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	2. Januar 2024

Inhaltsverzeichnis

Abbildungsverzeichnis

Abkürzungsverzeichnis

BYOD	Bring-Your-Own-Device
CAPTCHA	Completely Automated Public Turing test to tell Computers and Humans Apart
DDoS	Distributed Denial of Service
DEC	Digital Equipment Corporation
IoT	Internet of Things
MFA	Multi-Faktor-Authentifizierung
NCCoE	National Cybersecurity Center of Excellence
NCSC	National Cyber Security Centre
NIST	National Institute of Standards and Technology
NVD	National Vulnerability Database
OSSTMM	Open Source Security Testing Methodology Manual
PDP	Policy Decision Point
PEP	Policy Enforcement Point
SDP	Softwaredefinierte Perimeter
SSO	Single-Sign-On
ZT	Zero-Trust
ZTA	Zero-Trust-Architektur

Glossar

Authentifizierung Unter Authentifizierung versteht man die Überprüfung der Identität einer Person, eines Systems oder einer Einrichtung, die versucht, auf eine bestimmte Ressource oder einen Dienst zuzugreifen. Sie stellt sicher, dass nur autorisierte Benutzer Zugang erhalten und verhindert gleichzeitig den unbefugten Zugriff. 5, 9–11, 13, 18

Autorisierung Autorisierung bezieht sich auf den Prozess der Gewährung oder Verweigerung des Zugangs zu bestimmten Ressourcen oder Funktionen auf der Grundlage der Identität, der Privilegien und der Berechtigungen des Benutzers. 3, 5, 9, 11, 13

CAPTCHA CAPTCHA steht für „Completely Automated Public Turing test to tell Computers and Humans Apart“ („vollautomatischer öffentlicher Turing-Test zur Unterscheidung von Computern und Menschen“). Es handelt sich dabei um eine Sicherheitsmaßnahme, die auf Websites verwendet wird, um festzustellen, ob der Benutzer ein Mensch oder ein Computerprogramm ist. CAPTCHAs beinhalten in der Regel visuelle oder auditive Hrausforderungen, die für Menschen leicht zu lösen sind, aber schwierig für Maschinen. 18

Client-Server Modell Client-Server ist eine Computerarchitektur, bei der ein Client, in der Regel ein Gerät oder Computer eines Benutzers, Dienste oder Ressourcen von einem zentralen Server anfordert. Der Server, bei dem es sich um einen leistungsstarken Computer oder ein Computernetz handelt, stellt dem Client die angeforderten Dienste oder Ressourcen zur Verfügung. Diese Architektur wird häufig in vernetzten Systemen verwendet und ermöglicht eine effiziente Verteilung von Ressourcen und Arbeitslast. 5

Datenintegrität Datenintegrität bezieht sich auf die Genauigkeit, Konsistenz und Zuverlässigkeit von Daten während ihres gesamten Lebenszyklus. Sie stellt sicher, dass Daten intakt und unverändert bleiben, frei von Fehlern, Korruption oder unbefugten Änderungen. 5, 11

ISO/OSI-Referenzmodell Ein Schichtenmodell, das die Struktur und den Aufbau von Netzwerkkommunikation standardisiert und in sieben Schichten unterteilt. Dies ermöglicht eine effiziente und standardisierte Kommunikation zwischen verschiedenen Computersysteme. 18

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). 5

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). 5

Respekt In der Datensicherheit bedeutet Respekt, die Daten gemäß aller Sicherheitsrichtlinien und -protokolle zu verarbeiten und zu speichern. Dies beinhaltet es, die Daten vor dem Speichern zu verschlüsseln, die Anfragen zu autorisieren, die Datenintegrität zu kontrollieren und die Datenübertragung und -zugriffe zu überwachen und zu kontrollieren. 11

Vertraulichkeit Vertraulichkeit ist eines der Schutzziele in der Informationssicherheit. Es bezieht sich darauf, dass Informationen nur von autorisierten Personen oder Systemen eingesehen oder genutzt werden können. Hierdurch wird gewährleistet, dass sensible Daten vor unbefugtem Zugriff geschützt sind. 11

1 Einleitung

35 Jahre nach dem ersten Cyberangriff[1] und 24 Jahre nach dem ersten Distributed Denial of Service (DDoS)-Angriff[2] 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.[3] Zudem ist der Anteil der Unternehmen, die von einem Cyberangriff betroffen waren, so hoch wie noch nie.[4] Auch die schnelle Verbreitung von Internet of Things (IoT)-Geräten erhöht die Erforderlichkeit des Absicherns von Netzwerken immens, um sowohl die Infrastruktur, als auch den Geräten zugängliche Daten zu schützen.[5] So sind viele Unternehmen, besonders solche die auf kritischer Infrastruktur basieren oder mit wichtigen Daten arbeiten, an einem möglichst idealen Schutz gegenüber diesen Angriffen 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 Cyberangriffe und von diesen verursachte Datenverluste in Unternehmen beeinflusst.

Die erwarteten Ergebnisse umfassen eine potenzielle Verringerung von Cyberangriffen und Datenverlusten. Zugleich werden mögliche Einflüsse auf die Benutzerfreundlichkeit und Produktivität der Mitarbeiter untersucht.

Dabei wird versucht, die Forschungsfrage „Wie trägt eine ZTA zur Erhöhung der Sicherheit in einem System unter Einbehalt von Benutzerfreundlichkeit und -produktivität bei?“ zu beantworten.

Zur Erstellung der Seminararbeit wird primär Literaturarbeit durchgeführt, welche sich auf eine systematische Analyse und Synthese bestehender wissenschaftlicher Quellen und Publikationen stützt.[6] Hierzu wird zunächst ausführlich nach bestehender Literatur recherchiert, welche dann nach Relevanz für das Thema selektiert wird. Anschließend wer-

[1] Vgl. *Shackelford*, *S.*, 2018.
[2] Vgl. *Emerging Technology from the arXiv*, 2019.
[3] *SonicWall*, 2023a, S. 21; *SonicWall*, 2023b, S. 33.
[4] *CyberEdge*, 2023.
[5] Vgl. *Syed*, *N. F.* et al., 2022, S. 57143.
[6] Vgl. *Fink*, *A.*, 2019, S. 6.

den 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 Forschungsfrage zu beantworten und die zu erwartenden Ergebnisse zu evaluieren.

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 (ZT)-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 ZT gegeneinander aufgewogen.

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

2 Grundlagen

ZTAs haben in den letzten Jahren an Bedeutung gewonnen, da traditionelle Sicherheitsansätze immer ineffektiver gegen moderne Cyberbedrohungen werden. In einer zunehmend vernetzten und digitalisierten Welt, in der Unternehmensdaten und -ressourcen ständig Bedrohungen ausgesetzt sind, wird die Implementierung einer ZTA zu essenziellen Sicherheitsstrategie.

Dieser Abschnitt widmet sich der eingehenden Analyse von ZTA, einschließlich ihrer historischen Entwicklung sowie den zugrunde liegenden Prinzipien.

