|  |
| --- |
| **BACHELORARBEIT**  für die Prüfung zum  Bachelor of Science  des Studiengangs Informatik Studienrichtung Informationstechnik  an der  Dualen Hochschule Baden-Württemberg Karlsruhe  von  Paul Schien  04.09.2023  Matrikelnummer 7816361  Kurs TINF20B3  Ausbildungsfirma Bundesanstalt für Wasserbau, Karlsruhe  Betreuer der Ausbildungsfirma Dipl.-Ing. Uwe Ziesche  Gutachter der Studienakademie Titel Matthias Merz |

Erklärung

(gemäß §5(4) der „Studien- und Prüfungsordnung DHBW Technik“ vom 01. 08. 2019)

Ich versichere hiermit, dass ich meine Bachelorarbeit mit dem Thema: „Untersuchung von Network Access Methoden und Optimierung einer bestehenden Lösung“ selbstständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel benutzt habe. Ich versichere zudem, dass die eingereichte elektronische Fassung mit der gedruckten Fassung übereinstimmt.

Ort, Datum Unterschrift

Abstrakt

Diese Arbeit befasst sich mit

Abstract

This

Inhaltsverzeichnis

Abbildungsverzeichnis V

Tabellenverzeichnis V

Abkürzungsverzeichnis V

1 Einführung 1

1.1 Motivation 1

1.2 IST-Zustand 1

2 Projektbeschreibung 1

2.1 Aufgabenstellung 1

2.2 Vorgehen 1

3 Grundlagen 1

3.1 Protokolle 1

3.1.1 802.1X 1

3.1.2 RAIDUS 1

3.1.3 WPA 2

3.1.4 Transportverschlüsselung 2

3.2 Zero Trust Prinzipien 2

4 Methoden 3

4.1 Network Access Control 3

4.2 Software-Defined Perimeter 3

4.3 Zero Trust Network Access 3

4.3.1 Zero Trust 1.0 3

4.3.2 Zero Trust 2.0 3

4.4 Vergleich der Methoden 3

5 Mögliche Lösungen 3

5.1 Cisco ISE 3

5.2 Macmon 3

5.3 Fortinet 3

6 Vergleich der Lösungen 3

7 Implementierung 3

8 Fazit 3

Literaturverzeichnis XIII

Abbildungsverzeichnis

[Abbildung 1: TestAbb 2](#_Toc139356728)

