Information Security

Netzwerkauthentifizierung mit Fokus auf KMUs

Evaluierung von Authentifizierungslösungen mit Berücksichtigung des IT-Budgets

Diplomarbeit

zur Erlangung des akademischen Grades

Diplom-Ingenieur/in

eingereicht von

Michael Sailer

is201816

im Rahmen des

Studienganges Information Security an der Fachhochschule St. Pölten

Betreuung

Betreuer/in: Dipl.-Ing. Gabor Österreicher, BSc

Mitwirkung: -

St. Pölten, 30. April 2023

(Unterschrift Verfasser/in)

(Unterschrift Betreuer/in)

Ehrenwörtliche Erklärung

Ich versichere, dass

- ich diese Diplomarbeit selbständig verfasst, andere als die angegebenen Quellen und Hilfsmittel nicht benutzt und mich sonst keiner unerlaubten Hilfe bedient habe.
- ich dieses Diplomarbeitsthema bisher weder im Inland noch im Ausland einem Begutachter/einer Begutachterin zur Beurteilung oder in irgendeiner Form als Prüfungsarbeit vorgelegt habe.
- diese Arbeit mit der vom Begutachter/von der Begutachterin beurteilten Arbeit übereinstimmt.

Der Studierende/Absolvent räumt der FH St. Pölten das Recht ein, die Diplomarbeit für Lehre- und Forschungstätigkeiten zu verwenden und damit zu werben (z.B. bei der Projektevernissage, in Publikationen, auf der Homepage), wobei der Absolvent als Urheber zu nennen ist. Jegliche kommerzielle Verwertung/Nutzung bedarf einer weiteren Vereinbarung zwischen dem Studierenden/Absolventen und der FH St. Pölten.

Ort, Datum *Unterschrift*

Kurzfassung

Der Zugriffsschutz im Netzwerk ist eine essenzielle Sicherheitsbarriere, um die Verfügbarkeit von Netzwerkressourcen auf die notwendigen Clients einzuschränken. Standards für die IT-Sicherheit (z.B. ISO 27001) definieren Anforderungen wie das Least-Privilege-Prinzip oder die Segmentierung von Netzwerken, die eine Implementierung einer Netzwerkauthentifizierung erforderlich machen. Die Kosten hierfür sind nicht für alle kleinen und mittleren Unternehmen (KMU) stemmbar, wodurch sich unterschiedliche Zielgruppen mit individuellen Anforderungen ergeben.
In dieser Arbeit werden drei unterschiedliche Ansätze verfolgt:

- Firmen mit bestehender IT-Infrastruktur und Know-how, deren Anforderungen nicht vom Microsoft RADIUS-Server gedeckt werden können (Open Source Network-Access-Control (NAC))
- (kleine) Firmen im Aufbau ihrer IT-Infrastruktur mit geringen Anforderungen an einen RADIUS-Server (All-in-one-Ansatz)
- (kleine) Firmen mit keiner oder wenig IT-Infrastruktur (Cloud-basierter Ansatz)

Die Arbeit verfolgt drei Ziele: Das erste Ziel ist die Recherche und Evaluierung von Open Source Network-Access-Control-(NAC-)Lösungen, die einen vergleichbaren Funktionsumfang wie die Produkte der Marktführer Cisco, Aruba und ForeScout versprechen. Die vielversprechendste Lösung wird dabei mithilfe eines Proof-of-Concepts (PoC) untersucht. Des Weiteren werden All-in-one-Lösungen gesucht, die neben der NAC-Funktionalität auch Features von branchenüblichen Verzeichnisdiensten, wie z.B. Microsoft AD, anbieten, wobei ein Produkt im Anschluss in einem PoC analysiert wird. Abschließend soll untersucht werden, welche cloudbasierten Lösungen für eine Netzwerkanmeldung existieren, die nicht von einer lokalen Server-Infrastruktur abhängig sind.

Im Zuge dieser Arbeit konnten einige Produkte identifiziert werden, die für den Einsatz in einem KMU denkbar sind. Mit PacketFence wurde ein NAC-Produkt in einem Proof-of-Concept untersucht, welche quelloffen, d.h. Open Source, ist und viele Anforderungen für eine Netzwerkauthentifizierung abdecken kann. In vereinzelten Bereichen, wie der Produktdokumentation oder der Untersuchung von Clients auf vordefinierte Richtlinien, gibt es allerdings einige Einschränkungen im Vergleich zu kommerziellen Produkten.

Zentyal wurde als All-in-one-Alternative zu Microsoft AD im Proof-of-Concept untersucht, wobei sich hier einige Schwächen und Einschränkungen in der IT-Sicherheit offenbarten. Es besteht Potential für den Hersteller, dieses Produkt zu verbessern, um anschließend in einer produktiven Umgebung eingesetzt werden zu können.
Die Recherche für den cloudbasierten Ansatz Ansatz hat einige kreative Lösungen aufgezeigt. So kann ein RADIUS-Server oder Captive Portal gänzlich in der Cloud betrieben werden. Mit Zscaler gibt es ein Produkt, welches eine andere Philosophie verfolgt und das Zero-Trust-Modell in der Cloud einsetzt, wodurch Berechtigungen feingranularer im Vergleich zu RADIUS-Server oder Captive Portal definiert werden können.

Abstract

Network access control is an essential security barrier to limit the availability of network resources to the necessary clients. Standards for IT security such as ISO 27001 define requirements such as the least privilege principle or the segmentation of networks, which require the implementation of network authentication. The costs for this are not affordable for all small and medium-sized enterprises (SMEs), resulting in different target groups with individual requirements.
Three different approaches are followed in this paper:

- Companies with existing IT infrastructure and know-how whose requirements cannot be met by the Microsoft RADIUS server (Open-Source network access control (NAC))
- (small) companies in the process of building their IT infrastructure with low requirements for a RADIUS server (All-in-one approach)
- (small) companies with no or little IT infrastructure (Cloud-based approach)

The work has three goals: The first objective is to research and evaluate open source network access control (NAC) solutions that offer similar functionality to the products of market leaders Cisco, Aruba, and ForeScout. The most promising solution will be reviewed using a proof-of-concept (PoC). Furthermore, all-in-one solutions that offer features of industry-standard directory services, such as Microsoft AD, in addition to NAC functionality will be searched, followed by a product analysis in a PoC. Finally, it will be evaluated which cloud-based solutions for network logon exist that are not dependent on a local server infrastructure.

In the context of this work, a number of products were identified that are suitable for use in an SME. With PacketFence, a NAC product was analyzed in a practical test, which is open source and can cover many requirements for network authentication. However, there are some limitations compared to commercial products in certain areas, such as product documentation or compliance assessment of clients.
Zentyal was proof-of-concept evaluated as an all-in-one alternative to Microsoft AD, revealing some weaknesses and limitations in IT security. There is potential for the manufacturer to improve this product for subsequent use in a production environment.

The research for the cloud-based approach revealed some creative solutions. For example, a RADIUS server or captive portal can be run entirely in the cloud. With Zscaler, there is a product that follows a different philosophy and uses the zero-trust model in the cloud, allowing permissions to be defined in a more fine-grained way compared to RADIUS server or Captive Portal.

Inhaltsverzeichnis

1 Einleitung

Aufgrund der Zunahme von Datendiebstahl (Data-Breach) aber auch allgemeinen Cyberangriffen auf Unternehmen, bauen diese vermehrt eine Information Security Management System (ISMS) auf. Die Zahlen der Zertifizierungen nach International Organization for Standardization (ISO) 27001 haben weltweit von ungefähr 5.000 im Jahr 2006 auf 33.290 im Jahr 2016 stetig zugenommen [1]. Die aktuellsten Daten aus dem Jahr 2020 bestätigen das Wachstum mit 44.486 zertifizierten Unternehmen nach ISO 27001 [2]. Gründe für ein ISMS und die Überprüfung dieser durch einen ISO-Standard sind vielfältig. Zu den wichtigsten Vorteilen zählen [3]:

- Einen Überblick über die Angriffsfläche des Unternehmens erhalten
- Eine potenzielle Reduzierung der Angriffsfläche, und ein damit vermindertes Risiko von Cyberangriffen und Geldstrafen mit Blick auf die Datenschutz-Grundverordnung (DSGVO)
- Einhaltung der geschäftlichen, rechtlichen, vertraglichen und regulatorischen Anforderungen
- Einschätzung und Bewertung des ISMS von außen

Die ISO 27001 bietet im Anhang A.9 [4] und A.13 [5] Ideen, um das Least-Privilege-Prinzip und die Segmentierung von Netzwerken einzuführen. Neben den Vorteilen für die Informationssicherheit bietet die Netzwerkauthentifizierung auch für die SystemadministratorInnen eine wesentliche Erleichterung in der Verwaltung der Netzwerk-Ports von Netzwerk-Switches. Neben der Authentifizierung kann ein Network Access Control (NAC) auch in der Autorisierung unterstützen, und die Endgeräte durch eine dynamische Zuweisung von Netzwerksegmenten bzw. VLANs voneinander trennen. So müssen beim Standard IEEE 802.1Q die VLAN-IDs nicht mehr statisch konfiguriert und laufend evaluiert werden.

Dem gegenüber steht die effiziente Verwaltung des IT-Budgets bzw. IT-Security-Budgets. Einer Studie mit amerikanischen Unternehmen zufolge beträgt das IT-Budget für KMUs ca. 6.9% des Firmenumsatzes, wobei dies nur auf einer groben Schätzung beruht und die Ausgaben stark zwischen den Branchen variieren [6]. Das IT-Security-Budget wiederum beträgt 2022 im Durchschnitt ca. 10% des IT-Budgets von amerikani-

schen und kanadischen Firmen [7]. IT-MitarbeiterInnen in KMUs arbeiten oftmals nicht als Vollzeitäquivalent für IT-Themen, und spezialisierte MitarbeiterInnen für die IT-Sicherheit sind oft zu teuer.

Wie im vorherigen Absatz ausgeführt, hat das IT-Budget und das Know-how der MitarbeiterInnen Grenzen und unterscheidet sich auch wesentlich innerhalb der Unternehmen und Branche. Zudem beeinflusst die Abhängigkeit von bestehender Infrastruktur die Auswahl und Implementierung eines Prozesses für eine Netzwerkauthentifizierung.
Daher liegt der Fokus dieser Arbeit auf den drei folgenden Zielgruppen:

- Firmen mit bestehender IT-Infrastruktur und Know-how, deren Anforderungen nicht vom Microsoft RADIUS-Server gedeckt werden können (Open Source NAC)
- (kleine) Firmen im Aufbau ihrer IT-Infrastruktur mit geringen Anforderungen an einen RADIUS-Server (All-in-one-Ansatz)
- (kleine) Firmen mit keiner oder wenig IT-Infrastruktur (Cloud-basierter Ansatz)

Nachstehend werden die Zielgruppen näher beschrieben:
Die erste Zielgruppe beschreibt Firmen, die bereits eine sehr umfangreiche IT inklusive deren Management besitzen und nun den Einsatz einer Netzwerkauthentifizierung prüfen bzw. mit der bestehenden Lösung unzufrieden sind. Microsoft bietet mit dem Network Policy Server (NPS) eine Active Directory (AD) integrierte Möglichkeit an, um mittels RADIUS Authentifizierungen durchzuführen. Der Funktionsumfang ist allerdings begrenzt und eignet sich primär für einfache Abbildungen in der Umsetzung. Daher bietet der Einsatz einer umfangreichen NAC-Lösung von den bekannten Herstellern wie Cisco, Hewlett Packard (HP), ForeScout und Co. viele Vorteile, wobei hier hohe Kosten anfallen können. Das Ziel hier ist also die Evaluierung einer kostenlosen NAC-Lösung mit ähnlichem Funktionsumfang wie zu den Produkten der oben genannten Hersteller.

Firmen der Zielgruppe 2 haben im Moment noch kein zentrales Management von BenutzerInnen-Konten im Einsatz, wollen dies aber in Zukunft umsetzen, um damit eine Anmeldung im Netzwerk abbilden zu können. Die Personalressourcen und das finanzielle Budget sind begrenzt, wodurch sich eine All-in-one-Lösung für Active Directory, Zertifikatsverwaltung und RADIUS-Server anbietet.

Zielgruppe 3 beschreibt jene Firmen, die keine bis minimale IT im Einsatz haben. Es sind jene Firmen, in denen kein zentrales Management der BenutzerInnen-Konten und Endgeräte stattfindet, und diese Aufgaben die MitarbeiterInnen selbst erledigen. Es existiert keine lokale Server-Infrastruktur, die für den Betrieb von Services zur Netzwerkauthentifizierung genutzt werden kann. Die Idee für diese Zielgruppe ist eine möglichst einfache, initial aufgesetzte (Cloud-)Lösung für die Anmeldung im Netzwerk, die wenig Wartungsaufwand benötigt und beim Setup der Endgeräte (Onboarding-Prozess) mehr Zeit benötigen darf.

Da jeder der Zielgruppen unterschiedliche Ausgangssituationen und Anforderungen haben, und spezifische Bedürfnisse besitzen, werden im Laufe der Arbeit in den spezifischen Kapiteln andere Schwerpunkte gesetzt. Des Weiteren wird der Fokus bei der Authentifizierung auf Zertifikate bzw. Single-sign-on gelegt. Die Eingabe der Kombination aus BenutzerInnen-Name und Passwort soll möglichst vermieden werden, da hiermit viele Nachteile rund um Bequemlichkeit, Usability und Sicherheit Einzug erhalten.

1.1 Gliederung der Arbeit

Dieses Dokument ist in elf Teile organisiert, die hier kurz beschrieben werden.

Kapitel 1 „Einleitung“ beschreibt die Forschungsfrage bzw. das Forschungsproblem im Detail, und stellt die Zielgruppen dieser Arbeit vor. Im nächsten Schritt werden Fachbegriffe in Kapitel 2 „Grundlagen“ näher beschrieben, die für das Verständnis dieser Masterarbeit förderlich sind. In Kapitel 3 „Stand der Forschung“ wird die Recherche zu wissenschaftlichen Arbeiten und Hintergrundinformationen dargestellt, welche einen Bezug zu dieser Arbeit haben. Mit Kapitel 4 „Herangehensweise“ werden die einzelnen Meilensteine im Detail aufgezeigt, die es zur Beantwortung der Forschungsfragen zu erreichen gilt. Darunter fällt die genaue Vorgehensweise bzw. die verwendeten Methoden und die Ziele der einzelnen Punkte. Zusätzlich wird der Versuchsaufbau und das eingesetzte Equipment vorgestellt.

Der erste große Aufgabenblock ist mit Kapitel 5 „Evaluierung von Open Source NAC-Produkten“ und Kapitel 6 „Proof-of-Concept - Open Source NAC“ die Recherche und Auswahl einer geeigneten Open-Source-Alternative zu den etablierten NAC-Produkten von Cisco, Aruba und Co., um diese anschließend in einem Proof-of-Concept zu untersuchen. Hier werden auch die fortgeschrittenen Funktionen der Marktführer vorgestellt, die deren Produkte im Vergleich zu einem RADIUS-Server aufweisen.

In Kapitel 7 „Evaluierung von On-Premises-Verzeichnisdiensten in Form eines All-in-one-Ansatzes“ und Kapitel 8 „Proof-of-Concept - All-in-one-Ansatz“ werden im ersten Schritt alternative Lösungen zu Microsoft AD DS in Form einer All-in-one-Lösung recherchiert, und später in einem praktischen Versuch mit Fokus der Netzwerkauthentifizierung auf deren tatsächliche Tauglichkeit überprüft. In Kapitel 9 „Evaluierung von Cloud-basierter Netzwerkauthentifizierung“ werden Möglichkeiten einer Cloud-basierten Anmeldung im Netzwerk theoretisch ausgearbeitet und miteinander verglichen. Die drei Ansätze werden anschließend in Kapitel 10 „Vergleich der Ansätze“ miteinander verglichen und Vorteile bzw. Nachteile hervorgehoben.

Abschließend wird im Kapitel 11 „Conclusio“ ein Fazit zu den vorgestellten Möglichkeiten einer Netzwerkauthentifizierung gezogen, die wichtigsten Ergebnisse präsentiert und die Forschungsfragen beantwortet. Zusätzlich werden die einzelnen Ansätze miteinander verglichen und deren Vor- und Nachteile gegenüber gestellt.

1.2 Vorwort zur Linguistik

Diese Arbeit wurde in der deutschen Hochsprache verfasst. Viele englische Begrifflichkeiten im Bereich der IT besitzen zwar eine deutsche Übersetzung, werden allerdings in der Praxis nicht verwendet und erhöhen das Risiko eines Missverständnisses. Aus diesem Grund werden in dieser Arbeit wesentliche Begriffe aus dem englischen nicht in den deutschen Sprachgebrauch übersetzt, um hier den Wahrheitsgehalt der Information nicht zu verfälschen.
Die Begrifflichkeiten „NAC-Lösung“ und „Netzwerkauthentifizierung“ sind beim Ansatz „Open Source NAC“ gleichzusetzen. Die Begriffe und Abkürzungen „AD“, „AD DS“ und „Microsoft AD“ haben die gleiche Bedeutung und beschreiben ein Windows-basiertes Active Directory Domain Service.

