FOM Hochschule für Oekonomie & Management

Hochschulzentrum Münster

Seminararbeit

im Studiengang Wirtschaftsinformatik

im Rahmen der Lehrveranstaltung
IT-Infrastruktur

über das Thema

Auswirkungen von Zero Trust Network Security zur Bekämpfung moderner Cyberbedrohungen

von

Joshua-Volkan Gramatzki

Betreuer:	Prof. Dr. Gregor Hülsken
Matrikelnummer	647100
Abgabedatum	27. November 2023

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungsverzeichnis

BYOD	Bring-Your-Own-Device
DDoS	Distributed Denial of Service
IoT	Internet of Things
PDP	Policy Decision Point
PEP	Policy Enforcement Point
ZT	Zero-Trust
ZTA	Zero-Trust-Architektur

Glossar

Authentifizierung Der Prozess der Überprüfung der Identität eines Clients, Gerätes oder Systems, um sicherzustellen, dass sie tatsächlich diejenige Partei sind, für die sie sich ausgeben. 4

Authentizität Bezeichnet die Eigenschaft der Echtheit der Daten. 8, 9

Autorisierung Der Prozess der Zuweisung von Berechtigungen und Zugriffsrechten an eine authentifizierte Partei, um festzulegen, welche Aktionen, Ressourcen oder Informationen sie nutzen oder verwalten darf. 3, 4, 8, 9

Client Ein Endpunkt in einem Client-Server Modell, der Anfragen an einen Server sendet und auf dessen Antworten wartet, um Dienste, Ressourcen oder Daten zu erhalten. 3

Integrität Die Vollständigkeit und Unversehrtheit von Daten muss gewährleistet werden. 4, 9

Policy Decision Point (PDP) Der PDP ist zentral und trifft Entscheidungen über den Zugriff auf Ressourcen basierend auf vordefinierten Sicherheitsrichtlinien. Er analysiert Anfragen und bildet die Grundlage für die Durchsetzung durch den Policy Enforcement Point (PEP). 3

Policy Enforcement Point (PEP) Der PEP ist eine Komponente, die Sicherheitsrichtlinien an Zugriffspunkten durchsetzt. Er regelt den Datenverkehr gemäß den Vorgaben des Policy Decision Point (PDP). 3

Vertraulichkeit Daten dürfen nur von Personen verarbeitet werden, die dafür berechtigt sind. 9

1 Einleitung

35 Jahre nach dem ersten Cyberangriff und 24 Jahre nach dem ersten Distributed Denial of Service (DDoS)-Angriff werden regelmäßig neue Sicherheitslücken in Netzwerken und Programmen gefunden und ausgenutzt. Die Anzahl der Mal- und Ransomware Angriffe sank zwar durch die Coronapandemie ein wenig, war davor jedoch auf einem historischen Maximum.[1]

Dürfen die Fußnoten in der Einleitung bestehen oder sollten die besser entfernt werden?

Zudem ist der Anteil der Unternehmen, die von einem Cyberangriff betroffen waren, so hoch wie noch nie.[2]

Auch die schnelle Verbreitung von Internet of Things (IoT)-Geräten erfordert immer stärker das Absichern von Netzwerken, um sowohl die Infrastruktur, als auch den Geräten zugängliche Daten zu schützen.[3] So sind viele Unternehmen, besonders solche die auf kritischer Infrastruktur basieren oder mit wichtigen Daten arbeiten, an einem möglichst idealen Schutz gegenüber diese Angriffe interessiert.

1.1 Zielsetzung

Diese Seminararbeit untersucht die Auswirkungen einer Zero-Trust-Architektur (ZTA) auf die Bekämpfung moderner Cyberbedrohungen. Dabei wird untersucht, wie die Implementierung einer ZTA die Häufigkeit von Cyberangriffen und von diesen verursachten Datenverlusten in Unternehmen beeinflusst. Zudem werden die möglichen Auswirkungen auf die Benutzerfreundlichkeit und Produktivität von Mitarbeitern betrachte.

Die erwarteten Ergebnisse umfassen eine potenzielle Verringerung von Cyberangriffen und Datenverlusten, da eine ZTA eine strikte Überprüfung von Netzwerkzugriffen bietet. Zugleich werden mögliche Einflüsse auf die Benutzerfreundlichkeit und Produktivität der Mitarbeiter untersucht, um einen ausgewogenen Ansatz zwischen sicherheit und Arbeitsleistung zu finden.

