

Community-Cloud:

Das Bereitstellungsmodell, das für eine begrenzte Anzahl von Einzelpersonen und Organisationen vorgesehen ist, sodass Dienste nur innerhalb von diesen genutzt werden, wird als Community-Cloud bezeichnet. Diese wird je nach Bedarf entweder intern oder extern bereitgestellt und gehostet (Gerardus, Cloud Community A Complete Guide, 2021).

2.3 Grid-Computing

2.3.1 Abstrakt

Die Entwicklung und weit verbreitete Nutzung von Grid-Computing wurde wegen des kontinuierlichen Wachstums von Verständnis der Anwendungsanforderungen als auch der Ausgereiftheit der Technologien, die verwendet werden, um diese Anforderungen zu erfüllen, vorangetrieben. Vor diesem Hintergrund findet nachfolgend eine

[6] https://aws.amazon.com/de/vpc/?nc1=h_ls

Einführung in die Grid-Anwendungen und -Technologien statt. Anschließend folgt eine Diskussion über die wichtigste Rolle, die das Ressourcenmanagement in zukünftigen Entwicklungen innehaben wird.

2.3.2 Einleitung

Der Begriff „Grid-Middleware“ wurde Mitte der 1990er Jahre geprägt, um eine vorgeschlagene verteilte Rechnerinfrastruktur für fortgeschrittene Wissenschaft und Technik zu bezeichnen. Seitdem wurden beim Aufbau einer solchen Infrastruktur und bei ihrer Erweiterung und Anwendung auf kommerzielle Computerprobleme große Fortschritte erzielt (Plaszczak & Wellner, 2006, Kap. 1). Mit der Entwicklung des Begriffs „Grid“ in vernetzten Rechnern und Rechnerclustern sowie durch erste dafür geeignete Anwendungen hat sich auch ein Verständnis für die Problematik von Grid-Technologien entwickelt. Grid-Konzepte und -Technologien wurden ursprünglich entwickelt, um die gemeinsame Nutzung von Ressourcen innerhalb wissenschaftlicher Kooperationen zu ermöglichen, wie z. B. im Gigabit-Test (EICKERMANN & HOMMES, 1999). Es folgten eine Menge von Anwendungstypen, die verteiltes Rechnen für rechenintensive Anwendungen umfassten. Ausgangspunkt dafür war die Notwendigkeit, dass die Beteiligten nicht nur Datensätze, sondern auch Software, Rechenressourcen und sogar Spezialinstrumente wie Teleskope und Mikroskope gemeinsam nutzen konnten(FOSTER u. a., 2001). Der Begriff virtuelle Unternehmen wird aufgrund von geographischer Verteilung und wegen Kollaborationen zwischen Unternehmen miteinander angewendet. Aus demselben Grund ist die gemeinsame Nutzung von Ressourcen in kommerziellen Umgebungen entstanden. Die Kollaborationen finden sich auch im On-Demand-Service und Rechenzentrum über das Internet wieder. So wie das World Wide Web als Technologie für die wissenschaftliche Zusammenarbeit begann und für das E-Business übernommen wurde, kann eine ähnliche Entwicklung für Grid-Technologien beobachtet werden.

2.3.3 Probleme vor Grid-Computing

Eine Reihe von Problemen sind vor Grid-Computing aufgetaucht. Die Unterschiede der Systeme erschwerten den Anwendern die Migration zwischen einzelnen Plattformen. Obwohl eine Vielzahl von Systemen verfügbar ist, die eine Reihe von Ressourcen bereitstellt, zögerten die Benutzer mit einer Umstellung bzw. neue Schritte in der IT zu machen. Eines der Hauptprobleme war die Übertragbarkeit von Daten, aber selbst einfache Schwierigkeiten wie der Systemzugriff waren schwierig zu handhaben. Ein weiteres Problem betraf die Sicherheit. Da Sicherheitsniveau für wissenschaftliche Nutzer war für industrielle Nutzer nicht hoch genug, oft mussten Systeme hinter einer Firewall versteckt werden. Gleichzeitig musste die typische Offenheit für wissenschaftliche Einstellungen gewahrt bleiben. Mit einer steigenden Zahl von Benutzern aus einer Vielzahl von Institutionen und Unternehmen wurde die Datenverwaltung zu einem wachsenden Problem. Dafür musste unter Berücksichtigung von Sicherheit und Vertraulichkeit ein

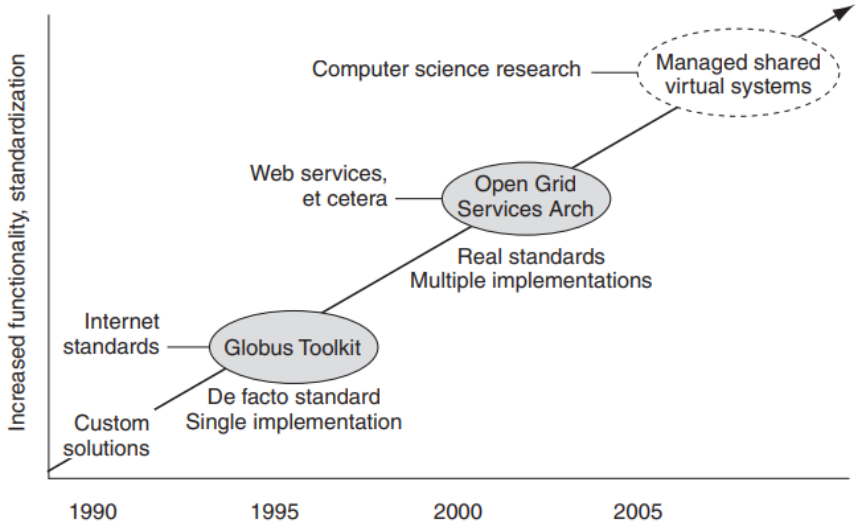
Datenmanagement in einer verteilten Umgebung entwickelt werden. Die Visualisierung von Daten wurde immer schwieriger. Nicht nur die wachsende Größe des Hauptspeichers führte zu größeren Datenmengen. Die Verteilung der Benutzer und die fehlende Bandbreite, um alle Daten zu übertragen, erforderten eine Änderung der Visualisierungskonzepte (Ferreira u. a., S. 36).

2.3.4 Virtuelle Organisationen

Web-Services und Peer-to-Peer-Systeme wurden in erste Reihe dafür entwickelt, als Problemlösung in dynamischen virtuellen Organisationen mit mehreren Institutionen einen Dateiaustausch zu ermöglichen. Diese gilt nicht für den direkten Zugriff auf Rechner, Software, Daten, Dienste und andere Ressourcen. Die gemeinsame Nutzung im Grid-System ist notwendigerweise stark kontrolliert, wobei Ressourcenanbieter und Verbraucher klar und sorgfältig definieren, was geteilt wird, wer teilen darf und unter welchen Bedingungen die gemeinsame Nutzung erfolgt. Eine Gruppe von Personen und/oder Institutionen, die durch solche Sharing-Regeln definiert werden, bilden das, was man eine virtuelle Organisation (VO)(Foster u. a., 2001, S. 36) nennt.

2.3.5 Grid-Technologie

Grids sind mehr als eine lukrative Technologie, sie sind vielmehr eine Richtung, in die sich Infrastruktur weiterentwickeln muss, wenn sie sozialen Strukturen und die Art und Weise, wie in Gesellschaft gearbeitet wird, unterstützen soll. Grid-Technologien bieten Mechanismen zum Teilen und Koordinieren der Nutzung verschiedener Ressourcen und ermöglichen somit die Schaffung virtueller Computersysteme aus geografisch und organisatorisch verteilten Komponenten, die ausreichend integriert sind, um die gewünschten Dienstqualitäten zu liefern. Zu diesen Technologien gehören Sicherheitslösungen, die die Verwaltung von Anmeldeinformationen und Richtlinien unterstützen, wenn Berechnungen mehrere Institutionen umfassen, Ressourcenverwaltungsprotokolle und -dienste zur Unterstützung des sicheren Fernzugriffs auf Computer- und Datenressourcen sowie die gemeinsame Zuweisung mehrerer Ressourcen. Darüber hinaus werden Informationsabfrageprotokolle und -dienste, welche Konfigurations- und Statusinformationen über Ressourcen, Organisationen und Dienste beinhalten, sowie Datenverwaltungsdienste, die Datensätze zwischen Speichersystemen und Anwendungen lokalisieren und transportieren, bereitgestellt. Grid-Technologien sind aus etwa 18 Jahren Forschung und Entwicklung sowohl in der Wissenschaft als auch in der Industrie hervorgegangen, die bis heute andauern. Wie in Abbildung 10 (Foster u. a., 2001, Abb. 4.2) dargestellt, kann diese Entwicklung in vier verschiedene Phasen unterschieden werden.



The evolution of Grid technologies.

Abbildung 10: Entwicklung der Grid-Technologie

2.3.6 Grid-Projekte

Grid hat sich als dominantes Modell für die Nutzung von IT-Infrastruktur etabliert. Sowohl in der Wissenschaft als auch in der Industrie wurden verschiedene Grid-Anwendungsszenarien untersucht. In der vorliegenden Arbeit wird eine repräsentative Auswahl von solchen Anwendungen dargelegt, die gemeinsam das breite Spektrum von Nutzungsszenarien vorstellen, welche die Einführung und Entwicklung von Grid vorantreiben. Diese Anwendungen umfassen rechenintensive, datenintensive, sensorintensive, wissensintensive und kooperationsintensive Szenarien und behandeln Probleme, die von Multiplayer-Videospielen und Fehlerdiagnosen in Düsentriebwerken über Erdbebentechnik bis hin zu Bioinformatik, biomedizinischer Bildgebung und Astrophysik reichen.

World-Wide-Teleskop:

Fortschritte in der digitalen Astronomie ermöglichen die systematische Vermessung des Himmels und die Sammlung riesiger Datenmengen von Teleskopen auf der ganzen Welt. Neue wissenschaftliche Entdeckungen können nicht nur durch die Analyse von Daten eines einzelnen Instruments gemacht werden, sondern auch durch den Vergleich und die Korrelation von Daten verschiedener Himmelsdurchmusterungen (FOSTER u. a., 2001). Das aufstrebende „World Wide Teleskope“ oder virtuelle Observatorium verwendet die Grid-Technologie, um Daten von Hunderten von einzelnen Instrumenten zusammenzuführen, was es einer neuen Generation von Astronomen ermöglicht, Analysen von beispiellosem Umfang durchzuführen. Während sich die unmittelbarsten Herausforderungen auf Datenformate und Datenmanagement beziehen,

ist die Notwendigkeit, die Rechenressourcen zu verwalten, die durch solche Datenanalyseaufgaben verbraucht werden, ein sich abzeichnendes Problem

UNICORE:

Als 1997 der Begriff des Grids geprägt war, wurde begonnen, am „Uniform Interface to Computing Resources“, kurz UNICORE, zu arbeiten. Dieser wird über eine grafische Oberfläche bedient. Um die Wissenschaftler nicht durch technische Hürden von ihrer eigentlichen Arbeit abzuhalten, implementiert das UNICORE Projekt alle notwendigen Komponenten für eine Grid-Umgebung als ”Komplettpaket“. Resultate und Statusinformationen werden dem Nutzer direkt angezeigt. Der UNICORE Client arbeitet über eine verschlüsselte Verbindung mit dem Server und authentifiziert seine Benutzer über ein Zertifikat. UNICORE wird hauptsachlich in Deutschland und im europäischen Ausland genutzt. In der Arbeit von FOSTER U. A. (2001) findet sich eine ausführliche Beschreibung der Projekte.

2.3.7 Grid-Architecture

Grid ist eine Computing-Infrastruktur (siehe Abbildung 11) (Padhy & Patra, 2012, Abb. 7)[7], die Rechner (PCs, Workstations, Server-Cluster, Supercomputer, Laptops, Notebooks, mobile Computer usw.) zusammenführt, um eine große Sammlung von Rechen-, Speicher- und Netzwerkressourcen zu bilden. Auf diese Weise soll es registrierten Benutzern oder Benutzergruppen ermöglicht werden, Probleme zu lösen oder einen schnellen Informationsabruf zu ermöglichen. Die Kopplung zwischen Hardware und Software mit speziellen Benutzeranwendungen wird erreicht, indem die Hardware, Software, Middleware, Datenbanken, Instrumente und Netzwerke als Rechenhilfsmittel gemietet werden.

[7] https://www.researchgate.net/publication/275405572_Evolution_of_Cloud_Computing_and_Enabling_Technologies

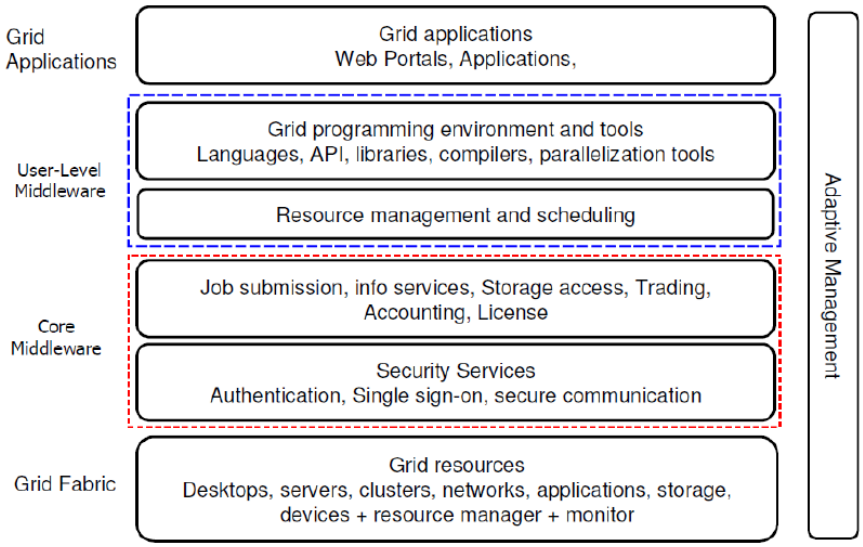


Abbildung 11: Grid-Computing Architecture

2.3.8 Sicherheit im Grid-System

Drei grundlegende Dienste müssen in einem Grid zur Herstellung von Sicherheit geleistet werden: Authentifizierung, Autorisierung und Verschlüsselung. Die Authentifizierung dient zur Feststellung, wer im Grid ist. Dies ist notwendig, um zu überprüfen, ob überhaupt Zugriffe auf Grid-Ressourcen zulässig sind. Dies kann dabei sowohl eine Person, also einen konkreten Grid-Nutzer als auch eine Grid Ressource wie z. B. einen bestimmten Server-Rechner betreffen. Nach erfolgter Authentifizierung kann der nächste Schritt erfolgen, die Autorisierung. Dabei wird entschieden, welchen Zugriff auf Grid-Ressourcen ein identifizierter Nutzer bzw. eine Grid-Ressource besitzt, d.h. was erlaubt ist. Damit Daten, die auf dem Weg zwischen autorisierten Einheiten übertragen werden, ebenfalls geschützt sind, gibt es einen Dienst der Verschlüsselung (engl.: encryption). Er sorgt für die Datenintegrität und soll die Vertraulichkeit der Daten gewährleisten. Dies geschieht durch die Verwendung von Schlüsseln. Deren sichere Erzeugung, Aufbewahrung, Verteilung und Überprüfung auf Echtheit fasst man unter dem Begriff des Schlüsselmanagements zusammen. Um die Details bei der Behandlung der Sicherheit im Grid verstehen zu können, sind einige grundlegende Techniken und bestimmte Begriffe zu klären (Jacob & International Business Machines Corporation. International Technical Support Organization., 2005, Kap. 3).

Symmetrische Verschlüsselung:

Hier wird ein einzelner Schlüssel verwendet, der sowohl für die Verschlüsselung als auch Entschlüsselung der Daten benutzt wird.

Asymmetrische Verschlüsselung (Public Key Cryptography):

Hier kommt ein Schlüsselpaar für die Verschlüsselung und Entschlüsselung zum Einsatz. Ein Beispiel für diese Art der Verschlüsselung ist die Verwendung eines sog. öffentlichen und privaten Schlüssels.

SSL (secure socket layer) Übertragung:

Ein Protokoll, das sich der Verwendung von asymmetrischer (und symmetrischer) Schlüsseltechniken bedient, um eine sichere Übertragung in einem Netzwerk herzustellen.

Öffentliche Schlüsselverwaltung:

Bezeichnet die gesamten Maßnahmen, Komponenten und Protokolle, die notwendig sind, um mit öffentlichen Schlüsseln umzugehen.

Gegenseitige Authentifizierung (Mutual Authentication):

Beide Kommunikationspartner authentifizieren sich beim jeweils anderen.

2.3.9 Was nicht im Grid umgesetzt werden kann

Das Grid ist keine Wunderwaffe, die jede Anwendung 1000-mal schneller ausführen kann, ohne dass weitere Maschinen oder Software gekauft werden müssen. Nicht jede Anwendung ist für die Ausführung in einem Grid geeignet oder aktiviert. Einige Arten von Anwendungen können einfach nicht parallelisiert werden. Bei anderen kann es sehr arbeitsintensiv sein, diese zu modifizieren, um einen schnelleren Durchsatz zu erreichen. Die Konfiguration eines Grids kann die Leistung, Zuverlässigkeit und Sicherheit der Computerinfrastruktur eines Unternehmens stark beeinflussen. Aus all diesen Gründen ist es für die Benutzer wichtig zu verstehen, wie weit sich das Grid heute entwickelt hat und welche Funktionen morgen oder in ferner Zukunft kommen werden.

