



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 10. Dezember 2023

Inhaltsverzeichnis

Abbildungsverzeichnis	iii
Tabellenverzeichnis	iv
Abkürzungsverzeichnis	v
Glossar	vi
1 Einleitung	1
1.1 Zielsetzung	1
1.2 Aufbau der Arbeit	2
2 Grundlagen	3
2.1 Definition einer Zero-Trust-Architektur	3
2.2 Entwicklung und historischer Hintergrund	3
2.3 Prinzipien und Konzepte von Zero-Trust	3
2.4 Vergleich zu herkömmlichen Sicherheitsansätzen	4
3 Moderne Cyberbedrohungen	5
3.1 Trends in der Cyberkriminalität	5
3.2 Arten von Cyberbedrohungen	5
4 Zero-Trust Architektur im Detail	8
4.1 Komponenten und Aufbau von Zero-Trust	8
4.1.1 Komponenten einer Zero-Trust Architektur	8
4.1.2 Aufbau einer Zero-Trust Architektur	8
4.2 Implementierung von Zero-Trust in Unternehmen	10
4.3 Vor- und Nachteile von Zero-Trust	10
4.3.1 Vorteile	11
4.3.2 Nachteile	11
5 Auswirkungen und Resultate von Zero-Trust	12
5.1 Verbesserung der Sicherheitsebene	12
5.2 Reduzierung von Angriffsflächen	12
5.3 Schutz sensibler Daten	13
5.4 Probleme	13
6 Fazit	14

Abbildungsverzeichnis

Abbildung 1: Erfasste Fälle von Cyberkriminalität nach Typ	6
Abbildung 2: Anteil einzelner Cyberkriminalitätstypen	6

Tabellenverzeichnis

Abkürzungsverzeichnis

BYOD	Bring-Your-Own-Device
DDoS	Distributed Denial of Service
IoT	Internet of Things
PDP	Policy Decision Point
PEP	Policy Enforcement Point
SDP	Software-defined Perimeter
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. 8–11

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, 10, 11

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, 10

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. 10

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. Zudem ist der Anteil der Unternehmen, die von einem Cyberangriff betroffen waren, so hoch wie noch nie. 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. 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 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.¹ Darüber hinaus ist eine ZTA ein Cybersicherheitsplan einer Einrichtung, der die Konzepte von ZT umsetzt und Zugriffsrichtlinien, Arbeitsabläufe und Beziehungen zwischen Komponenten umfasst.²

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 entfernt 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.³

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,

¹ Vgl. *Rose, S. et al.*, 2020, S. 4.

² Vgl. ebd., S. 4.

³ 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.⁴

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

2.4 Vergleich zu herkömmlichen Sicherheitsansätzen

⁴ Vgl. *Rose, S. et al.*, 2020, S. 6-7.

3 Moderne Cyberbedrohungen

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.⁵

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-Dollar⁶ gekostet, was gegenüber dem Vorjahr ein Zuwachs von fast 18% darstellt.⁷ 2021 wurden so ungefähr 6,9 Milliarden Euro für IT-Sicherheitsmaßnahmen ausgegeben, was einem Zuwachs von fast 22% gegenüber dem Vorjahr entspricht,⁸ davon wurden geschätzt 1,7 Milliarden Euro für Softwarelösungen ausgegeben.⁹

Wie die Kosten und Ausgaben für Cyberkriminalität steigen auch die möglichen Methoden der Angreifer. Abbildung 1 zeigt nach den Statista Market Insights,¹⁰ dass die Anzahl der Fälle von Cyberkriminalität fast stetig zunimmt.

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 Insights¹¹ dargestellt wird.

3.2 Arten von Cyberbedrohungen - Malware, Phishing, DDoS

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

⁵ Vgl. *Bundeskriminalamt*, 2023.