Tabellenverzeichnis

Tabelle 1: TestTabelle2 2

Abkürzungsverzeichnis

BAW Bundesanstalt für Wasserbau

IEEE Institute of Electrical and Electronics Engineers

LAN Local Area Network

WLAN Wireless Local Area Network

RADIUS Remote Authentication Dial-In User Service

ZTNA Zero Trust Network Access

# Einführung

## Motivation

## IST-Zustand

# Projektbeschreibung

## Aufgabenstellung

Innerhalb der BAW wird

## Vorgehen

# Grundlagen

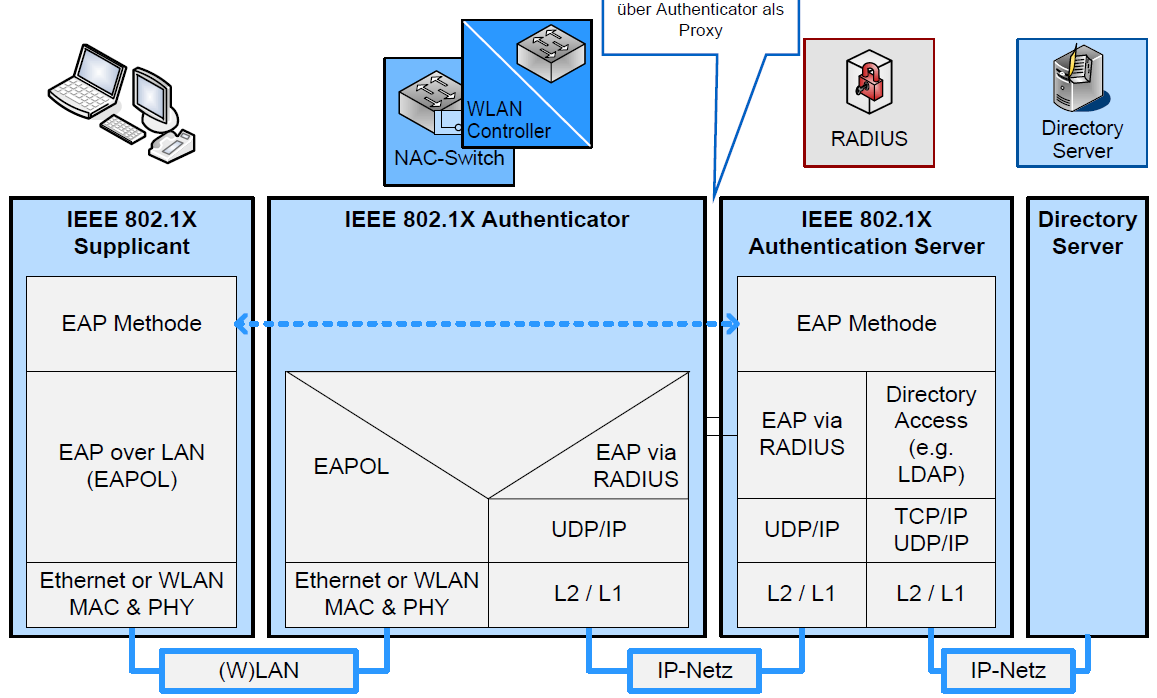
## Protokolle

### 802.1X

Die Anforderungen an 802.1X ist eine Unterbindung vom unkontrollierten Anschluss von Geräten. Dadurch wird Zugriff auf das Unternehmensnetz nur für Unternehmensgeräte gewährt. Dieser Zugriff sollte nur gewährt werden, wenn die Authentisierung erfolgreich beendet wurde und weitere Konfigurationsvorgaben erfüllt werden.

|  |  |  |
| --- | --- | --- |
| Version | Release | Name |
| v1 | 13.07.2001 | IEEE 802.1X-2001 |
| v2 | 13.12.2004 | IEEE 802.1X-2004 |
| v3 | 05.02.2010 | IEEE 802.1X-2010 |
| v4 | 28.02.2020 | IEEE 802.1X-2020 |

Mit der Zeit sind mehrere Versionen von 802.1X entwickelt worden. Die relevanten Funktionen sind in der Version IEEE 802.1X-2004 dazugekommen und ist daher auch die am weitesten verbreitete Version. Das Endgerät wird als Supplikant bezeichnet, welchem der Zugriff gewährt werden muss. Die Rolle des Authentikators übernimmt der Netzzugangspunkt, da dieser direkt mit dem Supplikanten kommuniziert und Zugriffberechtigung umsetzt. Der Authentikator leitet die Authentifizierungsanfrage an einen zentralen Authentifikation Server weiter, welcher an weitere Systeme angeschlossen werden kann. Diese angeschlossen Systeme können benutzt werden um Unternehmensweite Credentials zu verifizieren. Die Kommunikation zwischen Supplikanten und Authentikatoren wird im lokalen LAN über EAPoL abgewickelt. Dabei werden die Daten in dem Authentikator nicht verarbeitet sondern als Proxy ein anderes EAP-Paket an den Authentifikation Server weitergeleitet.



#### Kontrollierte Ports

Zur Trennung von Signalisierungs- und Nutzdaten kann ein kontrollierter Port [engl. controlled Port] eingesetzt werden. Mit Hilfe dieser Art von Ports können bestimmte Protokolle als auch Ports an den Supplikanten weitergeleitet werden oder vom Supplikanten empfangen werden. Es muss durch den verwendeten Authenticator unterstützt werden. Die Namensgebung dieser Funktion ist zwischen unterschiedlichen Herstellern nicht eindeutig jedoch wird die Funktionsweise gleich beworben.