2.1 Definition einer ZTA

ZT bezeichnet eine Sammlung an Maßnahmen der Cybersicherheit, welche darauf basieren, die Verteidigungen von netzwerkbasierten Umfängen auf Nutzer und Ressourcen umzuleiten.[7] Darüber hinaus ist eine ZTA ein Cybersicherheitsplan einer Einrichtung, der die Konzepte von ZT umsetzt und Zugriffsrichtlinien, Arbeitsabläufe und Beziehungen zwischen Komponenten umfasst,[8] welche das reduzieren der vergebenen Berechtigungen auf ein Minimum beinhalten.

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

Zscaler hat im Jahr 2022 die Entwicklung des ZT-Konzepts knapp zusammengefasst.[9] Die ersten Grundsteine, die zur Entwicklung des ZT-Konzepts führten, wurden 1987 gelegt. In diesem Jahr wurde von Entwicklern der Digital Equipment Corporation (DEC) eine Studie zum Thema Firewall-Technologie veröffentlicht, wodurch die „Festung mit Burggraben“ als Standardmodell der Netzwerksicherheit etabliert wurde.[10]

Im Jahr 1994 wurde der Begriff „ZT“ im Rahmen einer Doktorarbeit über Computersicherheit geprägt. Der Autor untersuchte Vertrauen als ein mathematisch beschreibbares,

[7] Vgl. *Rose*, *S.* et al., 2020, S. 4.
[8] Vgl. ebd., S. 4.
[9] Vgl. *zscaler*, 2022.
[10] Vgl. ebd.

endliches Gut.[11] Wenn ein Angreifer die Firewall überwinden kann, stünde ihm das ganze Netzwerk zur Verfügung.[12]

Die erste Version des 802.1X-Protokolls[13] wurde im Jahr 2001 veröffentlicht und als Standard für Netzzugangskontrollen eingeführt. In diesem Protokoll wird die Authentifizierung von Netzverbindungen sowie die Vergabe von Zugriffsrechten auf Netzwerkebene vorgesehen. Dadurch, dass das Protokoll komplexe Vorgänge vorschreibt, war es nicht zur allgemeinen Implementierung geeignet.[14] Zusätzlich wurde auch in 2001 die erste Version des Open Source Security Testing Methodology Manual (OSSTMM) mit dem Fokus auf Vertrauen veröffentlicht.[15]

Im Jahr 2008 wurde die dritte Version des OSSTMM veröffentlicht, welche in einem ganzen Kapitel über die Schwachstelle „Vertrauen“ in Systemen befasst.[16]

Eine weitere Prägung des Begriffes „ZT“ fand im Jahr 2010 statt, als der Analyst Kindervag in einem Forschungsbeitrag die Verlagerung der Authentifizierung und Cybersicherheit in den Datenpfad vorsieht und auch die Segmentierung zwischen einzelnen Sitzungen fordert. Weiterhin wird das Paradigma des Netzwerkzugangs verhaftet, der Sicherheitsperimeter wird allerdings ins Netzwerk verschoben.[17]

2018 arbeiteten Forscher von National Institute of Standards and Technology (NIST) und National Cybersecurity Center of Excellence (NCCoE) zusammen an einem Projekt, welches zur Veröffentlichung der NIST Leitlinie SP 800–207[18] im Jahr 2020 als ein erstes einheitliches Framework für ZTAs führte. Diese definiert ZT als eine Sammlung verschiedener Konzepte und Ideen, welche die Unsicherheit bei anfragenbezogenen Zugriffsentscheidungen in Informationssystemen verringern sollen. Diese Veröffentlichung leitete einen Paradigmenwechsel ein, da erstmals ZT nicht mehr im Kontext des Netzwerkzugangs definiert wird.[19]

Im Jahr 2021 hat das National Cyber Security Centre (NCSC) im Vereinigten Königreich empfohlen, dass Netzwerkarchitekten einen ZT Ansatz für neue IT-Lösungen in Anbetracht nehmen insbesondere wenn signifikante Nutzung von Cloud-Services geplant

[11] Vgl. *Marsh*, *S. P.*, 1994.
[12] Vgl. *IDG Network World Inc.*, 1994, S. 29.
[13] Vgl. IEEE Standard for Port Based Network Access Control, 2001.
[14] Vgl. *zscaler*, 2022.
[15] Vgl. *Herzog*, *P.*, *Barceló*, *M.* et al., 2001.
[16] Vgl. *Herzog*, *P.*, *Barceló Marta Lee*, *R. E.*, 2010.
[17] Vgl. *zscaler*, 2022; Vgl. *Kindervag*, *J.*, *Balaouras*, *S.*, *Coit*, *L.*, 2010.
[18] *Rose*, *S.* et al., 2020.
[19] Vgl. *zscaler*, 2022.

ist.[20] Zusätzlich wurden im Jahr 2022 alle US-Behörden zur Umstellung auf ZT bis 2024 verpflichtet.[21]

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.[22]

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,
- Das Unternehmen überwacht und misst die Datenintegrität 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.[23]

[20] *NCSC*, 2021.
[21] Vgl. *zscaler*, 2022.
[22] Vgl. *Rose*, *S.* et al., 2020, S. 4.
[23] Vgl. ebd., S. 6-7.

3 Moderne Cyberbedrohungen

Die zunehmende Digitalisierung und Vernetzung von Systemen hat eine Vielzahl von Vorteilen mit sich gebracht, aber auch die Entstehung und Verbreitung moderner Cyberbedrohungen begünstigt. In diesem Abschnitt werden moderne Cyberbedrohungen im Kontext von ZTA untersucht.

Es werden die verschiedenen Arten von Bedrohungen, wie beispielsweise Ransomware, Phishing und DDoS-Angriffe, sowie deren potenzielle Auswirkungen auf Unternehmen und Organisationen beleuchtet. Der Fokus liegt darauf, ein umfassendes Verständnis für die Bedrohungslandschaft zu entwickeln, um die Notwendigkeit und Relevanz von ZTA als Antwort auf diese zunehmend raffinierten und vielschichtigen Angriffe zu unterstreichen.

3.1 Trends 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.[24]

Analog zu der Anzahl der aufgezeichneten Fälle steigen auch die Kosten, welche durch Cyberkriminalität verursacht werden, sowie die Ausgaben, welche für IT-Sicherheit in Deutschland vorgenommen werden, stetig. 2018 haben Cyberkriminalitätsvorfälle deutsche Unternehmen durchschnittlich $13,12$ Millionen US-Dollar[25] gekostet, was gegenüber dem Vorjahr eine Steigerung von fast 18% darstellt.[26] 2021 wurden so ungefähr $6,9$ Milliarden Euro für IT-Sicherheitsmaßnahmen ausgegeben, was einer Steigerung von fast 22% gegenüber dem Vorjahr entspricht.[27] Hiervon wurden geschätzt $1,7$ Milliarden Euro für Softwarelösungen ausgegeben.[28]

Wie die Kosten und Ausgaben für Cyberkriminalität steigen auch die möglichen Methoden der Angreifer. Abbildung 1 zeigt nach den Statista Market Insights,[29] dass die Anzahl der Fälle von Cyberkriminalität fast stetig zunimmt.