⁶ Heutiger Wert ungefähr 10,23 Millionen Euro

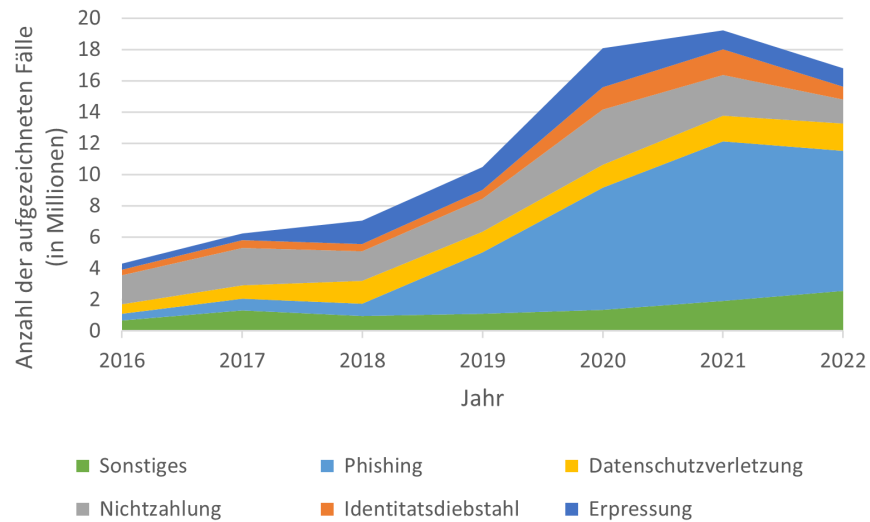
⁷ Vgl. *Accenture*, 2019.

⁸ Vgl. *Bitkom*, 2022.

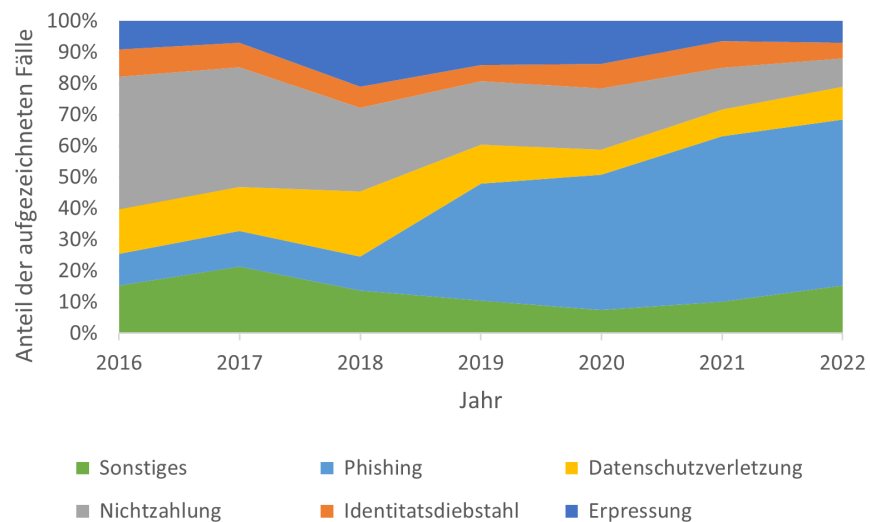
⁹ Vgl. *Bitkom*, 2020.

¹⁰ Vgl. *Statista Market Insights et al.*, 2023.

¹¹ Vgl. ebd.



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



**Abbildung 2: Anteil einzelner Cyberkriminalitätstypen.
Stand September 2023**

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.*¹²

Definition 3.2. *Malware bezeichnet eine Software, welche ausschließlich Systeme angreift, welche entweder keine anderen Systeme beschädigen, oder welche Malwaresysteme angreifen.*¹³

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 noch permanent angegriffen, es wird lediglich die Verfügbarkeit dieser Ressourcen unterbunden.*¹⁴

Diese Angriffe zielen auf verschiedene Angriffsflächen und haben verschiedene Ziele, welche das korrumpieren 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.

¹² Vgl. Bhavsar, V., Kadlak, A., Sharma, S., 2018, S. 27.

¹³ Vgl. Kramer, S., Bradfield, J. C., 2010, S. 108f.

¹⁴ Vgl. Douligieris, 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 erforderliche Sicherheit zu garantieren. Dies geschieht durch regelmäßiges Überprüfen der Authentizität und Autorisierung der Systeme.¹⁵

4.1 Komponenten und Aufbau von Zero-Trust

Jede ZTA wird durch 3 Eigenschaften definiert. Diese stellen sicher, dass (i) Auf alle Ressourcen unabhängig ihrer physischen oder logischen Position ein sicherer Zugriff erfolgen muss, (ii) Strenge Zugriffskontrollmaßnahmen bestehen, und zuletzt (iii) Jeglicher Netzwerkverkehr erfasst und aufgezeichnet wird.¹⁶

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.¹⁷ 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.¹⁸

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.¹⁹

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 Nair²⁰ dargestellten, Schritten bestehen:

¹⁵ Vgl. *D'Silva, D., Ambawade, D. D.*, 2021, S. 3.

¹⁶ Vgl. ebd., S. 2.

¹⁷ Vgl. *Buck, C. et al.*, 2021, S. 4.

¹⁸ Vgl. *D'Silva, D., Ambawade, D. D.*, 2021, S. 3.

¹⁹ **akamai:online.**

²⁰ **horne-2021.**

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

Horne und Nair stellen weiter dar, wie die einzelnen Schritte einer Überprüfung ablaufen.²¹

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.

