BWCAMPUSNETZ

Zukunftsfähige Konzepte für die Campusnetze
an Universitäten und Hochschulen

Grundlagen des Zero-Trust-Ansatzes und Fallstudie am Beispiel des Netzwerks der Universität Mannheim

Federführung bei der Erstellung dieses Dokuments: Universität Mannheim
Kontakt: team@bwcampusnetz.de

1 Einführung

Der Zero-Trust-Ansatz ist eine umfassende Sicherheitsstrategie, deren Grundidee ist, dass keiner Entität (Device, System, ...) innerhalb oder außerhalb des Netzwerks grundsätzlich vertraut wird. Stattdessen wird jeder Entität eine Überprüfung und Authentifizierung auferlegt. Das Zero Trust Modell basiert auf den folgenden Prinzipien:

1. **Vertrauen nicht voraussetzen (Never Trust, Always Verify)**: Im Zero-Trust-Modell wird keiner Entität grundsätzlich vertraut, unabhängig von ihrem Standort oder ihrer Position im Netzwerk. Stattdessen erfolgt immer eine Überprüfung, bevor Zugriff gewährt wird.

2. **Minimale Berechtigungen (Least Privilege)**: Benutzer und Systeme erhalten nur die minimalen Berechtigungen, die für ihre spezifischen Aufgaben erforderlich sind. Dies reduziert das Risiko von Missbrauch oder unbefugtem Zugriff.

3. **Mikrosegmentierung**: Das Netzwerk wird in kleine, isolierte Segmente aufgeteilt, um den Datenverkehr zu beschränken und die Ausbreitung von Angriffen zu minimieren. Dies hilft, die Auswirkungen von Sicherheitsverletzungen zu begrenzen.

4. **Kontinuierliche Überwachung (Continuous Monitoring)**: Ein kontinuierlicher Überwachungsansatz wird implementiert, um den Netzwerkverkehr, Benutzeraktivitäten und Systemzustände in Echtzeit zu überwachen. Dies ermöglicht eine frühzeitige Erkennung von Anomalien oder verdächtigem Verhalten.

5. **Sicherheitsrichtlinien durchsetzen (Enforce Security Policies)**: Klare Sicherheitsrichtlinien werden festgelegt und durchgesetzt, um sicherzustellen, dass ihnen sämtliche Aktivitäten im Netzwerk entsprechen.

Durch die Implementierung des 5-Säulen-Modells strebt Zero Trust an, eine robuste und durchgängige Sicherheitsarchitektur zu schaffen. Eine zentrale Rolle hierbei spielt die Identität. Sie bildet die Basis für die rollenbasierte Zugriffskontrolle.

2 Zero Trust Best Practices Paper des BSI

Das Positionspapier „Zero Trust“ des Bundesamts für Sicherheit in der Informationstechnik (BSI) aus dem Jahr 2023 bietet Leitlinien für die Implementierung von Zero-Trust-Architekturen. Es bietet eine umfassende Übersicht über die Prinzipien des Zero Trust-Ansatzes, die verschiedenen Implementierungsstufen sowie praktische Empfehlungen für Organisationen, die ihre Sicherheitsarchitekturen entsprechend modernisieren möchten. Weitere Informationen sind im vollständigen Positionspapier „Zero Trust“ des BSI von 2023 zu finden. [1]

3 Identitäten an der Universität

In einem Campus existiert üblicherweise eine eindeutige Identität für jeden Nutzenden, hier als Uni-ID bezeichnet. Jedem wird eine eindeutige Uni-ID beim Eintritt in die Universität, sei es als Studierende oder als Mitarbeitende, zugeordnet. Um die Uni-ID für Zero Trust nutzen zu können, ergeben sich die folgenden Anforderungen:

1. **Authentifizierung und Mehr-Faktor-Authentifizierung (MFA)**: Es muss sichergestellt werden, dass alle mit ihrer Uni-ID stark authentifiziert werden. Mehr-Faktor-Authentifizierung sollte genutzt werden, um die Sicherheit zu erhöhen, soweit sie bereitgestellt wird.

