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	28. Dezember 2023

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungsverzeichnis

BYOD	Bring-Your-Own-Device
DDoS	Distributed Denial of Service
IoT	Internet of Things
NVD	National Vulnerability Database
PDP	Policy Decision Point
PEP	Policy Enforcement Point
SDP	Softwaredefinierte 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. 8–10, 12

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, 12

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 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.[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-Dollar[6] 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 Insights[11] 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.

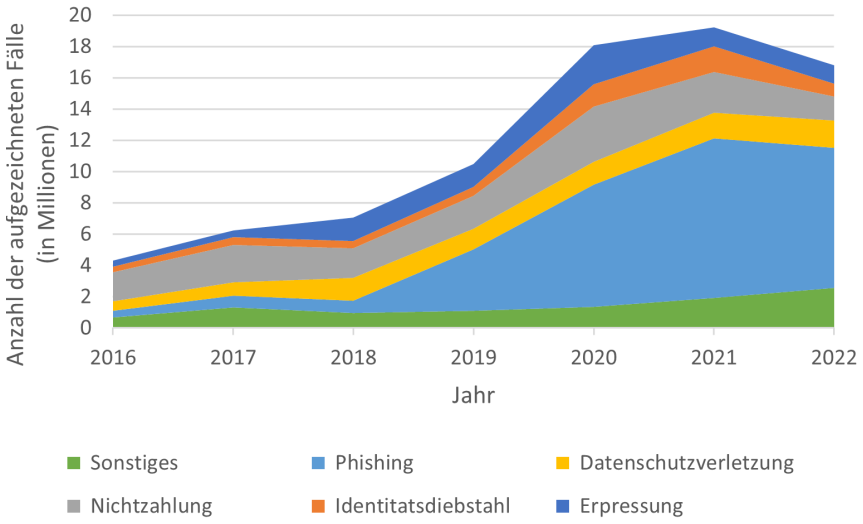

Abbildung 1: Erfasste Fälle von Cyberkriminalität nach Typ. Stand September 2023

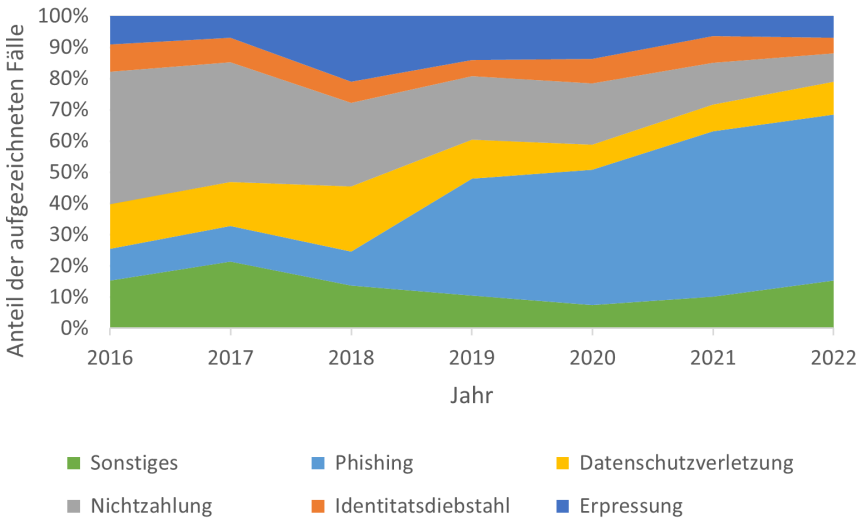

Abbildung 2: Anteil einzelner Cyberkriminalitätstypen. Stand September 2023

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 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.

[12] Vgl. *Bhavsar*, *V.*, *Kadlak*, *A.*, *Sharma*, *S.*, 2018, S. 27.
[13] Vgl. *Kramer*, *S.*, *Bradfield*, *J. C.*, 2010, S. 108f.
[14] 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.[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 Nair dargestellten, Schritten bestehen:[20]

[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] Vgl. *Akamai*, 2023, Was sind die Komponenten von Zero Trust.
[20] 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:[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] 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:[22]

- 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 erforderten 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] 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.[25]

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 Sicherheitsab teilungen an der digitalen Transformation teilzuhaben, anstatt ausschließlich als Verwalter wahrgenommen zu werden.[26]

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.[27]

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

[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. *Cunningham*, *C.*, *Pollard*, *J.*, *Holmes*, *D.*, 2019, S. 11.
[27] Vgl. ebd., S. 8.

teuer darstellen.[28] 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.[29]

Darüber hinaus kann die Implementierung einer ZTA komplex und zeitaufwendig sein, sowie signifikante Änderungen in bestehenden Netzwerkinfrastrukturen und Sicherheitsmaßnahmen erfordern.[30]

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.

Zudem wird das Datenbewusstsein und die Dateneinsicht in einer ZTA erhöht. Hierdurch 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.[31] 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.[32] 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.[33] Bei Malware-Programmen werden entsprechende Trigger

[28] Vgl. *Shore*, *M.*, *Zeadally*, *S.*, *Keshariya*, *A.*, 2021, S. 33.
[29] Vgl. ebd., S. 28.
[30] Vgl. *Shore*, *M.*, *Zeadally*, *S.*, *Keshariya*, *A.*, 2021, S. 33; Vgl. *Buck*, *C.* et al., 2021, S. 11.
[31] Vgl. *Cunningham*, *C.*, *Pollard*, *J.*, *Holmes*, *D.*, 2019, S. 9; Vgl. *Buck*, *C.* et al., 2021, S. 4.
[32] Vgl. *Shore*, *M.*, *Zeadally*, *S.*, *Keshariya*, *A.*, 2021, S. 30.
[33] Vgl. *Cunningham*, *C.*, *Pollard*, *J.*, *Holmes*, *D.*, 2019, S. 7.