1.3 Forschungsfragen

Wie bereits der Titel dieser Diplomarbeit mit „Netzwerkauthentifizierung mit Fokus auf KMUs“ impliziert, wird in dieser Forschungsarbeit überprüft ob und wie eine Netzwerkauthentifizierung bei kleinen und mittleren Unternehmen technisch umgesetzt werden kann. Konkret stellen sich die folgenden Forschungsfragen:

- Welche kostenlosen NAC-Lösungen im Vergleich zu den kommerziellen Produkten gibt es und welche Erkenntnisse lassen sich aus einem Proof-of-Concept gewinnen?
- Welche Alternativen zu den branchenüblichen On-Premises-Verzeichnisdienste in Form eines All-in-one-Ansatzes gibt es, und können diese für die lokale Netzwerkauthentifizierung herangezogen werden?
- Welche Cloud-basierte Lösungen zur Anmeldung im Netzwerk existieren, die nicht auf der üblichen AD-Infrastruktur vor Ort aufbauen?

2 Grundlagen

In Kapitel 2 „Grundlagen“ werden nun wichtige Grundlagen dargelegt, auf denen diese Forschungsarbeit aufbaut.

2.1 Definition von kleinen und mittleren Unternehmen (KMU)

Laut der Wirtschaftskammer Österreichs (WKO) [8] gibt es keine verbindliche Definition, stattdessen wird auf die Empfehlung der EU-Kommission [9] verwiesen. Diese nennt insgesamt vier Kriterien, um Unternehmen in unterschiedliche Kategorien von „Kleinstunternehmen“ bis „Großunternehmen“ einzustufen. Die Tabelle 2.1 gibt hierzu einen Überblick der Kategorien:

	MitarbeiterInnen	Umsatz	Bilanzsumme	Eigenständigkeit
Kleinstunternehmen	bis 9	<= 2 Mio Euro	<= 2 Mio Euro	Stimmrechte
Kleinunternehmen	bis 49	<= 10 Mio Euro	<= 10 Mio Euro	im Fremdbesitz
Mittlere Unternehmen	bis 249	<= 50 Mio Euro	<= 43 Mio Euro	<25 %
Großunternehmen	ab 250	>50 Mio Euro	>43 Mio Euro	

Tabelle 2.1: Übersicht der Definition von KMUs

Allerdings ist anzumerken, dass in der Empfehlung der EU-Kommission [9, p. 5-6, Art. 3 Abs. 2-4] Ausnahmen für das Kriterium „Eigenständigkeit“ bestehen. Zusätzlich gibt die WKO zu bedenken, dass in der Praxis die Einordnung aufgrund mangelnder Informationen der Unternehmen schwieriger ist und die Anzahl der MitarbeiterInnen das primäre Kriterium ist, nach dem Unternehmen den Kategorien zugeordnet werden.

2.2 SaaS, PaaS und IaaS im Überblick

Die drei Begriffe SaaS, PaaS und IaaS bedeuten im Allgemeinen einen Cloud-Computing-Servie, der von einem Drittanbieter zur Verfügung gestellt wird, deren Abkürzungen folgende Bedeutung haben:

- IaaS = Infrastructure-as-a-Service
- PaaS = Platform-as-a-Service
- SaaS = Software-as-a-Service

Die Abkürzungen beschreiben den Anteil der ausgelagerten Komponenten in die Cloud. Umso mehr dieser Schichten an einen Cloud Provider ausgelagert werden, desto weniger Kontrolle besitzt man bzw. mehr Bereiche werden vom Anbieter verwaltet. Die Abbildung 2.1 von Red Hat [10] bietet hierfür einen Überblick der oben beschriebenen Kategorien inklusive derer Schichten und setzt diese mit einer On-Premises Server-Infrastruktur in Vergleich.

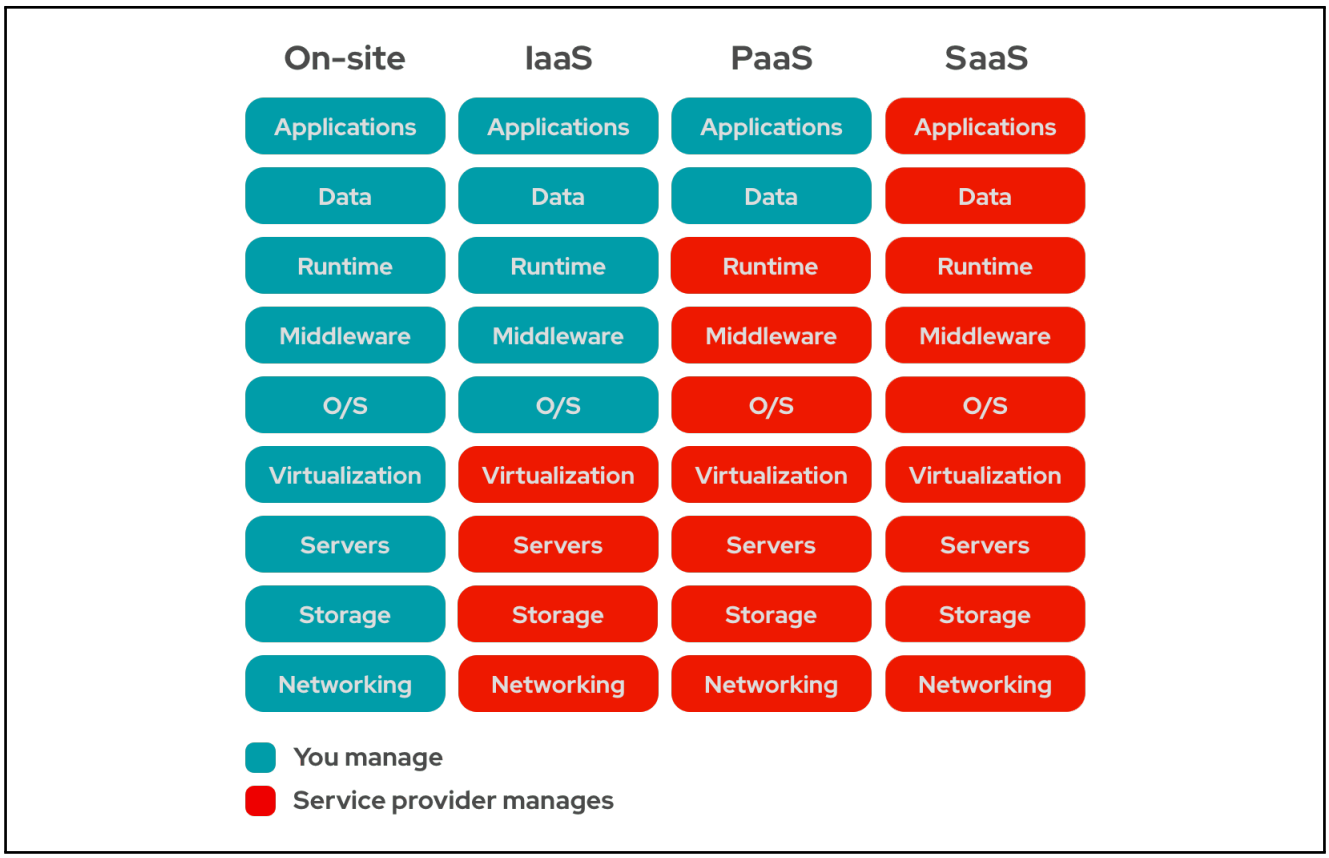


Abbildung 2.1: Übersicht der Cloud-Computing Modelle [10]

2.2.1 On-Premises

Der Begriff On-Premises bedeutet so viel wie „in den eigenen Räumlichkeiten“ oder „vor Ort“ und meint auf die IT bezogen die Nutzung der unternehmenseigenen Server in einer eigenen IT-Umgebung. Die Infrastruktur ist somit vollständig unter der Kontrolle des Unternehmens, wodurch Vorteile wie die Datenhoheit und Datenschutz aber auch Nachteile wie erhebliche Kosten durch Schulung der MitarbeiterInnen und Wartungsaufwand entstehen [11].

2.2.2 Infrastructure-as-a-Service

Im Vergleich zum On-Premises-Modell fällt bei IaaS die Virtualisierungstechnologie inklusive deren Komponenten wie Speicher und Netzwerk weg. Der Cloud-Anbieter stellt ein Infrastruktur-Service wie Speicher oder Virtualisierung über eine Cloud oder dem Internet zur Verfügung, die Kosten werden den Unternehmen hingegen nach dem Pay-as-you-go-Prinzip verrechnet, wodurch nur der tatsächliche Verbrauch bezahlt werden muss. Die physische Wartung der eigenen Server-Infrastruktur im Serverraum bzw. im Rechenzentrum entfällt und Infrastruktur kann bequem via Dashboard oder Application Programming Interface (API) angelegt oder entfernt werden. Für die Unternehmen bietet sich an, dass temporär für eine Entwicklungsumgebung oder ressourcenintensive Zeiten wie Weihnachten bei Online-Shops zusätzliche Kapazität gebucht werden kann [10].

2.2.3 Platform-as-a-Service

PaaS geht hier einen Schritt weiter und stellt neben den Leistungen von IaaS auch eine Reihe an nützlichen Werkzeugen bereit [12]. So erhalten EntwicklerInnen beispielsweise eine fertige Entwicklungsumgebung und können sich auf das Kerngeschäft der Softwareentwicklung konzentrieren – Aufwand für Software- und Hardwarewartung entfällt gänzlich. [10] Während die Vorteile einer Cloud zunehmen, steigt auch der Kontrollverlust über die Systeme. Hier ist sogar ein Vendor Lock-in möglich, da nur bestimmte Programmiersprachen von den einzelnen PaaS-Anbietern unterstützt werden [12].

2.2.4 Software-as-a-Service

SaaS beschreibt die weitreichendste Auslagerung eines Services an einen Cloud-Anbieter. Die AnwenderInnen interagieren direkt mit der Software, während im Hintergrund Software-Updates, Hardware-Wartungen und Fehlerbehebungen vom Anbieter durchgeführt wird. Mit ungefähr 1,8 Milliarden monatlichen BenutzerInnen ist Google Mail eine sehr populäre SaaS-Applikation [13]. Die Vorteile für kleine Unternehmen

liegen mit dem geringsten Aufwand auf der Hand, allerdings besteht hier auch die größte Abhängigkeit, wodurch das Vertrauen zum Cloud-Provider umso wichtiger ist [10].

2.3 IT-Budget/IT-Security-Budget

Das IT-Budget ist die Schätzung der IT-Ausgaben des Unternehmens für einen Zeitraum von 12 Monaten. Das IT-Budget umfasst u.a. Hardware, Software, Personal, Outsourcing, Disaster Recovery und Raumkosten, die mit der Unterstützung der IT im Unternehmen verbunden sind. Die Kosten umfassen auch alle Steuern (mit Ausnahme der Mehrwertsteuer, die dem Unternehmen erstattet wird) [6].

In der Praxis sind Informationen für die Ausgaben der Unternehmen äußerst gering und undurchsichtig. Das IT-Budget variierte je nach anstehenden Projekten und müsste über mehrere Jahre normalisiert gesehen werden. Zusätzlich bestehen in der Praxis oft Unklarheiten welche Ausgaben tatsächlich dem IT-Budget zuzuschreiben sind, wodurch womöglich die Ausgaben zwischen Firmen schwer miteinander vergleichbar sind. Vor allem kleine Firmen können oder wollen nicht ein Vollzeitäquivalent als IT-AdministratorIn einstellen und die MitarbeiterInnen übernehmen daher womöglich zusätzlich Nicht-IT-relevante Tätigkeiten, wodurch eine genaue Abrechnung der tatsächlich abgeleisteten Stunden ebenfalls schwerfällt. Abschließend muss erwähnt werden, dass die Ausgaben für die IT auch stark zwischen den Branchen schwankt [14].

Einer Studie der Firma „Ailean Inc“ zufolge betragen die Ausgaben für die IT bei kleinen Firmen 6.9%, bei mittelgroßen Unternehmen 4.1% und bei großen Unternehmen 3.2% des Jahresumsatzes. Befragt wurden Firmen in den USA, wodurch hervorgehoben werden muss, dass die Schwellen hinsichtlich der Größeneinteilung nicht direkt auf die KMUs in Österreich übertragen werden können. So definiert „Computer Economics“ die kleinen Firmen mit einen IT-Budget von weniger als 5 Mio. Dollar, die mittelgroßen Unternehmen mit zwischen 5 Mio. und 20 Mio. Dollar und die großen Unternehmen mit mindestens 20 Mio. Dollar [14].

Übertragen auf die Einteilung im Abschnitt 2.1 „Definition von kleinen und mittleren Unternehmen (KMU)“ bedeutet das, dass zumindest alle KMUs als kleines Unternehmen gelten, wenn die USA als Referenz herangezogen wird. Basierend auf den Angaben der Umsätze mit den prognostizierten 6.9% als IT-Budget, bedeutet das, dass den Unternehmen zwischen ca. 140.000 Euro und ca. 3.5 Mio. Euro für IT bereitstehen.

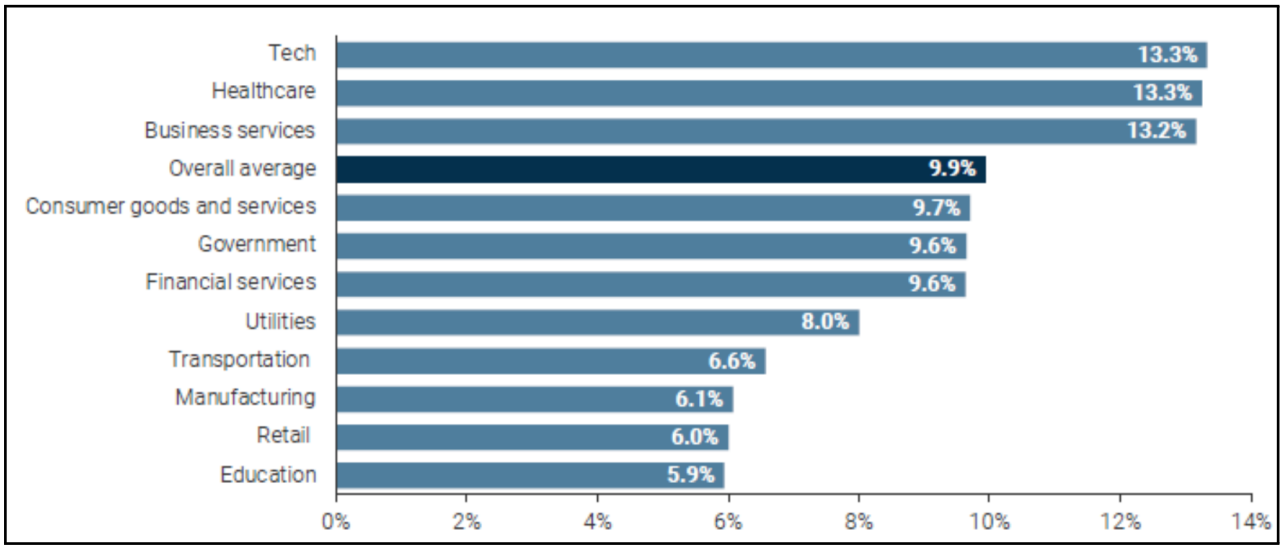


Abbildung 2.2: Ausgaben für IT-Security als Prozentsatz vom IT-Budget für das Jahr 2022 [7]

Im Jahr 2022 beträgt das Budget für IT-Security-Maßnahmen im Durchschnitt 9.9% vom IT-Budget, allerdings variieren auch hier die Ausgaben sehr stark zwischen den Branchen. Eine Übersicht über die Ausgaben im Verhältnis mit der Branche liefert die Abbildung 2.2 [7].

2.4 SAMBA

Samba ist eine Zusammenstellung aus vielen Open-Source-Programmen und stellt seit 1992 die Funktionalität als Datei- und Druckerserver für alle Endgeräte bereit, die für den Dateizugriff Server Message Block (SMB) bzw. Common Internet File System (CIFS) unterstützen. Samba selbst steht unter der Lizenz „GNU General Public License“ kostenlos verfügbar und kann beliebig eingesetzt werden [15]. Mit der Version Samba 4, welche im Jahr 2012 veröffentlicht wurde, unterstützt Samba die Bereitstellung eines Active Directory Domain Controller auf Gesamtstrukturfunktionsebenen (Forest functional level) von Windows Server 2008 R2 [16]. Mit Stand Februar 2023 ist die Version 4.17 aktuell, wobei der Lebenszyklus einer Version alle sechs Monate vom Status heruntergestuft wird. In den ersten sechs Monaten wird eine Version vollständig unterstützt, bis es anschließend in den nächsten sechs Monaten mit geringerem Fokus Updates für Fehler und Sicherheitslücken erhält, um schlussendlich die letzten sechs Monate ausschließlich mit Sicherheitsupdates versorgt zu werden [17].

Samba erfreut sich großer Beliebtheit und ist in vielen Linux-Distributionen enthalten. Zusätzlich integrieren viele Firmen Samba in ihre eigenen großen Produkte, wie diese Übersicht [18] zeigt. Darüber hinaus gibt es eine lange Liste [19] an Firmen, die Support beim Einsatz von Samba anbieten.

2.5 Backporting

Backporting beschreibt eine Möglichkeit Fehler und Sicherheitslücken in Programmen zu beheben, ohne dass dabei die Stabilität des Betriebssystems und der darauf laufenden Services zu gefährden. Dazu werden die Fixes aus der neuen Version extrahiert, und in die alte Version zurückportiert bzw. integriert. Primär werden beim Backporting Fehler und Sicherheitslücken in der Software gelöst, neue Funktionen werden hingegen nicht behandelt und sind erst in den neuen Versionen zu finden. Der Grund für diesen Aufwand besteht darin, dass die Systeme möglichst stabil laufen sollen und vor allem bei großen Programmen die Abhängigkeiten zu anderer Software unübersichtlich und kompliziert werden kann. Zusätzlich können neue Versionen neben der Fehlerbehandlung auch neue Funktionen beinhalten, die Veränderungen im Betrieb bewirken können, auf die die EntwicklerInnen nicht vorbereitet sind [20].