[24] Vgl. *Bundeskriminalamt*, 2023, S. 5.
[25] Heutiger Wert ungefähr $11,88$ Millionen Euro – Stand 29/12/23 16:10 PST, Bloomberg
[26] Vgl. *Accenture*, 2019.
[27] Vgl. *Bitkom*, 2022.
[28] Vgl. *Bitkom*, 2020.
[29] Vgl. *Statista Market Insights* et al., 2023.

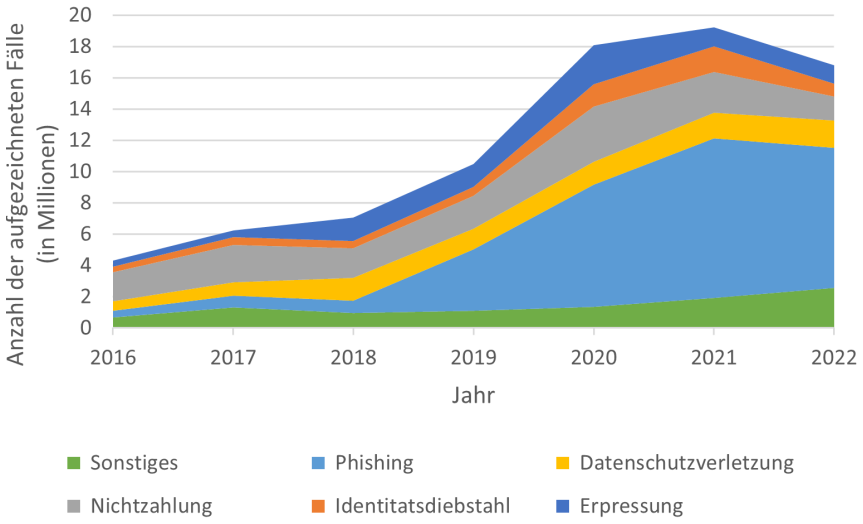


Abbildung 1: Erfasste Fälle von Cyberkriminalität nach Typ. Stand September 2023

Einzig im Jahr 2022 wurde ein Rückgang der erfassten Fälle aufgezeichnet. Besonders der Anteil der Phishingangriffe hat im Vergleich zu 2018 stark zugenommen, wohingegen die Nichtzahlung von Leistungen stark abgenommen hat, wie in Abbildung 2 aus den Statista Market Insights[30] dargestellt wird.

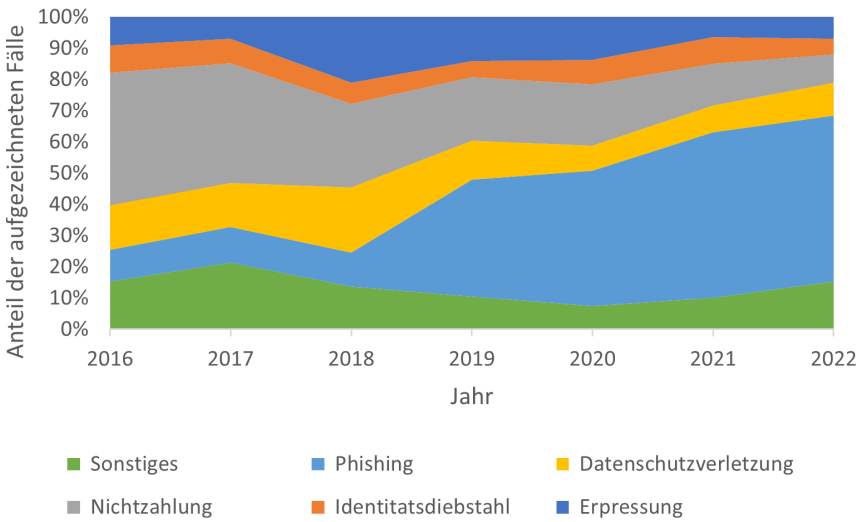


Abbildung 2: Anteil einzelner Cyberkriminalitätstypen. Stand September 2023

[30] Vgl. *Statista Market Insights* et al., 2023.

3.2 Arten von Cyberbedrohungen - Malware, Phishing, DDoS

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

Definition 3.2.1. *Phishing bezeichnet den Versuch, an vertrauliche Informationen eines Nutzers wie Anmeldedaten oder Kreditkarteninformationen zu gelangen, indem ein System sich innerhalb eines Kommunikationsvorgangs als vertrauenswürdig ausgibt.*[31]

Definition 3.2.2. *Malware bezeichnet eine Software, welche ausschließlich Systeme angreift die entweder keine anderen Systeme beschädigen oder Malwaresysteme angreifen.*[32]

Definition 3.2.3. *Unter DDoS-Angriffen werden Vorgänge verstanden, die gezielt versuchen, einem Netzwerk oder einem Computer die Möglichkeit zu nehmen, gewohnte Dienste auszuführen. Bei solchen Angriffen werden die vorhandenen Daten und Systeme weder direkt noch permanent angegriffen, es wird lediglich die Verfügbarkeit dieser Ressourcen unterbunden.*[33]

Definition 3.2.4. *Als Ransomware wird schädliche Software bezeichnet, die darauf abzielt, digitale Daten zu verschlüsseln und den Zugriff auf diese zu verhindern. Die Angreifer fordern oftmals ein Lösegeld für die Wiederherstellung des Zugriffs. Präventive Maßnahmen gegen Ransomware umfassen häufig komplexe Sicherheitsprotokolle und regelmäßige Datensicherungen.*

Jeder diese Angriffe zielt mit voneinander unterschiedlichen Absichten, welche das Korruptieren von Daten oder Systeme oder das Hindern des Zugriffs auf Daten und Systeme beinhalten können, auf eigene Bereiche in einem System.. Um diese Angriffe abzuwehren, gibt es verschiedene Methoden. Eine davon ist das Implementieren einer ZTA.

[31] Vgl. *Bhavsar*, *V.*, *Kadlak*, *A.*, *Sharma*, *S.*, 2018, S. 27.
[32] Vgl. *Kramer*, *S.*, *Bradfield*, *J. C.*, 2010, S. 108f.
[33] Vgl. *Douligeris*, *C.*, *Mitrokotsa*, *A.*, 2003, S. 190.