²¹ horne-2021.

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'Silva und Ambawade²² 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.
- 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

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.

²² 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 erforderlichen Ressourcen. Dies sorgt dafür, dass ein nahezu umfassender Schutz vor Angriffen besteht, welcher besonders Sicherheitslücken in Systemen, die durch, beabsichtigte oder unbeabsichtigte, Vertrauensbrüche entstehen, angreift.²³ Zudem ist eine ZTA flexibler, was die Nutzung von Anwendungen und Geräten betrifft, da die Sicherheitsarchitektur sich nicht auf einzelne Perimeter verlassen muss.²⁴ Gleichmaßen 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.²⁵

Besonders Unternehmen, welche ihre Ressourcen primär in Cloud-Systemen verwaltet werden einfachere Prozesse in der Umwandlung auf eine ZTA haben, da die Sicherheitsprotokolle bei diesen Systemen meist flexibler einzurichten sind.

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 teuer darstellen.²⁶ Zudem ist die Nutzererfahrung mit dem System geringer als gewünscht ausfallen, da jede Anfrage eine neue Autorisierung und Authentifizierung erfordert, was besonders zu Anfängen eine nicht vernachlässigbare Zeitdauer in Anspruch nehmen kann.²⁷

Darüber hinaus kann die Implementierung einer ZTA komplex und zeitaufwendig sein, sowie signifikante Änderungen in bestehenden Netzwerkinfrastrukturen und Sicherheitsmaßnahmen erfordern.²⁸

²³ Vgl. *Edo, O. C. et al.*, 2022, S. 146.

²⁴ Vgl. *Shore, M., Zeadally, S., Keshariya, A.*, 2021, S. 28; Vgl. *Hunter, S.*, 2020.

²⁵ Vgl. *Shore, M., Zeadally, S., Keshariya, A.*, 2021, S. 28.

²⁶ Vgl. ebd., S. 33.

²⁷ Vgl. ebd., S. 28.

²⁸ 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

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 zuvor bereits dargestellt auf ein Minimum reduziert, wodurch die Sicherheit erhöht wird.

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.²⁹ 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.³⁰ Hierdurch wird die Anzahl der möglichen ausnutzbaren Lücken im System reduziert.

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.³¹ Besonders gegen DDoS-Angriffe bietet eine ZTA starken Schutz, da die meist automatisierten Angriffe durch die Mikrosegmentierung nur geringe Bereiche des Systems anwählen können.³²

Des Weiteren trägt die Verwendung von Software-defined Perimeter (SDP) dazu bei, dass eine „Black Box“ gebildet wird, welche die Infrastruktur und Ressourcen vor öffentlichem Zugriff verbirgt.³³

²⁹ Vgl. *Buck, C. et al.*, 2021, S. 4.

³⁰ Vgl. *Shore, M., Zeadally, S., Keshariya, A.*, 2021, S. 30.

³¹ Vgl. *Shore, M., Zeadally, S., Keshariya, A.*, 2021, S. 20; Vgl. *Buck, C. et al.*, 2021, S. 4.

³² Vgl. *Eidle, D. et al.*, 2017, S. 289.

³³ Vgl. *Buck, C. et al.*, 2021, S. 4; Vgl. *Kumar, P. et al.*, 2019, S. 1.

5.3 Schutz sensibler Daten

Um eine ZTA einzurichten 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.³⁴

5.4 Probleme

³⁴ Vgl. *Ahmed, I. et al.*, 2020, S. 2-3; Vgl. *Balaouras, S., Cerrato, P., Cunningham, C.*, 2018; Vgl. *Buck, C. et al.*, 2021, S. 4; Vgl. *Kumar, P. et al.*, 2019, S. 1.

6 Fazit

Literaturverzeichnis

- Accenture* (2019): Schätzung der urchschnittlichen Kosten durch Cyberkriminalitäts-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]
- 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
- 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]
- 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]
- 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

Edo, Onome Christopher, Tenebe, Theophilus, Etu, Egbe-Etu, Ayuwu, Atamgbo, Emakhu, Joshua, Adebisi, 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

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

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

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

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>

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]

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]

Internetquellen

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]

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 und daneben strafrechtlich gem. § 156 StGB verfolgt werden kann. Darüber hinaus ist mir bekannt, dass ich bei schwerwiegender Täuschung exmatrikuliert und mit einer Geldbuße bis zu 50.000 EUR nach der für mich gültigen Rahmenprüfungsordnung belegt werden kann.

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, 10.12.2023

(Ort, Datum)



(Eigenhändige Unterschrift)