ausgelöst, die vor dem schädlichen Datenverkehr warnen.[34] 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.[35]

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.[36] Besonders gegen DDoS-Angriffe bietet eine ZTA starken Schutz, da die meist automatisierten Angriffe durch die Mikrosegmentierung nur geringe Bereiche des Systems anwählen können.[37]

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.[38]

Die Möglichkeit, allen Datenverkehr zu überwachen trägt zudem dazu bei, den Schaden, den Datenausbrüche verursachen, zu begrenzen oder sogar ganz zu verhindern.[39] 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.[40] Mit bisher genutzten Lösungen beträgt die Zeit, die es benötigt wird, über einen Sicherheitsvorfall benachrichtigt zu werden, im Median 78 Tage.[41]

Die Segmentierung eines Netzwerkes trägt außerdem dazu, der Schnelllebigkeit der Technologien und Netzwerke, sowie den Problemen beim Bearbeiten und Schützen der Schwachstellen entgegenzuwirken. So wurden zum Beispiel im Jahr 2018 allein wurden ungefähr 16.500 Einträge der National Vulnerability Database (NVD) der USA hinzugefügt, im Jahr 2022 bereits ungefähr 25.200.[42]

[34] Vgl. *Cunningham*, *C.*, *Pollard*, *J.*, *Holmes*, *D.*, 2019, S. 7.
[35] Vgl. ebd., S. 7.
[36] Vgl. *Shore*, *M.*, *Zeadally*, *S.*, *Keshariya*, *A.*, 2021, S. 20; Vgl. *Buck*, *C.* et al., 2021, S. 4.
[37] Vgl. *Eidle*, *D.* et al., 2017, S. 289.
[38] Vgl. *Buck*, *C.* et al., 2021, S. 4; Vgl. *Kumar*, *P.* et al., 2019, S. 1.
[39] Vgl. *Cunningham*, *C.*, *Pollard*, *J.*, *Holmes*, *D.*, 2019, S. 6.
[40] Vgl. ebd., S. 6.
[41] Vgl. *FireEye*, 2019, S. 5.
[42] Vgl. *Cunningham*, *C.*, *Pollard*, *J.*, *Holmes*, *D.*, 2019, S. 6; Vgl. *CVE Details*, 2023.

5.3 Schutz sensibler Daten

Eventuell subsection „Datenverarbeitung“ nennen und zwei subsubsections zu „Datenschutz“ und „Datenspeicherung“ schreiben?

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.[43]

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:[44]

- 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 Subjet erlaubt und verweigert wurde, zusammen mit dem zugehörigen Ressourcentyp[45] und der Empfindlichkeitsstufe, der Zugriffsart[46] und die Dauer[47] 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.

5.4 Probleme

Abbildung 3 zeigt, welchen Problemen Unternehmen weltweit begegnen, die sie daran hindern, eine ZTA in ihrem Unternehmen einzurichten.[48]

[43] Vgl. *Ahmed*, *I.* et al., 2020, S. 2-3; Vgl. *Balaouras*, *S.*, *Cerrato*, *P.*, *Cunningham*, *C.*, 2018.
[44] Vgl. *Colombo*, *P.*, *Ferrari*, *E.*, *Tümer*, *E. D.*, 2021, S. 161.
[45] z. B. Datensatz, Zeilendaten, Datenstrom
[46] z. B. Lesen, Schreiben, Lesen und Schreiben
[47] z. B. sofort/kontinuierlich und die zugehörige Länge
[48] Vgl. *Fortinet*, 2023.

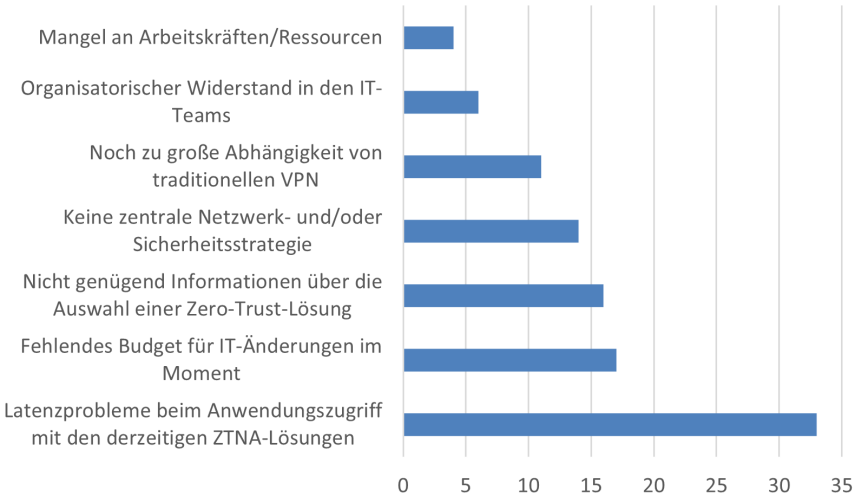

Abbildung 3: Wichtigste Herausforderungen beim Aufbau einer weltweiten Zero-Trust-Strategie im Jahr 2023
Werte in Prozent

Zusätzlich zu diesen Problemen gibt es beim Aufbau einer ZTA auch die Bedenken um die Sicherheit gespeicherter Daten, welche wie in Unterabschnitt 5.3 aufgeführt wurden zur effektiven Zugriffsüberprüfung erforderlich sind.

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]

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]

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

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)

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]

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*, *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

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

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]

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/

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

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

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

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, 28.12.2023

(Ort, Datum)

(Eigenhändige Unterschrift)