### RAIDUS

RADIUS ist ein Server-Client Protokoll, welches Autorisierung, Authentifizierung und Accounting von Geräten durchführt. Dabei wird ein Challenge Response Verfahren angewandt, welches auch mit unterschiedlichen Transportverschlüsselungsverfahren unterstützt wird. Zur Durchführung der Autorisierung und Authentifizierung wird der UDP Port 1812 benutzt. Port 1813 ist dem Accounting zugeteilt. Im RFC-2865[1] wird darauf hingewiesen, dass in alten Implementationen jeweils Port 1645 und 1646 benutzt wird, sich jedoch mit dem „datametrics“ Service überschneidet und nicht genutzt werden soll. Die Transaktionen zwischen den Clients und dem Radius-Server laufen mit einem ausgetauschten Secret, welches benutzt wird um den Inhalt der Pakete, wie eventuelle Zugangsdaten, zu verschlüsseln. Mittels Attributen wird das Protokoll flexibel erweitert und ermöglicht somit eine Informationsübertragung, welcher nicht standardisiert werden muss.

Die Verwendung von UDP wurde in diesem RFC außerdem gerechtfertigt. Die Entscheidung wurde getroffen, da mehrere charakteristische Eigenschaften praktisch für RADIUS sind. Falls die Verbindung zu einem RADIUS Server im Netzwerk gestört ist, muss ein anderer angesprochen werden. Dafür muss eine Kopie der Anfrage gespeichert und zur erneuten Übertragung benutzt werden. Die in TCP eingebaute Bestätigen eines Paketes wird vom RADIUS Protokoll nicht benötigt und wird daher von dem Ersteller des RFCs als unnötiger Overhead bezeichnet. Außerdem ist das erfolgreiche Zustellen eines Paketes nach mehreren Minuten nicht nützlich, da ein anderer Server im Netzwerk innerhalb dieser Zeit die Authentifizierung erfolgreich abschließen kann. Für die Implementation ist die Einfachheit von UDP auch geeigneter, da TCP mehrere Events auslösen kann, die unterschiedlich gehandelt werden müssten.

#### Aufbau

Der Aufbau des Paketes ist in Abbildung 1 dargestellt. Es beginnt mit einem Code, welcher ein Oktett lang ist und identifiziert den Typ vom Paket. Das folgende Oktett gibt den Identifier an und wird benutzt, um zu klassifizieren, auf welches Paket geantwortet wird. Der Server kann daran Duplikate von Paketen erkennen. Da ein Absender nicht innerhalb kurzer Zeit über dem gleichen Port nicht den gleichen Identifier für ein anderes Paket benutzen darf. Das Feld für die Länge ist 2 Oktette groß und beschreibt die gesamte Länge in Anzahl der Oktetten des Pakets mit den Feldern für Code, Identifier, Length, Authenticator und Attribute. Sie ist mindestens 20 und maximal 4096. Der Authenticator ist 16 Oktette lang und wird abhängig von der Art des Paketes gebildet. In einem Access-Request Paket ist es eine 16 Oktett lange Nummer, welche Request Authenticator im Verfahren genannt wird. Im einem Response Paket wird der Authenticator aus einem MD5-Hash berechnet, welcher über das gesamte RAIDUS Paket gebildet wird:

MD5(Code + ID + Length + RequestAuth + Attributes + Secret)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
|  |  |  |  |  |

Tabelle : Die wichtigsten RADIUS Attribute

Asd

Abbildung : TestAbb

### WPA

### Transportverschlüsselung

#### EAP

#### TLS

## Zero Trust Prinzipien

Das nachfolgende Modell Zero-Trust basiert auf drei Sicherheitskonzepten. Es handelt es sich um den sicheren Zugriff, geringste Privilegien und Sichtbarkeit. Der sichere Zugriff muss aus einer verlässlichen starken Datenquelle kommen und muss für jeden Zugriff authentisiert werden. Dabei wird zwischen einer Nutzer Authentifizierung und Maschinen Authentifizierung unterschieden. Beide Authentifizierungsquellen sind in einer Implementierung möglich. Das Verfahren zur Authentifizierung wird nicht eingeschränkt, jedoch durch den Wortlaut „starken Datenquelle“ definiert. Nach der Authentifizierung werden die geringsten Privilegien gewährt, welche sich nach Bedarf erhöhen können. Das Sicherheitskonzept der Sichtbarkeit sieht vor, dass ein nicht authentifizierter Nutzer die Anwendung nicht sehen und erreichen kann.