Zur Erstellung der Seminararbeit wird primär Literaturarbeit durchgeführt, welche sich auf eine systematische Analyse und Synthese bestehender wissenschaftlicher Quellen

[1] *SonicWall*, 2023a, S. 21; *SonicWall*, 2023b, S. 33.
[2] *CyberEdge*, 2023.
[3] Vgl. *Syed*, *N. F.* et al., 2022, S. 57143.

und Publikationen stützt. Hierzu wird zunächst ausführlich nach bestehender Literatur recherchiert, welche dann nach Relevanz für das Thema selektiert wird. Anschließend werden die gewählten Quellen sorgfältig gelesen und analysiert. Die relevanten Informationen dieser werden extrahiert, dies beinhaltet Daten, Fallstudien und Expertenmeinungen.

Die gesammelten Ergebnisse werden darauf in einem ganzheitlichen Ansatz zusammengeführt, um die Forschungsfragen zu beantworten und die zu erwartenden Ergebnisse zu entwickeln. Zuletzt werden die Stärken und Schwächen der identifizierten Literatur kritisch bewertet, um die Glaubwürdigkeit und Relevanz der verwendeten Quellen sicherzustellen.

Die Wahl der methodischen Herangehensweise ermöglicht eine gründliche Untersuchung des Themas, indem sie auf etablierte wissenschaftliche Erkenntnisse und Fachwissen zurückgreift. Dies gewährleistet eine fundierte und objektive Analyse der Auswirkungen einer Zero-Trust Netzwerkarchitektur auf moderne Cyberbedrohungen und die Mitarbeitererfahrung.

1.2 Aufbau der Arbeit

Abschnitt 2 führt verschiedene Grundlagen für die Ausarbeitung dieser Seminararbeit ein. Zunächst werden ZTAs definiert, sowie die Entwicklung und der historische Hintergrund dieser erklärt. Darauf werden Prinzipien von ZTA dargestellt und ein Vergleich zu anderen Sicherheitsansätzen gebildet.

Abschnitt 3 stellt verschiedene Arten von Cyberbedrohungen wie Malware- oder Phishingangriffe dar. Zudem werden die Trends in der Cyberkriminalität erläutert.

In Abschnitt 4 wird der Aufbau und die Komponenten von ZTA, sowie die Implementierung dieser in Unternehmen gezeigt. Außerdem werden Vor- und Nachteile von Zero-Trust gegeneinander aufgewogen.

Zuletzt werden in Abschnitt 5 die Auswirkungen auf die Sicherheit von Netzwerke, sowie die Reduzierung der Angriffsfläche erläutert. Zudem belichtet dieser Abschnitt, wie Zero-Trust sensible Daten schützt, zeigt die Messbarkeit der Auswirkungen auf die Sicherheit und stellt Probleme dar.

2 Grundlagen

2.1 Definition einer ZTA

Zero-Trust (ZT) bezeichnet eine Sammlung an Maßnahmen der Cybersicherheit, welche darauf basieren, die Verteidigungen von netzwerkbasierten Umfängen auf Nutzer und Ressourcen umzuleiten.[4] Darüber hinaus ist eine ZTA ein Cybersicherheitsplan einer Einrichtung, der die Konzepte von ZT umsetzt und Zugriffsrichtlinien, Arbeitsabläufe und Beziehungen zwischen Komponenten umfasst.[5]

Das Ziel einer ZTA ist es, unautorisierten Zugriff auf Daten und Leistungen zu verhindern und hierbei das Durchführen der Zugriffskontrollen so detailliert wie möglich zu gestalten.

2.2 Entwicklung und historischer Hintergrund

Überlegen, ob dieses Kapitel im Text bleibt oder entfent wird

2.3 Prinzipien und Konzepte von Zero-Trust

In einem System, welches ZT implementiert, muss jede Anfrage bevor sie auf die Ressourcen zugreifen kann, in einem Policy Decision Point (PDP)/Policy Enforcement Point (PEP) überprüft werden.[6]

Eine ZTA wird mit dem Gedanken entwickelt und umgesetzt, die folgenden Grundsätze umzusetzen:

- Alle Datenquellen und Rechenleistungen werden als Ressourcen angesehen,
- Unabhängig der Netzwerkposition ist jegliche Kommunikation gesichert,
- Der Zugriff auf einzelne Ressourcen erfolgt auf einer Pro-Sitzung Grundlage,
- Zugriff auf Ressourcen wird durch dynamische Regelungen festgelegt und kann von verschiedenen Attributen, wie die Identität des Clients beeinflusst werden,

[4] Vgl. *Rose, S.* et al., 2020, S. 4.
[5] Vgl. ebd., S. 4.
[6] Vgl. ebd., S. 4.