4 ZTA im Detail

Da in einer ZTA keinem Gerät und keiner Anwendung vertraut wird, aber alle unterstützt werden, sind verschiedene Maßnahmen notwendig um die erwünschte Sicherheit zu garantieren. Dies geschieht durch regelmäßiges Überprüfen der Authentizität und Autorisierung der Systeme.[34]

4.1 Komponenten und Aufbau von Zero-Trust

Jede ZTA wird durch drei Eigenschaften definiert. Diese stellen sicher, dass (i) auf alle Ressourcen unabhängig von ihrer physischen oder logischen Position ein sicherer Zugriff erfolgen muss, (ii) strenge Zugriffskontrollmaßnahmen bestehen, und zuletzt (iii) jeglicher Netzwerkverkehr erfasst und aufgezeichnet wird.[35]

4.1.1 Komponenten einer Zero-Trust Architektur

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.[36] Drei der Grundmethoden 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.[37]

ZT sollte nicht als einzelne Technologie gesehen werden, sondern stellt durch viele Anforderungen, Kontrollen und Prinzipien einen umfassenden Schutz dar, welcher selbst bei verschwimmender Grenze zwischen Privatem und Arbeit nicht minder wirkt.[38]

4.1.2 Aufbau einer Zero-Trust Architektur

Eine ZTA lässt jede Anfrage eine Vertrauensevaluation durchgehen. Eine solche Evaluation kann aus den folgenden, von Horne und Nair dargestellten, Schritten bestehen:[39]

[34] Vgl. *D'Silva*, *D.*, *Ambawade*, *D. D.*, 2021, S. 3.
[35] Vgl. ebd., S. 2.
[36] Vgl. *Buck*, *C.* et al., 2021, S. 4.
[37] Vgl. *D'Silva*, *D.*, *Ambawade*, *D. D.*, 2021, S. 3.
[38] Vgl. *Akamai*, 2023, Was sind die Komponenten von Zero Trust.
[39] Vgl. *Horne*, *D.*, *Nair*, *S.*, 2021, S. 3.

1. Vertrauensfaktoren, darunter unter anderem
    - Nutzerauthentifizierung,
    - Nutzerrolle oder -profil,
    - Gerätauthentifizierung,
    - Geräteart und -status,
    - IP-Adresse, bzw. Ort,
    - Details der Zugriffsanfrage,
    - Verhaltensdaten,
2. Vertrauensalgorithmus,
3. Anforderungen und Anforderungsadministrator, mit den folgenden Richtlinien
    - Vertrauensgrenzwerte,
    - Grundsätze zur Einhaltung der Richtlinien,
    - Richtlinien für Endgeräte,
    - Datenschutzrichtlinien
4. Erlauben oder Ablehnen der Zugriffsanfrage.

Die Überprüfung nach dem 4. Schritt der vorherigen Auflistung läuft dabei wie folgt ab:[40]

1. Dabei wird die Anfrage zunächst auf die einzelnen Faktoren überprüft und evaluiert.
2. Anschließend wird aus dem Resultat dieser Evaluation ein Vertrauenswert berechnet, mit welchem die Anfrage überprüft und einzelne Richtlinien zugeschrieben werden.
3. Zuletzt wird, sofern ein ausreichender Vertrauenswert vorhanden ist, die Anfrage unter Einhaltung der Richtlinien akzeptiert, andernfalls abgelehnt.

[40] Vgl. *Horne*, *D.*, *Nair*, *S.*, 2021, S. 3.

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 werden die folgenden Annahmen genommen:[41]

- 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.
- 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 müssen.

4.3 Vor- und Nachteile von Zero-Trust

Eine ZTA bietet verschiedenste Vor- und Nachteile, angefangen von den verbesserten Sicherheitsmetriken, endend bei einer komplexeren Infrastruktur. Dieser Abschnitt listet und erläutert einzelne dieser Eigenschaften.

[41] Vgl. *D'Silva*, *D.*, *Ambawade*, *D. D.*, 2021, S. 3.

4.3.1 Vorteile

Bei erfolgreicher Implementierung einer ZTA hat jeder Teil des Netzwerkes nur für ein Minimum der Zeit Zugriff auf das Minimum der erforderten Ressourcen. Dies sorgt dafür, dass ein nahezu umfassender Schutz vor Angriffen besteht, welche besonders Sicherheitslücken in Systemen, die durch, beabsichtigte oder unbeabsichtigte, Vertrauensbrüche entstehen, abzielen.[42] Zudem ist eine ZTA flexibler, was die Nutzung von Anwendungen und Geräten betrifft, da die Sicherheitsarchitektur sich nicht auf einzelne Perimeter verlassen muss.[43] Gleichermaßen stellt eine ZTA eine bessere Einsicht in den Netzverkehr und das Nutzerverhalten dar, was es erneut vereinfacht, Risiken zu erkennen und auf diese zu reagieren.[44]

Besonders Unternehmen, welche ihre Ressourcen primär in Cloud-Systemen verwalten werden einfachere Prozesse in der Umwandlung auf eine ZTA haben, da die Sicherheitsprotokolle bei diesen Systemen meist flexibler einzurichten sind. Zudem ist eine ZTA in digitalen Unternehmen sehr effektiv, da solche keine klare Perimetergrenze haben, sondern überall existieren wo Kunden, Mitarbeiter oder Partner mit den Diensten interagieren und Daten genutzt werden. Hierdurch ist eine auf Perimeter basierende Sicherheitsstrategie nicht ausreichend. Eine ZTA hingegen ermöglicht es, neue Services schnell zu unterstützen, ohne dass eine Verbindung zum gesamten Unternehmesnetzwerk geöffnet wird. Dies ermöglicht es den Sicherheitsabteilungen an der digitalen Transformation teilzuhaben, anstatt ausschließlich als Verwalter wahrgenommen zu werden.[45]

Zusätzlich reduziert eine ZTA die Managementkosten, indem Anzahl und Arten von Sicherheitskontrollen verringert und somit die Anzahl der Managementkonsolen im System reduziert werden. Dies führt zu einer effizienteren Nutzung von Ressourcen und ermöglicht es den Sicherheitsmitarbeitern in einem Unternehmen, mehr Zeit für substantielle Sicherheitsaktivitäten aufzuwenden.[46]

4.3.2 Nachteile

Während die Vorteile primär auf der technischen Seite einer ZTA liegen, existieren auch Nachteile, welche auf physischer Ebene Auswirkungen zeigen. So kann sich das Einrichten einer ZTA durch das Erwerben neuer, notwendiger Werkzeuge und Technologien als

[42] Vgl. *Edo*, *O. C.* et al., 2022, S. 146.
[43] Vgl. *Shore*, *M.*, *Zeadally*, *S.*, *Keshariya*, *A.*, 2021, S. 28; Vgl. *Hunter*, *S.*, 2020.
[44] Vgl. *Shore*, *M.*, *Zeadally*, *S.*, *Keshariya*, *A.*, 2021, S. 28.
[45] Vgl. *Cunningham*, *C.*, *Pollard*, *J.*, *Holmes*, *D.*, 2019, S. 11.
[46] Vgl. ebd., S. 8.

kostenintensiv darstellen.[47] Zudem kann die Nutzererfahrung mit dem System geringwertiger als gewünscht ausfallen, da jede Anfrage eine neue Autorisierung und Authentifizierung erfordert, was besonders zu Anfängen eine nicht vernachlässigbare Zeitdauer in Anspruch nehmen kann.[48]

Darüber hinaus kann die Implementierung einer ZTA selbst komplex und zeitaufwendig sein, sowie signifikante Änderungen in bestehenden Netzwerkinfrastrukturen und Sicherheitsmaßnahmen erfordern.[49]

[47] Vgl. *Shore*, *M.*, *Zeadally*, *S.*, *Keshariya*, *A.*, 2021, S. 33.
[48] Vgl. ebd., S. 28.
[49] Vgl. *Shore*, *M.*, *Zeadally*, *S.*, *Keshariya*, *A.*, 2021, S. 33; Vgl. *Buck*, *C.* et al., 2021, S. 11.