2. **Benutzer- und Geräteidentifikation**: Es sollte sicherstellt werden, dass die Uni-ID eindeutig mit der Nutzenden verknüpft ist. Auch die zugeordneten Geräte sollten zumindest erfasst werden. Mehr ist mit der allgemein üblichen BYOD-Policy nicht zu vereinbaren.

3. **Zugriffskontrolle basiert auf Verantwortlichkeiten**: Den Uni-IDs sind einzelne Attribute zugeordnet, bspw. können Zugehörigkeiten zu Mitarbeitenden, Studierenden oder bestimmten Instituten abgebildet werden. Hieraus werden zukünftig Flavours generiert. Klare Zugriffsrechte basierend auf den Rollen und Verantwortlichkeiten der Nutzenden müssen festgelegt werden.

4. **Gerätesicherheit**: Der Zustand der Endgeräte soll mit einfließen. Durch (aktuell geplante) Endpunktverwaltung kann festgestellt werden, ob Endgeräte von Nutzenden (Uni-IDs) sicher konfiguriert sind, also bspw. alle benötigten Patches installiert sind und keine verbotene Software enthalten ist. Nur diese Geräte dürfen auf besonders sensible Services und Inhalte zugreifen, d.h. dürfen in diese speziellen Netzsegmente eine Verbindung herstellen.

5. **Überwachung und Protokollierung**: Die Aktivitäten von Entitäten sollten überwacht, relevante Ereignisse protokolliert und Warnungen für verdächtige Aktivitäten eingerichtet werden. Dies geschieht üblicherweise durch eine Logfile-Auswertung.

6. **Sicherheitsbewusstsein der User**: Alle Nutzenden sollten hinsichtlich Sicherheitsbewusstsein geschult werden, insbesondere bezogen auf den Schutz ihrer Uni-IDs. Sensibilisierung für Phishing-Attacken und andere Sicherheitsbedrohungen sind essentielle präventive Maßnahmen. Dies findet üblicherweise bereits durch die Informationssicherheit der Universität statt und spielt unabhängig von dem Einsatz von Zero Trust eine wichtige Rolle.

7. **Regelmäßige Sicherheitsprüfungen und Audits**: Regelmäßige Sicherheitsprüfungen und Audits sollten durchgeführt werden, um sicherzustellen, dass die Sicherheitsrichtlinien effektiv umgesetzt werden und potenzielle Schwachstellen identifiziert und behoben werden können.

Im Folgenden werden die Punkte 5 bis 7 als gegeben vorausgesetzt und werden nicht weiter betrachtet, da sie den Rahmen einer eher technischen Darstellung einer Zero-Trust-Lösung sprengen.

4 Konzept zur Einführung der Zero-Trust-Architektur

Die geplante Zero-Trust-Architektur orientiert sich an dem Positionspapier „Zero Trust“ des BSI. Der gewählte Ansatz ist, die Referenzarchitektur nach NIST (aus dem BSI Positionspapier „Zero Trust“) umzusetzen. Dieser sieht wie folgt aus:

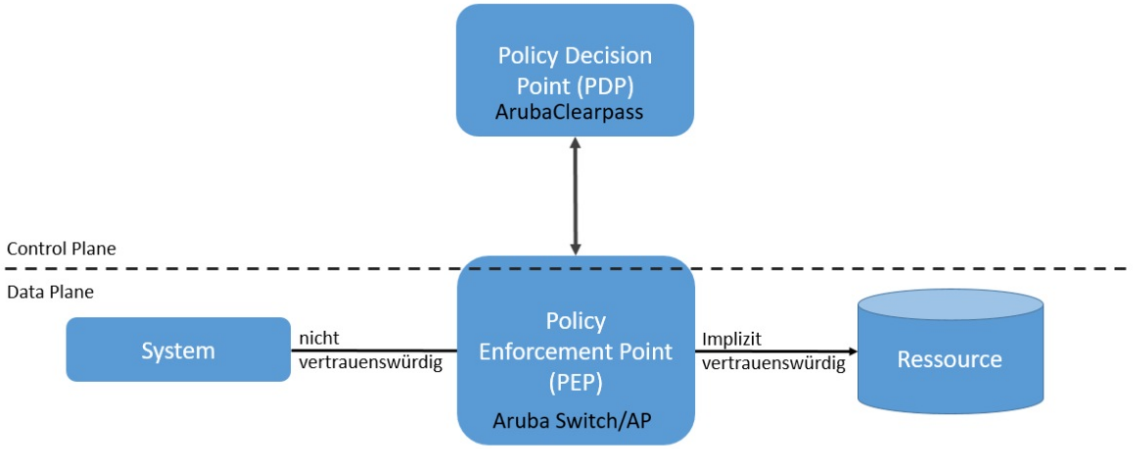

Abb. 4.1: Referenzarchitektur nach NIST

Der Proof of Concept erfolgte mit Hardware- und Software-Komponenten von HP/Aruba. Hier ist bereits eine gute Unterstützung für Template-basierte Konfiguration und die Umsetzung einer Zero Trust Lösung vorhanden. Das vorgestellte Konzept kann jedoch auch mit anderer Hard- und Software umgesetzt werden. Hierzu müssen statt der entsprechenden Komponenten von HP/Aruba andere mit einer vergleichbaren Funktionalität gewählt werden. Wichtig ist, dass alle im Netz vorhandenen Komponenten die Lösung unterstützen. Ein homogenes Netzwerk ist hier notwendig. Für eine erfolgreiche Planung und Umsetzung von Zero Trust ist eine enge Zusammenarbeit von Netzwerkmanagement und Identitätsmanagement (IDM) unabdingbar. So findet zum Zeitpunkt der Erstellung dieses Dokuments eine Anpassung der Identitätsattribute im Bereich IDM statt; diese wird mit den Bedürfnissen des geplanten Zero Trust Models abgeglichen. Als Ansatz für die Integration von Zero

Trust in unsere Bestandsumgebung haben wir das aus dem „Zero Trust Maturity Model“ hervorgehende Modell gewählt, welches in fünf themenspezifische Säulen strukturiert ist.

Abb. 4.2: Zero Trust Maturity Model

Die fünf Säulen des Modells sind wie folgt:

Identität Diese Säule konzentriert sich auf die Authentifizierung und Autorisierung von Nutzenden. Es stellt sicher, dass jede Identität eindeutig verifiziert wird, bevor sie Zugriff auf Ressourcen erhält. In dieser Säule ist ein zentrales Identitätsmanagementsystem von entscheidender Bedeutung. Dies ist üblicherweise gegeben und die dort vorhandenen Attribute können genutzt werden.

Gerät Die Gerätesäule befasst sich mit der Identifizierung und Verwaltung der Geräte, die auf das Netzwerk zugreifen. Hier können bestehende Datenbestände (MAC-Adressen) genutzt werden und esbesteht die Möglichkeit, Arbeitsgeräte und BYOD entsprechend zu kategorisieren. Damit kann man auf seinem Arbeitsgerät mit der gleichen Uni-ID sicherheitskritische Dienste nutzen, die mit einem mitgebrachten Gerät nicht zur Verfügung stehen. Darüber hinaus soll hier der Zustand eines Endgeräts (bspw. Betriebssystemversion inkl. Sicherheitsupdates) einfließen.

Netzwerk Diese Säule stellt sicher, dass das Netzwerk segmentiert und überwacht wird, um unbefugten Zugriff zu verhindern. Sicherheitsrichtlinien werden basierend auf dem Verhalten und den Attributen der Geräte und Benutzer durchgesetzt. Dies wird beim Einsatz von einer HP/Aruba Lösung durch die Komponente ClearPass realisiert.