- Das Unternehmen überwacht und misst die Integrität aller eigenen und verbundenen Ressourcen,
- Jegliche Ressourcen Authentifizierung und Autorisierung ist dynamisch und erzwungen, bevor Zugriff gewährt werden kann,
- Das Unternehmen sammelt so viele Informationen über den aktuellen Status der Ressourcen, Netzwerkinfrastruktur und Kommunikationen wie möglich und nutzt diese, um die Sicherheit zu erhöhen.[7]

Eventuell ibidem entfernen mit „\makeatletter\blx@ibidreset\makeatother“

2.4 Vergleich zu herkömmlichen Sicherheitsansätzen

[7] Vgl. *Rose, S.* et al., 2020, S. 6-7.

3 Moderne Cyberbedrohungen

3.1 Trends und Entwicklungen in der Cyberkriminalität

In den letzten Jahren hat die Anzahl der Cyberkriminalitätsfälle in Deutschland stark zugenommen. So wurden zwar für das Jahr 2022 ein Rückgang von 6.5% gegenüber dem Vorjahr an erfassten Fällen aufgezeichnet, jedoch bildet sich in dem Zeitraum von 2012 bis 2022 ein Gesamtwachstum von 112% an erfassten Cyberkriminalitätsfällen.[8]

Analog zu der Anzahl der aufgezeichneten Fälle steigen auch die Kosten, die Cyberkriminalität verursacht, sowie die Ausgaben die für IT-Sicherheit in Deutschland vorgenommen werden stetig. 2018 haben Cyberkriminalitätsvorfälle deutschen Unternehmen durchschnittlich 13,12 Millionen US-Dollar[9] gekostet, was gegenüber dem Vorjahr ein Zuwachs von fast 18% darstellt.[10] 2021 wurden so ungefähr 6,9 Milliarden Euro für IT-Sicherheitsmaßnahmen ausgegeben, was einem Zuwachs von fast 22% gegenüber dem Vorjahr entspricht,[11] davon wurden geschätzt 1,7 Milliarden Euro für Softwarelösungen ausgegeben.[12]

Wie die Kosten und Ausgaben für Cyberkriminalität steigen auch die möglichen Methoden der Angreifer. Abbildung 1 zeigt, dass die Anzahl der Fälle von Cyberkriminalität fast stetig zunimmt.

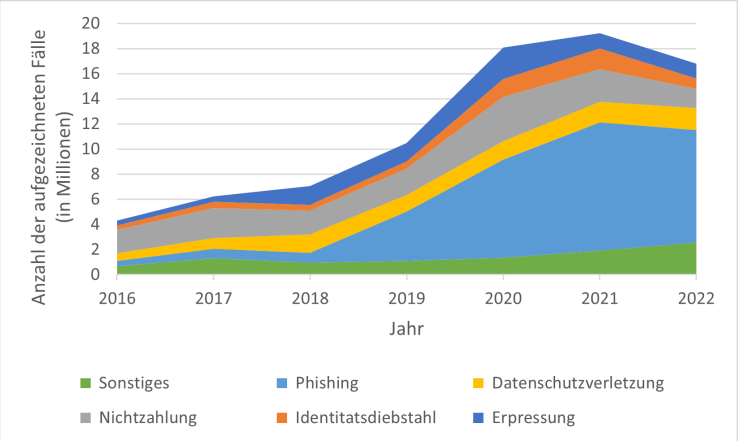


Abbildung 1: Erfasste Fälle von Cyberkriminalität nach Typ.[13] Stand September 2023

[8] Vgl. *Bundeskriminalamt*, 2023.
[9] Heutiger Wert ungefähr 10,23 Millionen Euro
[10] Vgl. *Accenture*, 2019.
[11] Vgl. *Bitkom*, 2022.
[12] Vgl. *Bitkom*, 2020.

Einzig im Jahr 2022 wurde ein Rückgang der erfassten Fälle aufgezeichnet. Besonders der Anteil, der Phishingangriffe hat im Vergleich zu 2018 stark zugenommen, wie in Abbildung 2 dargestellt wird.