5 Auswirkungen und Resultate von Zero-Trust

Die Implementierung einer ZTA kann tiefgreifende Auswirkungen auf die Sicherheit, Produktivität und Benutzerfreundlichkeit in Unternehmen haben. In diesem Abschnitt werden die potenziellen Auswirkungen und Resultate von ZTAs eingehend untersucht. Dabei werden die erwarteten positiven Effekte wie die Verringerung von Cyberangriffen und Datenverlusten durch striktere Überprüfung von Netzwerkzugriffen, sowie mögliche Einflüsse auf die Benutzerfreundlichkeit und Produktivität der Mitarbeiter beleuchtet.

Durch die Analyse der Auswirkungen und Resultate von Zero-Trust wird verdeutlicht, wie diese Architekturen dazu beitragen können, die Sicherheitslandschaft zu transformieren und Unternehmen zu schützen, ohne die Arbeitsabläufe zu beeinträchtigen.

5.1 Verbesserung der Sicherheitsebene

Eine ZTA trägt zur Verbesserung der Sicherheitsebene von Systemen bei, indem es einen Paradigmenwechsel in der Cybersicherheit darstellt. Das Vertrauen in Personen, Geräte und Prozesse wird wie zuvor bereits dargestellt auf ein Minimum reduziert, wodurch die Sicherheit erhöht wird.

Zudem wird das Datenbewusstsein und die Dateneinsicht in einer ZTA erhöht. Deswegen und durch die kontinuierliche Überwachung des Datenverkehrs ermöglicht es, sowohl verdächtige Verhaltensweisen und Angriffe schneller zu erkennen und zu unterbinden, als auch aus vergangenen Vorfällen Fehler zu erkennen und die bestehenden Sicherheitsmaßnahmen entsprechend anzupassen.[50] Durch Mikrosegmentierung, dem Aufteilen eines Netzwerkes in kleinere Segmente, und dem Gewähren von Zugriff ausschließlich auf die für die Anfrage benötigten Ressourcen wird sichergestellt, dass kein überflüssiger und ungewollter Datenverkehr durchgeführt wird.[51] Hierdurch wird die Anzahl der möglichen ausnutzbaren Lücken im System reduziert.

Ein nach ZT eingerichtetes Netzwerk ist außerdem weniger anfällig gegenüber Malware, da die segmentierten Bereiche des Netzwerkes es schwieriger bis unmöglich machen, die Malware im System zu verbreiten. Allein das Betreten des Netzwerkes der Malware, nachdem z. B. ein Mitarbeiter einen Phishing Link ausgeführt hat, wird erschwert, da die Daten durch die Netzwerkeinrichtung zunächst überprüft werden, bevor sie auf dem Gerät des Nutzers ankommen.[52] Bei Malware-Programmen werden entsprechende Trigger

[50] Vgl. *Cunningham*, *C.*, *Pollard*, *J.*, *Holmes*, *D.*, 2019, S. 9; Vgl. *Buck*, *C.* et al., 2021, S. 4.
[51] Vgl. *Shore*, *M.*, *Zeadally*, *S.*, *Keshariya*, *A.*, 2021, S. 30.
[52] Vgl. *Cunningham*, *C.*, *Pollard*, *J.*, *Holmes*, *D.*, 2019, S. 7.

ausgelöst, die vor dem schädlichen Datenverkehr warnen.[53] Gleichzeitig kann eine ZTA auch das Ausbreiten eines Malware-Programmes unterbinden, welches z. B. über einen korrupten USB-Stick in das System eingebracht wird, da das Programm durch die Segmentierung nur schwierig auf andere Geräte im Netzwerk übergreifen kann.[54]

5.2 Reduzierung von Angriffsflächen

Durch die Mikrosegmentierung eines Netzwerks mit einer ZTA in kleinere, isolierte Segmente werden Angriffe auf das Segment begrenzt, in dem sie stattfinden, ohne sich auf andere Segmente ausbreiten zu können. Dies reduziert das Risiko von Datenlecks und unbefugtem Zugriff.[55] Besonders gegen DDoS-Angriffe bietet eine ZTA starken Schutz, da die häufig automatisierten Angriffe durch die Mikrosegmentierung nur geringe Bereiche des Systems anwählen können.[56]

Des Weiteren trägt die Verwendung von Softwaredefinierte Perimeter (SDP) dazu bei, dass eine Black Box gebildet wird, welche die Infrastruktur und Ressourcen vor öffentlichem Zugriff verbirgt.[57]

Die Möglichkeit, allen Datenverkehr zu überwachen trägt zudem dazu bei, den von Datenausbrüchen verursachten Schaden zu begrenzen oder sogar ganz zu verhindern.[58] Viele Lösungen benötigen Wochen bis Monate, um einen Vorfall zu erkennen, sodass in vielen Fällen externe Akteure wie Kunden oder Partner die Firma über den Vorfall informieren.[59] Mit bisher genutzten Lösungen beträgt die Zeit, die es benötigt, über einen Sicherheitsvorfall benachrichtigt zu werden, im Median 78 Tage.[60]

Die Segmentierung eines Netzwerkes trägt außerdem dazu bei, der Schnelllebigkeit der Technologien und Netzwerke, sowie den Problemen beim Bearbeiten und Schützen der Schwachstellen entgegenzuwirken. So wurden zum Beispiel allein im Jahr 2018 ungefähr 16.500 Einträge der National Vulnerability Database (NVD) der USA hinzugefügt, im Jahr 2022 bereits ungefähr 25.200.[61]

---

[53] Vgl. *Cunningham*, *C.*, *Pollard*, *J.*, *Holmes*, *D.*, 2019, S. 7.
[54] Vgl. ebd., S. 7.
[55] Vgl. *Shore*, *M.*, *Zeadally*, *S.*, *Keshariya*, *A.*, 2021, S. 20; Vgl. *Buck*, *C.* et al., 2021, S. 4.
[56] Vgl. *Eidle*, *D.* et al., 2017, S. 289.
[57] Vgl. *Buck*, *C.* et al., 2021, S. 4; Vgl. *Kumar*, *P.* et al., 2019, S. 1.
[58] Vgl. *Cunningham*, *C.*, *Pollard*, *J.*, *Holmes*, *D.*, 2019, S. 6.
[59] Vgl. ebd., S. 6.
[60] Vgl. *FireEye*, 2019, S. 5.
[61] Vgl. *Cunningham*, *C.*, *Pollard*, *J.*, *Holmes*, *D.*, 2019, S. 6; Vgl. *CVE Details*, 2023.