Abbildung 2.3: Versionsschema Red Hat am Beispiel des Pakets Bash [20]

In Abbildung 2.3 ist das Versionsschema von Red Hat für das Paket „Bash“ dargestellt. Es zeigt, dass neben dem Namen, der Version und der kompilierten Architektur ein zusätzliches Versionsfeld eingebaut wird, um weiterhin eine Übersicht über die behobenen Sicherheitslücken in den Backports gewährleisten zu können. Backporting wird unter anderem bei den Linux-Distribution von Red Hat (RHEL, CentOS) oder Debian (inklusive Ubuntu) angeboten [20][21][22].

2.6 Active Directory

Active Directory (AD) ist ein Produkt von Microsoft und vereint einige Komponenten, die zusammen einen De-facto-Standard im Bereich des Verzeichnisdienstes darstellen. Zu den Hauptkomponenten zählen:

- Lightweight Directory Access Protocol (LDAP)
- Server Message Block (SMB)
- Domain Name System (DNS)
- Kerberos

Informationen in AD werden als Objekte abgespeichert, deren Eigenschaften wiederum über Attribute definiert werden. Objekte können in zwei Hauptkategorien eingeteilt werden – Container wie Organisationseinheiten (engl. Organizational Unit (OU) oder Gruppen, die weitere AD-Objekte enthalten können und Blätter (Leafs) wie Computer, BenutzerInnen und Drucker, die keine AD-Objekte beinhalten können [23].

Eine Active-Directory-Gesamtstruktur (Active Directory Forest) ist die höchste Organisationsebene innerhalb von Active Directory. Innerhalb von Gesamtstrukturen können wiederum mehrere Domänen existieren. In einer Domäne bzw. Gesamtstruktur können Windows-Server mit unterschiedlicher Version als Domänencontroller eingesetzt werden, wobei die Gesamtstrukturfunktionsebene bzw. Domänenfunktionsebene den gemeinsamen Nenner vorgeben. Mit neuen Versionen werden neue Features und Sicherheitsfunktionen unterstützt, die erst dann verwendet werden können, wenn alle ein bestimmtes Niveau haben. Soll in einer Domäne die Domänenfunktionsebene Windows Server 2016 eingesetzt werden, so müssen alle Domänencontroller mindestens Windows Server 2016 oder höher sein.

2.7 Zero-Trust-Modell

Beim Zero-Trust-Modell handelt es sich um Sicherheitskonzept, welches grundsätzlich allen Diensten, AnwenderInnen und Geräten misstraut. Hier wird kein Unterschied zwischen Diensten, AnwenderInnen und Geräten innerhalb oder außerhalb des eigenen Netzwerks gemacht. Sämtliche Zugriffe werden überprüft und alle BenutzerInnen und Dienste müssen sich authentifizieren.

Ziel des Modells ist es, das Risiko für Firmennetze bzw. Firmenanwendungen zu minimieren und vor internen und externen Bedrohungen zu schützen. Herkömmliche Sicherheitskonzepte stufen lediglich externe Zugriffe als Risiko ein und vertrauen den internen Systemen [24].

2.8 Zugriffsschutz im Netzwerk

Der Zugriffsschutz im Netzwerk beschreibt die Verfügbarkeit von Netzwerkressourcen auf entsprechende Endgeräte, die auch tatsächlich Zugriff haben sollen. Hierfür bieten sich einige Methoden an, die von einfachen Lösungen bis hin zu komplexen Systemen reichen.

Die einfachste Lösung ist die Isolierung der Endgeräte, in der alle Clients im gleichen Netzwerksegment sind, aber nicht untereinander kommunizieren können. Mit dieser Methode ist allerdings die Freigabe von internen Netzwerkressourcen nicht möglich.

Port-Security beschreibt einen Ansatz, bei dem die MAC-Adresse des Clients überprüft wird. Netzwerkgeräte wie Netzwerk-Switches, die auf Layer 2 arbeiten, verknüpfen einen Switch-Port mit einer oder mehreren MAC-Adressen. Hierdurch wird erreicht, dass nur noch erlaubte MAC-Adressen mit dem Switch kommunizieren können. Da die manuelle Zuordnung von MAC-Adressen und Switch-Ports zeitaufwendig sein kann, bietet sich in der Praxis „Sticky MAC Address“citecisco2022portsecurity an, wodurch dynamisch gelernte MAC-Adressen in die Konfiguration übernommen werden und nicht nach einem Neustart des Switches verloren gehen.

Der Nachteil an dieser Methode ist die Tatsache, dass keine Authentifizierung stattfindet und die MAC-Adresse nicht fälschungssicher ist. Physisch exponierte Geräte wie Drucker haben oft die MAC-Adresse außen am Gehäuse stehen, wodurch der Schutz von Port-Security leicht umgangen werden kann.

Mit 802.1X ist die Anmeldung von Clients im Netzwerk erforderlich, wobei die Authentifizierung und Autorisierung an einer zentralen Stelle durchgeführt wird. Die Zugangsdaten von Computer oder BenutzerInnen werden hierzu an den Netzwerk-Switch oder dem AP übertragen, der diese an einen neutralen Server weiterleitet und die Anmeldung überprüft. Das Ergebnis der Validierung wird anschließend an den Authenticator zurückgemeldet, der den Zugriff blockiert oder erlaubt inklusive spezifischer Berechtigung (z. B. VLAN-ID). In der Praxis wird 802.1X häufig eingesetzt und hat sich zum De-facto-Standard in der Netzwerkauthentifizierung entwickelt. Der Standard wird von vielen Geräten und Systemen unterstützt, wodurch die Gefahr eines Vendor Lock-ins nicht besteht.

Für jene Geräte, die nicht mit 802.1X kompatibel sind, existiert mit MAC Authentication Bypass (MAB) eine alternative Möglichkeit den Zugriff ins Netzwerk zu verwalten. Hier wird, wie bei Port-Security, die MAC-Adresse des Clients für die Evaluierung des Zugriffs herangezogen, allerdings entscheidet, wie bei

802.1X, eine neutrale Stelle, ob der Zugriff gewährt oder abgelehnt wird. Der Vorteil zu Port-Security ist die zentrale Registrierung der MAC-Adressen, wodurch die manuelle Konfiguration der Switches entfällt, und die Sichtbarkeit im Monitoring-System bzw. einem NAC.

Bevor eine der zuvor beschriebenen Lösungen in Betracht gezogen werden kann, sollte im Vorhinein der gewünschte Schutzbedarf des Unternehmens evaluiert und ausgearbeitet werden. Dabei ist wichtig festzustellen, welche Kategorien von Assets geschützt werden sollen, um eine möglichst realistische Einschätzung des Bedarfs treffen zu können.

2.9 Benutzername-Passwort-Kombination vs. Zertifikat

Eine Benutzername-Passwort-Kombination beschreibt den Zusammenhang zwischen einem BenutzerInnen-Namen wie Nickname, E-Mail-Adresse, Telefonnummer, usw. und einem möglichst sicheren Kennwort. Mithilfe des BenutzerInnen-Namens kann das jeweilige System die AnwenderIn eindeutig erkennen, mit dem Passwort weist diese anschließend nach, dass es sich tatsächlich um die vorgegebene Person handelt [25].

Ein Zertifikat im IT-Kontext beschreibt einen digitalen Ausweis für eine Person oder Gerät. Im Hintergrund existieren zwei Zeichenketten, die über einen kryptografischen asymmetrischen Algorithmus wie Rivest–Shamir–Adleman (RSA) oder Elliptic Curve Cryptography (ECC) zusammenhängen. Einer der Zeichenketten heißt öffentlicher Schlüssel und ist somit allen bekannt; die zweite Zeichenkette ist der geheime Schlüssel und nur die Person bzw. das Gerät darf diesen wissen.

Dem „Data Breach Investigations Report 2021“ von Verizon zufolge soll mit 61% die Verwendung von missbrauchten Zugangsdaten wie Kennwörter der primäre Angriffsvektor sein, der den Zugriff auf interne Systeme durch unautorisierte Angreifer ermöglicht. Des Weiteren zeigt der Bericht auf, dass dabei Phishing in über einem Drittel der „Data Breaches“ genutzt wurde. AnwenderInnen neigen dazu, dass diese einfache Kennwörter verwenden oder sie bei mehreren Systemen gleichzeitig einsetzen, und die Verantwortung für den eigenen Schutz auf die Unternehmen übertragen [26].

Microsoft empfiehlt daher im Kontext von WLAN und VPN den Wechsel von einer Passwort-basierenden Anmeldungen wie „PEAP-MSCHAPv2“ und „EAP-MSCHAPv2“ zu einer Zertifikat-basierenden Authen-

tifizierung wie „PEAP-TLS“ oder „EAP-TLS“ [27].

2.10 IEEE 802.1Q

Der Standard IEEE 802.1Q, oder auch umgangssprachlich „dot1q“ oder „VLANs“, setzt auf Schicht 2 des OSI-Modells an und beschreibt in der Netzwerktechnik eine Möglichkeit der Netzwerksegmentierung. Mit diesem Standard wird ein physischer Netzwerk-Switch in mehrere, virtuelle Switches „zerschnitten“. Clients, die mit unterschiedlichen virtuellen Switches bzw. Netzwerksegmenten verbunden sind, können nun nicht mehr direkt miteinander kommunizieren. Diese Methode hat den Vorteil, dass nun die Broadcast-Domäne kleiner wird und es somit eine positive Auswirkung auf die Netzwerkleistung hat. Zusätzlich bewirkt diese Trennung einen Sicherheitsvorteil, da nun die Geräte über vorab definierte Regeln kommunizieren müssen bzw. die Kommunikation gänzlich unterbunden werden kann, falls dies nicht gewünscht ist [28].

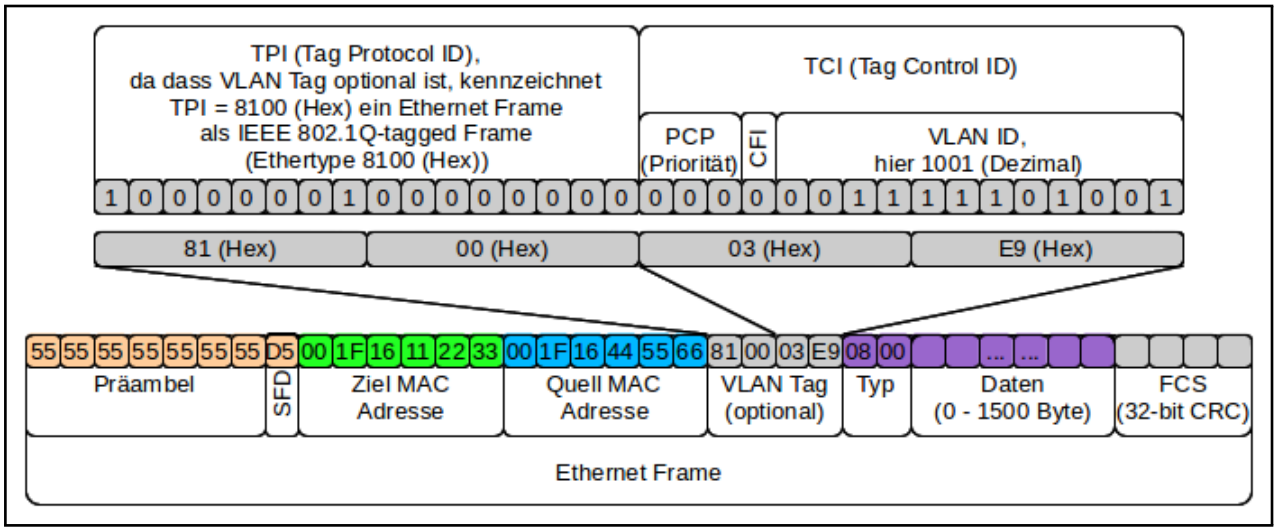


Abbildung 2.4: Aufbau Ethernet Frame mit 802.1Q [29]

Technisch wird diese Segmentierung mit dem Anpassen des Ethernet-Frames umgesetzt. Hierfür werden die notwendigen Informationen in zwei 2Byte-Blöcken zwischen der Quell-MAC-Adresse und dem „EtherType“, der das Layer3-Protokoll in der Payload definiert, ergänzt. In Abbildung 2.4 wird diese Anpassung grafisch dargestellt [29].

2.11 IEEE 802.1X

Mit dem Standard IEEE 802.1X existiert ein Framework, mit dem eine Geräteauthentifizierung- und autorisierung ermöglicht wird, um die eigenen Netzwerke abzusichern und interne Services somit vor unerwünschten Zugriffen zu schützen. Während bei IEEE 802.11 bzw. WLAN zumindest mit WPA2/3-Personal und der Eingabe eines Pre-shared-Keys (PSK) eine Möglichkeit besteht, die Zielgruppe einzuschränken, gibt es bei IEEE 802.3 bzw. LAN nur schlecht skalierbare Lösungen wie Port-Security. Der flächendeckende Einsatz in der Praxis darf allerdings stark angezweifelt werden, da diese Lösung einen hohen Aufwand bedeutet und dennoch False-Positives nicht vermieden können.
Mit 802.1X müssen sich alle Entitäten zuerst korrekt authentisieren, bevor diese an der Netzwerkkommunikation teilnehmen können – das betrifft sowohl WLAN als auch LAN.

Der Standard führt hierfür drei Rollen ein:

- Supplicant = Endgeräte wie Notebook, Smartphones, etc.
- Authenticator = Netzwerk-Switch, WLAN-Controller, Access Point (AP)
- Authentication Server = AAA-Server

Der Supplicant bzw. eine Software am Client der MitarbeiterInnen weist sich gegenüber dem Authenticator aus und überträgt dabei die Zugangsdaten über das Protokoll Extensible Authentication Protocol (EAP), wobei mit Extensible Authentication Protocol over Local Area Network (EAPoL) und Extensible Authentication Protocol over Wireless (EAPoW) angepasste Varianten für das spezifische Übertragungsmedium bestehen. Solange die Authentifizierung nicht abgeschlossen ist, werden ausschließlich EAP-Frames angenommen, und der restliche Netzwerkverkehr wird verworfen. Dieser Zustand wird in der Abbildung 2.5 von NetworkLessons [30] dargestellt, wobei hier ein physischer Switch-Port abgebildet ist und daher EAPoL zum Einsatz kommt.

Der Authenticator verpackt die EAP-Pakete in eines der AAA-Transportprotokolle wie RADIUS oder Diameter und schickte diese zum Authentication Server. Dieser entscheidet anschließend, ob der Zugriff gewährt oder abgelehnt wird, und meldet die Antwort zurück zum Authenticator. Ist die Anmeldung erfolgreich, so wird der Zugriff freigeschalten, andernfalls kann das Endgerät keine Verbindung zum Netzwerk herstellen. Die Abbildung 2.6 von SecureW2 [31] liefert hierfür eine Übersicht der einzelnen Rollen in 802.1X.