2.4 IT-Governance

2.4.1 Einleitung

Es stellt sich die Frage, ob die IT fähig ist, ein Unternehmen und dessen Kunden nachhaltig zu unterstützen und/oder ob eine Unterstützung ausschließlich mit der Leitung des Unternehmens ohne kooperative Interaktion mit allen Abteilungen, die im Laufe der Arbeitsprozesse beteiligt sind, möglich ist. Die Herausforderungen an die Informationstechnologie (IT) sind heutzutage vielfältig. Daneben erhöhen die laufenden Umstände im globalen Wirtschaftsbereich den Druck, eine höhere Leistung mit weniger,

begrenzten Ressourcen und erhöhter Komplexität zu gewährleisten. Daher liegt das Etablieren einer umfassenden IT-Governance in der Verantwortung des Verwaltungsrats (VR) und der Geschäftsleitung (GL) und ist ein wichtiger Bestandteil der Unternehmensführung und -aufsicht. Demgegenüber besteht jedoch die klare Erwartung an die IT, dass die angebotenen Dienstleistungen die Geschäftsentwicklung in einem zunehmend internationalen Umfeld fördern: IT soll Kosten reduzieren, ein umfassendes Risikomanagement ermöglichen, als Innovationsmotor der Unternehmung fungieren, eine konsistent hohe Qualität aufweisen und letztlich jederzeit auf Benutzerbedürfnisse abgestimmt sein. Eine auf den ersten Blick fast unlösbare Aufgabe. Erfolgreich operierende IT-Abteilungen werden zunehmend nach dem Selbstverständnis einer Fachabteilung geführt. Der daraus resultierende unternehmerische Nutzen ist unverkennbar, denn wichtige Entscheidungen werden partnerschaftlich und gemeinsam zwischen VR, GL und IT getroffen. Im Allgemeinen hat sich das Verständnis für IT-bezogene Themen stark verbessert, und die Unternehmensleitung steuert die IT nach klaren Metriken. Genau hier setzt die IT-Governance an: Sie legt den Entscheidungsspielraum und den Verantwortungsrahmen fest, um das gewünschte Verhalten bei der Nutzung und im Umgang mit der IT sicherzustellen und die Übereinstimmung mit den Werten und übergeordneten Zielen des Unternehmens sicherzustellen. Die IT-Governance stellt sicher, dass die Bedürfnisse, Bedingungen und Möglichkeiten der Stakeholder evaluiert werden, damit es möglich ist, ausgewogene, vereinbarte Unternehmensziele festzulegen, die Richtung durch Priorisierung und Entscheidungsfindung vorzugeben sowie die Performance und Compliance anhand der vereinbarten Richtung und Ziele zu überwachen. Produkte und Dienstleistungen werden sich ebenso verändern wie die Organisation, in der und über die sie angeboten werden. Dies gilt natürlich auch für die darunter liegende „Technik“, die auf Anwendungssystem- und Infrastrukturebene dafür sorgt, dass der Betrieb sicher und störungsfrei läuft. Eine Steuerung der IT-Funktion auf „Zuruf“ oder auf „Sicht“ ist, anders als es früher einmal gewesen sein mag, nicht mehr möglich. Denn fehlende Strategien und Planungen kosten künftig nicht einfach unnötig Geld, sie können durch die daraus entstehenden Wettbewerbsnachteile auch rasch das Weiterbestehen des gesamten Unternehmens gefährden. Schließlich ist die Konkurrenz vielfältiger, schneller und innovativ geworden. Oftmals entstehen sogar dort vollkommen neue Konkurrenten, wo sie zunächst nicht vermutet würden. Ein Beispiel hierfür ist die Entwicklung autonom fahrender Autos durch einen Konzern, der sein Geschäft mit Suchmaschinen begonnen hat. Oder die Entwicklung im Finanzdienstleistungsbereich, in dem sogenannte FinTechs die Geschäftsmodelle manch etablierter Filialbank zur Disposition stellen (Buchta u. a., 2009, Kap. 2.2).

2.4.2 Definition

Das IT-Governance Institut (www.itgi.org) hat sie definiert (Niemann, 2005, Kap. 2.6). Sie liegt in der Verantwortung des Vorstands und des Managements, damit die Ziele der Organisationsstrukturen und Prozesse in sicheren Ebenen gewährleistet werden. Die IT-Governance die IT, die Unternehmensstrategie und Ziele sicher. IT-Governance

bringt insofern Vorteilte mit sich, dass die Aufgaben der IT erfüllt werden, das kontinuierliche Planen und Optimierung von IT-Ressourcen auf eine effektive Ebene gebracht wird, das Evaluieren von der Performance im Unternehmen bezüglich der IT ständig gemessen und die Risiken gemindert werden.

2.4.3 Grundlage der IT-Governance

Das Etablieren der Aufgaben der IT-Governance führt zu Diskussionen, die im Zusammenhang zwischen Unternehmensarchitektur und IT-Governance entstehen, um deren Ziele zu erfüllen. Ein Teil der Diskussion ist hierbei die IT-Strategie. Die drei Parteien definieren das IT-Governance-Framework anhand deren Architecture-Management, Portfolio-Management sowie Programme- und Service-Management. Wenn die Unternehmensführung das Management-Informationssystem auf neue Ebenen umstellen würde, müssten die Schritte aus Abbildung 12 befolgt werden (Niemann, 2005, S. 36). Da eine Aktualisierung Risiken treffen könnte, muss eine Auswertung für Schwachstellen, Komplexität und Heterogenität von unterschiedlichen Softwaresystemen erstellt werden. Die Abbildungen 13[8] und14 (Niemann, 2005, Abb. 2–10) geben dem Autor die Schritte für die Weiterführung seines Projekts.

On a dark night, a man was on his hands and knees under a lamppost searching inch by inch for a lost object. A policeman came along and asked what he was doing. “Looking for my house keys”, was the answer. “And where did you drop them?” “Over there by the bushes”, was the answer. “Then why are you looking here?” “Because the light is better.”

Abbildung 12: Optimierung ohne Information ist eine Fahrt im Dunkeln

[8] https://rmtp.de/leistungen/it-strategie-it-governence/

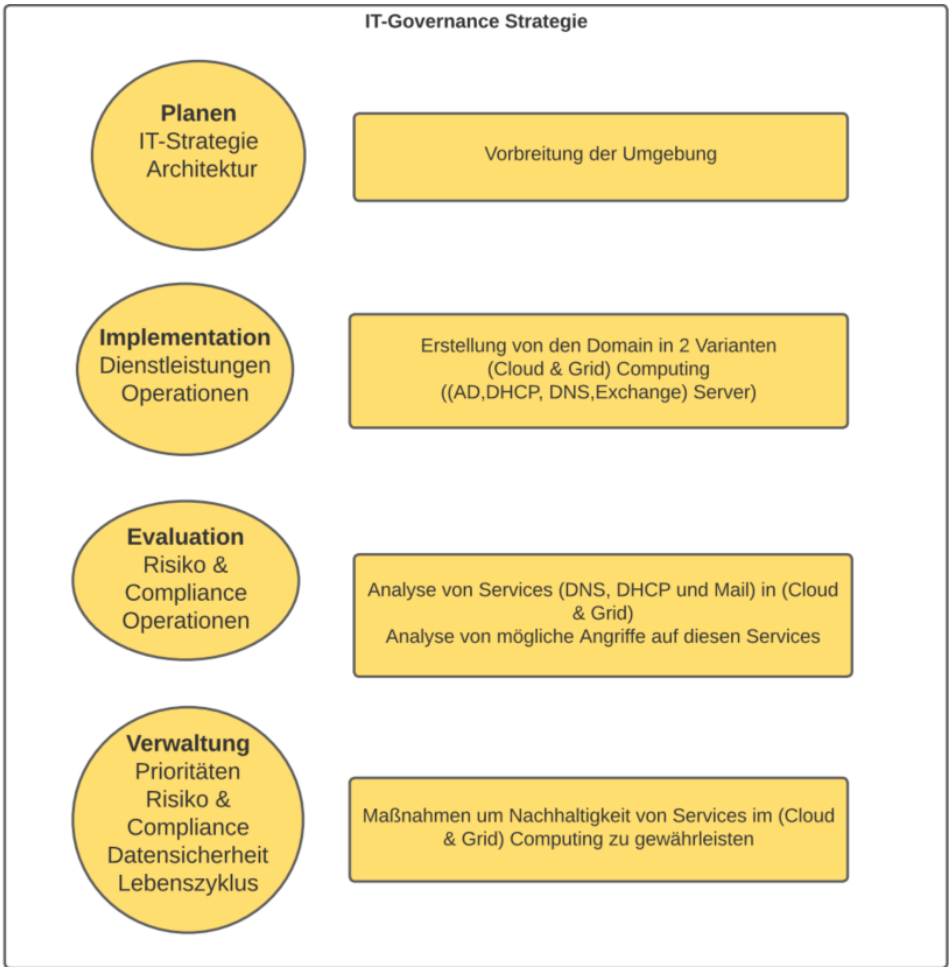


Abbildung 13: IT-Governance Strategie

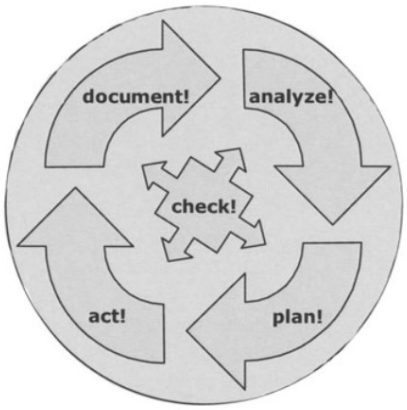


Abbildung 14: Unternehmensarchitektur

Der Unternehmensarchitektur-Zyklus

1. IT-Planung

IT-Planung ist der Erfolgsfaktor der IT-Governance, welche zur richtigen Umsetzung von IT-Strategien benötigt wird. Um den strukturellen Rahmen der IT-Governance

einzuhalten, muss die IT eine effektive Weise für die Umsetzung verfolgen. Andernfalls könnten falschen Entscheidungen in der IT-Planung einen kontinuierlichen Verlust bedeuten. Informationskriterien für die IT-Strategie sind:

Effektivität, Integrität, Vertraulichkeit, Effizienz, Verfügbarkeit, Einhaltung regulatorischer Erfordernisse und Zuverlässigkeit.

In dieser Phase ist es für die IT besonders relevant, dass die Analyse im Unternehmen nicht getrennt von geregeltem Austausch von alten Geräten. Wenn diesen Fall getroffen wurde, dann führt die Planung nicht zu den gewünschten Ergebnissen, sondern zu Fehlentwicklungen. Die IT benötigt daher eine grundlegende Methode, um eine hinreichende differenzierte und funktionsfähige Leistung erbringen zu können. Diese basiert auf den verfügbaren analysierten Systeminformationen. Daher wurde in dieser Arbeit IT-Governance Regeln gefolgt.

2. IT -Performance-Management

Wenn die IT ihre Rolle als Werttreiber für das Unternehmen erfüllen soll, müssen die Leistungen der IT mess- und steuerbar sein. Hierfür sind geeignete IT-Systeme zu verwenden, die zu einer Prozessoptimierung Auswertung liefern. Daher legt die Unternehmensführung Regeln fest, um Schutzziele sicher zu stellen (Buchta u. a., 2009, S. 20). Diese Schutzziele sind:

Vertraulichkeit

Vertraulichkeit besagt, dass übertragene oder gespeicherte Daten ausschließlich von autorisierten Personen gelesen werden dürfen. In der Betrachtung der Netzwerksicherheit steht ausschließlich der Datenaustausch. Dies bedeutet, dass kein Zugriff auf gesendeten Daten von Dritten möglich ist. Dafür wird die Kommunikation verschlüsselt, um die Vertraulichkeit im Bereich der Netzwerksicherheit vor Angriffen zu schützen. Ein Angreifer kann aus belauschtem Netzwerkverkehr keine Daten rekonstruieren.

Integrität

Wenn eine Änderung von Daten ausschließlich durch autorisierte Personen stattgefunden hat, wurde die Integrität gewährleistet. Integrität der Daten bedeutet demnach, dass sämtliche personenbezogenen Daten vor unbefugtem Zugriff oder Manipulation durch Dritte geschützt werden müssen. Aufgrund dieser Informationssicherheit muss jegliche Veränderung der Daten einer verantwortlichen Person zugeordnet werden. Wenn die Kommunikation zwischen zwei Systeme sicher ist, ohne manipulative Auswirkung, kann hier von Integrität gesprochen werden. Der Datenverkehr darf nicht durch fremden Zugriff verändert werden können. Ist es trotz allem zu einer Manipulation gekommen, so muss in der Auswertungs- bzw. Evaluationsphase erwähnt werden, dass eine Integritätsverletzung stattgefunden hat.

Verfügbarkeit

Daten und Dienste müssen dem autorisierten Nutzer in der IT jederzeit zur Verfügung stehen. Dies kann durch das Ergreifen von technischen und organisatorischen Maßnahmen erfolgen, die potenzielle Ausfallfaktoren reduzieren und den konstanten Zugriff auf persönliche Daten gewährleisten. Die Verletzung der Verfügbarkeit aufgrund eines unerfüllten Dienstes bzw. ausfallenden Netzwerkes sollte in die Maßnahmeplanung einbezogen werden.

3. Analyse der Unternehmensarchitektur

In der Analysephase werden Risiko (Niemann, 2005, S. 67) und Compliance analysiert. Für die Entwicklung/Umsetzung von Systemen und IT-Services bedarf es einiger Regeln, um komplexes Management zu vermeiden. In dieser Phase sind Tools (siehe Abschnitt 2.6) zur Analyse zu verwenden. Der Standort der betroffenen Systeme hat Einfluss auf die Analyse. Hierbei stellt sich die Frage, ob betroffene Systeme lokal oder aus dem Internet erreichbar sind.

4. Evaluieren

Nachdem die Informationen in den vorherigen Phasen gesammelt wurden, werden sie in dieser Phase evaluiert. Stärken und Schwächen hinsichtlich der Anforderungen, Systemerreichbarkeit, System- und Kommunikationssicherheit sowie Vertrauenswürdigkeit der Erwartungen sollen somit festgestellt werden.

2.5 Netzwerk Dienste

2.5.1 Active Directory

In einer Domain ist ein Dienst für die Verwaltung von Objekten notwendig, welcher den Nutzern zur Verfügung steht und die Administratorenarbeit vereinfacht. Solch ein Dienst ist Active Directory (AD). AD ist ein Verzeichnisdienst von Microsoft, welcher ab Windows 2000 in Betrieb gekommen ist. Die Nutzung von Active Directory in der lokalen Domain dient dazu, dass abgespeicherte Informationen von Nutzern und Gruppen, Computern und Geräten sowie Anwendungen und weitere Dienste zentralisiert werden. Es wird daher auch das Netzwerkbetriebssystem von Microsoft genannt. Die Informationen werden genutzt, um einzelne Objekte des Netzwerks durch Kerberos zu authentifizieren und zu autorisieren. Die Verwaltung von abgespeicherten Daten benötigt Zeit, daher empfehlt sich, diese an einem sicheren Ort zu speichern. Des Weiteren können den Nutzern bestimmte Zugriffsrechte zugeteilt werden. Dabei wird zwischen Rechnerrechten und Nutzerrechten unterschieden. Rechnerrechte sind an einen Rechner gebunden, es spielt keine Rolle, welcher Nutzer den Rechner benutzt. Die Arbeitsweise in AD ist objektorientiert. Das bedeutet, dass alle betrachteten Daten im Netzwerk als

Objekte angesehen werden, welche besondere Attribute aufweisen. Sie können auch als Container und Non-Container oder Blattknoten bezeichnet werden. Active Directory bildet den Aufbau eines Unternehmensnetzwerks hierarchisch ab, wie es auch in einem Dateisystem praktiziert wird. Der Administrator hat die Aufgabe, Nutzern und anderen Objekten in dem Netzwerk Berechtigungen zuzuweisen. Außerdem werden sogenannte Organisationseinheiten (OUs) genutzt, um Objekte und weitere OUs zu gruppieren. Das Erstellen von OUs bringt den Vorteil mit sich, dass das Verwalten nicht aufwendig ist. Dabei bildet sich eine Baum- beziehungsweise Foreststruktur, welche sich aus dem Zusammenschluss von mindestens einer Domäne, OUs und weiteren Objekten bildet. Der Server, auf dem die Administration der Domäne vonstatten geht, wird als Domain Controller bezeichnet (Schieb, 2018, Kap. 2).

2.5.2 DHCP

Jedem Endgerät kann eine IP-Adresse zugewiesen werden, welche statisch eingestellt wird. Diese Vorgehensweise gilt jedoch nur für Geräte, die in der Regel feste IP-Adressen brauchen. Für Einrichtungen, welche täglich von Mitarbeitenden verwendet werden, ist die statische Adressierung nicht geeignet, da für die statische Adressierung eine feste IP-Adresse einer jeden Einrichtung hinzufügt werden muss. Diese Arbeit ist ziemlich aufwändig und schwer zu realisieren. Deswegen wird für Endgeräte eine dynamische Adressierung bereitgestellt. Von einer dynamischen Adressierung ist die Rede, wenn einem Host bei einer neuen Verbindung mit einem Netz eine neue IP-Adresse zugewiesen wird. Im LAN-Bereich wird die dynamische Adressierung durch DHCP (Dynamic Host Configuration Protocol) verarbeitet. Dieses Protokoll ermöglicht eine automatische Zuweisung der Netzwerkkonfiguration an Hosts durch den Server, statt einer manuellen Einstellung. Wo ohne DHCP-Einstellung, wie die IP-Adresse, die Netzmaske, die Gateway-Adresse oder die DNS-Serveradresse manuell konfiguriert werden müssen, verteilt der DHCP-Dienst die Einstellungen an die am Netzwerk angeschlossenen Hosts. In der Regel wird ein Client/Server-Modell verwendet. Ein DHCP-Client sendet einen Antrag an den DHCP-Server, um die Konfiguration wie beispielsweise die IP-Adresse, Subnetzmaske anzufordern. Der DHCP-Server antwortet dem Client mit einer Nachricht, in dem die gewünschten Informationen enthalten sind. Deswegen umfasst eine DHCP-Struktur mindestens zwei Aufgaben, nämlich den DHCP-Client und den DHCP-Server (siehe Abbildung 15 Client-Server-Nachrichten für IP-Vergabe). In manchen Fällen gibt es noch ein DHCP-Relay-Agent, um die vom Client gesendeten Anträge an den DHCP-Server weiterzuleiten (Schieb, 2018, Kap. 2).