5.3 Datenverarbeitung

5.3.1 Datenschutz

Um den Datenschutz in einem System während der Implementierung einer ZTA zu gewährleisten werden im Allgemeinen fünf Schritte vorausgesetzt. Diese sind (i) das Identifizieren der sensiblen Daten, (ii) das Erfassen des Datenflusses der sensiblen Daten, (iii) der Entwurf der ZT-Parametern, (iv) das kontinuierliche Überwachen des Systems mit Sicherheitsanalysen und (v) das Einführen der Steuerung und Automatisierung der Sicherheitsmaßnahmen.[62]

Mit diesen wird sichergestellt, dass nur direkt zusammenhängende Daten mit denselben Berechtigungen aufrufbar sind, sowie der kontinuierliche Zugriff auf die Daten während der Umstellung bereitgestellt.

5.3.2 Datenspeicherung

Zusätzlich werden in einer ZTA viele Daten, darunter auch Nutzerdaten, gespeichert, damit sichergestellt werden kann, welcher Akteur auf welche Daten, Systeme und Dienste zugreifen kann, bzw. darf. Für diese Daten wird für jeden Akteur ein Register eingerichtet, welches die folgenden Daten beinhalten kann:[63]

- die Anzahl der erfolgreichen und nicht erfolgreichen Verbindungsanfragen, sowie die Frequenz dieser;
- jeder in Anspruch genommene Dienst, der zu einer Zugriffsentscheidung führt, und für jeden dieser Dienste die Häufigkeit und Anzahl dieser Anfragen;
- jede angeforderte Datenressource, die dem Subjekt erlaubt und verweigert wurde, zusammen mit dem zugehörigen Ressourcentyp[64] und der Empfindlichkeitsstufe, der Zugriffsart[65] und die Dauer[66] sowie alle verfügbaren Daten, die den Zugriffskontext bezeichnen, wie z. B. Zeit, Ort und Systemzustand;
- die Historie aller dem Akteur entzogenen Berechtigungen;
- aktueller Satz von Akteursattributen zusammen mit jeder beobachteten Änderung dieser Eigenschaften.

[62] Vgl. *Ahmed*, *I.* et al., 2020, S. 2-3; Vgl. *Balaouras*, *S.*, *Cerrato*, *P.*, *Cunningham*, *C.*, 2018.
[63] Vgl. *Colombo*, *P.*, *Ferrari*, *E.*, *Tümer*, *E. D.*, 2021, S. 161.
[64] z. B. Datensatz, Zeilendaten, Datenstrom
[65] z. B. Lesen, Schreiben, Lesen und Schreiben
[66] z. B. sofort/kontinuierlich und die zugehörige Länge

5.4 Probleme

Abbildung 3 zeigt, welchen Problemen Unternehmen weltweit begegnen, die sie daran hindern, eine ZTA in ihrem Unternehmen einzurichten.[67]

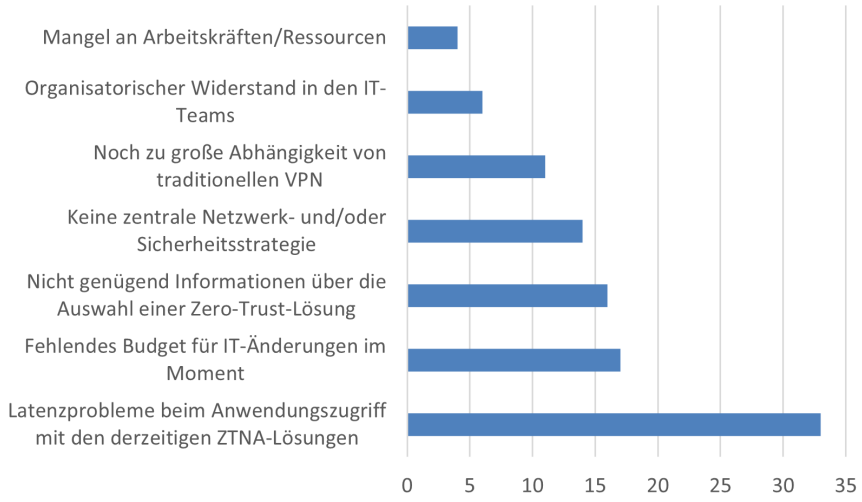


Abbildung 3: Wichtigste Herausforderungen beim Aufbau einer weltweiten Zero-Trust-Strategie im Jahr 2023
Werte in Prozent

Zusätzlich zu diesen Problemen gibt es beim Aufbau einer ZTA auch die Bedenken um die Sicherheit gespeicherter Daten, welche wie in Unterunterabschnitt 5.3.2 aufgeführt wurden, zur effektiven Zugriffsüberprüfung erforderlich sind. Jedoch ist es möglich, auch diese Daten innerhalb der ZTA zu speichern, sodass auch sie von dem Schutz des Netzwerkes profitieren. Hierbei muss allerdings beachtet werden, dass die Systeme und Akteure, die Einfluss auf die Zugriffsentscheidung über Anfragen von Systemen und Nutzern haben, auch auf die gespeicherten Daten Zugriff besitzen müssen, andernfalls bringt die Speicherung der Daten keinen Nutzen.

Darüber hinaus kann es für Unternehmen zu Problemen kommen, wenn eine ZTA eingerichtet werden soll, da die betroffenen Systeme während der Einführung nicht nutzbar sind. Da eine ZTA auch in bestehende Systeme partiell eingeführt werden kann, ist dies kein äußerst Hindernis.

5.5 Auswirkungen auf die Produktivität

Wie jede Sicherheitsmaßnahme in der Informationstechnik stellt auch ZT einen Eingriff in die Nutzerproduktivität dar. So stellten 2021 für ungefähr 22% der Arbeitnehmer in Eu-

[67] Vgl. *Fortinet*, 2023.

ropa und den USA, die Remote Work betrieben, komplexe Passwörter und Multi-Faktor-Authentifizierung (MFA)-Anforderungen und für ungefähr 25% der Arbeitnehmer ein Mangel an Single-Sign-On (SSO)-Möglichkeiten Herausforderungen dar.[68]

Die siebte Ebene des ISO/OSI-Referenzmodell befasst sich mit der Anwendung, mit welcher die Nutzer interagieren. Auf dieser Ebene findet auch die Authentifizierung der Nutzer statt, meist nur mit einem Nutzernamen und einem Passwort. Jedoch können die Authentifizierungsanforderungen an die Nutzer auch deutlich komplexer gestaltet werden, wie z. B. mit MFA-Anforderungen, oder CAPTCHA.