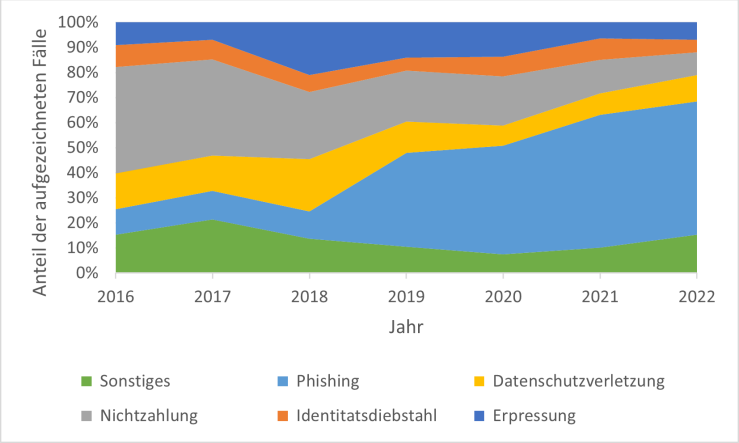


Abbildung 2: Anteil einzelner Cyberkriminalitätstypen.[14] Stand September 2023

3.2 Arten von Cyberbedrohungen - Malware, Phishing, DDoS

Die drei häufigsten Methoden von Cyberattacken sind Malware, Phishing und DDoS Angriffe.

Definition 3.1. *Phishing bezeichnet den Versuch, an vertrauliche Informationen wie Anmeldedaten oder Kreditkarteninformationen zu gelangen, indem ein System innerhalb eines Kommunikationsvorgangs als vertrauenswürdig ausgibt.*[15]

Definition 3.2. *Malware bezeichnet eine Software, welche ausschließlich Systeme angreift, welche entweder keine anderen Systeme beschädigen, oder welche Malwaresysteme angreifen.*[16]

Definition 3.3. *Unter DDoS-Angriffen werden Vorgänge verstanden, gezielt versuchen, ein Netzwerk oder einen Computer die Möglichkeit zu nehmen, gewohnte Dienste auszuführen. Bei solchen Angriffen werden die vorhandenen Daten und Systeme weder direkt*

[13] Vgl. *Statista Market Insights* et al., 2023
[14] Vgl. ebd.
[15] Vgl. *Bhavsar*, *V.*, *Kadlak*, *A.*, *Sharma*, *S.*, 2018, S. 27.
[16] Vgl. *Kramer*, *S.*, *Bradfield*, *J. C.*, 2010, S. 108f.

noch permanent angegriffen, es wird lediglich die Verfügbarkeit dieser Ressourcen unterbunden.[17]

Diese Angriffe zielen auf verschiedene Angriffsflächen und haben verschiedene Ziele, welche das korruptieren von Daten oder Systeme oder das Hindern des Zugriffs auf Daten und Systeme beinhalten können. Um diese Angriffe abzuwehren, gibt es verschiedene Methoden, eine davon ist eine ZTA.

[17] Vgl. *Douligeris*, *C.*, *Mitrokotsa*, *A.*, 2003, S. 190.

4 ZTA im Detail

Da in einer ZTA keinem Gerät und keiner Anwendung vertraut wird, alle aber unterstützt werden, sind verschiedene Maßnahmen notwendig, die erwünschte und oft erforderte Sicherheit zu garantieren. Dies geschieht durch regelmäßiges Überprüfen der Authentizität und Autorisierung der Systeme.[18]

4.1 Komponenten und Architektur von Zero-Trust

Es gibt verschiedene Methoden, eine ZTA einzurichten, von denen viele das Konzept teilen, die Kontrolle nahe an den Anwendungen und Nutzern zu halten, anstatt sie in der Netzwerkinfrastruktur auszulagern.[19] Drei der Grundkomponenten einer ZTA sind Anwendungsauthentifizierung, Gerätauthentifizierung und Vertrauen, da eine ZTA im Gegensatz zu anderen Sicherheitsinfrastrukturen die Authentizität regelmäßig überprüft, die Nutzergeräte überprüft und Widersprüchlichkeiten in Anwendungen der Nutzer überwacht und erkennt.[20]

4.2 Implementierung von Zero-Trust in Unternehmen

Eine ZTA kann sowohl in einem neuen System implementiert werden, als auch in einem bereits bestehenden eingearbeitet werden. Hierfür nennen D'Silvia und Ambawade[21] folgende Annahmen:

- Das LAN innerhalb eines Netzwerkes sollte nicht implizit als vertraute Zone behandelt werden.
- Mit dem aktuellen Trend, dass in Unternehmen Bring-Your-Own-Device (BYOD) eingeführt wird, wird davon ausgegangen, dass Geräte, die mit dem Netzwerk verbunden sind, keine Instanz des Unternehmens sind, da jedes Gerät manipuliert werden kann.
- Ressourcen sind niemals vertrauenswürdig, d. h. vom Standpunkt der Sicherheit aus gesehen muss jede Ressource kontinuierlich bewertet werden und darf nur solange genutzt werden, wie sie benötigt wird.

[18] Vgl. *D'Silva*, *D.*, *Ambawade*, *D. D.*, 2021, S. 3.
[19] Vgl. *Buck*, *C.* et al., 2021, S. 4.
[20] Vgl. *D'Silva*, *D.*, *Ambawade*, *D. D.*, 2021, S. 3.
[21] Vgl. ebd., S. 3.

- Cloud-Dienste sind ein wesentlicher Bestandteil jedes Unternehmensnetzwerkes geworden und verdeutlichen, dass nicht alle Unternehmensressourcen innerhalb der Unternehmensinfrastruktur liegen.
- Alle Verbindungsanfragen von außerhalb des Unternehmens, wie z. B. Remote Desktop, müssen autorisiert und authentifiziert werden. Alle Daten müssen mit Respekt, Vertraulichkeit, Integrität und Quellenauthentifizierung übertragen werden
- Ausgehend der obigen Annahmen ist es essenziell, dass alle Ressourcen und Kommunikation zwischen dem Unternehmen und externer Infrastruktur einer ständigen Sicherheitsstrategie unterliegen muss.

4.3 Vor- und Nachteile von Zero-Trust

5 Auswirkungen und Resultate von Zero-Trust

5.1 Verbesserung der Sicherheitsebene

5.2 Reduzierung von Angriffsflächen

5.3 Schutz sensibler Daten

5.4 Messbare Auswirkungen auf die Sicherheit

5.5 Probleme

6 Fazit

Literaturverzeichnis

Accenture (2019): Schätzung der urchschnittlichen Kosten durch Cyberkrime-Vorfälle in Unternehmen in ausgewählten Ländern weltweit in den Jahren 2016 bis 2018, (in Millionen US-Dollar), Graph, statista, Dublin: Statista Research Department, 2019-03-05, URL: https://de.statista.com/statistik/daten/studie/499313/umfrage/gesamtkosten-durch-cybercrime-in-unternehmen-in-ausgewaehlten-laendern/ [Zugriff: 2023-11-14]

Bhavsar, *Vaishnavi*, *Kadlak*, *Aditya*, *Sharma*, *Shabnam* (2018): Study on Phishing Attacks, en, in: International Journal of Computer Applications, Bd. 182, 33, o. O., 2018-12, [Zugriff: 2023-11-24]

Bitkom (2020): Ausgaben für IT-Sicherheit in Deutschland nach Segment in den Jahren 2017 bis 2019 und Prognose bis 2021, (in Milliarden Euro), Graph, statista, Deutschland: Statista Research Department, 2020-10-06, URL: https://de.statista.com/statistik/daten/studie/151727/umfrage/ausgaben-fuer-it-sicherheit-in-deutschland/ [Zugriff: 2023-11-14]

Bitkom (2022): Ausgaben für IT-Sicherheit in Deutschland in den Jahren 2017 bis 2021 und Prognose bis 2025, (in Milliarden Euro), Graph, statista, Deutschland: Statista Research Department, 2022-10-25, URL: https://de.statista.com/statistik/daten/studie/1041736/umfrage/ausgaben-fuer-it-security-in-deutschland/ [Zugriff: 2023-11-14]

Buck, *Christoph*, *Olenberger*, *Christian*, *Schweizer*, *André*, *Völter*, *Fabiane*, *Eymann*, *Thorsten* (2021): Never trust, always verify: A multivocal literature review on current knowledge and research gaps of zero-trust, in: Computers & Security, 110 (2021), Nr. 102436, S. 26