Anwendung Die Anwendungssäule gewährleistet, dass nur autorisierte Anwendungen auf das Netzwerk zugreifen und innerhalb des Netzwerks kommunizieren dürfen. Es werden Sicherheitsmaßnahmen implementiert, um Anwendungen vor Bedrohungen zu schützen. Diese Säule kann in einem der Forschung und Lehre gewidmeten Umfeld nur schwer umgesetzt werden und bietet sich eher für statische Umgebungen an. Dies würde höchstens automatisiert funktionieren und ist deswegen im Campusnetz erst in einem idealen Reifegrad realisierbar.

Daten In dieser Säule liegt der Fokus auf dem Schutz sensibler Daten. Es werden Richtlinien und Technologien verwendet, um sicherzustellen, dass Daten verschlüsselt und nur von autorisierten Uni-IDs und Anwendungen zugänglich sind. Auch hier ist das universitäre Umfeld meist zu dynamisch, um über definierte Regeln derartige Policies umzusetzen. Auch dies würde höchstens automatisiert funktionieren und ist deswegen im Campusnetz erst in einem idealen Reifegrad realisierbar.

Jede Säule enthält Funktionen, die bei einer Integration von Zero Trust-Prinzipien in Bestandsumgebungen zu berücksichtigen sind. Weiterhin kann jede dieser Säulen unabhängig voneinander weiterentwickelt und integriert werden, was eine schrittweise Implementierung der Zero-Trust-Prinzipien ermöglicht. Durch die Koordination und das Zusammenspiel dieser Säulen wird eine umfassende Sicherheitsarchitektur geschaffen, die den heutigen Bedrohungen effektiv begegnen kann. Auch können so Zero-Trust-Prinzipien Schritt für Schritt in Bestandsumgebungen „eingeschlichen“ werden.

Die schrittweise Integration geschieht in drei Reifegraden:

Klassisch (KL) In der Infrastruktur erfolgen hauptsächlich manuelle Konfigurationen und manuelle Zuweisungen von Attributen auf Grundlage von statischen Sicherheitsrichtlinien.

Fortschrittlich (FO) Es existieren einige säulenübergreifende Koordinationen, eine zentrale Sichtbarkeit in/über die Infrastruktur und ein zentrales Identitätsmanagement. Sicherheitsrichtlinien werden basierend auf Input und Output säulenübergreifenden durchgesetzt.

Als Fernziel:

Ideal (ID) Es existiert ein vollständig automatisiertes Zuweisen von Attributen zu Ressourcen, die dynamische Sicherheitsrichtlinien basieren auf automatisierten Triggern. Dies

ist in einem Campusnetz unerreichbar, könnte jedoch in bestimmten Netzsegmenten mit hohem Schutzbedarf, bspw. in Netzen der Verwaltung, realisiert werden.

Im ersten Schritt erfolgte eine Umsetzung mit Fokus auf die Säulen Identität, Gerät und Netz in einem Testumfeld, das Ziel war ein Proof of Concept. Generell benötigt man ein Konzept, das den Schutzbedarf und benötigten Berechtigungen im Campusumfeld abbildet. Im BSI- Standard 200-2 (IT-Grundschutz-Methodik) ist das Vorgehen bei der Schutzbedarfsfeststellung so definiert, dass zunächst der Schutzbedarf der Geschäftsprozesse ermittelt wird. Hierzu korrelieren die Services. Daraus wird dann der Schutzbedarf der weiteren Assets, z.B. auch der Netzwerksegmente und IT-Systeme, abgeleitet. Im Campusumfeld ist es so, dass bestimmte Services, die den Umgang mit personenbezogenen Daten oder Finanzdaten beinhalten, vorwiegend in bestimmten Organisationseinheiten (wie bspw. der Verwaltung) genutzt werden. Von daher ist es möglich, wenn man sich am höchsten Schutzbedarf orientiert und zusätzliche Schutzmechanismen (wie bspw. Verschlüsselung in der Anwendung selbst) mit einbezieht, den verschiedenen Organisationseinheiten (beispielsweise Bibliothek, Verwaltung oder Studentenschaft, Studierende) oder zumindest den verschiedenen Rollen in Organisationseinheiten (bspw. Personaldezernat in der Verwaltung, Forschende eines Instituts), einen Schutzbedarf anhand des Schutzbedarfs der benötigten Services zuordnen. Diese Schutzbedarf kann man Nutzenden bzw. deren Uni-IDs zuordnen.