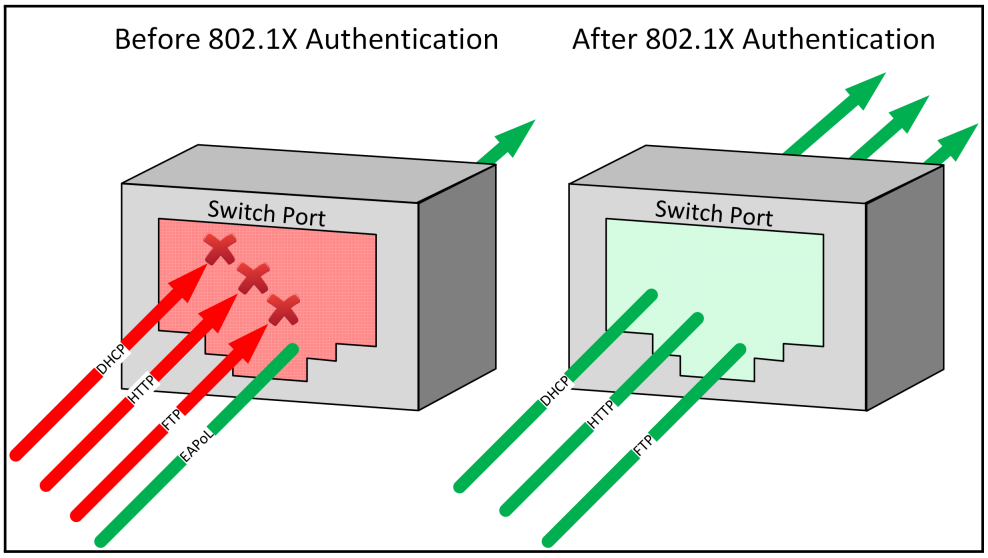


Abbildung 2.5: Zustand eines Switchports vor und nach einer Authentifizierung [30]

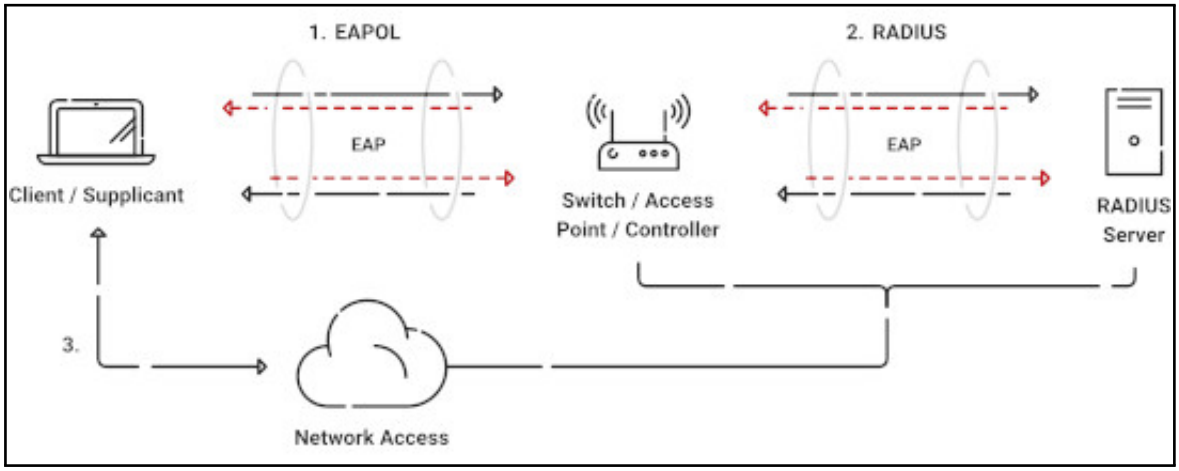


Abbildung 2.6: Konzept IEEE 802.1X [31]

2.12 AAA

Der Begriff „AAA“ ist eine Abkürzung für Authentication, Authorization und Accounting, und beschreibt ein Framework, um Zugriff auf Services zu kontrollieren, Richtlinien zu erzwingen und die Nutzung der einzelnen Services zu protokollieren, um später eine Kostenabrechnung durchzuführen. Im Kontext einer Netzwerkauthentifizierung liegt der Fokus auf der Authentifizierung (Welche Person bekommt Zugriff?) und Autorisierung (Was darf diese Person machen?). Das dritte „A“ für Accounting hat allerdings ebenfalls eine wichtige Rolle, weil hierüber das Logging von Systemereignissen wie Neustarts von Geräten oder ausgehenden Verbindungen mit Telnet oder Secure Shell (SSH) realisiert wird [32]. Vereinfacht gesagt erhält der AAA- oder Authentication-Server die Anfrage von Clients und entscheidet, ob Zugriff erlaubt bzw. abgelehnt werden soll, und wenn ja mit welchem Zugriff (z. B. VLAN-ID). [33]

Für die Übertragung der Daten zwischen dem Authenticator (Switch) und dem AAA-Server existieren diverse Protokolle wie RADIUS, TACACS+ oder Diameter, welcher als Nachfolger von RADIUS gilt [34].

RADIUS steht für Remote Authentication Dial-In User Service und das Konzept existiert bereits über 30 Jahre [35]. Im Jahr 1997 wurde es schließlich im Request for Comments (RFC) 2058 und RFC 2059 definiert, und später durch andere RFCs ersetzt oder ergänzt [36]. Viele Provider nutzen RADIUS für die Einwahl von KundInnen in ein analoges, ISDN-, DSL-Netzwerk [34]. Aufgrund dieses Alters existieren bereits einige Schwächen im Protokoll. Während bei RADIUS ausschließlich die Zugangsdaten wie Passwörter mit einem mittlerweile veralteten Verschlüsselungsalgorithmus geschützt werden, wird bei TACACS+ das gesamte Paket nach dem TACACS+-Header verschlüsselt [37].

Das RADIUS Attribut „2“ bzw. „User-Password“ wird in zwei Schritten verschleiert [38, p. 11-21]:

- Schritt 1: Mithilfe des Hashalgorithmus „MD5“ wird der Hash-Wert aus dem „Shared Secret“, ein zuvor auf dem Client und Server hinterlegtes Passwort, und dem „Request Authenticator“, einer Zufallszahl, berechnet.
  $MD5(SharedSecret + RequestAuthenticator)$
- Schritt 2: Anschließend wird dieser Hash-Wert mit dem Passwort der BenutzerIn mittels XOR verknüpft.
  $Ergebnis\ von\ Schritt1 \oplus Passwort\ von\ BenutzerIn$

Zusätzlich beinhalten die RADIUS-Pakete des RADIUS-Servers (Access-Accept, Access-Reject und Access-Challenge) ein Feld mit dem Namen „Response Authenticator“, welches das MD5-Hash-Ergebnis einiger Felder im RADIUS-Paket inklusive dem Shared Secret enthält [38, p. 11]. Eine Übersicht der eingesetzten Felder liefert die folgende mathematische Darstellung:

$$ResponseAuth = MD5(Code+ID+Length+RequestAuthenticator+Attributes+SharedSecret)$$

Das Code-Feld beschreibt den Typ des RADIUS-Pakets wie beispielsweise „Access-Request“, „Access-Accept“ oder „Access-Reject“. Die RADIUS-Attribute enthalten hingegen Informationen, die für die Authentifizierung und Autorisierung benötigt werden, wie zum Beispiel „User-Name“, „User-Password“ oder „NAS-IP-Address“.

Zusammengefasst enthält die Antwort vom RADIUS-Server eine mit dem MD5-Hash-Algorithmus erstellte Signatur des RADIUS-Pakets. Mit RFC 2869 wurde die Unterstützung für EAP definiert, wodurch die Möglichkeit zusätzlicher Authentifizierungsmethoden um Smartcards, Kerberos, Zertifikate, usw. erweitert wurde [39].

In der Praxis kann der AAA-Server oft nicht selbst entscheiden ob die Zugangsdaten des Endgeräts korrekt sind. Daher existiert in vielen Unternehmen zumindest ein weiterer Service mit dem Namen „Identity-Provider“, der die Zugangsdaten verwaltet und diese auf Gültigkeit überprüfen kann. Wie die Abbildung 2.7 zeigt, kann dies beispielsweise ein Active Directory oder eine CA sein.

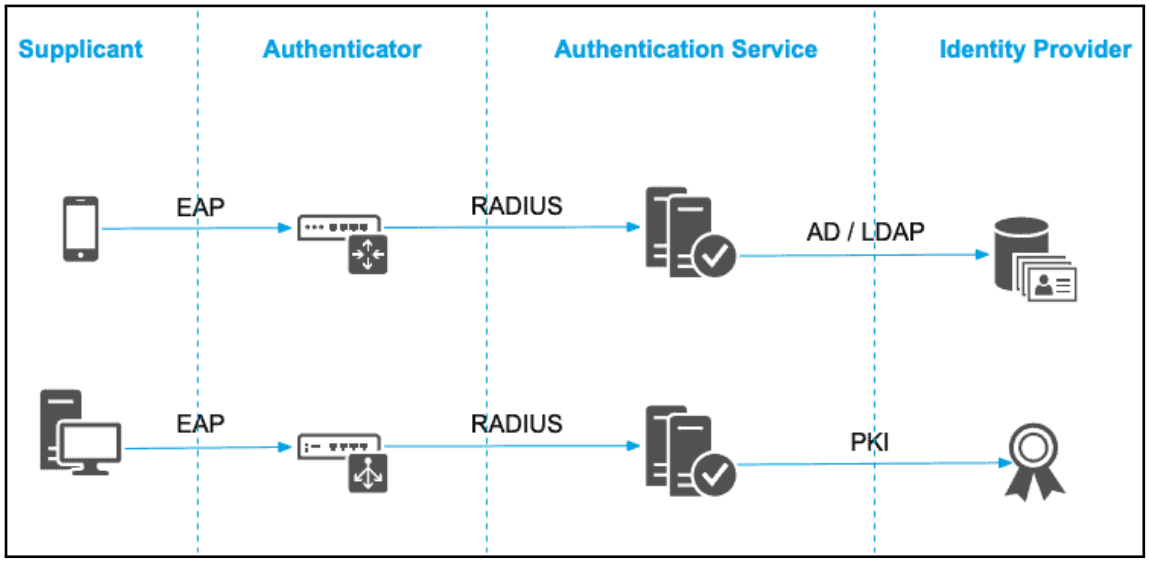


Abbildung 2.7: Konzept IEEE 802.1X mit Identity-Provider [40]

2.13 NAC-Lösung

NAC oder Network Access Control setzt auf AAA auf und ergänzt dieses Konzept um einige Features. Als Hersteller von NAC-Lösungen weist Cisco u.a. folgende Fähigkeiten seinen Produkten zu [41]:

- „Policy lifecycle management“: Zusammen mit der Analyse von Endgeräten (Profiling) können so spezifische Zugriffsrechte basierend auf Abteilungen, Endgeräten oder deren Sicherheitsrichtlinien erteilt werden.
- „Profiling and visibility“: Erkennt und kategorisiert die AnwenderInnen und deren Endgeräte
- Netzwerkzugang für Gäste: Beschreibt das Management für den Zugang der Gäste ins Netzwerk, um beispielsweise Zugriff ins Internet zu erhalten. Das beinhaltet auch die Registrierung und Authentifizierung der Gäste, die Verwaltung über die Dauer des Zugriffes und das allgemeine Monitoring der Gäste.
- Überprüfung der Sicherheitsrichtlinien: Hier werden die AnwenderInnen und deren Endgeräte mit den vorab konfigurierten Zugriffsrichtlinien abgeglichen. Besitzt ein Notebook beispielsweise kein aktives AntiViren-Programm bzw. sind deren Signaturen über einen Schwellenwert, kann der Zugriff automatisch blockiert oder das Endgerät isoliert werden.

Garnter [42] zufolge können die Funktionen einer NAC-Lösung in die drei Kategorien „Base Features“, „Optional Integrations“ und „Emerging Use Cases“ eingeteilt werden. In Abbildung 2.8 wird die Einteilung inklusive der zugeordneten Features dargestellt.

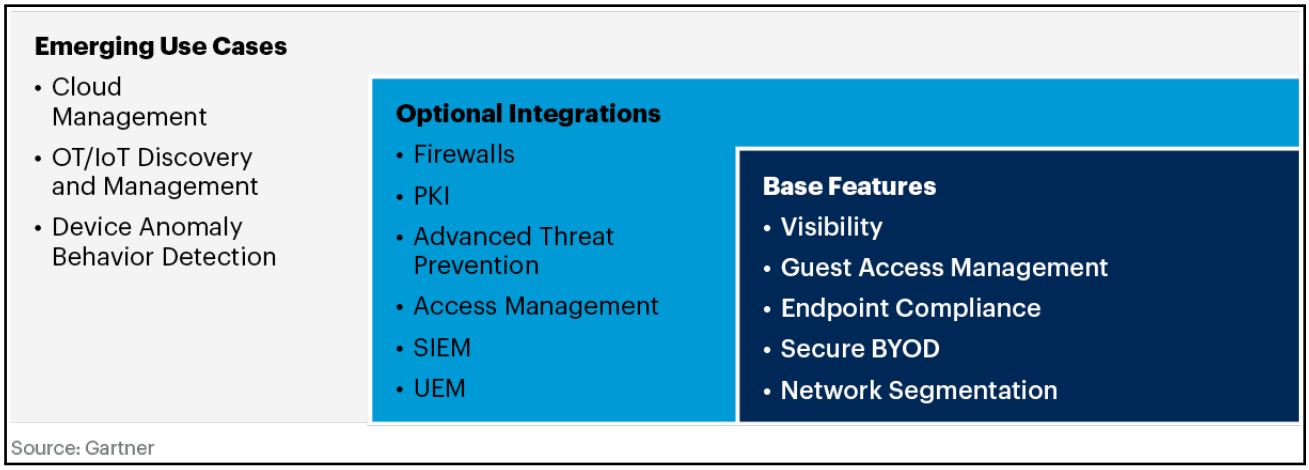


Abbildung 2.8: Funktionsvielfalt von NACs laut Gartner [42]

Anhand der Einschätzung von Garnter kann abgelesen werden, dass die Grundfunktionen bereits seit vielen Jahren angeboten werden und somit ausgereift sind, aber hier die Vernetzung zwischen den Features teils eingeschränkt ausgenutzt wurde. Über die Jahre haben sich die Plattformen der Anbieter entwickelt und es wurden Möglichkeiten geschaffen, andere Firmen von Sicherheitslösungen wie Firewalls, IDS/IPS, SIEM und Co. in das eigene Ecosystem einzubinden. Hier liegt der Fokus auf der Anreicherung von Informationen, um mit diesen anschließend treffsichere Entscheidungen und Reaktionen liefern zu können. Mit Cloud, Internet of Things (IoT) bzw. Operational Technology (OT) und dem abnormalen Verhalten von Geräten kommen nun Themen in der IT auf, die allgemein relativ neu am Markt vertreten sind, und noch möglicherweise Entwicklungsbedarf haben.
Es muss zudem festgehalten werden, dass durch eine Recherche viele Definitionen zu NACs gefunden werden, die aber alle ungefähr die gleichen Funktionen beschreiben.

2.14 RadSec

Wie bereits zuvor in Kapitel Abschnitt 2.12 „AAA“ aufgezeigt, existiert das RADIUS-Protokoll bereits seit geraumer Zeit und mittlerweile existieren einige Schwächen im Protokoll. Während dies bei Systemen vertretbar ist, welche gänzlich auf eine On-Premises Infrastruktur setzen, besteht ein Risiko von Angriffen und Informationsverlust durch Abhörungen bei Übertragungen in die Cloud.
Abhilfe soll hier der RFC 6614 [43] und RFC 7360 [44] bieten, welche die Übertragung von RADIUS-Paketen in einen verschlüsselten Tunnel absichert. Während der erste RFC auf Transport Layer Security (TLS) und somit Transmission Control Protocol (TCP) setzt, basiert der zweite RFC auf Datagram Transport Layer Security (DTLS) und User Datagram Protocol (UDP). Für den RFC 6614[1] gibt es auch mit „RadSec“ [2] einen sprechenden Namen [46], welcher auf Seite der Authenticator bereits bei einigen Herstellern wie Cisco [47], HP Aruba [48] und Juniper [49] zur Verfügung steht.

Für den Fall, dass die Hardware keine Unterstützung für RadSec besitzt, kann auf den frei verfügbaren RadSec Proxy zurückgegriffen werden, der RADIUS-Pakete entgegennimmt und diese anschließend verschlüsselt überträgt. Die Anwendung kann beispielsweise auf dem RADIUS-Server oder einem dedizierten Server installiert werden und unterstützt die Verschlüsselung mit TLS und DTLS [50].

[1] RFC 6614 wurde bereits durch RFC 8996 [45] aktualisiert und erfordert nun „TLS1.2 oder höher“ anstatt „TLS1.1 oder höher“.
[2] Die IANA hat den Namen „RadSec“ dem Netzwerk-Port „2083“ für sowohl TCP (RFC 6614) als auch UDP (RFC 7360) zugewiesen.

Wie bereits erwähnt bietet Microsoft mit seinem NPS einen sehr populären RADIUS-Server an, wobei dieser keine native Unterstützung für RadSec besitzt. Auch hier kann der kostenlose RadSec Proxy helfen, in dem die RADIUS-Pakete vom NPS über den Proxy in die Cloud weitergeleitet (forwarden) werden [46].

Es muss allerdings erwähnt werden, dass laut dem RFC 6614 [43, Sec. 2.3.4] das geheime Passwort (Secret) als „RadSec“ definiert sein muss. Dennoch wird mit RadSec die Netzwerkübertragung über einen unsicheren Kommunikationskanal abgesichert, wodurch bei der Auswahl von Cloud-RADIUS-Servern darauf geachtet werden sollte, dass der Anbieter auch den RFC 6614 unterstützt.

2.15 Validierung der Zertifikate

Obwohl mit WPA2/3-Enterprise und 802.1X ein De-facto-Standard existiert, und dieser als sicher gilt, kann es dennoch sein, dass die Zugangsdaten der MitarbeiterInnen in fremde Hände fallen. Dies kann dann passieren, wenn die Endgeräte der AnwenderInnen keine Validierung des Zertifikats vom RADIUS-Server durchführen [51].

AngreiferInnen strahlen über einen eigenen Access Point (AP) jene Service Set Identifier (SSID) aus, die sie angreifen wollen. Früher oder später wird sich ohne diese Validierung ein Endgerät mit dem Fake-AP verbinden, wobei hier nützliche Informationen wie Zugangsdaten abgefangen werden können. In der Praxis ist das Ergebnis des Angriffs von vielen Faktoren wie beispielsweise der gewählten EAP-Verfahren abhängig. Allerdings kann dieser Angriffsvektor vermieden werden, wenn eine Validierung des Server-Zertifikats durchgeführt wird.

Zu Beginn der Anmeldung bei 802.1X tauschen der RADIUS-Server und der Client Daten bezüglich eines kryptografischen Handshakes aus, wobei hier auch das Zertifikat des Servers übertragen wird. Ist diese Überprüfung auf den Endgeräten aktiviert, wird nun kontrolliert, ob das Zertifikat legitim ist und ob diesem vertraut wird. Der digitale Nachweis kann hierfür von einer öffentlichen oder internen Zertifizierungsstelle (engl. Certificate Authority, CA) ausgestellt worden sein. Das Endgeräte prüft nun, ob dieser das Zertifikat von der CA installiert hat bzw. ob diesem vertraut wird. Falls die Überprüfung positiv ausfällt, wird eine Verbindung herstellt.

Dieser Check des Zertifikats kann nicht nur während der Anmeldung unter Verwendung von EAP-TLS oder PEAP durchgeführt werden, sondern bereits vorab beim Kommunikationsaufbau zwischen Authenticator und Authentication Server über das Protokoll RadSec [52].
Darüber hinaus ist beim Betriebssystem Android in der aktuellen Version (Android 13) die Validierung des Zertifikats bei der Verbindung mit WPA2-Enterprise Netzwerken erforderlich [53] – mit WPA3-Enterprise wurde dies eine allgemeine Anforderung [54].