Während diese erweiterten Anforderungen die Authentizität des Nutzers sicherstellen, so sind sie für den Nutzer zunächst ein Eingriff in seine Produktivität und den Arbeitsfluss. Dadurch ist es notwendig, bei der Nutzerauthentifizierung eine Balance zwischen Sicherheit und Produktivität zu finden.[69]

[68] Vgl. *Citrix*, *Sapio Research*, 2021, S. 27.
[69] Vgl. *Pace*, *K. A.*, 2004, S. 7.

6 Fazit

Mit dieser Seminararbeit sollten die Auswirkungen einer ZTA auf die Sicherheit eines Systems, sowie auf den Datenverlust dargestellt werden. Mithilfe einer ausführlichen Analyse der existierenden Literatur wurden diese Auswirkungen veranschaulicht. Des Weiteren bietet diese Arbeit eine ausführliche Einführung in das Thema ZT und stellt den Aufbau einer ZTA dar.

Die Analyse der bestehenden Literatur zeigte, dass eine ZTA in verschiedenen Unternehmen weltweit bereits genutzt wird und die Auswirkungen dieser messbar sind. Besonders im Verwaltungsbereich auf Bundesebene sind ZTAs verbreitet, wie in Unterabschnitt 2.2 dargestellt wurde.

Die zentralen Auswirkungen einer ZTA, sowie das Potenzial in der weiteren Verbreitung dieser, sind eine Verringerung der Häufigkeit von Cyberangriffen und damit verbundenen Datenverlusten in Unternehmen. Dies wird durch die strikte Überprüfung von Netzwerkzugriffen bereitgestellt, wodurch eine ZTA eine robuste Sicherheitslösung darstellt. Dabei muss jedoch beachtet werden, dass eine ZTA einen Einschnitt in die Benutzerfreundlichkeit und Geschwindigkeit des Systems darstellt, da für die Überprüfungen verschiedene Daten eingegeben, gesammelt und gespeichert werden müssen. Dies stellte im Jahr 2023 für ungefähr ein Drittel der Unternehmen eine Herausforderung beim Aufbau einer ZTA dar, wie in Abbildung 3 dargestellt ist.

Zusammenfassend lässt sich in Bezug auf die Forschungsfrage „Wie trägt eine ZTA zur Erhöhung der Sicherheit in einem System unter Einbehalt von Benutzerfreundlichkeit und -produktivität bei?“ sagen, dass eine ZTA eine positive Wirkung auf die Sicherheit in einem System hat, auch wenn Einbußen in Nutzerfreundlichkeit und -produktivität beachtet werden. Damit diese zusätzlich auf einem gleichen Niveau wie vor der Einführung bleiben, müssen weiterführende Maßnahmen getroffen werden.

ZT ist ein vergleichsweise altes Konzept, die Grundlagen dafür wurden bereits in den 1990er Jahren gelegt, große Verbreitung erfährt das Konzept jedoch erst seit ein paar Jahren. Besonders Kindervag, NIST und NCSC trugen stark zur Verbreitung und Forschung an ZT bei, sodass es heute nahezu ein vollständig ausgearbeitetes Konzept ist, das Unternehmen nur noch implementieren müssen.[70]

Die vorliegende Seminararbeit hat ausschließlich die direkten Auswirkungen einer ZTA, sowie den grundlegenden Aufbau einer solchen betrachtet. In einer tiefergehenden Betrachtung kann es daher sinnvoll sein, die Interaktionen einer ZTA in Kombination mit

[70] *Kindervag*, *J.*, *Balaouras*, *S.*, *Coit*, *L.*, 2010; *Rose*, *S.* et al., 2020; *NCSC*, 2021.

anderen Sicherheitsmaßnahmen zu untersuchen. Desweiteren kann die Analyse möglicher Maßnahmen zur Steigerung der Nutzerfreundlichkeit und -produktivität in einer ZTA ein Betrachtungsmerkmal einer weiterführenden Arbeit sein.

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] (siehe S. 6)

Ahmed, *Iftekhar*, *Nahar*, *Tahmin*, *Urmi*, *Shahina Sultana*, *Taher*, *Kazi Abu* (2020): Protection of Sensitive Data in Zero Trust Model, in: Proceedings of the International Conference on Computing Advancements, ICCA 2020, Dhaka, Bangladesh: Association for Computing Machinery, 2020 (siehe S. 16)

Balaouras, *Stephanie*, *Cerrato*, *Peter*, *Cunningham*, *Chase* (2018): Five Steps To A Zero Trust Network | Forrester, o. O., 2018-10-01, URL: https://www.forrester.com/report/five-steps-to-a-zero-trust-network/RES120510 [Zugriff: 2023-12-10] (siehe S. 16)

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] (siehe S. 8)

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] (siehe S. 6)

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] (siehe S. 6)

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 (siehe S. 9, 13–15)

Bundeskriminalamt (2023): Polizeilich erfasste Fälle von Cyberkriminalität in Deutschland von 2007 bis 2022, statista, Deutschland: Statista Research Department, 2023-07-12, URL: https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2022.html [Zugriff: 2023-11-13] (siehe S. 6)

Citrix, *Sapio Research* (2021): The state of security in a hybrid world, o. O.: Citrix, 2021-10 (siehe S. 18)

Colombo, *Pietro*, *Ferrari*, *Elena*, *Tümer*, *Engin Deniz* (2021): Access Control Enforcement in IoT: state of the art and open challenges in the Zero Trust era, in: 2021 Third IEEE

International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA), o. O., 2021, S. 159–166 (siehe S. 16)

Cunningham, *Chase*, *Pollard*, *Jeff*, *Holmes*, *David* (2019): The eight business and security benefits of zero trust, Business Case: The Zero Trust Security Playbook, Englisch, in: Forrester Reseach November (2019) (siehe S. 12, 14, 15)

CVE Details (2023): Number of common IT security vulnerabilities and exposures (CVEs) worldwide from 2009 to 2023 YTD, Englisch, CVE Details, o. O.: Petrosyan, Ani und CVE Details, 2023-04, URL: https://www.statista.com/statistics/500755/worldwide-common-vulnerabilities-and-exposures/ [Zugriff: 2023-12-27] (siehe S. 15)

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/ (siehe S. 1)

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 (siehe S. 9, 11)

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 (siehe S. 8)

Edo, *Onome Christopher*, *Tenebe*, *Theophilus*, *Etu*, *Egbe-Etu*, *Ayuwu*, *Atamgbo*, *Emakhu*, *Joshua*, *Adebiyi*, *Shakiru* (2022): Zero Trust Architecture: Trend and Impact on Information Security, in: International Journal of Emerging Technology and Advanced Engineering, Bd. 12, 7, o. O., 2022-01-07, S. 140–147 (siehe S. 12)

Eidle, *Dayna*, *Ni*, *Si Ya*, *DeCusatis*, *Casimer*, *Sager*, *Anthony* (2017): Autonomic security for zero trust networks, in: 2017 IEEE 8th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON), o. O., 2017, S. 288–293 (siehe S. 15)

