Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Finanzdepartement EFD

Nationales Zentrum für Cybersicherheit NCSC
Informatiksicherheit SEC

26. Juli 2023

Technologiebetrachtung

«Zero Trust»-Prinzip

1 Einführung

In seinen Grundsätzen und Prinzipien verweist Kapitel 3 Absatz 3 der Si001 [1] auf das «Zero Trust»-Prinzip, das sich zwar nicht präzis definieren, aber wenigstens dahingehend umschreiben lässt, dass «das Sicherheitsdispositiv eines Schutzobjekts wenn möglich so gestaltet sein sollte, dass die Sicherheitsanforderungen […] autonom erfüllt werden können und das Objekt so von seiner Umgebung isoliert und abgeschottet ist, dass minimale Annahmen über die Sicherheit der Umgebung gemacht werden müssen.» Dabei beziehen sich die Sicherheitsanforderungen auf die in [1] genannten, sind aber grundsätzlich beliebig.

Im Rahmen dieser Technologiebetrachtung wird der Hintergrund des «Zero Trust»-Prinzips erörtert, die Möglichkeiten und Risiken aufgezeigt, sowie Schlussfolgerungen gezogen und ein Ausblick gegeben. Da es sich bei «Zero Trust» nicht um ein auf die Bundesverwaltung beschränktes Thema handelt, beziehen sich die Ausführungen zunächst einmal auf den allgemeinen Fall einer modernen IT-Infrastruktur bzw. -Landschaft, wie sie auch ausserhalb der Bundesverwaltung auftreten und im Einsatz stehen kann. Erst am Schluss werden die Implikationen auf die Situation und das Zonenmodell der Bundesverwaltung skizziert.

2 Hintergrund

Das «Zero Trust»-Prinzip bzw. -Modell ist aus der Erkenntnis heraus entstanden, dass sich IT-Infrastrukturen bzw. -Landschaften im Laufe der Zeit grundlegend verändert haben und sich heute nur noch schwer mit Hilfe von physischen und/oder logischen Perimetern abschotten bzw. schützen lassen. Exemplarisch für diese Veränderungen sind in Abbildung 1 die physischen und logischen Perimeter für ein Rechenzentrum (a), eine typische Client-/Server-Architektur (b) und Cloud Computing (c) dargestellt. Man beachte, dass sich zunehmend viele (Client- und Server-) Systeme ausserhalb der Perimeter befinden und der entsprechende Perimeterschutz zunehmend an Bedeutung verliert. Das gilt sowohl für den logischen Perimeter als auch in verstärktem Masse für den physischen Perimeter. Heute sind grosse Teile der IT dezentral organisiert und umfassen viele Endgeräte in allen möglichen Formfaktoren, wie z. B. Arbeitsplatzrechner, Laptops, Tablets und Smartphones. Entsprechend wird es für eine Organisation immer schwieriger, die Grenzen ihrer IT-Infrastruktur und damit auch ihre Perimeter festzulegen. Begriffe wie «Deperimeterisierung[1]» und zunehmen-

[1] https://collaboration.opengroup.org/jericho/commandments_v1.2.pdf

de Schwierigkeiten beim Betrieb von Perimeter-basierten Sicherheitstechnologien, wie z. B. Firewalls und Proxy-Server, zeugen von dieser Entwicklung und stellen bereits heute eine grosse Herausforderung dar.