2.16 Onboarding Software

Da die Konfiguration von 802.1X an vielen Stellen durchgeführt werden muss, und allgemein ein hohes Verständnis der Materie voraussetzt, kann es hier zu Fehlern in der Umsetzung kommen. So kann es etwa passieren, dass die oben erwähnte Überprüfung des Server-Zertifikats nicht aktiviert wird und somit ein potenzieller Angriffsvektor besteht.

Zusätzlich kann beispielsweise bei kleinen Firmen oder bei Bring-your-own-device (BYOD) kein zentrales Management der Endgeräte verfügbar sein, wodurch die Konfiguration, Zertifikate, usw. manuell auf die Geräte übertragen werden müssen, damit diese Zugriff auf das eigene Netzwerk erhalten.

Für diese Situation stellen Firmen wie SecureW2 mit „JoinNow MultiOS“ eine Software zur Verfügung, die von vielen Betriebssystemen unterstützt wird, und mit der die Konfiguration und die notwendigen Zertifikate für die Kommunikation auf dem Endgerät installiert werden kann [55]. Im konkreten Fall von SecureW2 empfiehlt dieser für diesen Onboarding-Prozess eine SSID ohne Kennwort zu erstellen, in welchem der Client manuell angemeldet und dabei zu einer speziellen Webseite von SecureW2 weitergeleitet werden, um die Software für das gewünschte Betriebssystem herunterzuladen [56].

3 Stand der Forschung

In Kapitel 3 „Stand der Forschung“ wird die aktuelle Literatur zu den drei Ansätzen vorgestellt.

3.1 802.1X Implementierungen für KMUs

Eine ausführliche Recherche zeigt, dass in diesem Bereich keine aktuellen Veröffentlichungen zu diesem Thema zu finden sind. Einzig eine Arbeit von Nicolae Tomai [57] aus dem Jahr 2007 versucht auf die Rahmenbedingungen von KMUs und deren Anforderungen beim Designen und Aufsetzen von sicheren drahtlosen Netzwerken einzugehen. Aufgrund des geringen Umfangs von sechs Seiten und der Tatsache, dass der Fortschritt in der IT große Sprünge macht, können die darin beschriebenen Informationen kaum verwertet werden. Zusätzlich werden die Themen sehr oberflächlich und allgemein beschrieben, und 802.1X wird nur marginal erwähnt.

Obwohl die Qualität der Studie und deren Ansätze mangelhaft ist, werden wichtige grundsätzliche Themen angesprochen. So ist es sicherlich sinnvoll, zuerst eine klare und durchdachte Lösung in der Theorie zu entwickeln, die später in die Praxis übertragen werden soll. Eine Bestandsaufnahme der aktuellen Geräte inklusive deren technischen Fähigkeiten hilft um Probleme, wie die fehlende Unterstützung von WLAN-Funktionen oder Verschlüsselungsmethoden, in der Implementierungsphase zu vermeiden. Zusätzlich soll sich jedes Unternehmen die Frage stellen, welche Anforderungen an drahtlose Netzwerke gestellt werden, und welcher Sicherheitsbedarf besteht.
Im Allgemeinen wird ein Lebenszyklus einer WLAN-Lösung beschrieben, der von der initialen Planungsphase über die Implementierung der tatsächlichen Lösung bis hin zur Entsorgungsphase umfasst. Darüber hinaus werden die folgenden Empfehlungen ausgesprochen:

- Die Verwendung von statischen IP-Adressen anstatt von DHCP
- Das Verstecken von Access Points vor Unbefugten
- Das Abdrehen von Access Points bei Nichtbenutzung

Diese Empfehlung können mit Hinblick auf aktuelle Sicherheitsmaßnahmen nicht unterstützt werden, da diese den täglichen Betrieb im Unternehmen negativ beeinflussen. Bedenkt man das geringe Budget von KMUs und den damit verbunden begrenzen IT-Ressourcen wäre es eine Verschwendung, wenn MitarbeiterInnen für manuelle Tätigkeiten wie der Verteilung von IP-Adressen oder dem Ein- und Ausschalten von Access Points eingesetzt werden. Mit Hinblick auf IPv6 wird ein Mechanismus zur Verteilung von Informationen im Netzwerk entweder über DHCPv6 oder SLAAC ein nahezu notwendiges Werkzeug sein. Des Weiteren werden die in dem Jahr 2007 aktuellen Authentifizierungs- und Verschlüsselungsvarianten vorgestellt.

3.2 Open Source NAC

Die Recherche nach einer Open Source basierten NAC-Lösung liefert zwei Arbeiten – der Fokus liegt einerseits auf Linux-Container wie Docker [58] und andererseits auf der Verwaltung von Identitäten und deren Richtlinien mit dem NAC-Produkt FlowNAC [59]. Die zuletzt genannte Forschungsarbeit erklärt das wie folgt:

„Some commercial products focus on preventing non-updated systems (e.g. antivirus, patches) to access the network and provide some mechanisms to update those systems. However, this latter aim is not the goal of FlowNAC, which focuses on managing the identity of end users and applying a policy that is based on this identity [59].“

Es gibt eine Arbeit aus dem Jahr 2013, die sich auf die Authentifizierung von IoT-Geräten spezialisiert hat. Hierfür wird im Vergleich zu RADIUS oder TACACS+ das alternative Übertragungsprotokoll PANA (Protocol for Carrying Authentication for Network Access) verwendet, um dieses zum ersten Mal für die Authentifizierung von eingeschränkten Geräten wie IoT in der Praxis zu testen [60].

Keine der oben beschriebenen Forschungsarbeiten können einen Beitrag zur Beantwortung der Forschungsfrage liefern. Mit der Suche nach der NAC-Lösung PacketFence konnte eine passende Arbeit gefunden werden, deren Ziel ähnlich zu diesem Ansatz ist. Allerdings liegt hier der Fokus auf der Implementierung einer NAC-Lösung in ein unbekanntes Unternehmen, von dem weder die Größe noch die Anforderungen im Detail bekannt sind. Interessant ist, dass auf eine zentrale Konfiguration der Windows-basierten Endgeräte mithilfe von Gruppenrichtlinien verzichtet wurde. Es wird abschließend ein System für das Unternehmen

empfohlen, bei dem sich die BenutzerInnen in einem Webportal anmelden und im Hintergrund die MAC-Adresse für die zukünftige Authentifizierung gespeichert bzw. herangezogen wird [61].

3.3 All-in-one-Ansatz

Für diesen Bereich der Forschungsarbeit gibt es ebenfalls wenig Input aus bereits vorhergehenden Forschungen zu entnehmen. Einzelne Arbeiten fokussieren sich ausschließlich auf Teilbereiche der Forschungsziele oder erarbeiten Ansätze, die so nicht übernommen werden können.

Eine Masterarbeit von Jarrod Schafer aus dem Jahr 2021 [62] beschreibt die Auswahl und den Betrieb von „Unified Endpoint Management“, welche die Verwaltung von BenutzerInnen-Konten und Endgeräten ermöglicht. Hier wurden die Produkte von Jumpcloud, Okta und Zentyal auf eine breite Funktionsvielfalt überprüft, und anschließend preislich miteinander verglichen.

Eine Forschungsarbeit von der Universität Bukarest [63] schneidet die fehlende Skalierung von WLANs mit einem PSK zur Authentifizierung an, und verweist hier auf eine Anmeldung auf 802.1X-Basis. Es werden die Preise von vier verschiedenen On-Premises RADIUS-Servern verglichen, wobei die Preise mit der Veröffentlichung dieser Forschung im Jahr 2010 vermutlich nicht mehr seriös herangezogen werden können. Als Alternative zu kommerziellen RADIUS-Produkten wird die Installation von dem bekannten Open Source RADIUS-Server „FreeRADIUS“ nahegelegt. Zusätzlich wird ein Leistungstest durchgeführt, bei dem die Transaktionen der Authentifizierungen von Endgeräten in einer Datei oder in den Datenbank-Produkten „PostgresSQL“ bzw. „MySQL“ abgespeichert werden.

Die Ergebnisse von Hendra Supendar [64] zeigen den Einsatz des Produkts Zentyal, um die Aufgaben einer Firewall und Bandbreitenmanagement zu erfüllen. Zusätzlich wird ein HTTP-Proxy verwendet, um den Netzwerkverkehr der Endgeräte zu prüfen und Werbung oder vordefinierte URL, zu blockieren. Auf den Einsatz als RADIUS-Server oder Zertifizierungsstelle (CA) wird nicht eingegangen.

Abschließend gibt es zwei Forschungsarbeiten [65] [66], deren Fokus auf der Installation und Inbetriebnahme des Produkts Zentyal liegt. Dieser Setup-Guide enthält in beiden Fällen viele hilfreiche Bilder, wodurch die Komplexität auch für Nicht-Experten möglichst geringgehalten wird. Während sich die zweite Arbeit auf die Services Datei-, Druck-, DHCP- und DNS-Server und AD Domänencontroller spezialisiert, wird

RADIUS bei der ersten Arbeit zumindest angeschnitten und ein Screenshot zeigt einen Client, der sich mit PEAP-MSCHAPv2 in einem WLAN anmelden möchte.

Keine der gefundenen Forschungsarbeiten liefert (detaillierte) Ergebnisse zum Einsatz eines RADIUS-Servers in Verbindung mit einer Zertifizierungsstelle (CA) auf einem All-in-one-Linux-Server. Bis auf ein Paper wird die Möglichkeit für eine 802.1X-Authentifizierung gänzlich unerwähnt gelassen. Die Machbarkeit aus der Kombination von Samba 4 AD DS, Certificate Authority und einem RADIUS-Server fokussiert auf einen Server, wird somit nicht behandelt.

3.4 Cloud-basierter Ansatz

Für dieses Kapitel der Diplomarbeit fällt die Beteiligung in der Forschung ebenfalls sehr niedrig aus. Aus dem Jahr 2021 gibt es von Toomas Ristola [67] eine Studie, die allerdings nahezu vollständig in der Sprache Finnisch geschrieben wurde, und somit eine Auseinandersetzung und Analyse stark erschwert.

Der Inhalt dieser Studie setzt den Fokus auf Cloud-basierte Verwaltung der Netzwerkgeräte wie APs, und setzt im Hintergrund auf eine Kombination von einem AD Domain Controller, AD Zertifizierungsstelle (CA) und Network Policy Server (NPS), die alle On-Premises betrieben werden. Im Konkreten wurde das System vom Hersteller „Ruckus Networks“ und deren Cloud-Plattform genutzt, und die Hardware R510, H320, R320 und H510 eingesetzt.
Die Einbindung der Cloud für die Authentifizierung der Endgeräte und AnwenderInnen wurde somit nicht berücksichtigt, und liefert somit auch keine Informationen für diese Diplomarbeit.

4 Herangehensweise

In Kapitel 4 „Herangehensweise“ werden nun jene Methoden vorgestellt, mit welchen die Forschungsfragen bzw. das Forschungsproblem in dieser Diplomarbeit beantwortet werden soll. Zusätzlich wird hier auf die Labor-Infrastruktur eingegangen, die für die praktischen Teile dieser Diplomarbeit verwendet wurden. Dieses dient der Dokumentation und Nachvollziehbarkeit, wie und auf welche IT-Komponenten die praktische Untersuchung durchgeführt wurde.

4.1 Übersicht der unterschiedlichen Ansätze für KMUs

Diese Arbeit beschäftigt sich mit der Implementierung einer Lösung zur Netzwerkauthentifizierung von Endgeräten, die nach einem bestimmten Schema zugelassen oder abgewiesen werden. Wie in allen Projekten gibt es auch hier keine Musterlösung oder „das perfekte Konzept“. Neben der Größe, dem finanziellen Budget und der Ausgangssituation des Unternehmens gibt es noch unzählig weitere Gründe für unterschiedliche Ansätze der Netzwerkauthentifizierung. Für alle Ansätze gilt, dass für die Anmeldung eine Benutzername-Passwort-Kombination vermieden werden sollte, und stattdessen eine zertifikatbasierte Anmeldung bzw. Anmeldung mithilfe von SSO bevorzugt wird. Für die Darstellung der Abbildung 4.1, 4.2 und 4.3 wurde die Grafik von LookingPoint [68] als Ausgangssituation herangezogen.

4.2 Allgemeine Annahmen

In dieser Diplomarbeit wird eine Top-Level-Domain genutzt, die ausschließlich für Testzwecke zur Verfügung gestellt wurde. Alle Domänen, die mit einem „.test“ enden, können für private Testzwecke eingesetzt werden und sind vom globalen DNS ausgenommen. Dies ist im RFC 2606 von 1999 definiert [69].
Der Kauf und die Einrichtung einer Domäne wird in dieser Arbeit nicht abgedeckt, und vom Unternehmen als bereits vorhanden angenommen.

Wie in dem Abschnitt 2.3 „IT-Budget/IT-Security-Budget“ beschrieben, haben KMUs im Durchschnitt ein IT-Budget von 6.9% ihres Jahresumsatzes zur Verfügung. Diese Zahl muss allerdings sehr vorsichtig betrachtet werden und kann daher nicht als Referenz herangezogen werden, ob ein Produkt erschwinglich oder zu teuer für ein KMU ist. Daher wird in dieser Arbeit der Ansatz verfolgt, dass die vorgestellten Produkte möglichst kostengünstig bzw. kostenlos sein sollen. Teilweise können die Kosten der unterschiedlichen Ansätze schwer miteinander verglichen werden. Die monatlichen Kosten von Cloud-Produkten stechen womöglich stärker heraus als eine kostenlose NAC-Lösung. Für einen objektiven Kostenvergleich müssen die Ausgaben für physische Hardware und deren Wartung, Software-Lizenzen, MitarbeiterInnen, Strom uvm. verglichen werden, die nur von jedem Unternehmen individuell beantwortet werden können.

Für den Ansatz der kostenlosen NAC-Lösung und dem All-in-one-Produkt wird der offene Standard IEEE 802.1X herangezogen, da dieser eine weite Verbreitung in der Praxis findet. Es existieren viele Geräte von diversen Herstellern, die 802.1X unterstützen, und die auch für KMUs erschwinglich sind. Der Cloud-Ansatz beinhaltet Alternativen, wenn 802.1X nicht zwangsläufig eingesetzt werden kann. Allgemein muss erwähnt werden, dass mit offenen Standards wie 802.1X ein Vendor Lock-in vermieden wird und ein Unternehmen so möglichst flexibel für zukünftige Entscheidungen bleibt.

4.3 Open Source NAC

4.3.1 Kurzbeschreibung des Ansatzes

Der erste Ansatz bietet sich für jene Firmen an, die bereits eine Microsoft-orientierte Infrastruktur im Einsatz haben und ihre Server On-Premises betreiben, allerdings mit dem Microsoft NPS an die Grenzen stoßen. Je nach Größe und Branche können sich Endgeräte ansammeln, die nicht über 802.1X authentifiziert werden können, und somit auf das unsichere MAB zurückgegriffen werden muss. Bereits hier besitzt der NPS Einschränkungen, in dem nur zwei Workarounds für die Authentifizierung von MAB angeboten werden können: MAC-Adresse als AD-Konto [70] bzw. Regex-Überprüfung der MAC-Adresse [71]. NAC-Lösungen hingegen bieten über einen RADIUS-Server hinaus viele zusätzliche Funktionen an, die dem Management und den AdministratorInnen helfen können. Hersteller wie Cisco und Aruba bieten mit der Cisco ISE und dem Aruba ClearPass Produkte mit einem großen Funktionsumfang und einem Ruf am Markt an. Diese Systeme können allerdings komplex und teuer sein, und nicht für alle Firmen finanziell stemmbar. Der Ansatz wird in Abbildung 4.1 dargestellt.

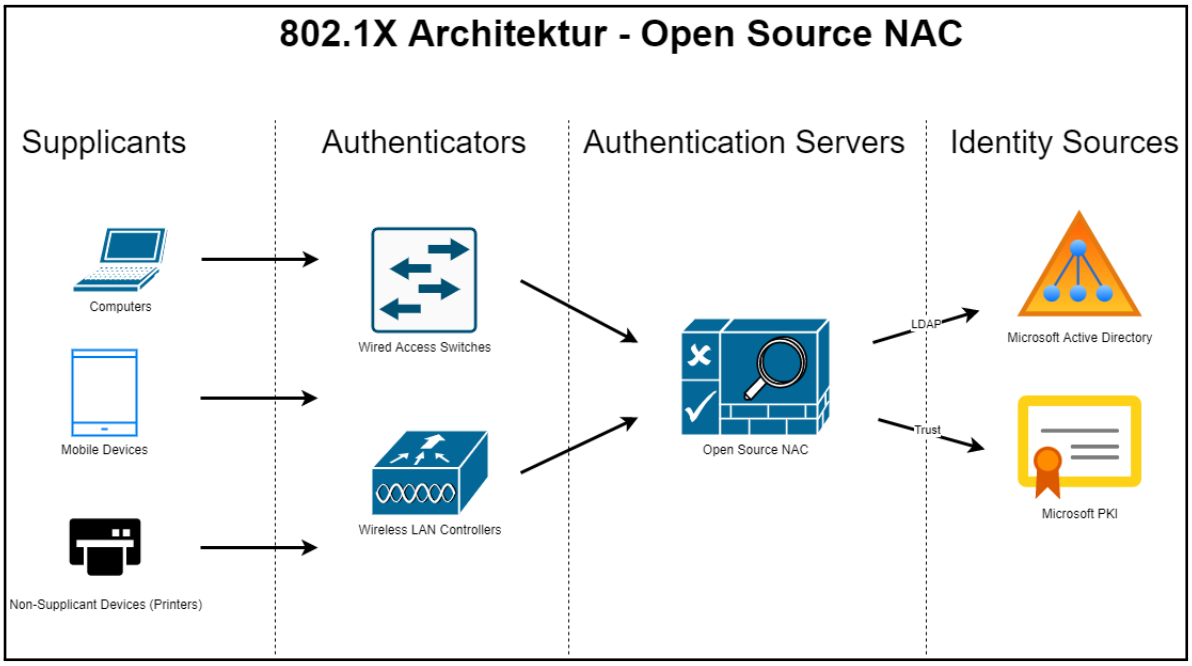


Abbildung 4.1: Open Source NAC

4.3.2 Ziele bzw. Nicht-Ziele

Im ersten Schritt soll eine ausführliche Recherche durchgeführt werden, welche kostenlosen Alternativen zu den Marktführern wie Cisco oder Aruba existieren. Potenzielle Produkte werden daraufhin miteinander verglichen, wobei ein Produkt daraufhin in einem PoC untersucht und bewertet wird.