Fink, *Arlene* (2019): Conducting Research Literature Reviews: From the Internet to Paper, Englisch, 5. Aufl., o. O., 2019 (siehe S. 1)

FireEye (2019): M-Trends 2019, value, report, o. O.: FireEye, 2019, URL: https://www.indevis.de/file-download/download/public/2080 [Zugriff: 2023-12-27] (siehe S. 15)

Fortinet (2023): Most important challenges when building a Zero Trust strategy worldwide in 2023, Englisch, Statista Umfrage Cybersecurity & Cloud 2018, Fortinet, o. O.: Fortinet, 2023-06-14, URL: https://www.statista.com/statistics/1368077/main-challenges-when-implementing-a-zero-trust-strategy-worldwide/ (siehe S. 17)

Herzog, *Pete*, *Barceló*, *Marta*, *Dupius*, *Clement*, *Bailey*, *Don*, *Hines*, *Michael S.*, *Dominguez Torres*, *Miguel Angel*, *Urunuela*, *Angel Luis*, *Klee*, *Peter*, *Jankowski*, *Rich*, *Schallock*, *Felix*, *IP*, *Vincent* (2001): Open-Source Security Testing Methodology Manual, Englisch, hrsg. von *Simonis*, *Drew*, *Hawthorm*, *Emily K.*, *Martinez i Barrachina*,

Jordi, o. O., 2001-05-05, URL: https://cdn.preterhuman.net/texts/other/osstmm.pdf [Zugriff: 2023-12-28] (siehe S. 4)

Herzog, *Pete*, *Barceló Marta Lee*, *Robert E.* (2010): The Open source Security Testing Methodology Manual - Contemporary Security Testing and Analysis, Englisch, o. O., 2010-12-14, URL: https://www.isecom.org/OSSTMM.3.pdf [Zugriff: 2023-12-28] (siehe S. 4)

Horne, *Dwight*, *Nair*, *Suku* (2021): Introducing zero trust by design: Principles and practice beyond the zero trust hype, in: Advances in Security, Networks, and Internet of Things, Dallas, Texas, USA: Springer, 2021, S. 1–9 (siehe S. 9, 10)

IDG Network World Inc. (1994): Network World, o. O., 1994-05-23 (siehe S. 4)

IEEE Standard for Port Based Network Access Control (2001), o. O., 2001-06-16, URL: https://ieeexplore.ieee.org/servlet/opac?punumber=7449 [Zugriff: 2023-12-28] (siehe S. 4)

Kindervag, *John*, *Balaouras*, *Stephanie*, *Coit*, *Linsey* (2010): Build security into your network's dna: The zero trust network architecture, in: Forrester Research Inc, 27 (2010) (siehe S. 4, 19)

Kramer, *Simon*, *Bradfield*, *Julian C.* (2010): A general definition of malware, in: Journal in Computer Virology, 6 (2010), Nr. 2, S. 105–114 (siehe S. 8)

Kumar, *Palash*, *Moubayed*, *Abdallah*, *Refaey*, *Ahmed*, *Shami*, *Abdallah*, *Koilpillai*, *Juanita* (2019): Performance Analysis of SDP For Secure Internal Enterprises, in: 2019 IEEE Wireless Communications and Networking Conference (WCNC), o. O., 2019, S. 1–6 (siehe S. 15)

Marsh, *Stephen Paul* (1994): Formalising Trust as a Computational Concept, Englisch, Diss., o. O.: University of Stirling, 1994-04, [Zugriff: 2023-12-28] (siehe S. 4)

Pace, *Kari A.* (2004): A Layered Security Model: OSI and Information Security, in: SANS Institute Global Information Assurance Certification Paper (2004) (siehe S. 18)

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 (siehe S. 3–5, 19)

Shore, *Malcolm*, *Zeadally*, *Sherali*, *Keshariya*, *Astha* (2021): Zero Trust: The What, How, Why, and When, en, in: Computer, 54 (2021), Nr. 11, S. 26–35, [Zugriff: 2023-12-05] (siehe S. 12–15)

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/ (siehe S. 1)

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/ (siehe S. 1)

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] (siehe S. 6, 7)

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 (siehe S. 1)

zscaler (2022): Zero Trust im Rückblick: vom Whiteboard zum Weißen Haus, o. O., 2022, URL: https://www.zscaler.de/resources/infographics/brief-history-zero-trust.pdf [Zugriff: 2023-12-28] (siehe S. 3–5)

Internetquellen

Akamai (2023): Was ist Zero Trust? Zero-Trust-Sicherheitsmodell, <https://www.akamai.com/de/glossary/what-is-zero-trust> (2023) [Zugriff: 2023-11-27] (siehe S. 9)

Emerging Technology from the arXiv (2019): The first DDoS attack was 20 years ago. This is what we've learned since. | MIT Technology Review, Englisch, <https://www.technologyreview.com/2019/04/18/103186/the-first-ddos-attack-was-20-years-ago-this-is-what-weve-learned-since/> (2019-04-18) [Zugriff: 2023-12-29] (siehe S. 1)

Hunter, *S.* (2020): The five business benefits of a zero trust approach to security, <https://securitybrief.com.au/story/the-five-business-benefits-of-a-zero-trust-approach-to-security> (2020-08-19) [Zugriff: 2023-12-06] (siehe S. 12)

NCSC (2021): Device Security Guidance, Englisch, <https://www.ncsc.gov.uk/collection/device-security-guidance/infrastructure/network-architectures> (2021-06-29) [Zugriff: 2023-12-28] (siehe S. 5, 19)

Shackelford, *Scott* (2018), Englisch, <https://theconversation.com/30-years-ago-the-worlds-first-cyberattack-set-the-stage-for-modern-cybersecurity-challenges-105449> (2018-11-01) [Zugriff: 2023-12-29] (siehe S. 1)

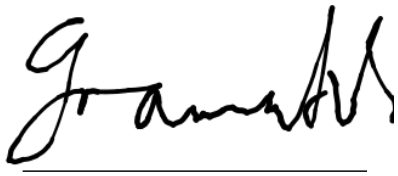
Ehrenwörtliche Erklärung

Hiermit versichere ich, dass ich die vorliegende Arbeit in allen Teilen eigenständig ohne Hilfe von Dritten angefertigt und keine anderen als die in der Arbeit angegebenen Quellen und zugelassenen Hilfsmittel verwendet habe. Sämtliche wörtlichen und sinngemäßen Übernahmen inklusive KI-generierter Inhalte sind kenntlich gemacht.

Die Arbeit habe ich in gleicher oder ähnlicher Form oder auszugsweise noch keiner Prüfungsbehörde zu Prüfungszwecken vorgelegt.

Mir ist bekannt, dass die Zuwiderhandlung gegen den Inhalt dieser Erklärung einen Täuschungsversuch darstellt, der das Nichtbestehen der Prüfung zur Folge hat.

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, 2.1.2024

(Ort, Datum)

(Eigenhändige Unterschrift)