## SIEM

Ein Security Information und Event Manager System wird verwendet, um mit Hilfe von Log Daten eine Virtualisierung für eine zentrale Sicht zu generieren und durch zusätzlichen Kontext Events zu erkennen. Splunk [9], ein Hersteller für eine verbreitete SIEM Lösung, definiert es als „einzelnes Security-Management-System, das volle Sichtbarkeit und Transparenz zu Aktivitäten innerhalb Ihres Netzwerks bietet“. SIEM besteht aus den beiden Sicherheitskonzepten SIM und SEM. Ersteres ist das Security Information Management [SIM], es entspricht den Werten für ein Log Management. Die Grundlegenden Aufgaben ist das Sammeln, Übertragen, Speichern, Weiter Leitung und einfachen Analyse von Log Daten. Diese Daten stammen aus verschiedenen Netzwerk-Komponenten und werden automatisiert durch den SIM behandelt. Daraus ergeben sich laut der Computerwoche [8] die grundlegenden Funktionen für „Richtlinien-orientierte Analysen auch zu Trends, periodische Berichte und Basisfunktionen für Alarm-Meldungen“.

SEM hingegen bezeichnet die Funktionen für Security Event Management, die Aufgabe besteht die Log Dateien zu korrelieren. Dabei folgt es definierten Richtlinien aber kann gleichzeitig auch mit festgelegten Standards automatisiert abgeglichen werden.

Ein SIEM fast beide Konzepte zusammen und ermöglich somit eine zentrale Steuerung von

Bekannte SIEM Lösungen sind außer dem zuvor gennannten Splunk die Firma

Die <Plattform xyz> schreibt zu dem Thema

# Methoden

## Network Access Control

## Software-Defined Perimeter

## Zero Trust Network Access

Zero Trust Network Access oder auch kurz ZTNA ist ein Konzept um eine Anwendung sicher mit einem steuerbaren Zugriff vom Internet zugriffsfähig zu machen.

### Zero Trust 1.0

Die ersten Implementierungen für eine Zero Trust Lösung wurd

Erstes Zero Trust Modell mit Funktionen und Aufbau

### Zero Trust 2.0

Fehler in 1.0 und dadurch entstehende Verbesserungen. Allgemeine Verbesserungen

## Vergleich der Methoden

Bei RADIUS ist ein Log-off möglich, wird bei Cisco Telefonen automatisch gemacht

# Mögliche Lösungen

## Cisco ISE

## Macmon

## Fortinet

# Vergleich der Lösungen

# Implementierung

# Fazit

Literaturverzeichnis

1. Remote Authentication Dial In User Service (RADIUS) [online] <https://www.rfc-editor.org/rfc/rfc2865> Abgerufen am: 06.06.2023
2. Aurand, Andreas LAN-Sicherheit dpunkt.verlag Heidelberg, 1. Auflage 2005
3. RADIUS Types – iana [online] <https://www.iana.org/assignments/radius-types/radius-types.xhtml> Abgerufen am: 15.06.2023
4. Remote Authentication Dial-In User Service (RADIUS) Protocol Extensions [online] <https://www.rfc-editor.org/rfc/rfc6929> Abgerufen am: 15.06.2023
5. Private Enterprise Numbers – iana [online] <https://www.iana.org/assignments/enterprise-numbers/> Abgerufen am: 15.06.2023
6. Secure Network Access - What is Zero Trust [online] <https://www.appgate.com/blog/what-is-zero-trust> Abgerufen am: 19.06.2023
7. What Is Zero Trust Network Access [online] <https://www.zscaler.com/resources/security-terms-glossary/what-is-zero-trust-network-access> Abgerufen am: 03.07.2023
8. Was SIM und SEM von SIEM unterscheidet [online] <https://www.computerwoche.de/a/was-sim-und-sem-von-siem-unterscheidet,2511108> Abgerufen am: 12.07.23
9. Was ist ein SIEM? [online] <https://www.splunk.com/de_de/data-insider/what-is-siem.html> Abgerufen am: 12.07.23