Es ist nicht das Ziel dieser Diplomarbeit, dass eine IT-Infrastruktur mit Microsoft-Produkten aufgesetzt und diese evaluiert werden. Die Untersuchung der ausgewählten NAC-Lösung nimmt eine funktionierende Infrastruktur mit Microsoft AD DS und CA als vorhanden an, die nun in diese integriert werden soll. Somit liegt der Fokus auf die Integrierung einer NAC-Lösung und nicht auf dem Setup und Betrieb der restlichen IT-Infrastruktur.

Es soll zwar eine Alternative zu etablierten Herstellern wie Cisco oder Aruba gesucht und in der Praxis getestet werden, allerdings wird es keinen direkten Vergleich zwischen den zuvor genannten Anbietern und der in dieser Diplomarbeit untersuchten NAC-Lösung geben. Die Produkte von u.a. Cisco oder Aruba gelten als Marktführer und werden daher oft erwähnt, sie werden aber nicht im Rahmen dieser Arbeit aktiv getestet.

4.3.3 Annahmen

Es wird angenommen, dass das Unternehmen, welchen diesen Ansatz verfolgt, bereits eine Microsoft AD Infrastruktur inklusive CA im Betrieb hat. Microsoft AD gilt als De-facto-Standard und wird in vielen Betrieben eingesetzt.

4.3.4 Beispielfirma

Die Beispielfirma für diesen Ansatz ist eine Forschungseinrichtung, in dem sowohl managed als auch unmanaged Endgeräte wie Workstations und Notebooks eingesetzt werden. Eine zusätzliche Herausforderung stellen 802.1X-inkompatible Geräte wie Drucker und IP-Kameras sowie IoT- und OT-Geräte dar, die für Forschungen zwangsläufig benötigt werden. Es existiert allerdings eine dedizierte IT-Abteilung, die Know-how in der Verwaltung von Windows- und Linux-Server besitzen.

4.4 All-in-one-Ansatz

4.4.1 Kurzbeschreibung des Ansatzes

Der zweite Ansatz ist dem ersten ähnlich, unterscheidet sich allerdings, dass der Authentication Server und die Identity-Sources auf einem einzelnen Server betrieben wird. Abbildung 4.2 liefert hierfür einen Überblick. Der Fokus liegt hier auf einer All-in-one-Lösung, die die Services wie AD DS, CA, RADIUS bereitstellt und Netzwerkauthentifizierungen durchführt. Diese Services werden zusätzlich für die Administration in einer vereinfachten Weise bereitgestellt, um die Komplexität für das IT-Personal zu reduzieren. Das Open-Source-Projekt „Samba4“ bildet die Grundlage für ein Active Directory Domain Services (AD DS), welche eine Domäne mit dem Forest Functional Level von „Windows Server 2008 R2“ bereitstellt und laut deren Dokumentation [16] somit auch für umfangreichere Unternehmen mit Windows 10 bzw. 11 Clients geeignet ist.

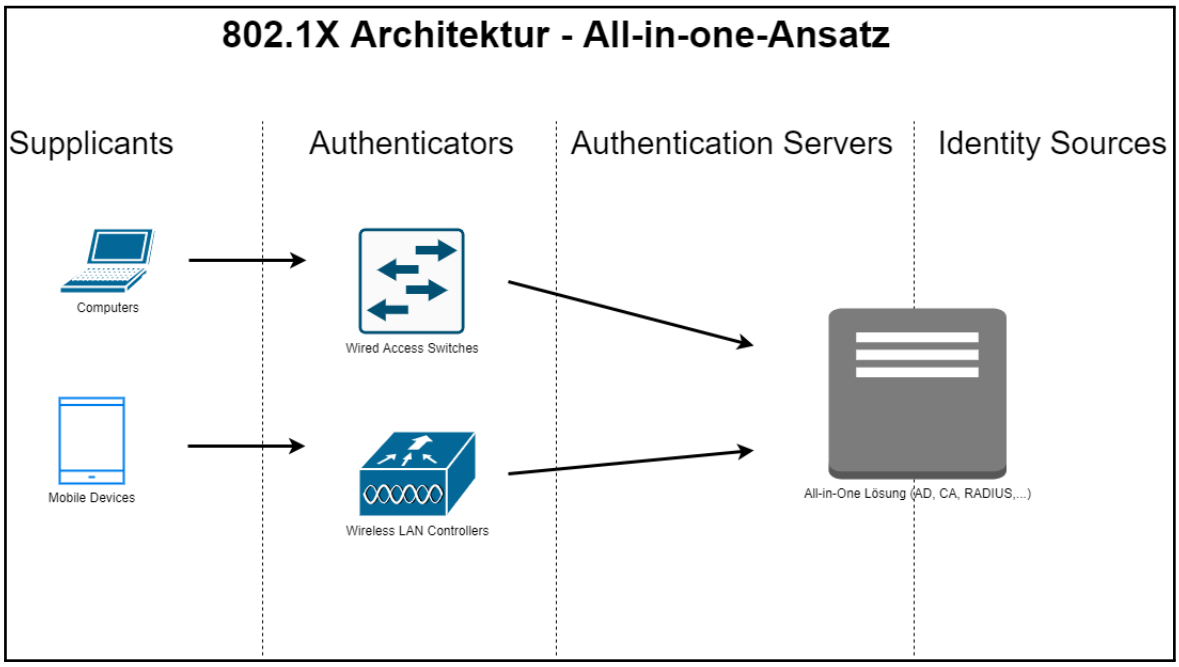


Abbildung 4.2: All-in-one-Ansatz

4.4.2 Ziele bzw. Nicht-Ziele

Für diesen Ansatz wird im ersten Schritt eine ausführliche Recherche durchgeführt und nach passenden Lösungen gesucht. Aus den Ergebnissen der Recherche wird anschließend eine Lösung ausgewählt, welches anschließend in einem praktischen Test umgesetzt und deren Erfahrungen notiert werden.

4.4.3 Annahmen

Es wird angenommen, dass entweder eine Virtualisierungstechnologie mit ausreichenden Ressourcen bereits im Einsatz ist oder ein physischer Server zur Verfügung steht. Zusätzlich besteht eine Firewall-Lösung, die das Gateway für die Subnetze und eine Verbindung ins Internet bereitstellt, und ein WLAN-Controller mit passenden Access Points, der RADIUS-Pakete verarbeiten kann und den Standard 802.1X unterstützt.

4.4.4 Beispielfirma

Die erste Beispielfirma für diesen Ansatz ist eine Firma, die frisch gegründet wurde, und somit auch über eine überschaubare Anzahl an Angestellten haben. Innerhalb des Unternehmens existiert oberflächliches IT-Wissen, allerdings keine Fachkenntnisse in der Administration von Windows-basierten Servern. Das zentrale Management der BenutzerInnen und der Endgerätekonfiguration soll allerdings von Anfang an in Betrieb sein.
Eine zweite Beispielfirma wäre jene Firma, die im Moment den Cloud-basierten Ansatz verwendet und nun ausgewählte Services zentral verwalten möchte.

4.5 Cloud-basierter Ansatz

4.5.1 Kurzbeschreibung des Ansatzes

Wie die Abbildung 4.3 zeigt, verfolgt der letzte Ansatz die Idee, dass der Authenticator (Switch, WLAN-Controller) den Authentifizierungsversuch vom Supplicant (Client, Endgerät) entgegennimmt und diesen an einen externen Server weiterleitet. Dieser externe Service stellt dabei die Funktion des Authenticaton Servers und der Identity Sources zur Verfügung und bestimmt, ob und welchen Zugriff das Endgerät zugewiesen bekommt. Zusätzlich werden alternative (Cloud)-Lösungen gesucht, die nicht das Modell von 802.1X verfolgen und dennoch einen Zugriffsschutz bieten.

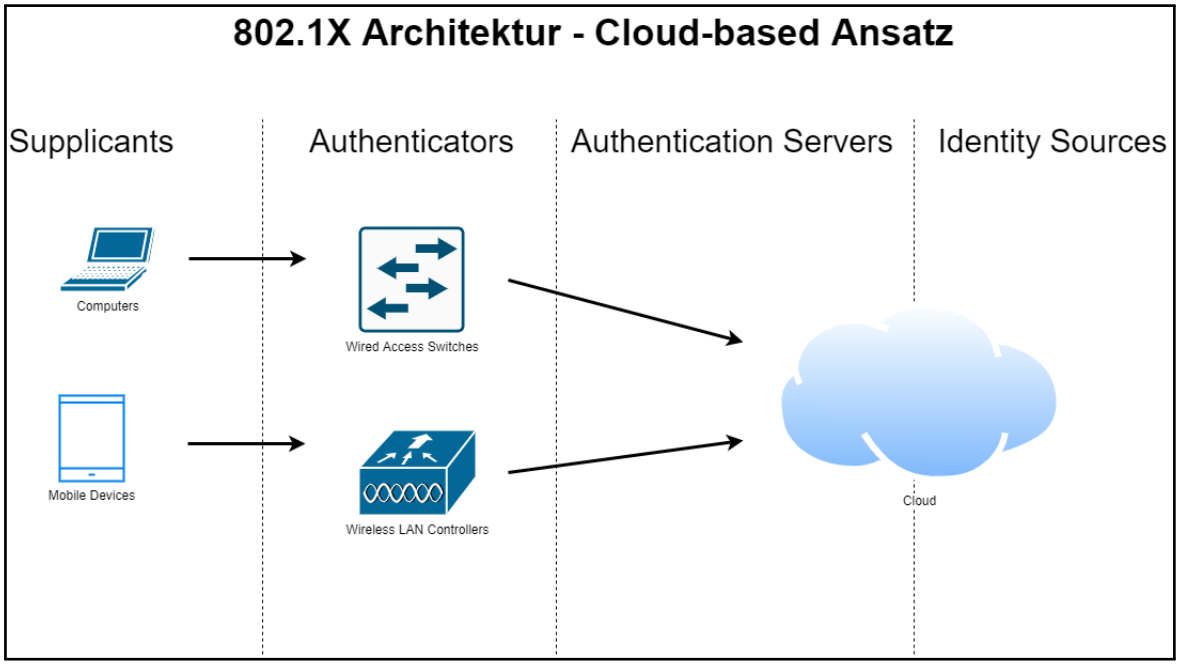


Abbildung 4.3: Cloud-basierter Ansatz

Dieser Ansatz bietet sich für Firmen an, die keine Server-Infrastruktur On-Premises besitzen und deren Fokus auf der Cloud liegt. Ein RADIUS-Server im klassischen Sinn ist allerdings ein Server, der lokal oder in einem externen Rechenzentrum und somit unter Kontrolle der jeweiligen Firma steht. Da womöglich das notwendige IT-Budget bzw. das Know-how bei den eigenen MitarbeiterInnen fehlt, die Notwendigkeit zum Schutz frei zugänglicher Netzwerkdosen allerdings besteht, kann hier eine SaaS- bzw. eine PaaS-Lösung einspringen. Durch den Cloud-basierten Ansatz werden die Kosten zusätzlich überschaubarer und in regelmäßigen Abständen bezahlt, wodurch der Verlust bei einer Fehlinvestition im Vergleich zu einer lokalen

Lösung ebenfalls niedriger ist. Sollte die Leistung des Cloud-Providers nicht passen, gibt es womöglich andere Firmen mit ähnlichen Leistungsumfang. Ein System für wenige MitarbeiterInnen aufzusetzen und dieses laufend zu warten inklusive Lizenz- und Patchmanagement, ist finanziell nicht attraktiv.

4.5.2 Ziele bzw. Nicht-Ziele

In dieser Arbeit wird eine ausführliche Recherche durchgeführt und evaluiert, welche Lösungen für diesen Einsatzzweck in Frage kommen.

Zu den Nicht-Zielen zählt die Überprüfung der Recherche in einem Praxisversuch. Die Ergebnisse werden ausschließlich theoretisch aufgelistet und bewertet.

4.5.3 Annahmen

Es wird die Annahme getroffen, dass sich dieser Ansatz aufgrund mangelnder lokaler Server-Infrastruktur primär an kleinere Firmen ohne zentrales Management der Endgeräte und BenutzerInnen richtet, und somit auch bestimmte Kompromisse akzeptiert werden. Aufgrund der geringen Größe der Firma wird eine homogene Ausgangssituation von Clients angenommen. Geräte, die keine Authentifizierung im Netzwerk unterstützen, können alternativ mit Port-Security oder mit der Abtrennung in einem eigenen Netzwerksegment abgesichert werden.

4.5.4 Beispielfirma

Für diesen Ansatz wird eine IT-Firma mit sechs Personen angenommen, in welcher jeder Angestellter einen lokalen Account auf dem eigens verwalteten Endgerät besitzt. Das Betriebssystem der Endgeräte ist eine Mischung aus Windows und beliebigen Linux-Distributionen. Die Firma hat ihren Hauptsitz in einer gemieteten Wohnung und bietet neben Räumlichkeiten für Büros auch einen Meetingraum. Der primäre Wunsch besteht darin, dass bei der Netzwerkauthentifizierung zwischen internen MitarbeiterInnen und externen Gästen unterschieden, und eine dementsprechende Netzwerksegmentierung mit unterschiedlichen VLANs durchgeführt wird.

4.6 Versuchsaufbau

Firewall/Router

Für die Kommunikation zwischen den einzelnen VLANs, wurde eine Fortinet FortiGate 60E mit dem Betriebssystem FortiOS 7.0.10 eingesetzt. Die Firewall stellt mit Ausnahme der VLAN-ID 202 für alle Subnetze das Gateway dar und die Firewall-Freischaltungen werden nach dem Least-Privilege-Prinzip konfiguriert. Die Verwaltung und Konfiguration erfolgten ebenfalls direkt auf der Firewall, die hier den WLAN-Controller spielt.

Access Point

Für die 802.1X-Tests im WLAN wurde der Fortinet AP FP223C genutzt.

Switches

Für die Router-on-a-Stick-Konfiguration und den LAN-basierten 802.1X-Tests wurden die zwei Cisco-Switches C3560-CG-8PC-S und C3560-CX-8TC-S verwendet. Der erste Switch wurde als Bindeglied zwischen Gateway und dem zweiten Switch verwendet. Hingegen wurde der zweite Switch für die Konnektivität zur der Server-Infrastruktur und für die tatsächlichen 802.1X-Test eingesetzt.

Server-Infrastruktur

Für die Virtualisierung der diversen Server wurde ein Desktop-PC der FH St. Pölten mit einem Intel i5-4200 und 32GB Arbeitsspeicher verwendet. Das Betriebssystem VMware ESXi-7.0.0-15843807 lief auf einer 250GB SSD, hingegen wurden die Daten der virtualisierten Server per iSCSI von dem NAS Synology DS918+ eingebunden.

Virtuelle Maschinen

Die folgenden Server inklusive deren Services wurden auf der oben erwähnten Hardware virtualisiert:

- Open Source NAC - Server1: DC1 + Root CA
- Open Source NAC - Server2: DC2 + Int CA
- Open Source NAC - Server3: PacketFence
- Open Source NAC - Server4: Nessus Essentials
- All-in-one-Ansatz - Server1: Zentyal

Plan

In Abbildung 4.4 wird der Versuchsaufbau übersichtlich dargestellt.