192.168.178.13	192.168.178.3	DHCP	342 DHCP Release
0.0.0.0	255.255.255.255	DHCP	342 DHCP Discover
192.168.178.3	255.255.255.255	DHCP	342 DHCP Offer
0.0.0.0	255.255.255.255	DHCP	365 DHCP Request
192.168.178.3	255.255.255.255	DHCP	342 DHCP ACK

Abbildung 15: Client -Server-Nachrichten für IP-Vergabe

Quelle: Eigene Quelle

2.5.3 Domain Name Service

In der Microsoft-Umgebung erfolgt die Verwaltung von Zugriffrechte durch Active Directory. Diese ist jedoch von einem Domain Namen Service (DNS) abhängig, welcher standarisiert wurde, um die Zuordnung von Objektnamen zu der zugehörigen IP-Adresse und umgekehrt zu vereinfachen. Die einem Endgerät zugewiesenen Domänen-Namen dienen zur besseren Identifizierung durch den Menschen. Domänen sind hierarchisch aufgebaut. Die Root (Wurzel) der Domain steht für die Stammdomäne, dann werden Domain-Namespaces in mehrere Server aufgeteilt, die sich wiederum mehreren Servern untergeordnet haben. Eine DNS-Zone kann mehrere Subdomains enthalten und auf einem Server können sich mehrere Zonen befinden (siehe Abbildung 17). Diese Zonen werden als Verwaltungsbereiche im Domain-Namespace betrachtet werden. Die einem DNS-Namen zugehörige IP-Adresse lässt sich über den Fully Qualified Domain Name (FQDN) (siehe die Abbildung 16) herausfinden. Dieser für jedes Endgerät einmalige DNS-Name besteht aus mehreren Segmenten, die durch Punkte getrennt sind. Dieses Segment stellt eine Domain in der Hierarchie dar. Um den Aufbau der Namenshierarchie des FQDN besser verstehen zu können, sollte dieser von rechts nach links betrachtet werden. Ganz rechts befindet sich die Top-Level-Domain (TLD), wie z. B. „.de“ oder „.org“, danach folgen die Subdomänen. Im Active Directory wird die Stammdomäne des Root-Servers aus einem Präfix und einem Suffix festgeschrieben, in der Schreibweise „Präfix.Suffix“. In einem Active Directory ist also ein DNS-Server wichtig (siehe die Abbildung 18) (Bless u. a., 2005, Kap. 10.6).

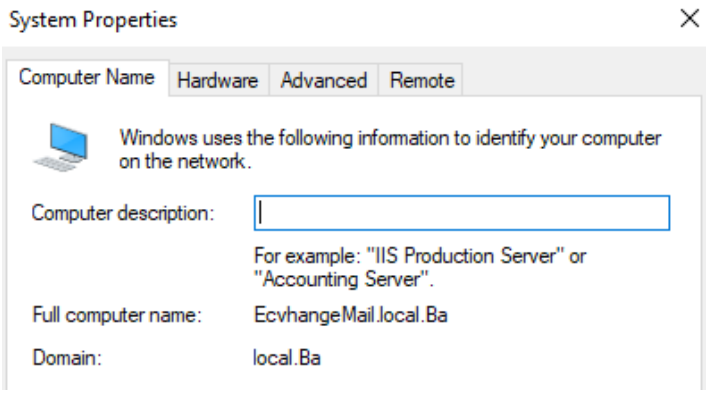


Abbildung 16: PC-Name

DNS-Name von Exchange Server. Quelle: Eigene Quelle

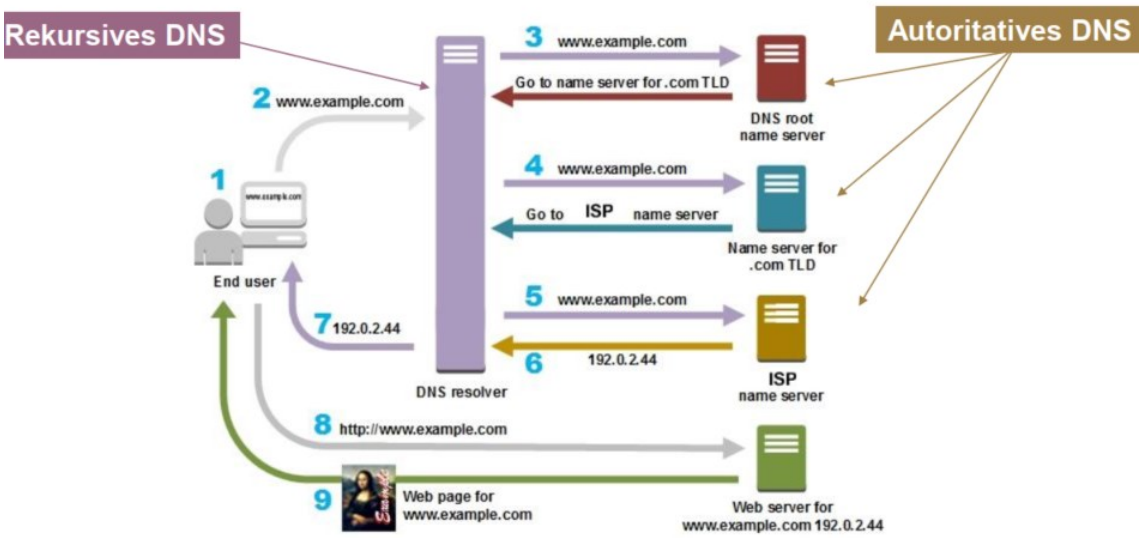


Abbildung 17: DNS-Schritte

Quelle: Prof. Bodach Modul: Abwehr von IT-Angriffen

Abbildung 18: Antrag im DNS-Server

Zugehörige Antrag im DNS-Server. Quelle: Eigene Quelle

2.5.4 Zugriffskontrolle (engl. Access Control)

Die Reglung von Zugriff-Möglichkeiten auf Ressourcen in einer Domain wird durch Zugriffskontrolle sichergestellt. Dafür gibt es Hauptarten von Zugriffskontrollen.

Role Based Access Control

Im Jahr 1992 wurde Role Based Access Control von D. Ferraiolo und R. Kuhn entwickelt (FERRAIOLO & KUHN, 1992). Die Rechte eines Nutzers werden anhand der Rolle in dem Unternehmen definiert. Diese bleiben über einen Zeitraum begrenzt konstant und die Zuweisung von Rechten kann einfach geändert werden. Auf diese Art und Weise können potenzielle Fehler vermieden werden, beispielsweise dass einem Nutzer keine oder mehrere Rechte zugewiesen werden (Igor K und Victor S, 2012, S. 97).

Attribute Based Access Control

Die Attribute Based Access Control wird eingesetzt, um eine Entscheidung für den Zugriff zu treffen. Zusätzlich gibt es Richtlinien (Policies), bei welchen anhand der Attribute entschieden wird, ob ein Subjekt berechtigt ist, am Objekt eine Aktion durchzuführen (Igor K und Victor S, 2012, S. 84).

2.5.5 MS Exchange Server

Dieser Server, der von Microsoft stammt, bietet dem Domain-Nutzer Mailserver-Dienste, Kontaktverwaltung sowie Kalendersoftware. Der Sever speichert seine Datenbank lokal. Die Voraussetzungen (© MICROSOFT 2022) für die Verwaltung von E-Mails müssen erfüllt werden, um sicherzustellen, dass die Kommunikation in der Domain überprüft wird und sicher geleitet wird. Dieser Server wird mit der Funktion, infizierte E-Mails und Spam vor der Zustellung auf dem Server zu filtern, unterstützt. Mithilfe der Server-Verwaltung können Sicherheitsmaßnahmen gegen gezielte Angriffe eingestellt werden. Für den E-Mail-Austausch in der Domain ist eine Software, welche E-Mail-Dienste unterstützt, wie bspw. Microsoft Outlook, notwendig (Schieb, 2018, Kap. 2).

2.5.6 E-Mail-Protokolle (SMPT, IMAP, POP3) :

Für die Funktionsweise eines E-Mail-Systems werden Protokolle zum Versenden, Transportieren und Empfangen sowie physische Server zum Weiterleiten, Speichern und Bereitstellen einer E-Mail benötigt (Bless u. a., 2005, Kap. 10.9).

SMPT

Protokoll SMTP übernimmt den Transport und die Übermittlung von E-Mails im Internet. Das Ziel des Protokolls ist es, eine E-Mail zuverlässig und effizient bis zum Ziel zu übertragen. In der Basisstruktur des SMTP-Modells (siehe Abbildung 19 (Bless u. a., 2005, Kap. 10.9)) sind der SMTP-Client des Senders und der SMTP-Server des Empfängers dargestellt. Der SMTP-Client ist dafür verantwortlich, dass die Nachricht zu einem oder mehreren SMTP-Server(n) übertragen wird und wenn ein Fehler auftritt, diesen zu melden.

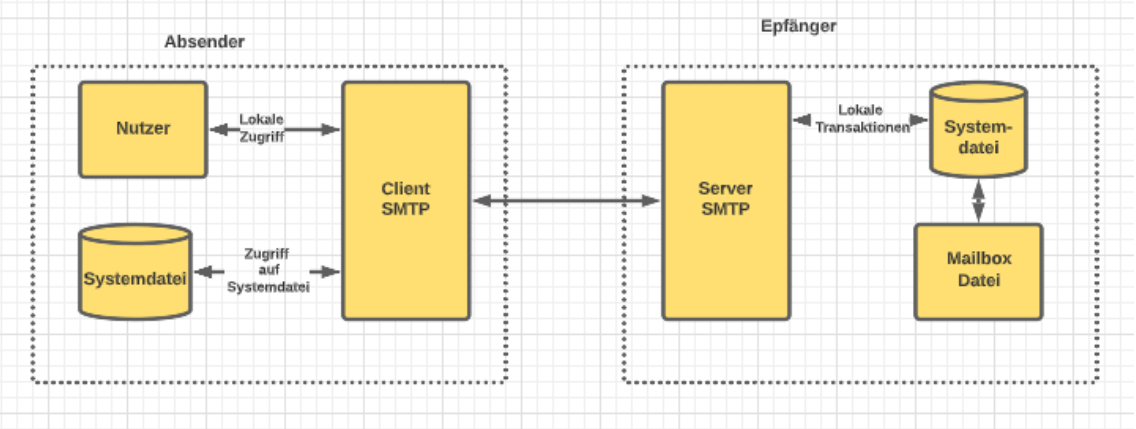


Abbildung 19: SMTP Client-Server

Der SMTP-Server kann drei verschiedene Rollen einnehmen:

1. Er ist ein "Gateway" (Message Submission Agent MSA). Er erhält die E-Mail von einem SMTP-Client und liefert sie aus oder fungiert als SMTP-Client und leitet sie weiter.

2. Er ist ein "Relay" (Mail Transfer Agent MTA). Er erhält die E-Mail entweder von einem MSA oder von einem anderen MTA. Er liefert die E-Mail aus oder fungiert als SMTP-Client und leitet sie weiter. Der MTA kann der Zieldomain angehören.

3. Er ist der Zieldomain zugehörig und die Nachricht wurde übermittelt und per

"local delivery" abgelegt. Er wird auch Mail Delivery Agent (MDA) genannt.

Eine Verbindung zum SMTP-Server des Empfängers kann direkt oder über mehrere SMTP-Server-Sprünge (engl. "Hops") erfolgen.

POP3

Protokoll POP3 ermöglicht den Zugriff und den Abruf von E-Mails am Mailserver, wobei die E-Mail heruntergeladen wird und gelöscht werden kann. Operationen zum Verändern der E-Mails am Mailserver sind daher nicht vorgesehen und die Verwaltung der E-Mails findet lokal statt (siehe Abbildung 20) (Bless u. a., 2005, Kap. 10.9).

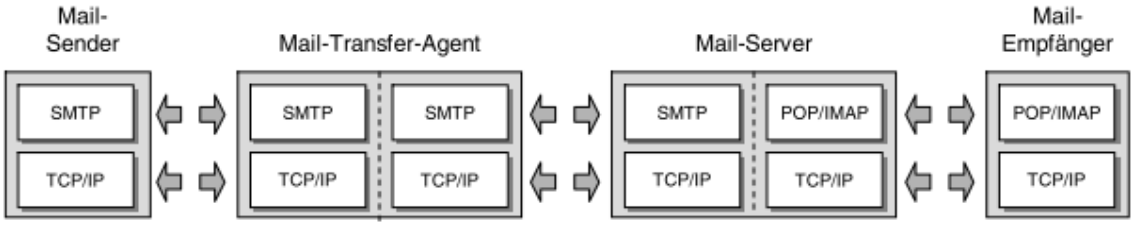


Abbildung 20: Mail Protokolle

IMAP

Im IMAP wiederum wird dem Benutzer der Zugriff und die Manipulation von E-Mails am Mailserver erlaubt, wodurch die E-Mails auf dem Server existent bleiben und von jedem Computer aus abgerufen werden können. Ein Benutzer kann somit auf dem Mailserver neue E-Mails verfassen, bestehende suchen, markieren oder löschen und in einer Ordnerstruktur verwalten. Die Schnittstelle zwischen dem Benutzer und dem Mailserver wird von einer E-Mail-Anwendung wie bspw. "Microsoft Outlook" übernommen, welche beide Protokolle nutzen kann (siehe Abbildung 20).

2.6 Tools

2.6.1 VMware ESXi

VMware ESXi ist ein Typ-1-Hypervisor, welcher ohne ein Host-Betriebssystem installiert wird. VMware ESXi gehört zu der VMware vSphere Suite, einer Sammlung von Software, die zur Verwaltung und zum Ressourcenmanagement bei Virtualisierung entwickelt wurde. Dabei wird der Hypervisor ESXi als Hauptkomponente der vSphere Suite gesehen. VMware ESXi 7.0(„Download the ESXi Installer“) ist die neueste Version dieses Hypervisors, welche im April 2022 letztmals aktualisiert wurde.

2.6.2 VMware Workstation Pro

VMware Workstation Pro gehört zu den Typ-2-Hypervisoren. Die Software kann auf vielen Linux und Windows Betriebssystemen installiert werden. Die letzte Version von VMware Workstation ist 17 Pro(„Download VMware Workstation Pro | DE“), welches im 17 November 2022 veröffentlicht wurde. Es existiert eine kostenfreie Testversion, welche für 30 Tage nutzbar ist. Workstation Pro ist in der Lage, mehrere VMs mit

unterschiedlichen Betriebssystemen zu erstellen und zu verwalten. Außerdem können virtuelle Netzwerke erstellt und verwaltet werden. Dafür ist die Konfiguration mehrerer virtueller Switches möglich. Außerdem kann Workstation Pro auch mit der VMware ESXi verbunden werden. Die gesamte Verwaltung der VMs wird zentral über das Workstation Pro Fenster gesteuert (siehe Abbildung 21). Das Programm ist so strukturiert, dass die einzelnen VMs in Registerkarten betrieben werden. Sie können zusätzlich in einzelne Fenster getrennt werden, um mehrere VMs gleichzeitig einsehen zu können.

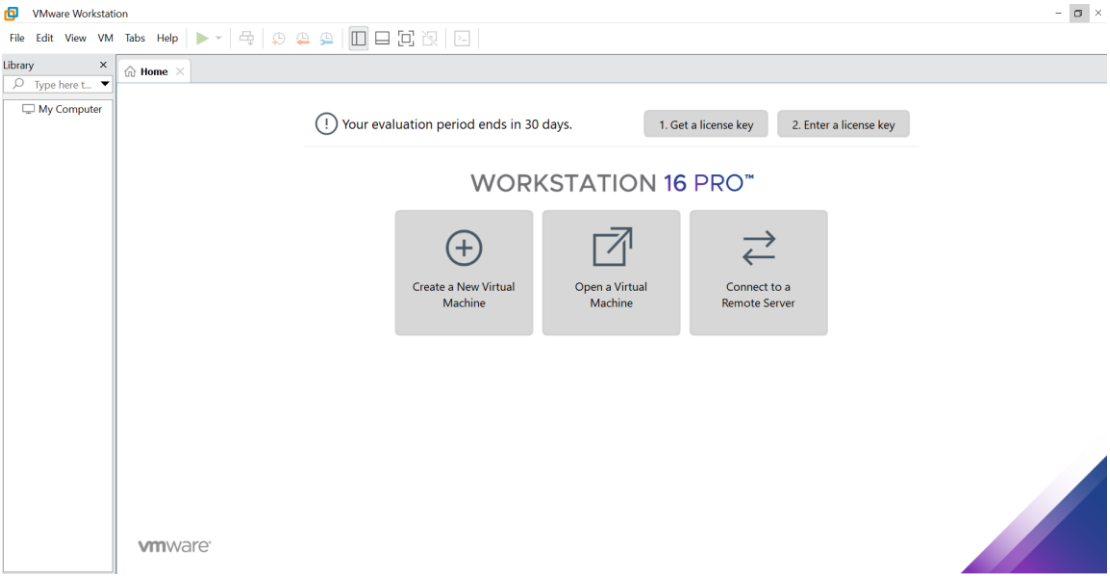


Abbildung 21: VMware Workstation 16 Pro Software Quelle: Eigene Abbildung

Bei dem erweiterten Setup zum Erstellen einer VM mit VMware Workstation Pro muss ausgewählt werden, mit welcher Version von Workstation Pro die VM kompatibel sein soll. Da eine Kompatibilität mit älteren Versionen bei der Laborumgebung nicht notwendig ist, sollte die neueste Version gewählt werden. Wurde ein Name für die VM, ein Speicherort auf dem Host Computer, sowie das Installationsmedium gewählt, müssen die Hardwareeinstellungen definiert werden. Bei Workstation Pro gibt es die Möglichkeit, die Firmware zu konfigurieren, dabei steht die Wahl zwischen BIOS und UEFI mit oder ohne Secure Boot. UEFI ist zwar moderner und bietet dem Nutzer mehr Komfort durch eine grafische Oberfläche. Jedoch kommt mit zunehmender Vereinfachung der grundlegenden Konfiguration auch ein Abfall der Sicherheit zustande. Das BIOS schließt direkt an die Hardware an. Das UEFI hat andererseits die Möglichkeit, beispielsweise Treiberupdates über das Internet herunterzuladen. Dadurch ist das UEFI jedoch angreifbarer als das BIOS(GABECI, 2020)[9], da eine Netzwerkschnittstelle über TCP/IP besteht. Für die Konfiguration virtueller Maschinen bedarf es der Zuweisung von CPUs und Prozessorkernen, Arbeitsspeicher, sowie der Wahl, welchen Netzwerk-Typ die VM nutzen soll. Diese Einstellungen sind nach der Installation der VM

[9] https://blog.devgenius.io/whats-the-difference-between-uefi-and-bios-c8bfed674f1f

änderbar. Falls also beim Betrieb Performance-Einbußen registriert werden, können die zugewiesenen Ressourcen auch im Nachhinein erhöht werden. Bei VMware Workstation werden standardmäßig zwei Prozessoren mit jeweils einem Kern, 2 GB Arbeitsspeicher und einer Festplattengröße von 60 GB zugewiesen. Des Weiteren kann, abhängig vom zu installierenden Betriebssystem, ausgewählt werden, welchen I/O-Controller-Typ die VM emulieren soll. Bei der Wahl des Input/Output-Controller-Typs gibt es nur die Möglichkeit zwischen LSI Logic SAS und einem para-virtualisiertem SCSI Controller (PVSCSI). Laut VMware ist PVSCSI eher für Storage Area Networks (SAN) geeignet, die sich auf das Speichern von großen Mengen an Daten konzentrieren. Demnach ist der LSI Logic SAS Controller die geeignetere Wahl, da er über eine bessere Leistung verfügt. Der nächste Schritt besteht darin, den virtuellen Disktypen zu bestimmen. Dabei kann zwischen IDE, SCSI, SATA und NVMe gewählt werden. NVMe (NVM Express) ist eine Softwareschnittstelle für SSD Festplatten. Sie wurde im Jahr 2011 erstmals (WIKIPEDIA, 2022) veröffentlicht und stellt somit die modernste Möglichkeit für die Schnittstellentechnologie zwischen Speicher und Software dar. Außerdem kann der Disktyp nach der Installation der virtuellen Maschine verändert werden.

