



Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital • Sicher • BSI •



*Zero Trust:
Ein ganzheitlicher
Sicherheitsansatz*

Zero Trust

Der gestiegene Vernetzungsbedarf durch Homeoffice, Clouds, oder Bring Your Own Device-Konzepte bringt den klassischen Perimeterschutz an seine Grenzen. Zero Trust beschreibt einen modernen, ganzheitlichen Ansatz zur Absicherung von internen sowie externen Zugriffen unter Berücksichtigung aller Entitäten einer IT-Infrastruktur.

Die 3 wichtigsten Aspekte von Zero Trust:



Authentifizierung und
Autorisierung jedes Zugriffs
auf jegliche Ressourcen



Einhaltung des Least
Privilege Prinzips für alle
Entitäten



Protokollierung, Monitoring und
Analyse sämtlicher Aktivitäten
und falls nötig das sofortige Er-
greifen von Gegenmaßnahmen

Aspekte von Zero Trust

7 Schritte zur Umsetzung von Zero Trust

1. Identifizieren und priorisieren Sie alle Geschäftsprozesse Ihrer Organisation

Für Zero Trust wird dabei eine deutlich differenziertere Ausarbeitung der Geschäftsprozesse benötigt, als sie zumeist vorliegt, da Zero Trust in jeden Geschäftsprozess einfließen muss. 70-80% der Umsetzung von Zero Trust finden vor einer IT-technischen Realisierung in der Organisation statt.

2. Identifizieren Sie alle involvierten Parteien innerhalb Ihrer Organisation

Welche Organisationseinheiten sind in die jeweiligen Geschäftsprozesse involviert? Die Antwort liefert auch die Rollen, welche später als Grundlage für die Zugriffsentscheidungen des Policy Decision Points gegenüber konkreten Entitäten dienen.

3. Identifizieren Sie weitere Vorgaben

Welche Gesetze, Verordnungen oder anderen Rechtseinflüsse könnten Einfluss auf die umzusetzenden Maßnahmen bzw. deren Reihenfolge haben?

4. Identifizieren Sie alle involvierten Ressourcen (v.a. Daten, Systeme, Anwendungen) Ihrer Organisation

Nach der Erarbeitung der Geschäftsprozesse müssen aus diesen die involvierten Ressourcen abgeleitet werden.

5. Formulieren Sie Sicherheitsrichtlinien, die die Zero Trust Maßnahmen enthalten.

Diese Richtlinien bilden den Rahmen für das Zusammenspiel von Entitäten, Berechtigungen und Ressourcen. Dies ist unabhängig von der technischen Umsetzung.

6. Erkunden Sie den Markt

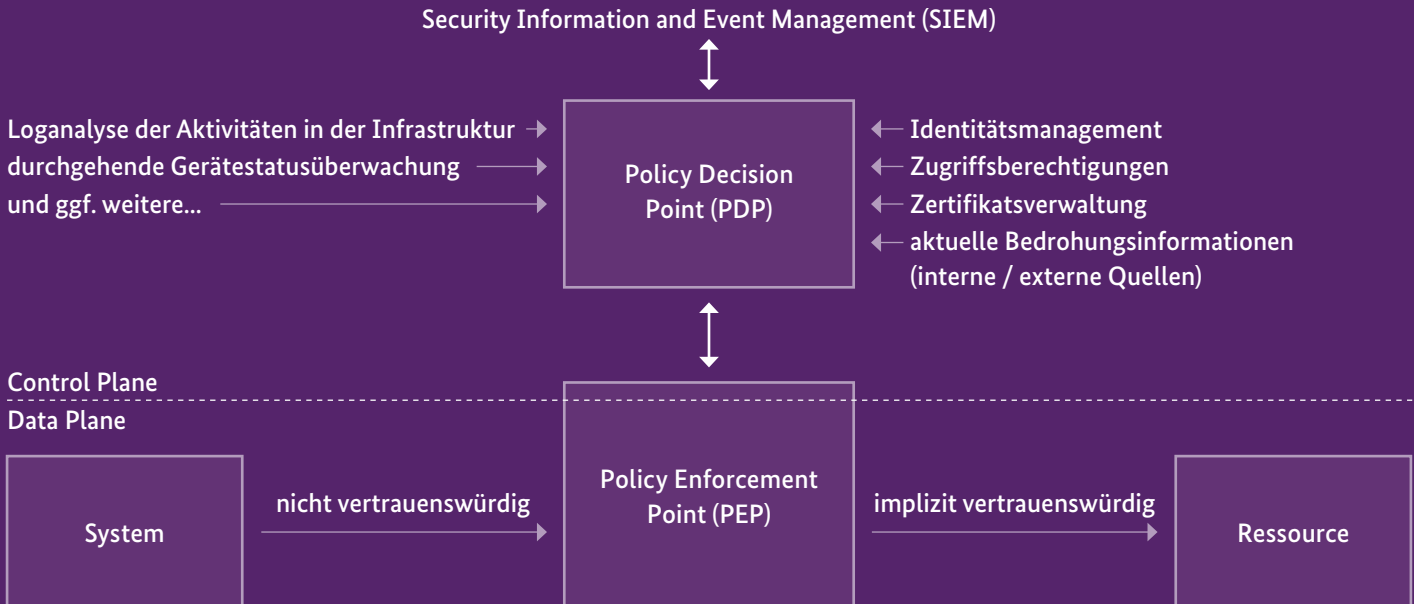
Ein ganzheitlicher Einsatz von Zero Trust macht eine umfassende Markterkundung nach geeigneten Produkten nötig, denn vorhandene Produkte umfassen nicht alle Zero Trust Funktionen. So ist zu Beginn detailliert zu prüfen, ob bestimmte Produkte überhaupt in einem Zusammenwirken einen ausreichenden Erfolg versprechen. Herstellerspezifische Kernkompetenzen können eventuell nur Teile des Gesamtbedarfes abdecken.

7. Priorisieren Sie die Umsetzung

Bei der Priorisierung von Maßnahmen sollte berücksichtigt werden, dass diese nachhaltig zum Zero Trust Modell beitragen, indem grundlegende Funktionen bereitgestellt werden.



Logische Musterarchitektur nach Zero Trust Prinzipien



Weitere Informationen
auf der BSI-Webseite

Impressum

Bundesamt für Sicherheit
in der Informationstechnik
Postfach 20 03 63
53133 Bonn
Tel.: 0800 274 1000
E-Mail: bsi@bsi.bund.de
www.bsi.bund.de

Bildnachweis

AdobeStock / ArtemisDiana

Stand

Oktober 2023