Zusätzlich werden die eingesetzten Geräte betrachtet, d.h. ein BYOD Gerät hat einen anderen Schutzbedarf als ein beruflicher/registrierter (zentral gemanagter) Laptop. Als Datenbasis wird hier eine Zuordnung der Nutzenden zu einer oder mehreren Organisationen benötigt und darüber hinaus die Kenntnis über die MAC Adresse der beruflichen Laptops. Unbekannte Geräte eines Nutzenden werden automatisch als BYOD Device betrachtet und erhalten, da sie ein größeres Sicherheitsrisiko darstellen, weniger Berechtigungen. Sobald die geplante Endpunktverwaltung für die beruflichen Endgeräte der Nutzenden zur Verfügung steht, können auch diese Daten verwendet werden.

Durch den Einsatz von Zero Trust wird dies technisch in eine entsprechende Mikro-Segmentierung „übersetzt“. Dies erfolgt analog zu dem üblichen Vorgehen zur Erstellung von Sicherheitszonen. Diese Zonen werden jedoch nun durch Zero-Trust-Prozesse und nicht mehr durch die fixe Zuordnung der Clientgeräte in bestimmte VLANs realisiert. Besonders kritische Dienste werden nur noch für berechtigte Nutzende auf sicheren Endgeräten zur Verfügung gestellt. Hierdurch entsteht eine starke Mikrosegmentierung, die besonders sensible Anwendungen kapselt.

Technisch gesehen gibt es hier verschiedene Ansätze. Oft werden aus diesen Informationen Rollen generiert und kombiniert, aus verschiedenen Rollen entsteht eine Kombination an Templates. Ein möglicher alternativer Ansatz ist ein Flavour-Konzept, bei dem durch die Kombination von Attributen keine Rollen, sondern sogenannte Flavours definiert werden, denen bestimmte Berechtigungen zugeordnet sind. Das ist ein eleganter Ansatz, da hier die komplexe Zuordnung verschiedener Attribute zu verschiedenen Schutzbedarfen und Berechtigungen an einer Stelle stattfindet und alle nachfolgenden Systeme die Flavours einfach verwenden können.

In jedem Fall wandert die Zuordnung der Berechtigungen von Nutzenden mit ihren Geräten aus der fixen Zuordnung zu einem VLAN mit einem bestimmten Sicherheitsbedarf in die Zero-Trust-Technologie. Im Gegensatz zu den bisher verwendeten VLANs ist hier eine Mikrosegmentierung möglich. Die technische Realisierung erfolgte testweise mit Komponenten der Firma HP/Aruba. Zu diesen gehören leistungsfähige Switche und Access Points (APs), die durch ein zentrales Cloudmanagement verwaltet werden. Zudem fungiert der Aruba ClearPass-Policy Manager als „Policy Decision Point“ und sorgt für eine sichere und effiziente Durchsetzung von Sicherheitsrichtlinien. Konkret bedeutete das, dass die Netzwerkkomponenten von HP/Aruba, versehen mit einem neuen Regelwerk für Clientgeräte, den Trust Templates, verwendet wurden.