2.6.3 Snapshots

Mit der in der VMware enthaltenen Snapshot-Funktion können bestimmte Abläufe sichergestellt werden. Storage-Snapshots kann angewandt werden, um die Image-Erstellung beschleunigen. Des Weiteren können Malware-Analysen ausgeführt werden und Änderungen am Dateisystem sowie Reaktionen der eingeschleusten Malware beobachtet und dokumentiert werden. Anschließend müssen die VMs auf einen zuvor erstellten Snapshot zurückgesetzt werden. Daran anschließend ist eine erneute Durchführung genau derselben Maßnahme ohne Änderung jeglicher Parameter möglich. Die Active Directory-Datenbank wird durch Änderungen und Handlungen der anderen VMs überschrieben. Aus diesem Grund muss auf allen VMs gleichzeitig ein Snapshot erstellt werden und ebenso muss das Zurückkehren auf einen erstellten Snapshot bei allem installierten VMs in diesem Projekt gleichzeitig durchgeführt werden.

2.6.4 Wireshark Packet Capture

Um Netzwerkverkehr analysieren zu können, muss dieser aufgezeichnet und abgespeichert werden können. Dabei hat sich Wireshark für die Aufzeichnung und Auswertung von Netzwerkverkehr durchgesetzt. Wireshark bietet dabei auch ein Graphical User Interface (GUI) für die direkte Auswertung der Daten. Der große Nachteil von Wireshark ist aber die komplexe Handhabung. Das GUI bietet zwar viele Analysemöglichkeiten, die sind aber nicht immer intuitiv auffindbar. Mit Wireshark ist eine genaue Analyse nur möglich, sofern das benötigte Knowhow angeeignet wurde. Andernfalls sind Auswertungen sehr zeitaufwändig. Netzwerkverkehr kann für spätere Analysezwecke auch in Dumps, sogenannten Packet Captures, abgelegt werden. Hierzu existiert

eine eigene Dateiendung Packet Caputre (PCAP) oder Packet Caputre Next Generation (PCAPNG). Wireshark bietet zusätzlich zur GUI- noch eine weitere CLI-Anwendung, namentlich TShark. TShark kann wie Wireshark Netzwerkverkehr aufzeichnen und gibt den aufgezeichneten Traffic auf der Konsole aus. TShark ermöglicht auch die Ausgabe eines aufgezeichneten Capture auf der Konsole. Dabei können einzelne Attribute oder direkt ganze Packets ausgegeben werden.

2.6.5 Securepoint-VPN

Ein VPN baut eine sichere Verbindung im Internet auf und fungiert als ein „privates“ Netzwerk, ähnlich einem LAN, in welchem berechtigte Gruppen direkt über den Server kommunizieren können.

Dafür werden zwei Komponenten benötigt:

Ein Server, bei dem sich sämtliche VPN-Teilnehmer anmelden und ein Client Programm, welches die Anmeldung am Server vornimmt. Die Verbindung wird in der Regel per IPSec oder SSL verschlüsselt. Die Kommunikation zwischen Client-Anwendungen und Server-Dienstleistungen wird durch die VPN-Software geleitet und mit dieser verschlüsselt bzw. entschlüsselt.

2.6.6 NAGIOS Betriebssystem

NAGIOS ist ein Open Source Monitoring System für Linux und Unix, welches in der Programmiersprache C entwickelt wurde. Es dient zur Überwachung von Hosts und deren Diensten. Mithilfe von NAGIOS ist es möglich, Prozesse, die in irgendeiner Art und Weise numerische oder boolesche Werte (Beispiel: Ping funktioniert oder funktioniert nicht) produzieren, zentral zu überwachen. Es werden neben der Überwachung von Servern und Workstations auch Netzwerk-Switche sowie Temperatur- und Feuchtigkeitssensoren für Drucker oder sonstige Endgeräte bereitgestellt, die mit einer Netzwerkschnittstelle sind. Diese müssen für NAGIOS definiert und zugehörige Services festgelegt werden. NAGIOS übernimmt die Überwachung anschließend von selbst und alarmiert den Systemadministrator bei Überschreitung kritischer Zustandsgrenzen. NAGIOS hat das Ziel gesetzt, dem Administrator eine Informationsflut zu ersparen, die Zustände (Unknown, Critical, Warning, OK) (siehe Abbildung NAGIOS Report) werden daher farbig dargestellt. Dazugehörige Check-Performance-Daten sind Messwerte, die mithilfe von NAGIOS-Grapher als Graph über der Zeit dargestellt werden. NAGIOS zeigt zusammen mit jedem festgestellten Problem zwei Parameter an.

Severity: Gibt an, wie groß die Gefahr durch die Sicherheitslücke ist. Dabei wird das Common Vulnerability Scoring System (CVSS)[10] als Basis verwendet.

QoD - Quality of Detection: Beschreibt als Prozentwert, mit welcher Zuverlässigkeit das Problem festgestellt wurde.

2.6.7 Common Vulnerability Scoring System

Wenn ein Unternehmen neue Technologien in den Betrieb einführt, müssen sensible Informationen im Hinblick auf das zusätzliche Risikoniveau gesichert werden, welches die neuen Komponenten für das gesamte System darstellt. Eine gängige Methode, die Informationssicherheitsspezialisten für diesen Prozess verwenden, ist das Common Vulnerability Scoring System (CVSS)(NATIONAL VULNERABILITY DATABAS, 2013)[11]. Das Common Vulnerability Scoring System bietet eine Methode zur Bewertung, wie anfällig eine Software für Angriffe ist. Viele Cybersicherheitsexperten verwenden den CVSS-Basiswert, der im Folgenden definiert sind, als primäre Metrik, um den Schweregrad einer ausnutzbaren Schwachstelle zu bestimmen. Dieses Framework hilft Unternehmen, die Integrität der Vertraulichkeit in Bezug auf die sensiblen Daten ihrer Kunden sicherzustellen.

Basis-Metriken

1. Ausnutzbarkeit-Metriken:

Exploitability-Metriken sind eine Darstellung der Schwachstelle, die formal auch als verwundbare Komponente bezeichnet wird. Daher sollte jede Ausnutzbarkeit von Metriken zur anfälligen Komponente bewertet werden und die Eigenschaften der Anfälligkeit widerspiegeln, die zu einem erfolgreichen Angriff führen. Bei der Bewertung von Basis-Metriken sollte davon ausgegangen werden, dass der Angreifer über fortgeschrittene Kenntnisse der Schwachstellen des Zielsystems verfügt, einschließlich der allgemeinen Konfiguration und der standardmäßigen Abwehrmechanismen (z. B. integrierte Firewalls, Sicherheitsbegrenzungen, Überwachungssystem für Netzwerksverkehr).

Angriffsvektor (Access Vector)

Diese Metrik bezieht sich auf die Möglichkeit der Ausnutzung von Schwachstellen. Der Metrik-Wert ist umso größer, je weiter entfernt sich der Angreifer befindet, um die anfällige Komponente auszunutzen. Die Annahme ist, dass die Anzahl potenzieller Angreifer für eine Schwachstelle, die über ein Netzwerk ausgenutzt werden könnte, größer ist als die Anzahl potenzieller Angreifer, die eine Schwachstelle ausnutzen

[10] https://nvd.nist.gov/vuln-metrics/cvss

[11] https://nvd.nist.gov/

könnten, die einen physischen Zugriff auf ein Gerät erfordert. Daher ergibt sich ein höherer Basiswert. Die Liste möglicher Werte ist in der nachfolgenden Tabelle dargestellt.

Tabelle 1: Beschreibung Angriffsvektor Metriken

Metrik-Wert	Beschreibung
Lokal (Physisch)	Der Angriff erfordert, dass der Angreifer die anfällige Komponente physisch berührt oder manipuliert. Die körperliche Interaktion kann kurz oder anhaltend sein.
Lokales Netz	Die anfällige Komponente ist an das lokale Netzwerk gebunden und der Weg des Angreifers erfolgt über Zugriffsrechte (Lese-,Schreib- , Ausführungsfunktionen). Entweder: Der Angreifer nutzt die Sicherheitsanfälligkeit aus, indem er lokal (z. B. Tastatur) oder remote (z. B. SSH) auf das Zielsystem zugreift. Oder: Der Angreifer verlässt sich auf die Benutzerinteraktion einer anderen Person, um Aktionen auszuführen, die erforderlich sind, um die Sicherheits-anfälligkeit auszunutzen (z. B. die Verwendung von Sozial-Engineering-Techniken, um einen legitimen Benutzer dazu zu bringen, ein schädliches Dokument zu öffnen).
Internet	Die anfällige Komponente ist an das Netzwerk gebunden. Eine solche Schwachstelle wird oft als "remote ausnutzbar" bezeichnet und kann als Angriff betrachtet werden, der auf Protokollebene einen oder mehrere Netzwerk-Hops entfernt ausgenutzt werden kann (z. B. über einen oder mehrere Router), wie einen Denial-of-Service (DoS).

Schwierigkeit (Attack Complexity)

Diese Metrik beschreibt die Bedingungen, die außerhalb der Kontrolle des Angreifers liegen müssen, um die Schwachstelle auszunutzen. Solche Bedingungen können das Sammeln von zusätzlichen Informationen über das Ziel oder Berechnungsausnahmen erfordern. Wichtig ist, dass die Bewertung dieser Metrik alle Anforderungen an Benutzerinteraktion ausschließt, um die Schwachstelle auszunutzen. Wenn eine bestimmte Konfiguration für einen erfolgreichen Angriff erforderlich ist, sollten die Basis-Metriken unter der Annahme bewertet werden, dass sich die anfällige Komponente in dieser Konfiguration befindet. Der Base Score ist am größten für die am wenigsten komplexen Angriffe. Die Liste möglicher Werte ist in untenstehender Tabelle dargestellt.

Tabelle 2: Beschreibung Schwierigkeit Metriken

Metrik-Wert	Beschreibung
Gering	Besondere Zugangsbedingungen bestehen nicht. Ein Angreifer kann die gezielte Komponente mit Erfolg ständig angreifen.
Mittel	Ein Angreifer trifft auf Schwierigkeiten bei jedem Angriff gegen die Komponente. Dies ist im Vergleich zum Vorherigen aufwändig.
Hoch	Ein erfolgreicher Angriff kann nicht nach Belieben durchgeführt werden, sondern erfordert einen hohen Aufwand des Angreifers.

Anmeldung (Authentication)

Diese Metrik beschreibt die Berechtigungsstufe, die ein Angreifer besitzen muss, bevor er die Schwachstelle erfolgreich ausnutzen kann. Der Base Score ist am höchsten, wenn keine Privilegien erforderlich sind. Die Liste möglicher Werte ist in der folgenden Tabelle dargestellt.

Tabelle 3: Beschreibung Anmeldung Metriken

Metrik-Wert	Beschreibung
Ohne	Der Angreifer ist vor dem Angriff nicht autorisiert und benötigt daher keinen Zugriff auf Einstellungen oder Dateien des anfälligen Systems, um einen Angriff durchzuführen.
Einfach	Der Angreifer benötigt Berechtigungen, die grundlegende Benutzerfunktionen bereitstellen, welche normalerweise nur Einstellungen und Dateien betreffen, die einem Benutzer gehören. Alternativ kann ein Angreifer mit niedrigen Rechten nur auf nicht vertrauliche Ressourcen zugreifen.
Mehrfach	Der Angreifer benötigt Berechtigungen, die eine signifikante Kontrolle über die anfällige Komponente ermöglichen, um Zugriff auf komponentenweite Einstellungen und Dateien zu ermöglichen.

2. Auswirkungs-Metriken

Impact Metrics messen die Auswirkungen auf Vertraulichkeit, Integrität und Verfügbarkeit des betroffenen Systems. Mit ihnen werden vorhandene, automatisch generierte Auswirkungen, welche als Ergebnis der Ausnutzung eintreten, definiert.

Vertraulichkeit (Confidentiality)

Diese Metrik misst die Auswirkungen auf die Vertraulichkeit der von einer Softwarekomponente verwalteten Informationsressourcen aufgrund einer erfolgreich ausgenutzten Schwachstelle. Vertraulichkeit bezieht sich auf die Beschränkung des Zugriffs und das Veröffentlichen von Informationen auf ausschließlich autorisierte Benutzer sowie auf die Verhinderung des Zugriffs oder das Veröffentlichen gegenüber Unbefugten. Der Basiswert ist am höchsten, wenn der Verlust an der betroffenen Komponente am höchsten ist. Die Liste möglicher Werte wird in der anschließenden Tabelle dargestellt.

Tabelle 4: Beschreibung Vertraulichkeit Metriken

Metrik-Wert	Beschreibung
Ohne	Es gibt keinen Verlust der Vertraulichkeit innerhalb der betroffenen Komponente.
Teilweise	Es gibt einen gewissen Verlust an Vertraulichkeit. Es wird Zugriff auf einige eingeschränkte Informationen erhalten, aber der Angreifer hat keine Kontrolle darüber, welche Informationen erhalten werden, oder die Menge oder Art des Verlusts ist begrenzt. Das Veröffentlichen von Informationen verursacht keinen direkten, ernsthaften Schaden für die betroffene Komponente.
Vollständig	Es kommt zu einem vollständigen Verlust der Vertraulichkeit, was dazu führt, dass alle Ressourcen innerhalb der betroffenen Komponente an den Angreifer weitergegeben werden. Alternativ wird nur Zugang zu einigen eingeschränkten Informationen erlangt, aber die veröffentlichen Informationen haben eine direkte, schwerwiegende Auswirkung.

Integrität (Integrity)

Diese Metrik ergibt die Auswirkung auf die Integrität einer erfolgreich ausgenutzten Schwachstelle. Integrität bezieht sich auf die Vertrauenswürdigkeit und Wahrhaftigkeit von Informationen. Der Basiswert ist am höchsten, wenn die Auswirkung auf die betroffene Komponente am größten ist. Die möglichen Werte sind in der folgenden Tabelle aufgelistet.

Tabelle 5: Beschreibung Integrität Metriken

Metrik-Wert	Beschreibung
Ohne	Es gibt keinen Integritätsverlust innerhalb der betroffenen Komponente.
Teilweise	Die Änderung von Daten ist möglich, aber der Angreifer hat keine Kontrolle über die Folgen einer Änderung oder der Umfang der Änderung ist begrenzt. Die Datenänderung hat keine direkten Auswirkungen auf die betroffene Komponente.
Vollständig	Es kommt zu einem totalen Integritätsverlust oder einem kompletten Schutzverlust.

Verfügbarkeit (Availability)

Diese Metrik ermittelt die Werte der Auswirkung auf die Verfügbarkeit der betroffenen Komponente, die eine ausgenutzten Schwachstelle haben. Da sich die Verfügbarkeit auf die Zugänglichkeit von Informationsressourcen bezieht, haben Angriffe Auswirkung auf die Netzwerkbandbreite, Prozessorzyklen oder Festplattenspeicher. Der Basiswert ist am höchsten, wenn die Auswirkung auf die betroffene Komponente am größten ist. Die Liste der möglichen Werte ist in untenstehender Tabelle dargestellt.

Tabelle 6: Beschreibung Verfügbarkeit Metriken

Metrik-Wert	Beschreibung
Ohne	Es gibt keine Auswirkungen auf die Verfügbarkeit innerhalb der betroffenen Komponente.
Teilweise	Die Leistung wird reduziert oder es gibt Unterbrechungen in der Ressourcen-verfügbarkeit. Auch wenn eine mehrmalige Ausnutzung der Schwachstelle möglich ist, hat der Angreifer nicht die Möglichkeit, legitimen Benutzern den Dienst vollständig zu verweigern. Die Ressourcen in der betroffenen Komponente sind entweder die ganze Zeit teilweise verfügbar oder nur zeitweise vollständig verfügbar, aber insgesamt gibt es keine direkten, schwerwiegenden Folgen für die betroffene Komponente.
Vollständig	Es kommt zu einem vollständigen Verlust der Verfügbarkeit, was dazu führt, dass der Angreifer den Zugriff auf Ressourcen in der betroffenen Komponente vollständig verweigern kann. Dieser Verlust ist

	entweder anhaltend (während der Angreifer den Angriff fortsetzt) oder dauerhaft (der Zustand bleibt auch nach Abschluss des Angriffs bestehen).

Die folgende Tabelle gibt einen Überblick über CVSS V3 und wie das Bewertungssystem Unternehmen dabei hilft, Sicherheitslücken zu sichern.

Tabelle 7: BASE SCORE Werte

Base Score	Rating
9,0 – 10	„Critical „severity rating „
7,0 – 8,9	„High “severity rating“
4,0 – 6,9	„Medium „severity rating“
1,0 – 3,9	„Low “severity rating“
0 – 1,0	„None “severity rating“

CVSS-Berechnung:

Exploitability = 20 * Zugriff * Schwierigkeit * Anmeldung

Impact = 10.41 * (1- (1-Vertraulichkeit) * (1-Integrität) * (1-Verfügbarkeit))

f(impact) = 0, wenn Impact=0, ansonsten 1,176

BaseScore = Aufrunden auf 1 Nachkommastelle (((0.6*Impact) +(0,4*Exploitability) -1,5) * f(Impact))

Quelle [12]

Tabelle 8: BASE SCORE-Berechnung V3

Ausnutzbarkeit	Stufen
Zugriff (Access Vector)	lokal (0.395) lokales Netz (0.646) Internet (1.0)
Schwierigkeit (Access Complex.)	hoch (0.35) mittel (0.61) gering (0.71)
Anmeldung (Authentication)	mehrfach (0.45) einfach (0.56) ohne (0.704)

Auswirkung	Stufen
Vertraulichkeit (Confidentiality)	keine (0.0) teilweise (0.275) vollständig (0.660)
Integrität (Integrity)	keine (0.0) teilweise (0.275) vollständig (0.660)
Verfügbarkeit (Availablility)	keine (0.0) teilweise (0.275) vollständig (0.660)

Quelle: Prof. Bodach. Modul: Abwehr von IT-Angriffen

[12] *Prof. Bodach. Modul: Abwehr von IT-Angriffen*

Tabelle 9: NAGIOS Report

Showing 1-15 of 44 total records | Page 1 of 3 | 15 Per Page | Go | Search...