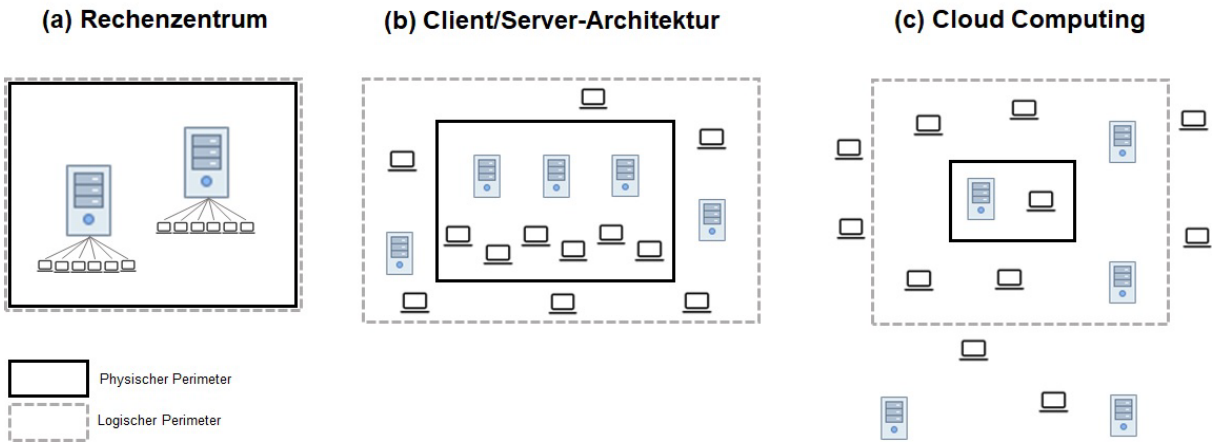

Abbildung 1: Veränderte IT-Infrastrukturen bzw. -Landschaften

Ohne definierten Perimeter müssen sowohl die Endgeräte als auch die diensterbringenden Server-Systeme in der Lage sein, sich gegenseitig zu authentifizieren und zu beweisen, dass sie zugelassen sind, bzw. sich mit Hilfe geeigneter Sicherheitstechnologien selbst zu schützen. Für BYOD-Umgebungen bedingt dies unter anderem auch den Einsatz von komplementären Sicherheitstechnologien, wie z. B. Agenten oder Mobile Device Management (MDM) Lösungen. Vor diesem Hintergrund hat 2009 John Kindervag mit seinem damaligen Team bei Forrester Research das «Zero Trust»-Modell postuliert [For10]. Während es bei diesem Modell ursprünglich um eine Verminderung der von Insidern ausgehenden Sicherheitsrisiken gegangen ist, stehen heute die Erkennung und Vermeidung von sogenannten «Lateral Movements» im Zentrum. Damit sind Vorgehensweisen eines Angreifers gemeint, mit denen er oder sie versucht, nach einem initialen Eindringen in ein Netzwerk weiter vorzudringen und weitere Konti zu kompromittieren, um seine oder ihre Zugriffsberechtigungen sukzessive zu erhöhen und das angegriffene Netzwerk letztlich zu kontrollieren.

Das «Zero Trust»-Modell basiert auf grundlegenden Konzepten und Prinzipien der IT-Sicherheit, wie beispielsweise, (i) dass auf Ressourcen unabhängig von deren Örtlichkeit nur sicher zugegriffen werden darf, (ii) dass die Zugriffskontrolle dem «Least Privilege»-Prinzip (vgl. Si001 Kapitel 3 Absatz 6) folgen muss, und (iii) dass sämtlicher Datenverkehr im Hinblick auf Sicherheitsrelevanz inspiziert und gegebenenfalls auch aufgezeichnet werden muss. Damit stellt es weniger ein konkretes Architekturmodell dar, als vielmehr ein neuer Denkansatz, der auf den Selbstschutz von IT-Ressourcen abzielt und ohne Perimeterschutz auskommen muss. Auch wenn in diesem Zusammenhang zuweilen von einem «Paradigmenwechsel» gesprochen wird, scheint dieser Begriff ein bisschen weit hergeholt. Geeigneter erscheint auf jeden Fall die Bezeichnung von «Zero Trust» als Prinzip. Dabei könnte man anstelle von «Zero Trust» auch von «Trust Establishment» sprechen, weil es letztlich um den Aufbau von Vertrauen und entsprechenden Vertrauensbeziehungen geht. Dabei sind zusätzlich und vermehrt auch dynamische Aspekte mit zu berücksichtigen. So reicht es z. B. im Rahmen einer Authentifikation nicht aus, die Kommunikationspartner zu Beginn einer Session zu authentifizieren, sondern die ausgetauschten Daten selbst müssen auch authentifiziert werden. In jedem Fall muss die Berücksichtigung von dynamischen Aspekten von kompetenten Mitarbeiterinnen und Mitarbeitern eines Security Operations Center (SOC) betreut und begleitet werden.

Auf der Grundlage des von Forrester Research vorgeschlagenen «Zero Trust»-Modells hat das U.S. amerikanische National Institute of Standards and Technology (NIST) verschiedene

Möglichkeiten aufgezeigt, wie eine Zero-Trust-Architektur (ZTA) umgesetzt werden kann [NIST20]. Eine ZTA sieht auf der Kontrollebene Policy Decision Points (PDPs) und auf der Datenebene Policy Enforcement Points (PEPs) vor und geht mit Konzepten einher, wie Mikrosegmentierung und Mikroperimeterisierung, sowie Enhanced Identity Governance (EIG). Konkret bedeutet das, dass Sicherheitsfunktionen nicht mehr zentral auf einem Perimeter, sondern dezentral und nahe an den Schutzobjekten implementiert sind. Symptomatisch für diesen Architekturansatz (und EIG) ist auch die plakative Aussage zu werten, dass die Identitäten der neue Perimeter sind.

3 Möglichkeiten und Risiken

Dem «Zero Trust»-Prinzip folgend muss ein Schutzobjekt so konzipiert sein, dass es sich selbst gegen Angriffe schützen und nicht autorisierte Zugriffsversuche abwehren kann. Aus sicherheitstechnischer Sicht ist das auch deshalb sinnvoll, weil es bei einer vom Schutzobjekt selbst vorgenommenen Sicherheitsprüfung grundsätzlich auch weniger Umgehungsmöglichkeiten gibt. Dafür geht das Ganze auf Kosten der Performanz und Skalierbarkeit. In der Tat sind Perimeter-basierte Sicherheitstechnologien gerade deshalb entworfen und breit umgesetzt worden, weil man damit die Sicherheitsfunktionen und deren Implementierung gerade auf ein paar wenige (zentrale) Systeme konzentrieren kann, und alle anderen Systeme sich um diese Funktionen nicht sorgen müssen. Diesen Vorteil muss man beim Einsatz von «Zero Trust» aufgeben.