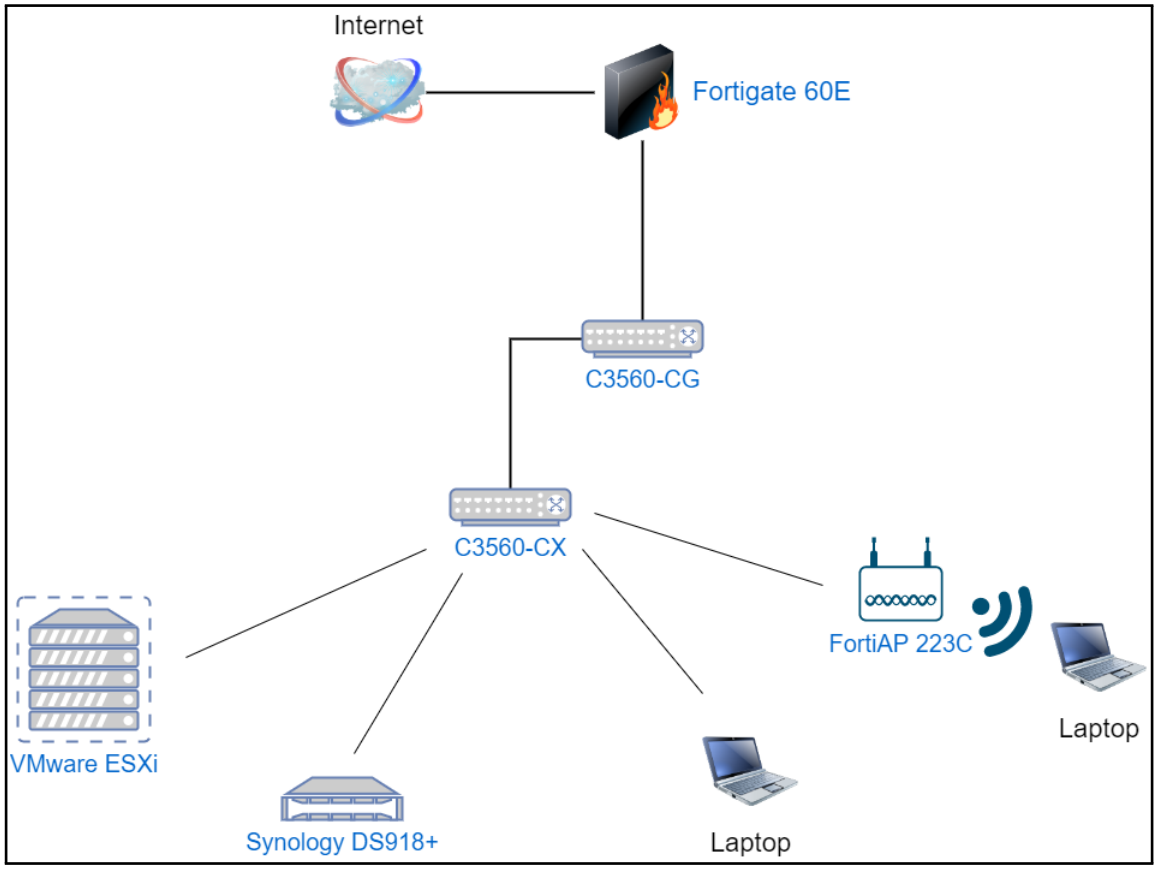


Abbildung 4.4: Plan der Labor-Infrastruktur

5 Evaluierung von Open Source NAC-Produkten

5.1 Einleitung

Mit dem Network Policy Server (NPS) stellt Microsoft einen sehr bekannten und einfachen RADIUS-Server zur Verfügung, der sich perfekt in das Ökosystem von Windows AD integriert. Die Entscheidung darüber, ob und mit welchen Berechtigungen ein Client oder eine BenutzerIn Zugriff in das Netzwerk bekommt, erfolgt mit vordefinierten Regeln. So wird überprüft, ob das Gerät beispielsweise der Abteilung Human Resources (HR) oder IT zugeordnet werden kann, und wird im Hintergrund mithilfe des Standards 802.1Q in Netzsegmente mit mehr oder weniger Berechtigungen zugewiesen. Diese Entscheidung folgt statisch, und die aktuellen Umstände bzw. der Kontext werden nicht näher berücksichtigt. Zusätzlich tauchen früher oder später in einem Unternehmen Geräte auf, deren Implementierung für 802.1X unzuverlässig ist oder schlichtweg nicht angeboten wird. Für diese Situation gibt es mit MAC Authentication Bypass (MAB) eine Alternative, diese Geräte dennoch in einen Prozess der Netzwerkauthentifizierung zu integrieren. Diese Möglichkeiten sind allerdings mit dem NPS nur umständlich umzusetzen, da die vorhandenen Ansätze (MAC-Adresse als AD-Konto [70] bzw. Regex-Überprüfung der MAC-Adresse [71]) in der Praxis schlecht skalieren.

Auf der einen Seite existiert mit dem NPS ein einfacher und rasch aufgesetzter RADIUS-Server, der aber auch schnell seine Grenzen erreicht hat. Auf der anderen Seite existieren NAC-Lösungen, die diese Einschränkungen nicht besitzen und darüber hinaus einige zusätzliche Funktionen anbieten. So können diese dynamisch auf Situationen reagieren, bei denen ein Endgerät bestimmte Richtlinien nicht erfüllt und anschließend den Zugriff ganz oder teilweise verbieten. Zusätzlich kann ein NAC einen aktuellen Überblick zu den erfolgreichen und fehlgeschlagenen Anmeldungen geben, wodurch eine bessere Einsicht an dieser sensiblen Stelle gegeben ist. Im Vergleich dazu liefert der NPS ebenfalls Logeinträge für durchgeführte und abgelehnte Authentifizierungen, diese müssen allerdings selbst aufbereitet werden.

5.2 Marktführer von NAC-Produkten

Aus den zuvor genannten Gründen kann sich daher der Umstieg von einem einfachen RADIUS-Server zu einem NAC lohnen. Basierend auf dem Garnter Magic Quadrant von NAC-Produkten für das Jahr 2013 [72] können die Produkte von Cisco, Aruba und ForeScout als Technologieführer definiert werden. Den Einschätzungen von Quadrant Knowledge Solutions [73] zufolge, deren System sehr dem Gartner Magic Quadrant ähnelt, wird die Marktposition für die Zeitspanne 2018 bis 2023 bestätigt.

Cisco ISE

Die Cisco Identity Service Engine (ISE) ist defacto der Nachfolger des Cisco Access Control System (ACS), welches bereits seit einigen Jahren nicht mehr aktiv von Cisco unterstützt und weiterentwickelt wird. Mit der ISE werden die Dienste von Cisco enger miteinander verzahnt und die Erfahrung innerhalb des Ciscos Ecosystem verbessert. Mit dem neuen Produkt werden nun u.a. die Anbindung von Produkten anderer Hersteller über pxGrid, die Integration von DNA Center und AnyConnect, und die Möglichkeit von Bedrohungs- und Schwachstellenscans eingeführt. Zusätzlich wurde die Unterstützung von TrustSec weiter ausgebaut [74]. Zusammengefasst bedeutet das allerdings auch, dass diese Vorteile vor allem dann ausgenutzt werden können, wenn möglichst viele Produkte vom gleichen Hersteller im Einsatz sind.

ISE verwendet im Hintergrund die drei folgenden Node-Typen [75]:

- PAN = Administration: Dieser Node-Typ gilt als zentrale Anlaufstelle für die Konfiguration der ISE. Hier werden die Einstellungen für die Richtlinien, Captive Portal, etc. angelegt und verwaltet.
- PSN = Policy Service: Die Konfiguration der ISE wird auf den PANs erstellt, und anschließend auf die PSNs synchronisiert. Diese Server führen die tatsächlichen Überprüfungen, Authentifizierungen sowie das Profiling durch, und stellt das Captive Portal zur Verfügung.
- MnT = Monitoring: Dieser Server sammelt und speichert alle Logs der anderen ISE-Server.

In kleinen Umgebungen können die Services für Logging und Administration auf einem Server betrieben werden. Mit der Version ISE 2.2 werden max. zwei PANs, zwei MnTs und 50 PSNs in einem System unterstützt. Cisco setzt bei der ISE auf ein Abomodell, deren Lizenzen auf 1-,3- oder 5-Jahres Basis abgeschlossen werden können. Zusätzlich gibt es primär die drei Lizenz-Pakete Premier, Advantage und Essentials, wobei Premier nur die Grundfunktionen und Essentials alle Features unterstützt. Für die Funktion des AAA-Servers wird das teuerste Pakete benötigt [76].

Cisco fokussiert sich bei der ISE auf eine zentrale Anlaufstelle für die Authentifizierung und Autorisierung. Hier hilft TrustSec, die die Segmentierung von Geräten weiter verbessert. Die Konfiguration für den Zugriff der Clients und MitarbeiterInnen auf Services kann an einer Stelle verwaltet werden – egal ob VPN, LAN oder WLAN genutzt wird. Die Filterung der Netzwerk-Freischaltungen wird nicht mehr nur auf einem Layer 3-Gerät wie Firewall oder Router überprüft, sondern kann zusätzlich auf Layer 2-Ebene wie Switches oder WLC durchgeführt werden und somit die Kommunikation zwischen zwei Clients dynamisch unterbinden. Die Freigaben erfolgen nun nicht mehr auf IP-Adressen-Ebene, sondern für jede einzelne Entität.

Aruba ClearPass

Mit Aruba ClearPass Policy Manager hat Hewlett Packard Enterprise (HPE) ein NAC-Produkt am Markt, welches laut Gartner zu den drei besten Lösungen am Markt gilt. In Verbindung mit der eingebauten CA soll das Onboarding neuer Geräte schneller und reibungsloser durchgeführt werden können [77]. Mit dem Konzept „Aruba 360 Secure Fabric“ bzw. „Aruba 360 Security Exchange“ existiert eine Plattform, um diverse Produkte anderer Hersteller in das HP Eco-System zu integrieren, und so eine Verbesserung in der Reaktionszeit von Bedrohungen und deren Abwehr zu haben. Aruba ClearPass kann als virtuelle Maschine oder auf dedizierter Hardware in drei unterschiedlichen Ausführungen verwendet werden, wobei für KMUs vermutlich der kleinste Server ausreichend ist. Darüber hinaus werden Lizenzen für die Verwendung der NAC-Funktionen benötigt, die als Abonnement oder dauerhafte Lizenz bezogen werden können. Allerdings ist in beiden Fällen das kleinste Paket eine Lizenz für 100 aktive Clients [78].

Forescout

Forescout bietet mit CounterACT bzw. der neuen Zero Trust-Plattform zwei NAC-Produkte an, wobei CounterACT, basierend auf der Datumsangabe in den Datenblättern und der Webseite allgemein, der Vorgänger zur neuen Plattform war. Im Moment werden acht Produkte von Forescout angeboten, die alle unter der neuen Plattform zusammenspielen und so eine möglichst optimale Erfahrung für den Kunden bieten soll. Der Hersteller stellt nicht viele Informationen zur Verfügung, wodurch viele Fragen wie Lizenzkosten oder der IT-Betrieb offen bleiben. Während die Aufgabenstellung von „eyeControl“ in Erfahrung gebracht werden konnte, ist das bei anderen Produkten wie „eyeSegment“ nicht so einfach machbar bzw. gibt es bei „eyeSight“ und „eyeInspect“ Überschneidungen. Es muss erwähnt werden, dass Forescout zu allen seinen einzelnen Produkten ein Datenblatt anbietet, diese beinhalten aber keine Details zu den Produkten [79].

Funktionen von NACs

Die drei oben beschriebenen Produkte wurden oberflächlich untersucht und vorgestellt – eine detaillierte Gegenüberstellung würden den zeitlichen Rahmen dieser Forschungsarbeit überschreiten. Basierend auf der theoretischen Untersuchung bieten allerdings alle NAC-Lösungen die gleichen Funktionen. Im Weiteren werden nun dennoch die Funktionen von NACs allgemein vorgestellt, die überwiegend von den Marktführern abgedeckt werden.

Die angebotenen Funktionen der populären NAC-Lösungen sind vielfältig, die Hersteller verlangen allerdings auch entsprechend für diesen Service bezahlt zu werden. Diese Kosten und Komplexität der Systeme stellen gerade für KMUs eine finanzielle Belastung dar.

5.3 Open Source NAC

Der Markt für Open Source NAC-Lösungen sieht im Jahr 2023 sehr überschaubar aus. Produkte wie FreeNAC oder OpenNAC, die vor einigen Jahren noch populär und aktiv eingesetzt wurden, wurden mittlerweile eingestellt. Im GitHub-Repository von FreeNAC [80] wird darauf hingewiesen, dass das Projekt seit 2009 im „maintenance mode“ steht und somit nicht weiterentwickelt wird. Die letzte Änderung im GitHub-Projekt stammt vom Jahr 2013. Zusätzlich wird erwähnt, dass sowohl die vorkonfigurierte VM als auch das Installationsskript nicht mehr zur Verfügung stehen. Die Webseite „https://www.freenac.net“, die Dokumentationen für FreeNAC bereitstellen soll, wird mittlerweile von der „Beijing Sport University“ verwendet.

Hingegen wird auf der Homepage [81] des Herstellers von OpenNAC hingewiesen, dass ihr Produkt nicht mehr länger zur Verfügung steht. Stattdessen wird ein exklusiver Fokus auf OpenNAC Enterprise gelegt, um alle Anstrengungen in die Erfüllung der Kundenwünsche zu legen. Alle Hinweise deuten darauf hin, dass das Open-Source-Projekt dem kommerziellen Nachfolger OpenNAC Enterprise zum Opfer gefallen ist.

5.3.1 PacketFence

Mit PacketFence stellt die Firma „Inverse inc.“ eine NAC-Lösung bereit, die Open Source ist und keine Lizenzkosten für den Betrieb verlangt. Nach eigener Auskunft existieren über 5.000 Installationen weltweit bei ca. 350.000 neu registrierten Clients in den letzten sieben Tagen. PacketFence basiert auf vielen bekannten Komponenten wie FreeRADIUS, Apache, MariaDB, OpenVAS, Snort oder Suricata auf, die selbst Open Source sind. Abbildung 5.1 liefert hierzu eine Übersicht der Komponenten inklusive deren Aufgaben.

PacketFence kann in zwei Modi eingesetzt werden: „Out of band“ oder „Inline“. Während die erste Vari-

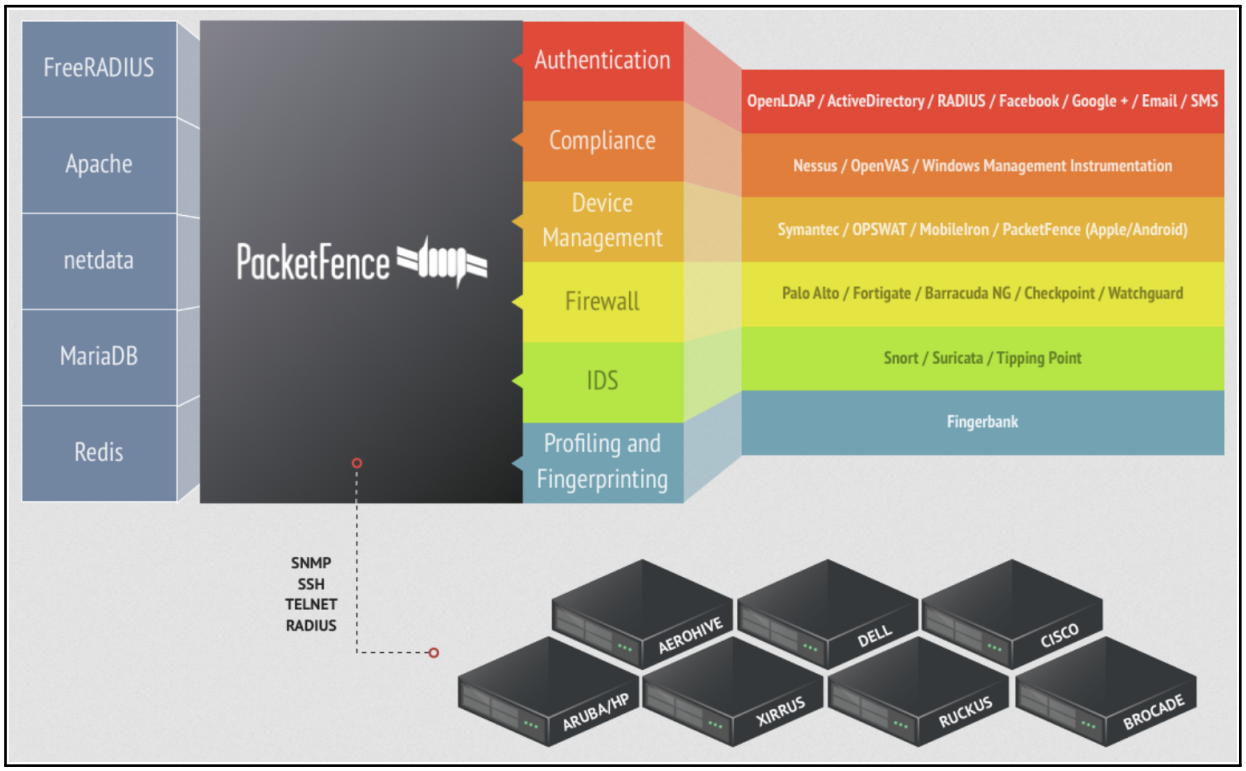


Abbildung 5.1: Übersicht der Software-Paketen, auf die PacketFence aufbaut [82]

ante das bekannte Konzept rund um 802.1X mit Supplicant und Authenticator beschreibt, kann der zweite Ansatz für die Authentifizierung von Legacy-Geräten eingesetzt werden. Hierfür stellt PacketFence das Default-Gateway für die Endgeräte bereit und agiert als transparente Firewall, die nur den authentifizierten Clients die Netzwerkkommunikation erlaubt. Beide Modi können dabei gleichzeitig eingesetzt werden. Dies könnte insofern umgesetzt werden, dass ein Switch-Port primär mit 802.1X geschützt ist, und sollte der Client nicht auf EAP-Pakete reagieren, die Inline-Methode als Fallback greift [82].