Der Einsatz von Flavours ist geplant, da diese aktuell im IDM eingeführt werden. Zum Zeitpunkt der Realisierung des Proof of Concept war dies jedoch noch nicht so weit fortgeschritten, dass es verwendet werden konnte. Deswegen wurde zunächst eine vereinfachte Version, passend zum aktuellen Umsetzungsgrad, d.h. mit Informationen noch aus nur einer Quelle, der IPDB, in der Informationen zu Nutzenden (inkl. Uni-ID) und deren Geräten hinterlegt sind, realisiert.

Aufgrund von Eigenschaften aus der IPDB wird durch das in ClearPass hinterlegte Regelwerk (Trust Templates) eine Zuordnung der Clientgeräte in bestimmte Netzsegmente vorgenommen. Hierbei wird zunächst folgendes zur Zuordnung herangezogen:

- Aktuell: basierend auf Geräteeigenschaften: registriertes Gerät (MAC-Adresse)
- Zukünftig:
  - Im ersten Schritt: basierend auf Identitätsattributen: diese sind im Verzeichnisdienst abgelegt und dort Rollen/Flavours zugeordnet

  - Im zweiten Schritt: zusätzlich hierzu werden Geräteinformationen aus der Endpunktverwaltung hinzugenommen.

Durch die Verknüpfung von Geräteattributen mit diesen Identitätsattributen wird eine darauf basierende Segmentierung im Netzwerk erreicht. Hier als Beispiel, wie der Access im LAN-Bereich aktuell, im ersten Ansatz, abläuft:

1. Das System wird an einen Switchport angeschlossen und sendet Pakete mit seiner MAC-Adresse.
2. Der Switch übermittelt die MAC-Adresse des Systems an die ClearPass-Instanz.
3. ClearPass fragt bei der bereits bestehende IPDB an, ob die MAC-Adresse registriert ist
4. Die IPDB gibt abhängig davon, ob die MAC existiert oder nicht, eine bestimmte VLAN-ID zurück.
5. ClearPass gibt diese VLAN-ID weiter an den Switch. (An dieser Stelle könnten später noch weitere Kriterien abgeprüft werden und zur Änderung der VLAN-ID führen).
6. Der Switch konfiguriert den Switchport in das der VLAN-ID entsprechende VLAN x.
7. Das System fragt nun im VLAN x per DHCP nach seiner IP-Adresse. (am Switch sind die Mechanismen „port-security“, „arp inspection“ und „dhcp-snooping“ aktiv)

Sobald das Flavour-Konzept existiert, werden die folgenden Änderungen vorgenommen: Für die Authentisierung wird zusätzlich zur jetzt ausschließlich verwendeten MAC-Adresse des Endgerätes in einem zweiten Schritt auch die Uni-ID des Nutzenden ausgewertet. In Schritt 3 wird zusätzlich für die Uni-ID das Flavour abgefragt und hinzugenommen, sodass sich je nach Antwort aus IPDB und Verzeichnisdienst für die Autorisierung unterschiedliche Rechte/Rollen ergeben.

Sobald die Endgeräteverwaltung realisiert ist, wird für bestimmte, sicherheitskritische Services zusätzlich hierzu noch der Zustand des Endgeräts abgefragt. Nur wenn es den sicherheitstechnischen Anforderungen (passendes Betriebssystem, alle Sicherheitsupdates eingespielt, keine unerlaubte Software installiert) entspricht, wird Zugriff auf diese Services zugelassen.