Die Möglichkeiten, die sich aus dem «Zero Trust»-Prinzip und den in [NIST20] ausgeführten Umsetzungsvarianten einer ZTA ergeben, bestehen in der Vereinfachung und Entschlackung von Netzwerkstrukturen und entsprechenden Zonierungen. Aufgrund der Tatsache, dass es in einer eigentlichen ZTA keine Perimeter mehr gibt, entfällt auch die Notwendigkeit, IT-Ressourcen als «intern» oder «extern» zu klassifizieren. Stattdessen werden alle Ressourcen in dem Sinne gleichbehandelt, als sie selbst für die Erbringung von Sicherheitsfunktionen und -diensten besorgt sein müssen. Diese Funktionen und Dienste können immer noch zentral erbracht werden, ihr Bezug ist aber dezentral organisiert und kann im Einzelfall diskutiert werden. So werden z. B. Authentifikationsdienste immer noch sinnvollerweise zentral erbracht, während z. B. Autorisationsdienste eher dezentral erbracht und vielleicht nur noch zentral koordiniert werden müssen (dieser Ansatz liegt z. B. auch dem Authentifikations- und Schlüsselverteilsystem Kerberos zugrunde). Es resultiert eine grössere Gestaltungsfreiheit und mehr Flexibilität. Als Kehrseite der Medaille ergeben sich die hauptsächlichen Risiken, dass eigentlich erforderliche Sicherheitsfunktionen und -dienste nicht oder nur unzureichend erbracht werden können. Ob das für ein Schutzobjekt tragbar ist, muss im Einzelfall aufgrund des Schutzbedarfs des Objektes entschieden werden.

4 Schlussfolgerungen und Ausblick

Während man in der IT-Sicherheit in der Vergangenheit sehr stark auf Perimeterschutz und entsprechende Zentralisierung von IT-Sicherheitsfunktionen gesetzt hat, erleben wir seit einiger Zeit im Rahmen von «Zero Trust» und ZTAs einen starken Trend zur Dezentralisierung und zu neuen «Trust Establishment»-Methoden. Glücklicherweise schliessen sich Perimeter-basierte Sicherheitstechnologien und «Zero Trust» nicht aus, d. h. bestimmte Sicherheitstechnologien lassen sich immer noch auf einem Perimeter (zentral) realisieren, während sich andere Sicherheitstechnologien eher (dezentral) auf oder in der Nähe der Schutzobjekten realisieren lassen. Insofern stellt auch das «Zero Trust»-Prinzip kein Allerheilmittel dar, das immer und in jedem Fall sinnvoll ist und eingesetzt werden muss. Stattdessen kann es sinnvoll dosiert in bestimmten Situationen eingesetzt werden, um ein Sicherheitsdispositiv insgesamt zu verbessern.

In der Bundesverwaltung kann es z. B. sinnvoll sein, die Anforderung S1 der Si001 [1] dahingehend aufzuweichen, dass ein IT-System nicht mehr zwangsläufig «einer Zone zugehören und gemäss der entsprechenden Zonenpolicy betrieben werden» muss, sondern alternativ dazu auch dem «Zero Trust»-Prinzip folgend für die Umsetzung der Sicherheitsdienste selbst besorgt sein kann. Das ist z. B. dann sinnvoll, wenn IT-Systeme oder Anwendungen in einer Public Cloud betrieben werden. Allerdings muss noch analytisch und/oder empirisch geprüft werden, ob in einer solchen Umgebung die Umsetzung von «Zero Trust» als neue Methode zum «Trust Establishment» überhaupt umgesetzt werden kann und wirksam ist. Dazu sind natürlich auch Erfahrungswerte in- und ausserhalb der Bundesverwaltung erforderlich.

Abkürzungen

BYOD	Bring Your Own Device
EIG	Enhanced Identity Governance
IT	Informationstechnologie
MDM	Mobile Device Management
NIST	National Institute of Standards and Technology
PDP	Policy Decision Point
PEP	Policy Enforcement Point
SOC	Security Operations Center
ZTA	Zero-Trust Architektur

Referenzen

[Si001] NCSC, Si001 – IT-Grundschutz in der Bundesverwaltung, Version 5.0 vom 1. März 2022

[For10] Forrester Research, «No More Chewy Centers: Introducing The Zero Trust Model Of Information Security», 2010

[NIST20] NIST Special Publication 800-207, Zero-Trust Architecture, August 2020