Host	Service	Status	Duration	Attempt	Last Check	Status Information
192.168.178.11	FTP	Critical	1h 15m 40s	5/5	2022-12-06 13:30:49	CRITICAL - Socket timeout
	HTTP	Warning	4m 2s	5/5	2022-12-06 13:31:30	HTTP WARNING: HTTP/1.1 403 Forbidden - 129 bytes in 0.001 seco response time
	IMAP	Critical	1h 14m 20s	5/5	2022-12-06 13:32:11	CRITICAL - Socket timeout
	POP	Critical	1h 13m 46s	5/5	2022-12-06 13:32:52	CRITICAL - Socket timeout
	Ping	Ok	1h 25m 4s	1/5	2022-12-06 13:33:33	OK - 192.168.178.11 rta 0.123ms lost 0%
	SMTP	Ok	1h 17m 32s	1/5	2022-12-06 13:34:14	SMTP OK - 0.002 sec. response time
	SSH	Critical	1h 12m 19s	5/5	2022-12-06 13:34:44	CRITICAL - Socket timeout

NAGIOS Report. Quelle: Eigene Quelle

Anhand des CVSS-Scores der gefundenen Schwachstellen erfolgt eine Priorisierung. So sollen sinnvolle Konfigurationsmöglichkeiten geschaffen werden, die die Verwaltung der Werte pro System unterschiedlich festlegen können, da die einzelnen Systeme eine unterschiedliche Wichtigkeit für ein Unternehmen haben.

3 Praktische Umsetzung

3.1 VMware ESXi

Für die Installation von VMware ESXi wird ein USB-Stick benötigt, auf welchem die IOS-Datei gespeichert wird. Während der Installation werden die Zugangsdaten für Supernutzer (Root) eingegeben. Vom Festplattenspeicher werden weniger als 200 MB belegt. Nach diesem Schritt sind sämtliche Netzwerkeinstellungen und Konfigurationen vom Hypervisor über direkten Zugriff steuerbar, wie in Abbildung 22 zu sehen ist. Über die Web-Oberfläche sind Fernzugriffe von einem Endgerät möglich, das einen Webbrowser hat und sich im gleichen Netzwerk befindet. Durch die Anwendung vCenter Server ist die Verwaltung von ESXi Host möglich.

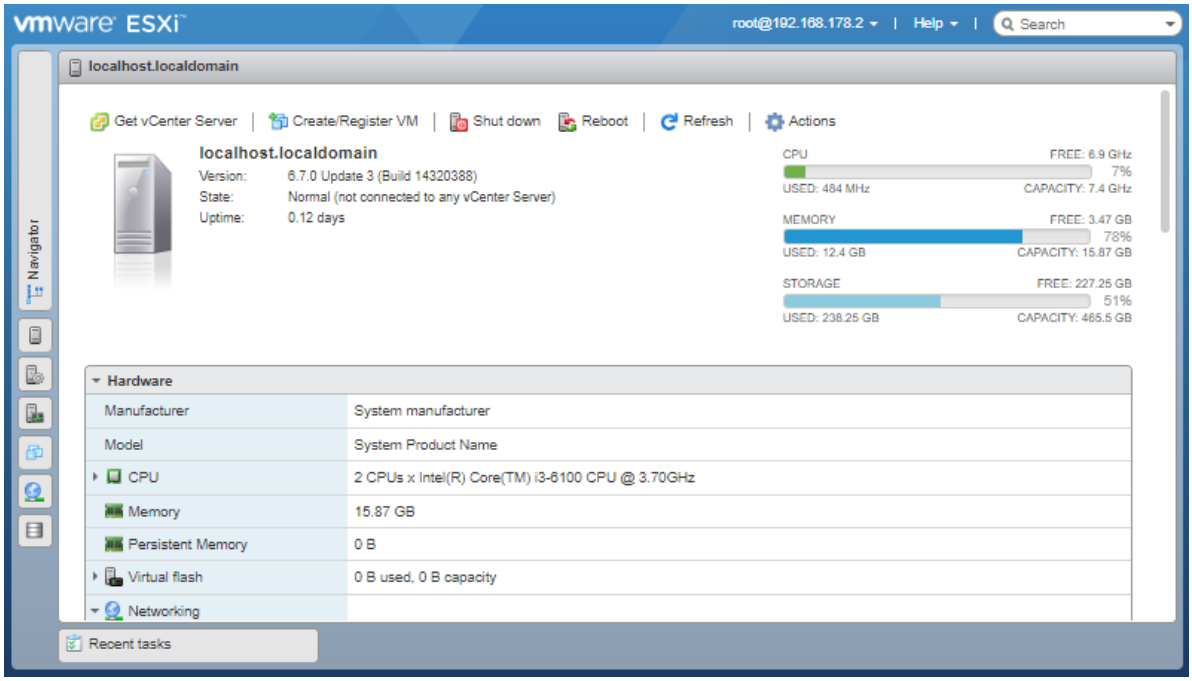


Abbildung 22: ESXi Web-oberfläche

Quelle: Eigene Abbildung

3.1.1 Vorbereitung des Windows Servers 2019 und Domänendiensten

Eine VM wird für Domaincontroller eingerichtet, welche auf dem Windows Server 2019 laufen muss. Der implementierte Verzeichnisdienst (engl. Active Directory) wird mithilfe des Windows Server Manger installiert, wie es in Abbildung 23 zu betrachten ist. Auf dem Server-Dashboard können Einstellungen bezüglich des Microsoft-Servers und dessen Eigenschaften konfiguriert werden. Diesem Server werden DC-Server, ein abgekürzter Name und eine IP-Adresse zugewiesen. Der Name des Domänencontrollers muss erkennbar sein. Anschließend wird der Domänenname eingegeben, zu welcher

der Server gehören muss. In der Systemverwaltung werden die TCP/IPv4-Einstellung ausgesucht und angepasst. Beim Einrichten eines DC-Servers, welche über eine lokale IP-Adresse verfügen sollte, muss zusätzlich der DNS-Serverdienst installiert werden. Nach erfolgter Installation müssen die Voraussetzungen für den Domänencontroller erfüllt und ein DNS-Dienst installiert werden, wie anhand Abbildung 24 zu sehen ist.

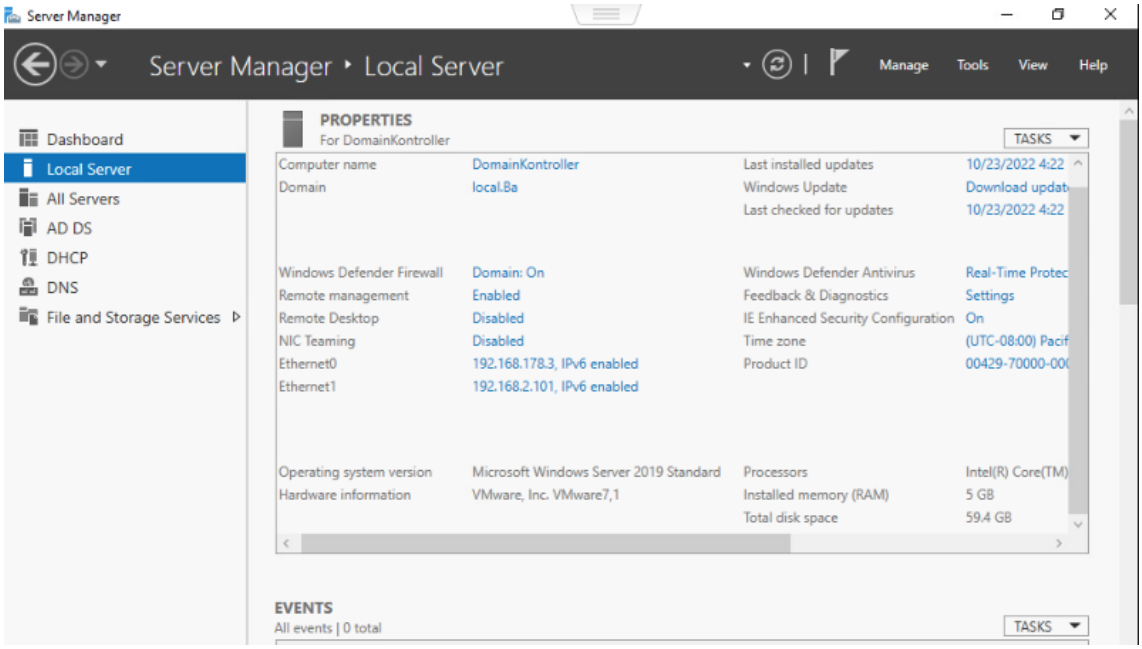
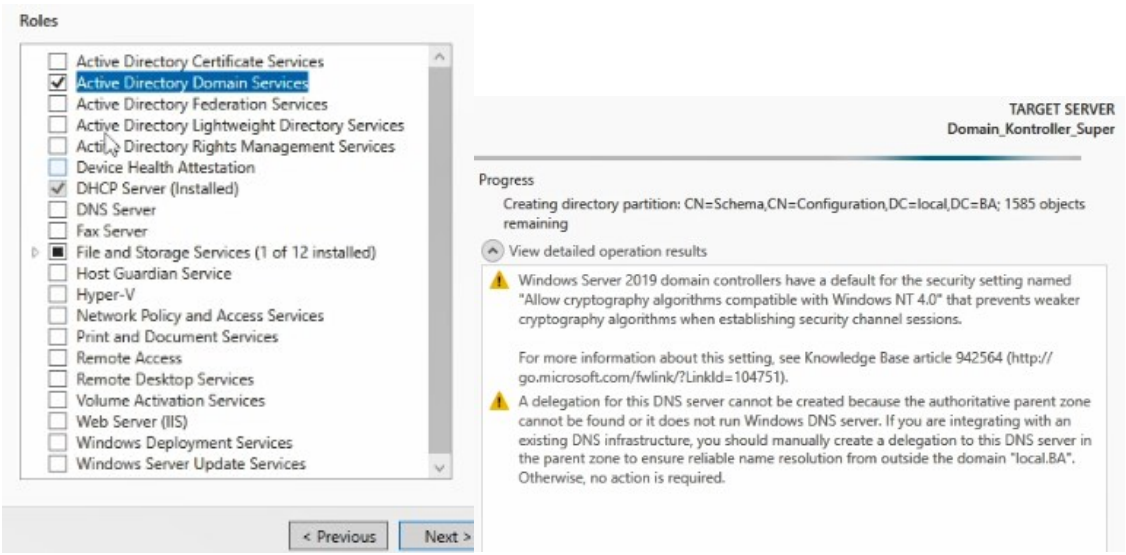


Abbildung 23: Server-Manager in Windows Server 2019

Quelle: Eigene Abbildung

Die Features, welche zu den gewählten Serverrollen gehören, werden dann automatisch hinzugefügt. Damit werden die notwendigen Komponenten für ein Active Directory und einen DNS-Server installiert.



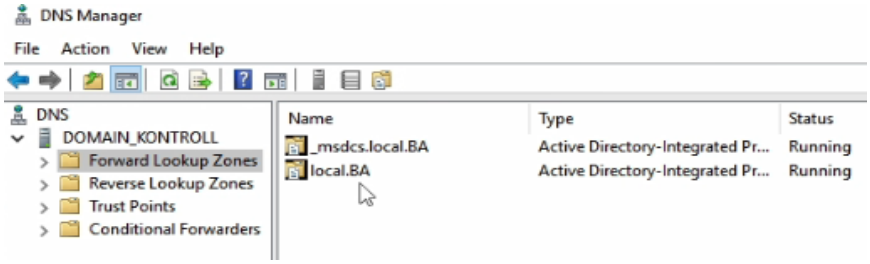


Abbildung 24: Auswahl der Serverrollen

Quelle: Eigene Abbildung

3.1.2 Vorbereitung der DHCP-Rolle

Nach der Installation einer Domain startet der Server automatisch neu. Im Anschluss ist die Rolle DHCP zu installieren. Innerhalb dieses Dienstes werden IP-Pools für dessen Netzwerk definiert, damit die Konfigurationen durch den Klienten bzw. das Endgerät erfolgen kann und diese die neue IP-Adresse automatisch erhalten können. Hierbei muss darauf geachtet werden, dass bestimmte IP-Adressen nicht in einem Pool definiert werden, um IP-Konflikte zu vermeiden. IP-Konflikten können zu einem Verlust der angebotenen Dienste aufgrund von nicht mehr erreichbaren Servern führen.

3.2 Installation des Microsoft Exchange Server

Für die Installation von Exchange Server 2019 wird ein Windows Server 2019 benötigt. Dem Exchange Server muss ein Name sowie eine feste IP-Adresse zugewiesen werden. Dieser muss den Domänencontroller erreichen, damit der MS Exchange Server der Domain beitreten kann. Nach einem Neustart des Servers ist dieses automatische Mitglied der erstellten Domäne. Dies kann auch im Domänencontroller überprüft werden, indem in den AD DS das Fenster „Active Directory Users und Computers“ geöffnet wird. Im Unterordner „Computers“ sind alle VMs zu sehen, die im Active Directory eingebunden sind. In diesem Fenster müssen dem Exchange Server VM-Mitgliedschaften für die Gruppen „Organisations-Admins“, „Schema-Admins“ und „Organisation“ zugeteilt werden. Diese Gruppenzuweisung gibt dem Exchange Server die erforderlichen Rechte, die zur Installation des Exchange Servers benötigt werden. Das Nutzerkonto, welches den Exchange Server verwalten soll, muss die Rechte von „Domänen-Admins“ der Exchange-Gruppe haben.

Nach einem Neustart von Exchange Server ist es nun möglich, sich mit dem Nutzernamen „Domänenname\Exchange Admin Name“ anzumelden. Damit Exchange Server installiert werden kann, wird zunächst Visual C++ 2013 benötigt. Außerdem muss (.NET) Framework 4.8 oder höher installiert sein. Diese Software ist kostenlos erhältlich. Des Weiteren wird Unified Communications Managed API 4.0 (UCMA 4) benötigt, was in der Exchange ISO inbegriffen ist. Diese ISO-Datei muss auf das Laufwerk in ESXi hochgeladen und in das CD/DVD Laufwerk eingebunden werden oder von einem

für ISO-Dateien formatierten USB-Stick kopiert werden. Bevor die Installation von Exchange beginnt, muss das Active Directory für die Installation vorbereitet werden. Dafür muss die Windows-PowerShell als Administrator geöffnet werden. Folgende Befehle sind auszuführen:

Install-WindowsFeature RSAT-ADDS

Um Exchange erfolgreich einrichten zu können, müssen vorher die Remote Server Administration Tools (RSAT) für Active Directory Domänendienste installiert werden.

.*Setup.exe/IAcceptExchangeServerLicenseTerms/PrepareSchema* – mit diesem Befehl wird das Active Directory Schema für Exchange Server erweitert.
.*Setup.exe/IAcceptExchangeServerLicenseTerms/PrepareAD/OrganizatioName:"First-Organisation"* – dieser Befehl bereitet das Active Directory vor. Mit der Neuinstallation von Exchange Server wird eine neue Exchange-Organisation gegründet, der ein Name zugewiesen werden muss. In diesem Beispiel heißt die Exchange Organisation „First Organisation". Nachdem die Einführung und die Lizenzbedingungen akzeptiert wurden, muss mit der Konfiguration fortgefahren werden. Es folgt die Installation der Postfachrolle sowie der erforderlichen Server-Rollen und -Features. Weiterhin kann entschieden werden, ob der integrierte Schutz vor Schadsoftware aktiviert werden soll. Diese sollte zunächst aktiviert bleiben. Nach einer erfolgreichen Bereitstellungsüberprüfung kann Exchange Server installiert werden.

Die Konfiguration des Exchange Servers wird über das Exchange Admin Center (EAC) vorgenommen, welches in Abbildung 25 zu sehen ist. EAC ist eine browserbasierte Verwaltungskonsole. Zunächst ist eine Anmeldung nur über den Administrator im EAC möglich. Da der zusätzliche Exchange Administrator, der den Mailserver verwalten soll, noch keine Rechte dafür hat, müssen unter dem Reiter „Berechtigungen" die Administratorrollen angepasst werden. Da sich der Exchange Admin um alle Dienste kümmern soll, die mit dem Mailserver zu tun haben, sollten alle Administratorrollen dem Exchange Administratoren zugewiesen werden. Im Anschluss sollte in den Einstellungen der Lizenzschlüssel eingegeben werden, um die Installation zu validieren. In dem Unterpunkt „Akzeptierte Domänen" im Reiter „Nachrichtenfluss" kann die Domäne hinzugefügt werden. Unter „E-Mail-Adressrichtlinie" muss definiert werden, wie die E-Mail-Adressen der Nutzer aufgebaut sind. Beispielsweise kann mit der Bezeichnung Alias, welcher dem Nutzernamen entspricht, die E-Mail-Adressrichtlinie „Alias@Domainname" sein. Eine weitere nützliche Maßnahme ist es, die Exchange Datenbank umzubenennen und ihren Speicherort festzulegen. Dies kann unter „Server" im Reiter „Datenbanken" vorgenommen werden. Es wird ein digitales Zertifikat, um sichere Kommunikation und eine zuverlässige Verbindung zwischen Exchange Servern zu gewährleisten, erstellt werden. Digitale Zertifikate[13] dienen dazu, die Identität eines Benutzers

[13] https://learn.microsoft.com/de-de/exchange/architecture/client-access/certificates?view=exchserver-2019

oder eines Computers zu überprüfen, damit eine verschlüsselte und vertrauenswürdige Verbindung zwischen zwei Kommunikationspartnern entstehen kann. Es gibt mehrere Möglichkeiten, ein Zertifikat zu erstellen. Zum einen kann ein Zertifikat intern erstellt und selbst signiert werden. Dies bringt einen hohen Administrationsaufwand beim Hinzufügen des Zertifikats mit sich. Wenn die Domains aus zwei Unternehmen verbunden sind, könnte auch mit den Active Directory Zertifikatdiensten in der Firma ein Zertifikat ausgestellt werden. Außerdem können digitale Zertifikate auch durch Drittanbieter erstellt und erworben werden (© MICROSOFT 2022).