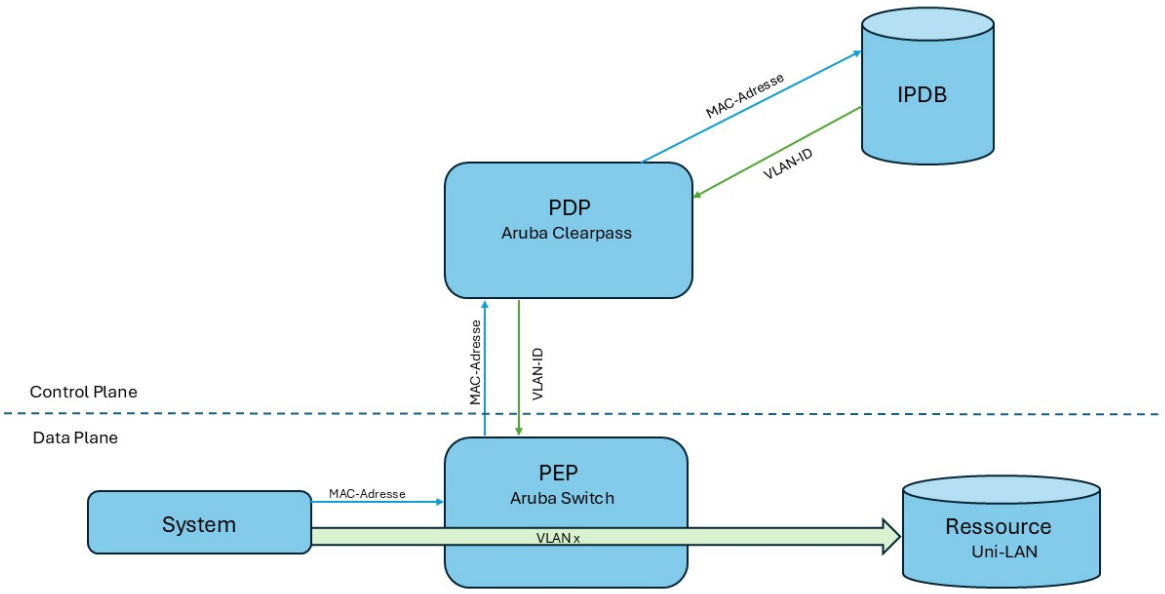

Abb. 4.3: Ablauf

5 Fazit

Das Konzept basiert darauf, dass eine schrittweise Integration der Zero-Trust-Prinzipien eine flexible und anpassbare Sicherheitsstrategie ermöglicht. Diese muss ein Konzept von Schutzbedarf und benötigten Berechtigungen der Nutzenden enthalten. Das Konzept selbst kann zunächst einfach gehalten und später angepasst werden, wichtig ist jedoch, dass es die grundlegenden Sicherheitsbedürfnisse erfüllt und mindestens die gleiche Sicherheit bietet, wie die bereits bestehende Netzwerkarchitektur ohne Einsatz von Zero Trust.

Durch die klare Fokussierung auf einzelne Key Points der Säulen Identität, Gerät und Netzwerk wird eine Grundlage geschaffen, die in Zukunft weiter ausgebaut werden kann. Für sicherheitskritische Umgebungen oder sich verschärfende Angriffsvektoren wäre eine vollständige Implementierung aller fünf Säulen des Zero-Trust-Modells, einschließlich der Säulen Anwendung und Daten, möglich und optimal. Dies würde eine umfassende Sicherheitsarchitektur schaffen, die den heutigen Bedrohungen höchst effektiv begegnen kann. Für ein Campusnetz kann durch diese flexible Herangehensweise ein geeignetes Maß an Sicherheit gefunden werden.

Die Verwendung von Komponenten der Firma HP/Aruba bietet eine praxisnahe Herangehensweise, wenn nicht genügend Personen zur Verfügung stehen, um Open-Source-Komponenten einzusetzen und entsprechend anzupassen.

In einem ersten, einfachen Proof of Concept in geeigneten Netzbereichen funktionierte der gewählte Ansatz. Eine globale und vollumfängliche Umsetzung von Zero Trust erfordert eine Zusammenarbeit vieler Teams und wird zu einem späteren Zeitpunkt erreicht werden.

6 Versionsverlauf

Version	Datum	Änderungen
1.0	08.09.2025	Initiale Veröffentlichung

Literaturverzeichnis

[1] *Positionspapier Zero Trust 2023*. Adresse: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeLeitlinien/Zero-Trust/Zero-Trust_04072023.pdf?__blob=publicationFile&v=4 (besucht am 08. 09. 2025).