Bundeskriminalamt (2023): Polizeilich erfasste Fälle von Cyberkriminalität in Deutschland von 2007 bis 2022, statista, Deutschland: Statista Research Department, 2023-07-12, URL: https://de.statista.com/statistik/daten/studie/295265/umfrage/polizeilich-erfasste-faelle-von-cyberkriminalitaet-im-engeren-sinne-in-deutschland/ [Zugriff: 2023-11-13]

CyberEdge (2023): Annual share of organizations affected by ransomware attacks worldwide from 2018 to 2023, Englisch, Cyberthreat Defense Report 2023, CyberEdge, o. O.: CyberEdge, 2023-05, URL: https://www.statista.com/statistics/204457/businesses-ransomware-attack-rate/

D'Silva, *Daniel*, *Ambawade*, *Dayanand D.* (2021): Building A Zero Trust Architecture Using Kubernetes, in: 2021 6th International Conference for Convergence in Technology (I2CT), o. O., 2021-04-04, S. 1–8

Douligeris, *C.*, *Mitrokotsa*, *A.* (2003): DDoS attacks and defense mechanisms: a classification, Englisch, in: Proceedings of the 3rd IEEE International Symposium on Signal Processing and Information Technology (IEEE Cat. No.03EX795), Darmstadt, Germany: IEEE, 2003-12-17, S. 190–193

Kramer, *Simon*, *Bradfield*, *Julian C.* (2010): A general definition of malware, in: Journal in Computer Virology, 6 (2010), Nr. 2, S. 105–114

Rose, *Scott*, *Borchert*, *Oliver*, *Mitchell*, *Stu*, *Connelly*, *Sean* (2020), Zero Trust Architecture, SP 800-207, United States of America, 2020-08, URL: https://doi.org/10.6028/NIST.SP.800-207

SonicWall (2023a): Annual number of malware attacks worldwide from 2015 to 2022, Englisch, Cyber Threat Report 2023, SonicWall, Milpitas, CA 95035, USA: SonicWall, 2023-03-27, URL: https://www.statista.com/statistics/873097/malware-attacks-per-year-worldwide/

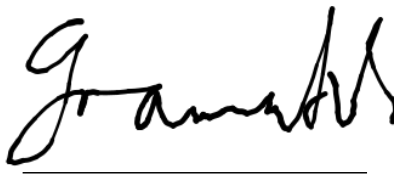
SonicWall (2023b): Annual number of ransomware attempts worldwide from 2017 to 2022, Englisch, Cyber Threat Report 2023, SonicWall, Milpitas, CA 95035, USA: SonicWall, 2023-03-27, URL: https://www.statista.com/statistics/494947/ransomware-attempts-per-year-worldwide/

Statista Market Insights, *National Cyber Security Organizations*, *FBI - Federal Bureau of Investigation*, *IMF* (2023): Cybersecurity - Worldwide, o. O., 2023-09, URL: https://www.statista.com/outlook/tmo/cybersecurity/worldwide [Zugriff: 2023-11-14]

Syed, *Naeem Firdous*, *Shah*, *Syed W.*, *Shaghaghi*, *Arash*, *Anwar*, *Adnan*, *Baig*, *Zubair*, *Doss*, *Robin* (2022): Zero Trust Architecture (ZTA): A Comprehensive Survey, in: IEEE Access, 10 (2022), S. 57143–57179

Ehrenwörtliche Erklärung

Hiermit versichere ich, dass die vorliegende Arbeit von mir selbstständig und ohne unerlaubte Hilfe angefertigt worden ist, insbesondere dass ich alle Stellen, die wörtlich oder annähernd wörtlich aus Veröffentlichungen entnommen sind, durch Zitate als solche gekennzeichnet habe. Ich versichere auch, dass die von mir eingereichte schriftliche Version mit der digitalen Version übereinstimmt. Weiterhin erkläre ich, dass die Arbeit in gleicher oder ähnlicher Form noch keiner Prüfungsbehörde/Prüfungsstelle vorgelegen hat. Ich erkläre mich damit nicht einverstanden, dass die Arbeit der Öffentlichkeit zugänglich gemacht wird. Ich erkläre mich damit einverstanden, dass die Digitalversion dieser Arbeit zwecks Plagiatsprüfung auf die Server externer Anbieter hochgeladen werden darf. Die Plagiatsprüfung stellt keine Zurverfügungstellung für die Öffentlichkeit dar.



Ahaus, 27.11.2023

(Ort, Datum)

(Eigenhändige Unterschrift)