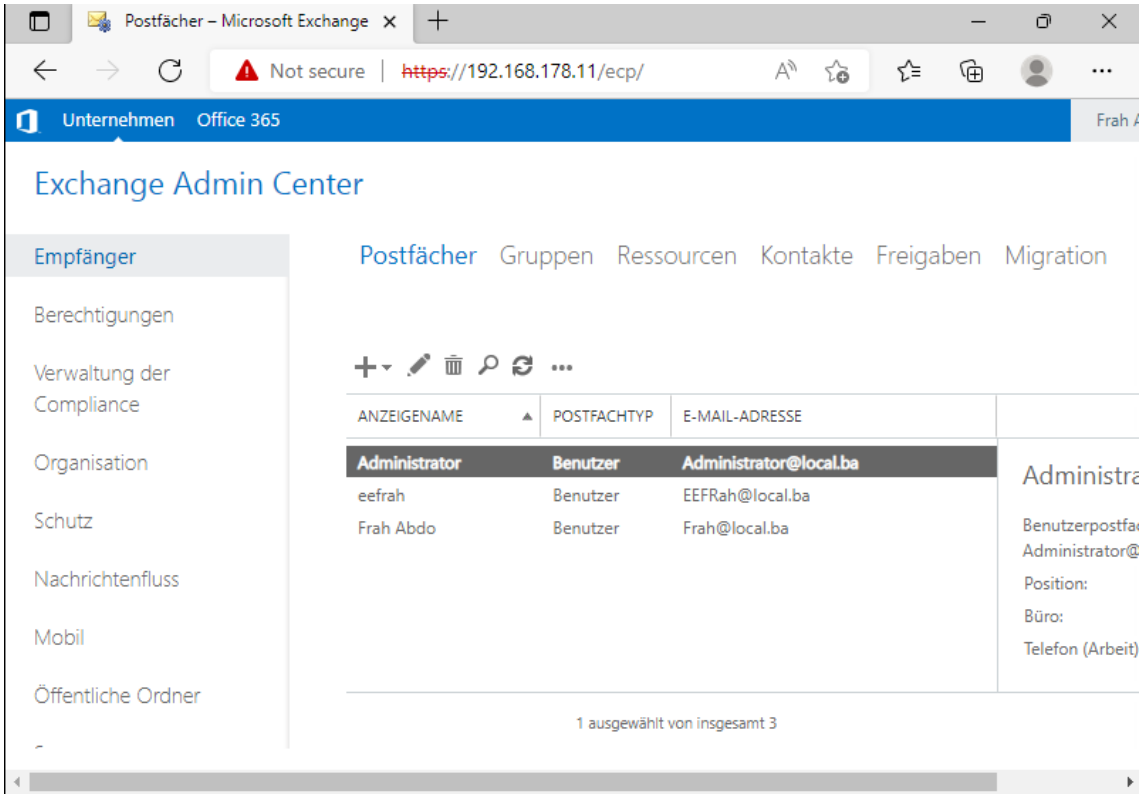


Abbildung 25: Exchange EAC-weboberfläche

Exchange 2019 Admin Center (EAC) nach einer Neuinstallation Quelle: Eigene Abbildung

3.3 Vorbereitung von Windows-Client

Der Windows-Client wird mit dem Betriebssystem Windows 10 Pro arbeiten. Die ersten Schritte nach der Installation von Betriebssysteme BSe sind wieder die Zuweisung der Computernamen und die Vergabe von IP-Adressen (IP-Adresse erhältlich vom DHCP-Server). Außerdem müssen die BSe der Active Directory Domäne hinzugefügt werden. Damit sind die BSe automatisch im Active Directory eingebunden. Im Domänencontroller müssen die Nutzer-Accounts erstellt werden. In der „Active Directory-Benutzer und -Computer-Übersicht“ müssen dafür im Ordner „Users“ neue Accounts erstellt werden. Es werden nur ein vollständiger Name und ein Benutzeranmeldename benötigt. Weiterhin müssen die Klienten in den Exchange Server eingebunden werden. Dazu

müssen im Exchange Server neue Exchange-Postfächer erstellt werden, welche den Active Directory-Konten zugeordnet werden. Über das Active Directory-Konto kann der Nutzer E-Mails verschicken und empfangen. Der Vorgang der Erstellung eines Postfaches für ein bereits existierendes Active Directory-Konto wird Postfachaktivierung genannt. Unter dem Reiter „Empfänger“ im EAC können neue Benutzerpostfächer angelegt werden.

3.4 Einrichten von VPN

Die folgende Darstellung zeigt die Erstellung einer Gruppe nutzungsberechtigter Personen von VPN (siehe Abbildung 26).

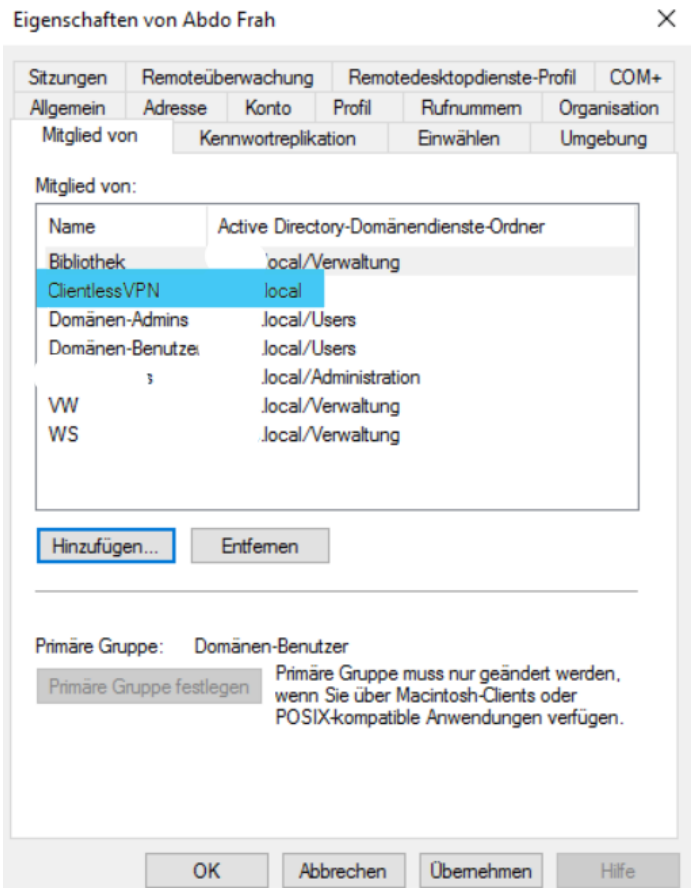


Abbildung 26: VPN-Gruppe

Quelle: Eigene Quelle

Um eine VPN-Nutzungsberechtigung in der Gruppe zu erhalten, muss auf dem Securepoint-Server bzw. der Firewall die dazugehörige Berechtigung eingeben werden. Diese steht in Zusammenhang mit Active Directory AD (siehe Abbildung 27).

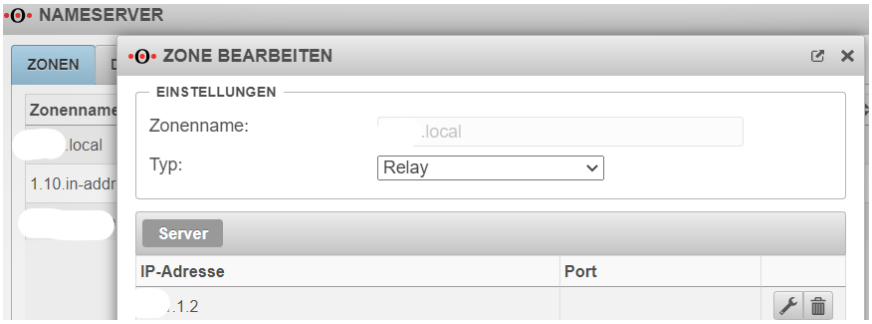


Abbildung 27: VPN-Gruppe mit AD verbinden

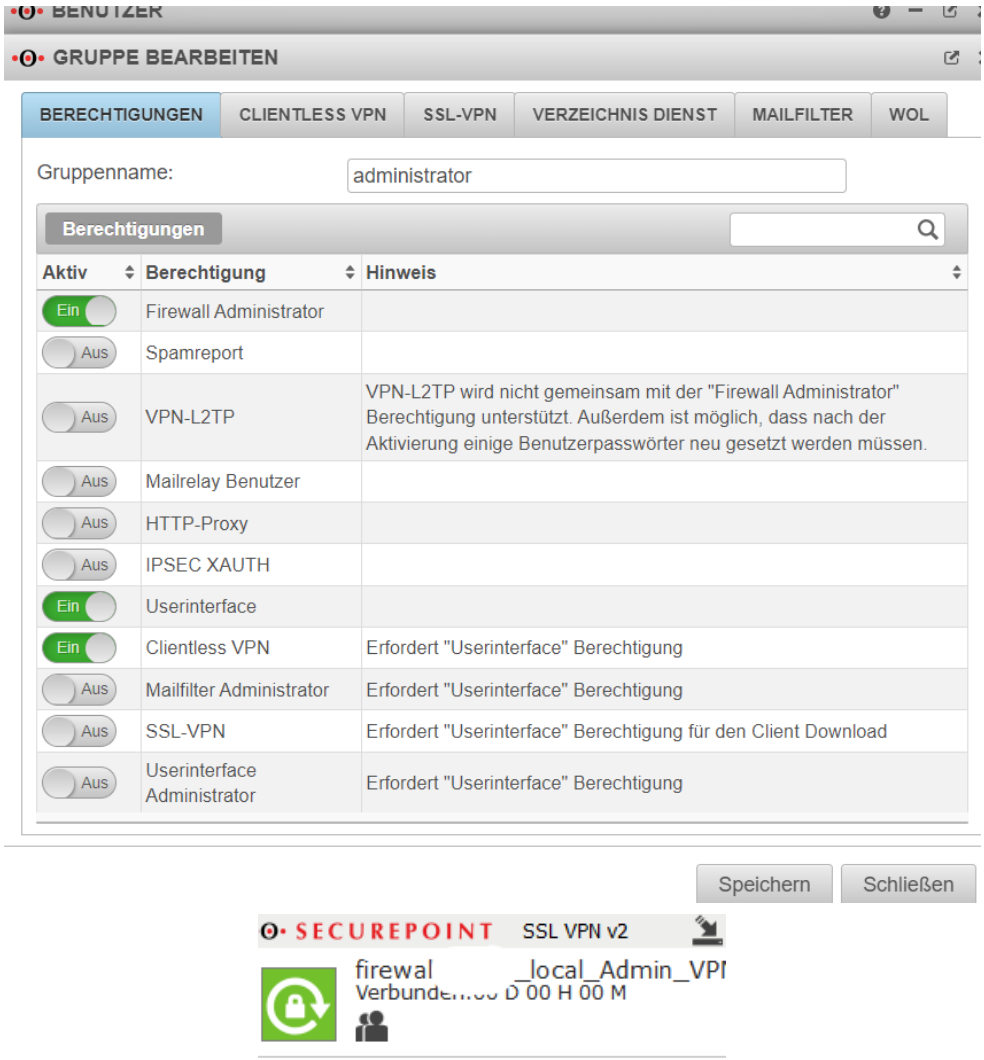


Abbildung 28: VPN-Zustand

Diese Verbindung gewährleistet eine Kommunikationsverbindung im Grid-System zwischen dem Exchange Server eines Unternehmens mit dem Exchange Server seines Tochterunternehmens, da die Domain einer Seite (von zuhause) nicht in öffentlichen-Root-DNS registriert wurde.

3.5 Netzwerk-Monitoring zu Verfügung stellen

Nachdem die Umgebung vorbereitet wurde, sind anschließend die Dienste im Grid- und Cloud-Computing zu überwachen. Hierzu werden die Ereignisprotokolle der Geräte IMAP, POP3, SMTP für Mail-Verkehr und UDP, TCP für DNS sowie DHCP erfasst. Die Softwarearchitektur ist auf dem Client/Server in Form einer Client-Anwendung oder der Management-Homepage ausgerichtet. Die Software enthält zudem eine Übersicht geeigneter Werkzeuge zur Datenaufbereitung.

3.5.1 Möglichkeiten des Monitorings

Zur Anforderungsanalyse ist das Überwachen des Netzwerkes sehr komplex und kann sogar bis in das kleinste Detail geschehen. Der Abschnitt soll einige Beispiele erklären und Hinweise auf den Sinn des Einsatzes der Überwachungsmöglichkeiten bieten.

Überwachen von Diensten

Bei der Überwachung von Diensten werden die entsprechenden Ports auf Erreichbarkeit geprüft. Gibt es einen administrativen Zugriff, kann unter Umständen sogar automatisch ein Dienst neugestartet werden, um die Erreichbarkeit womöglich wiederherstellen zu können. Ein Beispiel ist ein FTP-Server, der über den Port 21 ausgeführt wird. Sobald dieser Port geschlossen bzw. nicht mehr erreichbar ist, kann eine Benachrichtigung an einen Administrator ausgegeben oder ein automatischer Neustart des FTP-Servers ausgelöst werden.

Überwachen von Datenbanken

Die Überwachung von Datenbanken geschieht in erster Linie ähnlich dem Prinzip zur Überwachung von Diensten. Einige Softwarehersteller bieten aber eine detailliertere Möglichkeit des Monitorings. Hierbei wird ebenfalls ein administrativer Zugang geschaffen, um auf die Management-Applikation des Datenbankservers zuzugreifen und weitere Informationen zu beschaffen. Darunter können z. B. Informationen über die Speicherauslastung der Datenbank oder Performance-Werte sein.

Überwachen von aktiven Netzwerkkomponenten

Aktive Netzwerkkomponenten sind in der Lage, bei Auftreten eines Fehlers selbst Nachrichten, sogenannte Traps, abzuschicken. Werden diese von einer Station richtig ausgewertet, erhält der Administrator sofort eine Information zur Ursache des Problems. Eine weitere Möglichkeit des Monitorings ist das intervallmäßige Pingen der Komponenten, um die Erreichbarkeit zu überwachen.

Überwachen von Ordnern

In manchen Fällen erweist sich eine Überwachung von Ordnern als notwendig. Dabei wird regelmäßig geprüft, ob eine Veränderung in dem entsprechenden Ordner auftritt. Dies kann z. B. eine durch einen Virus gelöschte Datei sein. Ein weiterer Anwendungsbereich ist die Sicherstellung der Verfügbarkeit von Netzlaufwerken.

Überwachen der Ressourcenauslastung

Ein Server oder eine Datenbank ist bei erhöhter Auslastung im Regelfall zwar erreichbar, aber sehr langsam. Um solche Probleme sofort beim Auftreten zu erkennen, können die Prozessorauslastung, die Auslastung des Arbeitsspeichers oder die Auslastung der Festplattenkapazität überwacht werden, um gegebenenfalls weitere Schritte einzuleiten.

4 Evaluation

Zur Betrachtung ein Szenario.

Ein Auftraggeber möchte in seinem Unternehmen das System für Exchange Server auf 2019 umstellen. Neben der geplanten Aktualisierung soll auch die kritische Infrastruktur bis zu einem ausgewählten Zeitpunkt realisiert werden. Geplant ist die Aktualisierung der gesamten Serverinfrastruktur inklusive Hardware-Austausch, Migration auf Exchange Server 2019 und Aufbau eines Failover-Systems.

4.1 Cloud-Governance

4.1.1 Planung

Das Projekt für Arbeitgeber umfasst folgende Punkte:

1. Umzug bestehender Services in ein neues Cloud-Computing-System
2. Aktualisierung der kompletten Server und Netzwerk Hardware
3. Konfiguration eines neuen Hypervisors mit VMware ESXi
4. Aktualisierung aller Serverbetriebssysteme auf Windows Server 2019
5. Migration der Outlook Speicherinfrastruktur auf neue Umgebung
6. Sicherstellung der Dienste

Schwachstellen in der Software bezeichnen allgemein eine Teilmenge von Bugs, also Fehler in Programmen bzw. in deren Quelltext oder Konfiguration. Ob diese Bugs jeweils Schwachstellen sind, hängt davon ab, ob sie zum einen ausgenutzt werden können und ob ihre Ausnutzung zu einem ungewollten Zustand, also der Verletzung mindestens eines der drei Schutzziele der Informationssicherheit führen kann.

4.1.2 IT -Performance-Management

Dienste befinden sich auf den Servern, die in VMware ESXi sind. Es besteht eine Gruppe für die Verwaltung der Domain und des Exchange Servers. Des Weiteren kann ein Postfach für alle Nutzer, die in der Domain registriert sind, eingerichtet werden. Die Verwaltung von IT-Ressourcen, Zugriff auf Server und die Verwendung von Tools, die für die Messung von Performance und Monitoring der Ressourcen erforderlich sind, obliegen ausschließlich der Unternehmensführung

4.1.3 Analyse der Unternehmensarchitektur

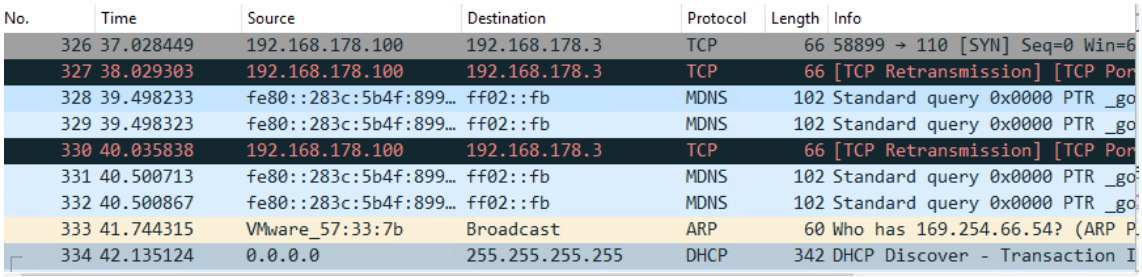
Netzwerkverkehr in Wireshark

Wireshark protokolliert den Netzwerkverkehr der Schnittstellen des Systems, auf dem es installiert ist. Es kann also alle ein- und ausgehende Verbindungen des jeweiligen Rechners untersuchen (siehe Abbildung 28). Gleichzeitig empfängt es auch alle Datenpakete, die an alle Systeme im Netzwerk gesendet werden (Broadcasts).

Tabelle 10: Wireshark Analyse

Merkmal	TCP	UDP
IP-Protokollnummer	6	17
Verbindung	Verbindungsorientiert. Aufbau einer Verbindung vor der Datenübertragung durch sog. Three-Way-Handshake, Abbau der Verbindung nach Beendigung.	Verbindungslos. UDP-Datagramme können ohne Verbindungsaufbau einfach abgeschickt werden.
Zuverlässigkeit	TCP überträgt verlorengegangene Segmente nochmals und bringt die Daten in die richtige Reihenfolge, bevor sie dem Empfänger übergeben werden. Was reingeht, kommt auch raus.	UDP-Datagramme werden bei Verlust durch UDP nicht nochmals übertragen, Datagramme werden nicht in die richtige Reihenfolge gebracht.
Schnittstelle zur Anwendung	Aus Sicht von Sender/Empfänger steht ein Bytestrom zur Verfügung. Sender kann durch den Strom beliebige Datenmengen verschicken, evtl. Segmentierung erfolgt durch das TCP-Protokoll.	Anwendung muss UDP jeweils ein Datagramm zum Senden übergeben. Maximale Kapazität festgelegt durch max. UDP-Datagrammgröße. Aufteilung größerer Datenmengen in mehrere Datagramme muss durch die Anwendung erfolgen.

Sende-/ Empfangsverhalten	Von der Anwendung an TCP übergebene Daten müssen durch das TCP-Protokoll beim Sender nicht sofort zum Empfänger geschickt werden. Wenn TCP-Segmente beim Empfänger ankommen, müssen sie nicht sofort an die empfangende Anwendung weitergegeben werden.	UDP sendet übergebenes Datagramm direkt ab und stellt empfangene Datagramme empfängerseitig sofort zur Verfügung.



No.	Time	Source	Destination	Protocol	Length	Info
326	37.028449	192.168.178.100	192.168.178.3	TCP	66	58899 → 110 [SYN] Seq=0 Win=6
327	38.029303	192.168.178.100	192.168.178.3	TCP	66	[TCP Retransmission] [TCP Por
328	39.498233	fe80::283c:5b4f:899…	ff02::fb	MDNS	102	Standard query 0x0000 PTR _go
329	39.498323	fe80::283c:5b4f:899…	ff02::fb	MDNS	102	Standard query 0x0000 PTR _go
330	40.035838	192.168.178.100	192.168.178.3	TCP	66	[TCP Retransmission] [TCP Por
331	40.500713	fe80::283c:5b4f:899…	ff02::fb	MDNS	102	Standard query 0x0000 PTR _go
332	40.500867	fe80::283c:5b4f:899…	ff02::fb	MDNS	102	Standard query 0x0000 PTR _go
333	41.744315	VMware_57:33:7b	Broadcast	ARP	60	Who has 169.254.66.54? (ARP P
334	42.135124	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction I

Abbildung 29: Netzwerkverkehr in Wireshark

Quelle: Eigene Quelle

Es wurde für die Analyse auf Wireshark Filter Funktion genutzt, um Protokoll-Pakete zu finden[14]

CVSS-Werte berechnen

HTTP

Tabelle 11: BASE SCORE-Berechnung von http Protokoll

Access Vector	LOCAL
Access Complexity	LOW
Authentication	NOT-REQUIRED
Confidentiality Impact	COMPLETE
Integrity Impact	PARTIAL
Availability Impact	COMPLETE
Impact Bias	AVAILABILITY
BASE SCORE	6,5

[14] https://www.wireshark.org/docs/dfref/

Nachfolgend sind die von NAGIOS ermittelten Werte im Zusammenhang mit dem Einrichten von geplanten Systemen für die Umstellung auf Cloud-Lösungen. Da der Wert von 6,5 lediglich ein mittleres Rating im Base Score trifft, könnte von außen auf das System zugegriffen werden und die Verbindung wäre nicht gesichert.

SMTP

Tabelle 12: BASE SCORE-Berechnung von SMTP Protokoll

Access Vector	LOCAL
Access Complexity	HIGH
Authentication	REQUIRED
Confidentiality Impact	COMPLETE
Integrity Impact	COMPLETE
Availability Impact	COMPLETE
Impact Bias	AVAILABILITY
BASE SCORE	3,4

Der Wert des SMTP-Protokolls ergibt ein LOW-Rating. Das System unterstützt die Kommunikationen, die SMTP durchführt und läuft somit auf sicherer Ebene.

POP3

Tabelle 13: BASE SCORE-Berechnung von POP3 Protokoll

Access Vector	LOCAL
Access Complexity	LOW
Authentication	REQUIRED
Confidentiality Impact	COMPLETE
Integrity Impact	COMPLETE
Availability Impact	COMPLETE
Impact Bias	AVAILABILITY
BASE SCORE	4,2

Ein weiteres Protokoll, das für den E-Mail-Service notwendig ist, trifft einen Wert von 4,2. Dieser ist in Medium-Bereich der Sicherheit bezüglich gezielter Systeme.

IMAP

Tabelle 14: BASE SCORE-Berechnung von IMAP Protokoll

Access Vector	LOCAL
Access Complexity	LOW

Authentication	REQUIRED
Confidentiality Impact	COMPLETE
Integrity Impact	COMPLETE
Availability Impact	COMPLETE
Impact Bias	AVAILABILITY
BASE SCORE	4,2

Für E-Mail-Services ist das IMAP-Protokoll zu nutzen. Sein Wert von 4,2 befindet sich im Medium-Bereich bezüglich der Sicherheitskriterien für gezielte Systeme.

TCP

Tabelle 15: BASE SCOR-Berechnung von TCP Protokoll

Access Vector	LOCAL
Access Complexity	HIGH
Authentication	REQUIRED
Confidentiality Impact	COMPLETE
Integrity Impact	COMPLETE
Availability Impact	COMPLETE
Impact Bias	AVAILABILITY
BASE SCORE	3,4

Um die Kommunikationen zwischen zwei Endgeräten im Netzwerk zu gewährleisten, wird das TCP-Protokoll benötigt. Dieses basiert auf Porten, welche vom Betriebssystem überwacht werden. Es wurde in dieser Arbeit Standard-Port überwacht.

UDP

Tabelle 16: BASE SCORE-Berechnung von UDP Protokoll

Access Vector	LOCAL
Access Complexity	LOW
Authentication	REQUIRED
Confidentiality Impact	NONE
Integrity Impact	NONE
Availability Impact	PARTIAL
Impact Bias	NORMAL
BASE SCORE	1,0

Das UDP-Protokoll läuft während der Umstellung auf sicherer Ebene. Daher besteht keine Gefahr während seines Einsatzes im Cloud-Computing-Projekt.

4.1.4 Evaluieren

Die ermittelten Werte sind vom Autor nach der projektbezogenen Technikinstallation in die entsprechenden Systeme eingetragen worden. Anschließend wurde die Domain inklusive der benötigten Rollen bzw. Dienste auf dem Windows-Server installiert. Der Mailserver, der für E-Mail-Services zuständig ist, wurde ebenfalls vorbreitet. Die am Monitoring beteiligten NAGIOS-Systeme wurden auf einer VM eingerichtet. Durch Aufruf der NAGIOS-Seite wurden dem Autor die ermittelten Werte für die Berechnung des Base Score, die im jeweiligen Protokoll präsentiert wurden, angezeigt. Des Weiteren wurde beim Versenden einer E-Mail die Kommunikation zwischen Absender-, Empfängersystem und Exchange Server auf Wireshark und NAGIOS überwacht.

SMTP, HTTP, TCP, UDP, IMAP und POP3 sind Protokolle, zu welchen jeweils ein Port für die Kommunikation im Netzwerk von iana[15] (IANA.ORG) definiert wird. Dienste wie HTTP können durch Port 80, FTP durch Port 21 und SMTP durch Port 25 zusammen mit den IP-Adressen des Clients und des Servers Verbindungen im gesamten Netzwerk identifizieren. Definierte Ports beinhalten Ports für Anwendungen. Hier wurde festgestellt, dass Angriffe auf die Dienste möglich sind, was zu einer Bedrohung der Netzwerksicherheit durch bewusstes Einwirken einer Person auf das Netz führen könnte. Als Angreifer wird nachfolgend eine Person bezeichnet, die versucht, das Netzwerk anzugreifen und zu manipulieren. Der interne Angreifer oder Innentäter ist eine Person, die rechtmäßiger Teil des Netzwerks ist bzw. rechtmäßigerweise Zugang zu den Systemen besitzt. Ein interner Angreifer könnte beispielsweise ein frustrierter oder gekündigter Mitarbeiter sein, der dem Unternehmen Schaden zufügen oder sich selbst bereichern möchte. Durch seine Position verfügt der interne Angreifer bereits über

[15] http://www.iana.org/

Zugang zu Endgeräten und somit auch zum Netzwerk. Möglicherweise verfügt er ebenfalls über (physikalischen) Zugang zu Teilen der Netzwerkinfrastruktur. So kann der Angreifer direkt, mittels manipulierter Pakete, Einfluss auf das Netzwerk nehmen und muss dabei in vielen Fällen keine weiteren Schutzmaßnahmen überwinden. Besonders wegen des oft weitreichenden Zugriffs und der fehlenden Schutzmaßnahmen geht von dieser Art des Angreifers in vielen Fällen eine große Gefahr aus. Dadurch, dass der Zugang zum Netz grundlegend ständig erlaubt ist, können dauerhafte oder wiederkehrende Angriffe ohne großes Aufsehen durchgeführt werden. So wird das Schadenspotential weiter erhöht. Es existieren verschiedene Angriffe auf lokale Netzwerke, die eine schwerwiegende Beeinträchtigungen der Schutzziele zur Folge haben können. Eine andere Lösung ist mindestens genau so effektiv wie die Beseitigung von Schwachstellen auf Computersystemen sein kann, ist die Prävention von Schwachstellen. Ein entscheidender Vorteil der Miteinbeziehung diese Lösung ist, dass Schwachstellen im Idealfall durch geeignete organisatorische sowie technische präventive Maßnahmen überhaupt nicht entstehen und die Gefahr einer Ausnutzung minimal gehalten wird.

Auf der Virtualisierungebene wurde eine gelegte Log-Datei in ESXi herausgezogen, um die getroffenen Verletzungen in VMs zu finden. Es wurde keine Verletzungen im ESXi System getroffen. Dies kann in Unternehmen der Fall sein, wenn die Kommunikation mit dem Hypervisor nicht geschützt oder durch unautorisierte VM betrieben sind.

4.2 Grid-Governance

4.2.1 Planung

Das Projekt für Arbeitgeber umfasst folgende Punkte:

1. Anpassung bestehender Services bzw. Dienste in Grid-Computing-System
2. Aktualisierung der kompletten Server- und Netzwerk-Hardware
3. Konfiguration einer sicheren Kommunikationsverbindung bzw. VPN zwischen den Servern
4. Aktualisierung aller Serverbetriebssysteme auf Windows Server 2019
5. Migration der Outlook-Speicherinfrastruktur auf neue Umgebung
6. Sicherstellung der Dienste

Schwachstellen im Einsatz von VPN-Verbindung bringen Bedrohungen für die IT mit sich, wenn sie von Unbefugten ausgenutzt werden. Durch das Festlegen geeigneter Maßnahmen kann eine Verletzung der Informationssicherheit verhindert und ein gezielter Sicherheitsschutz gewährleistet werden.

4.2.2 IT -Performance-Management

Dienste befinden sich auf den Servern, die geografisch verteilt sind. Für die VPN-Nutzung wurde eine autorisierte Gruppe erstellt. Die kontinuierliche Verwaltung dieser Gruppe ist aufwändig. Das Weiteren muss für die Verwaltung der Domains eine Administrationsgruppe erschaffen werden, in welcher die IT-Ressourcen aller beteiligten Unternehmen verwaltet werden. Hierbei ist es möglich, dass Angreifer Zugriff auf ein Objekt erhalten, beispielsweise auf DNS-Server. DNS-Antworten werden verfälscht und die Anfrage so auf ein anderes Ziel umgeleitet. DNS verwendet TCP für die Zonenübertragung und UDP für den Namen. Hierbei fragt es entweder normal (primär) oder umgekehrt ab (MANDL, 2018). Zur Prävention gegen eine Bedrohung auf den Server muss stets sichergestellt sein, dass der Zugriff auf diesen Dienst restriktiv gestaltet ist. Dadurch wird es Angreifern erschwert, an Objekten dieses Namespaces Änderungen vorzunehmen.

4.2.3 Analyse der Unternehmensarchitektur

CVSS-Werte

HTTP

In der unteren Tabelle sind die ermittelten Werte vom Einsatz des HTTP-Webdienstes in Grid-Computing-Umgebung dargestellt.

Tabelle 17: BASE SCORE-Berechnung von http Protokoll

Access Vector	REMOTE
Access Complexity	HIGH
Authentication	REQUIRED
Confidentiality Impact	COMPLETE
Integrity Impact	PARTIAL
Availability Impact	PARTIAL
Impact Bias	AVAILABILITY
BASE SCORE	**3,7**

SMTP

Untenstehende Tabelle zeigt die ermittelten Werte vom Einsatz des SMTP- Maildienstes in Grid-Computing-Umgebung.

Tabelle 18: BASE SCORE-Berechnung von SMTP Protokoll

Access Vector	REMOTE
Access Complexity	HIGH
Authentication	REQUIRED
Confidentiality Impact	COMPLETE
Integrity Impact	COMPLETE
Availability Impact	COMPLETE
Impact Bias	INTEGRITY
BASE SCORE	**4,8**

POP3

Nachfolgend die Tabelle der ermittelten Werte vom Einsatz des POP3-Protokolls für Maildienste in Grid-Computing-Umgebung.

Tabelle 19: BASE SCORE-Berechnung von POP3 Protokoll

Access Vector	REMOTE
Access Complexity	LOW
Authentication	REQUIRED
Confidentiality Impact	COMPLETE
Integrity Impact	COMPLETE
Availability Impact	PARTIAL
Impact Bias	NORMAL
BASE SCORE	**5,4**

IMAP

Zu betrachten sind nachfolgend die ermittelten Werte vom Einsatz des IMAP im Maildienst in Grid-Computing-Umgebung.

Tabelle 20: BASE SCORE-Berechnung von IMAP Protokoll

Access Vector	REMOTE
Access Complexity	LOW
Authentication	REQUIRED
Confidentiality Impact	COMPLETE
Integrity Impact	COMPLETE
Availability Impact	PARTIAL
Impact Bias	INTEGRITY
BASE SCORE	**5,6**

TCP

Die untere Tabelle demonstriert die ermittelten Werte vom Einsatz des TCP-Protokolls in Grid-Computing-Umgebung.

Tabelle 21: BASE SCORE-Berechnung von TCP Protokoll

Access Vector	REMOTE
Access Complexity	HIGH
Authentication	REQUIRED
Confidentiality Impact	COMPLETE
Integrity Impact	COMPLETE
Availability Impact	PARTIAL
Impact Bias	INTEGRITY
BASE SCORE	**4,4**

UDP

Die ermittelten Werte vom Einsatz des UDP-Protokolls in Grid-Computing-Umgebung stehen sind anhand der nachfolgenden Tabelle zu sehen.

Tabelle 22: BASE SCORE-Berechnung von UPD Protokoll

Access Vector	REMOTE
Access Complexity	LOW
Authentication	REQUIRED
Confidentiality Impact	NONE
Integrity Impact	NONE
Availability Impact	PARTIAL
Impact Bias	NORMAL
BASE SCORE	**1,4**

4.2.4 Evaluieren

Für die Weiterführung seines Projekts hat der Autor in Grid-Computing die geographisch verteilte Technik-Umgebung eingerichtet. Ohne VM ist die Vorbereitung aufwendig. Zuerst wird die Domain sowie deren notwendige Rollen bzw. Dienste auf dem Windows-Server installiert, gefolgt von der Einrichtung des Domain-Controllers und DNS-Servers auf einem Server. Auch der Mailserver wurde einem Server zugewiesen, um dessen Funktionalität zu gewährleisten. Die VPN-Verbindung wurde dabei von Securepoint übernommen. Die ermittelten Werte nutzt der Autor nach der Technikinstallation für sein Projekt. Der für den E-Mailservice zuständige Mailserver wurde ebenfalls vorbreitet. Es sollte für Monitoring die Betriebssysteme einen NAGIOS Server vorbereit und die Verbindung mit ihm versorgt. Durch Aufruf der NAGIOS Seite erhielt der Autor die für den Base Score ermittelten Werte, die im jeweiligen Protokoll präsentiert wurden. Die Überwachung der Kommunikation zwischen Absender, Empfängersystem und Exchange Server erfolgte auf Wireshark und NAGIOS während des Versendens einer E-Mail. Getroffene Protokolle in dieser Analyse sind SMTP, HTTP, TCP, UDP, IMAP sowie POP3. Der Webdienst von HTTP-Protokoll durch Port 80 hat den Wert von 3,7 getroffen, da die Verbindung zwischen den beteiligten Komponenten durch eine sicheren VPN-Kanal hergestellt wurde. Der Autor hat alle betroffenen Ports für seine Studie betrachtet und dabei festgestellt, dass die Sicherheit der Kommunikation der Komponenten des Proxy-System durch den Einsatz von sicheren Verschlüsselungsalgorithmen erreicht wird. Die eingesetzten Algorithmen werden vom BSI empfohlen und gelten aktuell als sicher. Um Fehler zu vermeiden, wurden die eingesetzten Verschlüsselungsalgorithmen nicht selbst implementiert. Ein externer Angreifer besitzt in der Regel keinen rechtmäßigen Zugriff auf das lokale Netzwerk. Es könnte sich beispielsweise um einen Konkurrenten mit Absicht der Industriespionage oder Sabotage handeln. Um in dem internen Netzwerk operieren zu können, muss hier zuerst

die Perimetersicherung überwunden werden. Dazu kann versucht werden, interne Endgeräte beispielsweise mittels Phishings zu kompromittieren und so eine Möglichkeit zum Zugriff auf das interne Netz zu erhalten. Alternativ wird direkt von außen versucht, den Perimeterschutz zu überwinden und so ins Netzwerk einzudringen. Ist das erste System im internen Netz unter der Kontrolle des Angreifers, kann er dieses dazu nutzen, um weitere Angriffe auf das LAN durchzuführen. Externe Angriffe können durch die Umsetzung einer guten Perimeter-sicherheit wesentlich erschwert werden. Außerdem erregen sie, im Gegensatz zu internen Angriffen, eher Aufmerksamkeit, da eine Kommunikation zum Angreifer über die Perimetergrenze hinweg erfolgen muss. Oft werden beispielsweise Network Intrusion Detection Systeme (NIDS) eingesetzt, die zumindest einen Teil solcher Angriffe erkennen können.

4.3 Fazit

Anhand dieser Auswertung ergeben sich folgende Anforderungen an einen Prototyp: Nachdem auf den Servern das Betriebssystem Windows Server 2019 installiert wurde, können die Ressourcen anschließend dynamisch und flexibel erweitert werden. Es ist notwendig, dass eine Verbindung zwischen den Exchange Servern, die geografisch verteilt sind, zustande kommt. Hierbei ist relevant, ob dies über VPN oder einen anderen Weg geschieht. Um die Sicherheit der Daten zu gewährleisten, werden unter den gegebenen Voraussetzungen potenzielle Ausweichmöglichkeiten für die eingesetzte Hardware betrachtet und ausgewertet. Die zukünftige Anwendbarkeit der Soft- bzw. Hardware wird auf ihre Zuverlässigkeit und die weitere Verfügbarkeit von benötigtem Support untersucht. Darüber hinaus wurde analysiert, inwieweit Exchange Server 2019 in Cloud-Computing funktionieren und ob es möglich ist, diese auch in Grid-Computing umzusetzen. In den ersten Fällen ist dies gut gelungen und wird aufgrund der besseren Eigenschaften in Bezug auf deren Verfügbarkeit, Effizienz und Integrität empfohlen. Die endgültige Entscheidung fällt daher auf die Umstellungen auf Cloud-Computing, welches alle Anforderungen des Arbeitgebers erfüllt.

4.4 Ausblick

In dieser Bachelorarbeit wurde der Grundstein für den Vergleich der IT-Governance in Cloud- und Grid-Computing gelegt. Ziel der Arbeit war eine Gegenüberstellung von Grid-Computing und Cloud-Computing hinsichtlich der Regeln und Ziele im IT-Governance-Prozess. So wurde definiert, dass die Planung der erste wichtige Schritt vor der Implementierung ist. Diese hängt von der Nutzung der IT-Ressourcen ab und ob diese in lokalen oder geografisch verteilten Netzwerken eingerichtet werden. Des Weiteren wurde bei der Implementierung mithilfe von Virtualisierung bzw. Hypervisor das Betriebssystem als Gast installiert und eine entsprechende Rolle für die Domain bzw. Dienste eingerichtet. Als Grundlage erfolgte die explizite Installation und Einrichten von VMware ESXi, Workstation pro, Windows Server 2019 Exchange-Server, die

auf eine VPN-Verbindung ansprechen. Da sie eine wesentliche Rolle in dieser Arbeit Spielen. In der nächsten Phase wurde durch die Nutzung der Tools Netzwerkverkehr analysiert als auch die E-Mail-Service bzw. die zuständigen E-Mail-Protokolle überwacht. Es kann festgehalten werden, dass die Vorbereitung auf VMware ESXi für Private Cloud-Computing nicht aufwändiger ist als die Vorbereitung für das Grid-System. Ein wesentlicher Vorteil des Cloud-Computing ist demzufolge, dass der Administrationsaufwand dabei gering ist. Da in einer Domain nacheinander Rollen installiert werden, sollten als Zwischenschritt Snapshots von Server-Systemen gesichert werden. Diese wurden in Sicherheitsausfälle auflaufende Punkte zurückgesetzt. Da Snapshot im Grid-System jedoch nicht enthalten ist, muss in der Planung nach anderen Sicherheitswegen gesucht werden, um das Betriebssystem zu schützen. Es muss nicht vergessen, dass die Nutzung von Cloud-Computing (in die drei Betriebsmodelle) ist mit Datenschutz verbunden. Diese Probleme sind immer betroffen, sobald die personenbezogenen den privaten Rechner verlasen. Der nächste Schritt bezogen auf Grid-System war die Erstellung einer Gruppe für die Nutzung der VPN-Dienste. Das Umsetzen dessen hat sich jedoch verzögert, da es kein sicheres Backup vorhanden war und dieser Teil (Grid-Computing) zunächst eingerichtet werden musste, um etwaige weitere DNS-Angriffe auf die Umgebung abzuwenden.

Literaturverzeichnis

© MICROSOFT 2022: *Vorbereitung von Active Directory und Domänen für Exchange Server, Active Directory Exchange Server, Exchange Server Active Directory, Exchange 2019 Active Directory | Microsoft Learn*. URL https://learn.microsoft.com/de-de/Exchange/plan-and-deploy/prepare-ad-and-domains?view=exchserver-2019. - abgerufen am 2022-12-03

AMAZON WEB SERVICES INC.: *Arten von Cloud Computing*, 2023a https://aws.amazon.com/de/types-of-cloud-computing/

AMAZON WEB SERVICES INC.: *AWS | Amazon Virtual Private Cloud (VPC) & VPS Hosting*, 2023b https://aws.amazon.com/de/vpc/?nc1=h_ls

BAUN, CHRISTIAN ; KUNZE, MARCEL ; NIMIS, JENS ; TAI, STEFAN: *Informatik im Fokus Cloud Computing Web-basierte dynamische IT-Services*, 2011 — ISBN 9783642184352

BEDNER, MARK: *Cloud Computing*, 2012 — ISBN 978-3-86219-080-5

BLESS, ROLAND ; MINK, STEFAN ; CONRAD, MICHAEL ; KUTZNER, KENDY ; BLAß, ERIK-OLIVER ; HOF, HANS-JOACHIM ; SCHÖLLER, MARCUS: *Sichere Netzwerkkommunikation* : Springer-Verlag, 2005

BUCHTA, DIRK ; EUL, MARCUS ; SCHULTE-CROONENBERG, HELMUT: *Strategisches IT-Management* : Gabler, 2009

D'ANTONI, JOEY: *Hybrid Cloud*, 2022 https://orangematter.solarwinds.com/2022/10/24/hybrid-cloud-benefits/

EICKERMANN, THOMAS ; HOMMES, FERDINAND: Metacomputing in the gigabit testbed west. In: *Workshop on wide area networks and high performance computing*, Springer, London (1999), S. 119–129

FERRAIOLO, DAVID F ; KUHN, D RICHARD: Role-Based Access Controls (1992), S. 554–563

FERREIRA, LUIS ; BERSTIS, VIKTORS ; ARMSTRONG, JONATHAN ; KENDZIERSKI, MIKE ; NEUKOETTER, ANDREAS ; BING-WO, RICHARD ; AMIR, ADEEB ; MURAKAWA, RYO ; U. A.: *Introduction to Grid Computing mputing with Globus lobus*

FOSTER, IAN ; KESSELMAN, CARL ; TUECKE, STEVEN: *The Anatomy of the Grid Enabling Scalable Virtual Organizations* *, 2001

GABECI, KEVIN: *What's the Difference between UEFI and BIOS?* | *by Kevin Gabeci* | *Dev Genius*, 2020 https://blog.devgenius.io/whats-the-difference-between-uefi-and-bios-c8bfed674f1f

GERARDUS, BLOKDYK: *Cloud Community A Complete Guide* , 2021

HÖLLWARTH, TOBIAS: *Cloud Migration der Weg in die Cloud*, 2013 — ISBN 9783826694585

IGOR K UND VICTOR S ; KOTENKO, I. ; SKORMIN, V. (Hrsg.): *Computer Network Security*, *Lecture Notes in Computer Science*. Bd. 7531. Berlin, Heidelberg : Springer Berlin Heidelberg, 2012 — ISBN 978-3-642-33703-1

JACOB, BART. ; INTERNATIONAL BUSINESS MACHINES CORPORATION. INTERNATIONAL TECHNICAL SUPPORT ORGANIZATION.: *Introduction to grid computing* : IBM, International Technical Support Organization, 2005 — ISBN 0738494003

JOHANNSEN, A. ; KANT, D.: IT-Governance, Risiko- und Compliance-Management (IT-GRC) – Ein Kompetenz-orientierter Ansatz für KMU. In: *HMD Praxis der Wirtschaftsinformatik 2020 57:5* Bd. 57, Springer (2020), Nr. 5, S. 1058–1074

MANDL, PETER: *TCP und UDP Internals*, 2018

MICROSOFT: *Software-as-a-Service* | *Microsoft Azure*, 2023a https://azure.microsoft.com/de-de/resources/cloud-computing-dictionary/what-is-saas/

MICROSOFT: *What is PaaS? Platform as a Service* | *Microsoft Azure*, 2023b https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-paas/

NATIONAL VULNERABILITY DATABAS: *NVD - Home*, 2013 https://nvd.nist.gov/

NIEMANN, KLAUS D.: *Von der Unternehmensarchitektur zur IT-Governance* : Vieweg+Teubner Verlag, 2005

ODGERS, JOSH: *Nutanix Distributed File*, 2015 https://www.joshodgers.com/2015/06/09/whats-next-scale-storage-separately-to-compute-on-nutanix/

PADHY, RABI PRASAD ; PATRA, MANAS RANJAN: Evolution of Cloud Computing and Enabling Technologies. In: *International Journal of Cloud Computing and Services Science (IJ-CLOSER)* Bd. 1, Institute of Advanced Engineering and Science (2012), Nr. 4

PLASZCZAK, PAWEL. ; WELLNER, RICHARD.: *Grid computing : the savvy manager's guide* : Elsevier/Morgan Kaufmann, 2006 — ISBN 0127425039

SCHIEB, JÖRG: Windows Server 2019 : Praxiseinstieg (2018) — ISBN 3958458874

SIEGERT, HANS-JÜRGEN ; BAUMGARTEN, UWE: *Betriebssysteme* : Oldenbourg Wissenschaftsverlag, 2010

VAQUERO, LUIS M ; RODERO-MERINO, LUIS ; CACERES, JUAN ; LINDNER, MAIK: *A Break in the Clouds: Towards a Cloud Definition*, 2009

VMWARE INC.: *Performance Evaluation of Intel EPT Hardware Assist*, 2008 https://www.vmware.com/pdf/Perf_ESX_Intel-EPT-eval.pdf

WIKIPEDIA: *NVM Express*. URL https://de.wikipedia.org/wiki/NVM_Express. - abgerufen am 2022-12-03

BIN XIAO, LAURENCE T. YANG, JIANHUA MA, CHRISTIAN MULLER-SCHLOER, YU HUA ; XIAO, B. ; YANG, L. T. ; MA, J. ; MULLER-SCHLOER, C. ; HUA, Y. (Hrsg.): *Autonomic and Trusted Computing*, *Lecture Notes in Computer Science*. Bd. 4610. Berlin, Heidelberg : Springer Berlin Heidelberg, 2007 — ISBN 978-3-540-73546-5

ZIMMER, DENNIS.: VMware & Microsoft Virtual Server : virtuelle Server im professionellen Einsatz ; [VMware GSX, ESX und Microsoft Virtual Server ; Virtualisierung im Vergleich ; Planung, Installation und Verwaltung], Galileo Press (2006) — ISBN 978-3-89842-701-2

VMWARE: *Snapshots in VMware ESXi und ESX (1015180)*, 2016 https://kb.vmware.com/s/article/1015180?lang=de

Erstellen eines Clusters, 2020
https://docs.vmware.com/de/VMware-vSphere/7.0/com.vmware.vsphere.resmgmt.doc/GUID-487C09CE-8BE2-4B89-BA30-0E4F7E3C66F7.html

SUMIT. SINGH: *Oracle EBS(R12) On Cloud*, 2021

Download the ESXi Installer. URL https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.esxi.install.doc/GUID-016E39C1-E8DB-486A-A235-55CAB242C351.html. - abgerufen am 2022-12-03. — © 2022 VMware, Inc.

Download VMware Workstation Pro | DE. URL https://www.vmware.com/de/products/workstation-pro/workstation-pro-evaluation.html. - abgerufen am 2022-12-03

IANA.ORG: Service Name and Transport Protocol Port Number Registry.

URL https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml

Anlagen

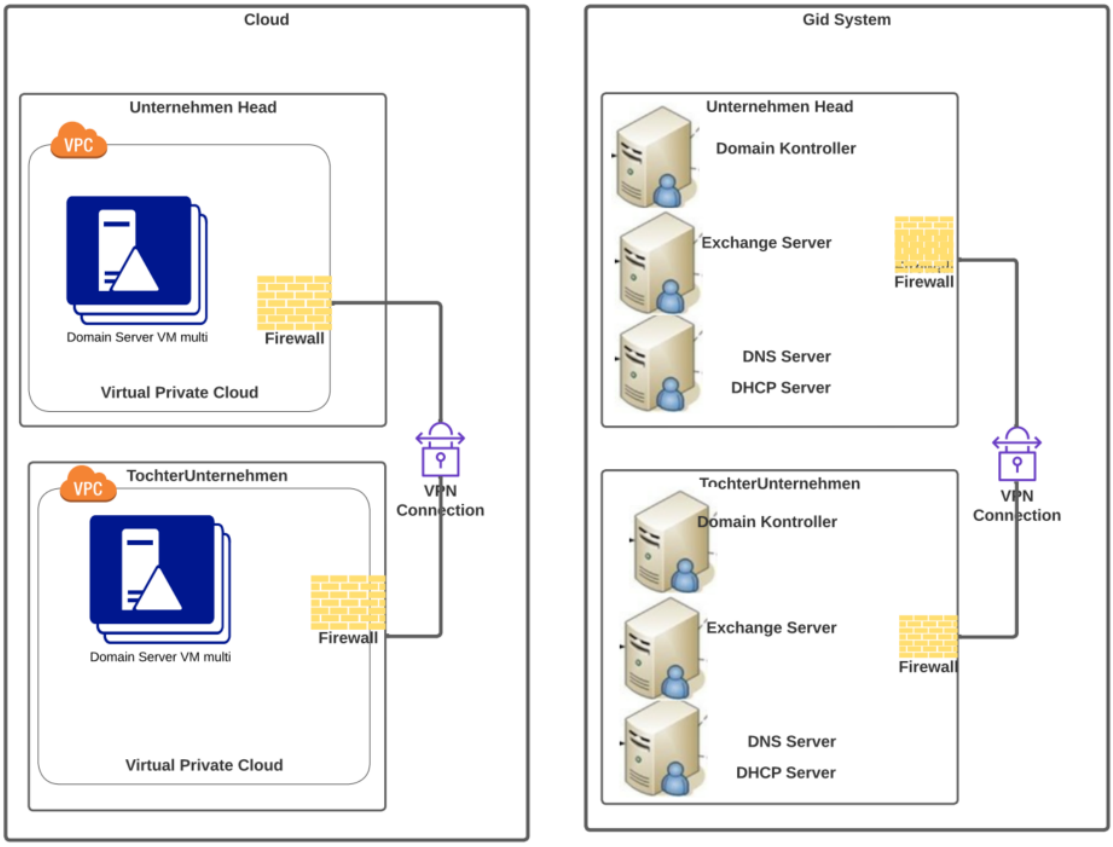


Abbildung 30: Domaine Übersicht

Excel Funktion für die BASE SCORE-Berechnung[16]

[16] https://www.first.org/cvss/v1/cvss-blank-scoring-1.0-sr.xls

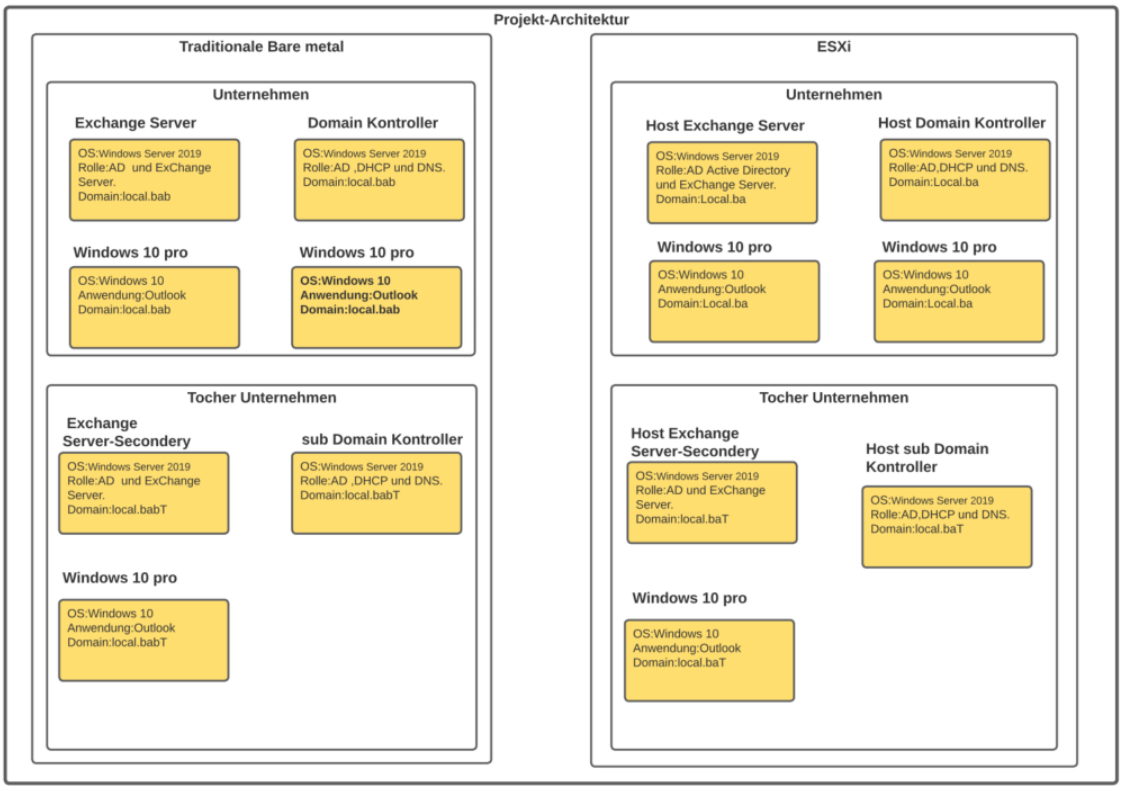


Abbildung 31: Projekt_Architektur

Eigenständigkeitserklärung

Hiermit erkläre ich, dass ich die vorliegende Arbeit selbstständig und nur unter Verwendung der angegebenen Literatur und Hilfsmittel angefertigt habe. Stellen, die wörtlich oder sinngemäß aus Quellen entnommen wurden, sind als solche kenntlich gemacht. Diese Arbeit wurde in gleicher oder ähnlicher Form noch keiner anderen Prüfungsbehörde vorgelegt.

Chemnitz, 01.02.2023	Abdo Frah
Ort, Datum	Vorname Nachname