PacketFence bietet die Integration von kommerziellen und kostenlosen Produkten zum Scannen von Schwachstellen, wie Tenable Nessus oder OpenVAS, an. Zusätzlich können sogenannte „Security Agents“ wie OPSWAT Metadefender Endpoint Managment oder Symantec Endpoint Protection Manager (SEPM) eingebunden werden, die auf den Clients als erweiterte AV-Lösung installiert sind. Des Weiteren kann der „Gesundheitsstatus“ von Geräten mithilfe von Windows Management Instrumentation (WMI) oder „Statement of Health“ (SoH) [83, p. 58-60] abgefragt werden, wobei letzteres ab Windows 10 nicht mehr unterstützt wird [84]. Mit diesen Möglichkeiten bietet PacketFence eine Plattform zum Scannen von Endgeräten, ob diese vordefinierte Richtlinien, wie aktives AV-Programm oder aktuellen Patchstand, erfüllen. Diese Über-

prüfungen der Clients können vor oder nach einer Registrierung durchgeführt werden, wobei die Geräte bei einem Verstoß entsprechend isoliert bzw. die Anmeldung abgelehnt werden kann.

Die Einbindung von firmenfremden Geräten wie Handys oder Tablets von Gästen oder den eigenen MitarbeiterInnen (BYOD) ins Netzwerk ist über viele Wege möglich. So kann die Anmeldung mit oder ohne Zugangsdaten, einem tagesabhängigen Kennwort oder mit der Verteilung von Vouchers durchgeführt werden. Zusätzlich können externe Firmen wie Facebook, Google oder GitHub für die Authentifizierung eingebunden werden. Eine finanzielle Abrechnung für die Benutzung des Netzwerks über Anbieter wie PayPal ist ebenfalls möglich.

Laut der Homepage von PacketFence sind allgemein alle Switches kompatibel, die selbst 802.1X bzw. MAB unterstützen. Darüber hinaus kann das NAC so konfiguriert werden, dass SNMP in Verbindung mit Port-Security als Anmeldung und Konfiguration des Switches herangezogen wird. Technisch wird dies so umgesetzt, dass initial eine falsche MAC-Adresse als Port-Security auf einem Switchport hinterlegt wird – es wird also bei jedem neuen Gerät zu einem Verstoß inklusive einer Meldung (SNMP-Trap) kommen, die PacketFence abfängt und darauf reagiert. Ist die anschließende Anmeldung des Clients erfolgreich, so wird der Switchport im Hintergrund in das vordefinierte VLAN verschoben und die MAC-Adresse in der Port-Security hinterlegt. Solange sich der Client bzw. deren MAC-Adresse nicht ändert, wird es zu keinem Verstoß der Port-Security kommen und somit auch keine neue Authentifizierung provozieren – egal ob die Verbindung zum Switch physisch oder durch einen Neustart unterbrochen wurde. Im Moment unterstützen die Hersteller Cisco, Edge-Core, HP, Intel, Linksys und Nortel diese Variante der Autorisierung [85, p. 29-31].

Neben der Switches werden auch diverse Anbieter von WLAN Access Points unterstützt – sowohl im Standalone-Betrieb oder in Kombination mit einem WLAN-Controller. Auf der Webseite von PacketFence wird eine Matrix angeboten, die einen Überblick bietet, welche Hersteller mit welchen Features der Anmeldung (SNMP, MAB, 802.1X kabelgebunden bzw. kabelos, etc.) kompatibel ist [82].

Von der Firma Inverse inc. werden diverse Dokumentation und Guides angeboten, die u.a. die Themen wie das initiale Setup, Durchführung von Major-Upgrades, Konfiguration der Netzwerkgeräten und Aufbau von High Availability (HA) abdecken. Darüber hinaus gibt es bei PacketFence eine Community, die mithilfe von „mailing lists“ und Internet Relay Chat (IRC) erreicht werden kann. Ein kommerzieller Support kann für 5.000 $ pro PacketFence-Server ebenfalls erworben werden, der eine Erreichbarkeit von 24/7 bei einer Reaktionszeit von einer Stunde verspricht. Die Anzahl der Incidents bzw. der Tickets sind unbegrenzt.

5.4 Fazit

In der Recherche zu kostenlosen NAC-Lösungen hat sich gezeigt, dass die Auswahl gering ist. Im Laufe der letzten Jahre wurden viele Projekte aufgegeben oder in andere Produkte umgewandelt. Einzig mit PacketFence wird eine Open-Source-Alternative zu Cisco ISE, Aruba ClearPass und Co. bereitgestellt, welches eine breite Palette an Funktionen unterstützt und laufend weiterentwickelt wird. Während die Marktführer primär die Integrierung von neuen Funktionen vorantreiben, wie es Cisco mit TrustSec macht, legt der Fokus von PacketFence auf der Anbindung von möglichst vielen Netzwerkgeräten. Neben der Authentifizierung von Clients mithilfe von 802.1X oder MAB wird auch der Inline- und SNMP-Ansatz angeboten. Vor allem dieses Out-of-the-box-Denken macht es möglich, dass viele Legacy-Geräte weiterverwendet werden können, auch wenn die damit einhergehenden Nachteile, wie der fehlenden Unterbindung der Kommunikation im gleichen Netzwerksegment, zusätzlich betrachtet werden müssen. Doch gerade für KMUs könnte dies besonders interessant sein.

PacketFence wird weltweit in über 5.000 Installationen verwendet und hat eine aktive Community. Zusätzlich kann Support vom Hersteller des Produkts erworben werden, der nach eigenen Angaben rasch auf Supportanfragen reagieren soll. Eine Analyse von 140 Unternehmen, die PacketFence im Einsatz haben, zeigt, dass diese großteils in der Branche IT oder Bildung zu finden sind und ihren Firmensitz in den USA haben. Die Mehrheit der Firmen mit einem jährlichen Umsatz zwischen 10 und 50 Mio. Dollar bzw. mit einer MitarbeiterInnen-Zahl zwischen 1.000 und 5.000 setzen die NAC-Lösung ein [86].

6 Proof-of-Concept - Open Source NAC

6.1 Einleitung

Wie das Kapitel 5 „Evaluierung von Open Source NAC-Produkten“ dargelegt hat, war die Auswahl für kostenlosen NAC-Produkte sehr gering. In weiterer Folge wird daher das einzig verfügbare NAC PacketFence in einem Proof-of-Concept näher untersucht.

6.2 Setup

Windows-Server

Für den Proof-of-Concept wurden zwei Windows-Server aufgesetzt, die als Domänencontroller und Zertifizierungsstelle (Root-CA, Int-CA) dienten. Es wurde eine Domäne mit dem Domänennamen „pf.test“ und der folgenden AD-Struktur aufgesetzt:

1. pf.test
    a) PF
        i. Users
            A. Domain Users
            B. Service Accounts
        ii. Computer
        iii. Groups

Zusätzlich wurde ein Notebook der Domäne hinzugefügt, um einen Test-Client für die verschiedenen Testkategorien zu haben.

PacketFence

PacketFence kann in drei Varianten installiert werden – auf einem bestehenden Linux-Server, mit einer vorbereiteten ISO-Datei oder mit dem „Zero Effort NAC“-Ansatz. Letzteres stellt ein vorinstalliertes bzw. vorkonfiguriertes PacketFence als eine Datei bereit, die auf VM-Hypervisor wie VMware ESX/ESXi oder Microsoft Hyper-V importiert werden kann. Für den Test wurde die Installation mit der ISO-Datei ausgewählt, da der Download von „Zero Effort NAC“ nicht funktioniert hat – die dazu benötigten Dateien sind auf Webseite von PacketFence verfügbar. Dem Installation Guide [85] zufolge benötigt der NAC-Server vier Prozessorkerne, 16GB Arbeitsspeicher und eine Festplatte mit 200GB – für den Proof-of-Concept wurden allerdings nur 12GB Arbeitsspeicher und 50GB Festplatte mangels Hardwareeinschränkung gewählt. Zusätzlich wurden zwei Netzwerkadapter hinzugefügt – einen für das Management des Servers und einen für Legacy-Geräte, die mit der Inline-Methode authentifiziert und autorisiert werden.

Im nächsten Schritt wurde mit der Windows-basierten CA ein Zertifikat für die Weboberfläche und dem RADIUS-Server vom NAC ausgestellt und installiert. Hier hat sich im Test gezeigt, dass es anschließend bei der Validierung der Zertifikatskette Probleme gibt, wenn die Anfrage (Request) und die Bestätigung (Issue) des Zertifikats direkt auf der CA durchgeführt wurde. In der Weboberfläche wird beim anschließend importierten Zertifikat der Status „Chain is valid“ angezeigt, im Webbrowser bzw. beim Authentifizieren mittels 802.1X wird hingegen nur ein selbstsigniertes Zertifikat angeboten. Stattdessen hat die Ausstellung und Konfiguration des Zertifikats mithilfe eines Certificate Signing Request (CSR) funktioniert, der vom NAC ausgestellt und anschließend von der CA signiert wurde.

Im nächsten Schritt wurde PacketFence ebenfalls in der Domäne hinzugefügt, um AD DS als Identity-Source für die Authentifizierungen verwenden zu können. Abschließend wurden die folgenden Netzwerksegmente bzw. VLAN-IDs auf der Firewall und den Switches angelegt, wobei, mit Ausnahme von Inline-Segment, die FortiGate das Gateway der Subnetze darstellt. Die folgenden Netzwerksegmente waren dabei im Einsatz:

- VLAN 201: Registration (10.0.201.0/24)
- VLAN 202: Inline (10.0.202.0/24 wobei PacketFence das Gateway ist)
- VLAN 203: Isolation (10.0.203.0/24)
- VLAN 210: AdminClients (10.0.210.0/24)
- VLAN 211: StandardClients (10.0.211.0/24)
- VLAN 212: MAB (10.0.212.0/24)

Schwachstellen-Scanner

Entgegen der Dokumentation von PacketFence, existiert in der Weboberfläche keine Möglichkeit WMI zur Überprüfung von Richtlinien zu konfigurieren. Es gibt schlichtweg keinen Eintrag für WMI unter den „Scan Engines“. Die Recherche zeigt, dass die Unterstützung für WMI im Jahr 2021 eingestellt wurde [87].

OpenVAS, oder auch unter den Namen Greenbone Community Edition oder Greenbone Vulnerability Management (GVM) bekannt, ist ein kostenloses Framework zum Scannen von Sicherheitsschwachstellen, die auf Endgeräten existieren. Es wurden diverse Ansätze für das Setup versucht, die sowohl auf einem Docker-Image und einer manuellen Installation basierten, aber keiner von denen lieferte einen funktionierenden Schwachstellen-Scanner. Entweder gab es Fehlermeldungen [88], die nicht behoben werden konnten, oder Dienste bzw. Services konnten anschließend nicht gestartet werden [89]. In einem Fall [90] konnte ein Docker-Image erfolgreich aufgesetzt werden, welches im Hintergrund bereits die neuesten Signaturen heruntergeladen hat, allerdings war die Anmeldung in der Weboberfläche mit einer Fehlermeldung von „Der Greenbone Vulnerability Manager reagiert nicht. Dies könnte an einer Systemwartung liegen. Versuchen Sie es später erneut, überprüfen Sie den Systemstatus oder kontaktieren Sie Ihren Systemadministrator.“ nicht möglich. Auch hier zeigt sich, dass der Fehler in der Community kein Einzelfall ist. In einem Foreneintrag [91] wird dieser Fehler auf ein Berechtigungsproblem zurückgeführt, während in einem GitHub-Eintrag [92] das Problem nicht weiterbearbeitet und die Anfrage geschlossen wurde. Die Meldungen hängen nicht direkt mit den in der Arbeit eingesetzten Docker-Images zusammen, inwiefern die Probleme zusammenhängen, kann nicht beurteilt werden.

Die Installation von Tenable Nessus Essentials konnte erfolgreich in einer virtuellen Maschine mit dem Betriebssystem Kali-Linux aufgesetzt werden. Nach der kostenlosen Aktivierung war ein Kontingent von 16 IP-Adressen zum Scannen verfügbar.

6.3 802.1X

Für den Proof-of-Concept wurde der Netzwerk-Switch C3560-CX von Cisco und die Firewall bzw. der WLAN-Controller von Fortinet als „Switches“ hinzugefügt, die wiederum Mitglieder der Default „Switch Groups“ waren. In PacketFence werden alle Netzwerkgeräte, die als Authenticator dienen, als „Switch“ bezeichnet. Zusätzlich wurden die Geräte im Modus „Production“ betrieben – im Modus „Testing“ hingegen wird keine Authentifizierung durchgeführt. Abschließend wurden die VLAN-IDs für die Rollen festgelegt, die in weiterer Folge bei der Authentifizierung zugewiesen werden.

Der Windows-Client wurde mittels Gruppenrichtlinien konfiguriert, sodass dieser Zertifikate automatisch bezieht und eine Netzwerkauthentifizierung mittels LAN und WLAN durchführen kann. Hier wurde ebenfalls die Server-Validierung aktiviert. Die Konfiguration von 802.1X und MAB für den Switch [85, p. 12] bzw. den WLAN-Controller [93, p. 208] wurde der Dokumentation von PacketFence entnommen

Im Test hat sich gezeigt, dass eine Netzwerkauthentifizierung mit 802.1X und PEAP-MSCHAPv2 sowohl für WLAN und LAN möglich war. Hingegen war die Anmeldung mit EAP-TLS weder über den Switch noch über den AP möglich. Der Grund hierfür wird in Abbildung 6.1 dargestellt.

```
Apr 2 14:38:20 servPF01 auth[16955]: (548) Rejected in post-auth: [admin01@pf.test] (from client 192.168.100.254/32 port 3 cli 80:56:f2:71:3e:3f)
Apr 2 14:38:20 servPF01 auth[16955]: (548) Login incorrect (sql_reject: Insufficient space to store pair string, needed 2075 bytes have 2048 bytes):
[admin01@pf.test] (from client 192.168.100.254/32 port 3 cli 80:56:f2:71:3e:3f)
Apr 2 14:38:26 servPF01 auth[16955]: (560) Rejected in post-auth: [admin01@pf.test] (from client 192.168.100.254/32 port 3 cli 80:56:f2:71:3e:3f)
Apr 2 14:38:26 servPF01 auth[16955]: (560) Login incorrect (sql_reject: Insufficient space to store pair string, needed 2075 bytes have 2048 bytes):
[admin01@pf.test] (from client 192.168.100.254/32 port 3 cli 80:56:f2:71:3e:3f)
Apr 2 14:38:31 servPF01 auth[16955]: (571) Rejected in post-auth: [admin01@pf.test] (from client 192.168.100.254/32 port 3 cli 80:56:f2:71:3e:3f)
Apr 2 14:38:31 servPF01 auth[16955]: (571) Login incorrect (sql_reject: Insufficient space to store pair string, needed 2075 bytes have 2048 bytes):
[admin01@pf.test] (from client 192.168.100.254/32 port 3 cli 80:56:f2:71:3e:3f)
Apr 2 14:38:37 servPF01 auth[16955]: (583) Rejected in post-auth: [admin01@pf.test] (from client 192.168.100.254/32 port 3 cli 80:56:f2:71:3e:3f)
Apr 2 14:38:37 servPF01 auth[16955]: (583) Login incorrect (sql_reject: Insufficient space to store pair string, needed 2075 bytes have 2048 bytes):
[admin01@pf.test] (from client 192.168.100.254/32 port 3 cli 80:56:f2:71:3e:3f)
```

Abbildung 6.1: Fehlermeldung bei der Authentifizierung mit EAP-TLS

Eine ausführliche Recherche zeigte, dass dieses Problem in der Community bekannt ist und immer wieder NutzerInnen von PacketFence über diesen Fehler klagen. Die Problematik basiert darauf, dass das sogenannte „linelog“-Modul eine fixe Buffergröße von 2048 Bytes besitzt und bei der Netzwerkauthentifizierung zu viele Attribute abgespeichert werden [94]. Es wurden verschiedene Ansätze getestet, um das Logging zu reduzieren und somit den Fehler zu beheben – allerdings führte keiner zu einem positiven Ergebnis. Einem Foreneintrag [95] zufolge soll der Fehler ein „buffer issue“ sein, der erst in nächsten Major-Version FreeRADIUS 4 behoben werden kann. Basierend auf der E-Mail-Adresse der VerfasserIn stammt diese Informationen von einer MitarbeiterIn des Herstellers.

Trotz der irreführenden Fehlermeldung konnte PacketFence dennoch konfiguriert werden, dass eine Netzwerkauthentifizierung mithilfe von EAP-TLS möglich war. Wichtig ist hier zu beachten, dass bei der „Authentication Source“ die „Search Attributes“ sAMAccountName und UserPrincipalName für eine „User Authentication“, und servicePrincipalName für eine „Computer Authentication“ hinterlegt sein müssen. Anschließend konnte der Windows-Client erfolgreich am Switch authentifiziert werden, wie der folgende Ausschnitt zeigt:

```
SW_3560cx#show dot1x all details
...
Dot1x Authenticator Client List
-------------------------------
EAP Method                  = TLS
Supplicant                  = 089e.01f0.af13
Session ID                  = C0A8643C0000001C02C081D7
    Auth SM State           = AUTHENTICATED
    Auth BEND SM State      = IDLE
```

MAB

Während die Anmeldung im Netzwerk mithilfe von 802.1X erfolgreich getestet werden konnte, war das mit MAC Authentication Bypass initial nicht möglich. Das grundlegende Problem ist hier, dass kaum Dokumentationen [96] für MAB mit Fokus auf PacketFence existieren und somit nur geraten werden konnte. Die Test-MAC-Adresse wurde hierbei als lokaler BenutzerIn, in einer lokalen Datei (Htpasswd) und im AD DS als eigener BenutzerIn hinterlegt, aber PacketFence konnte diese Konfiguration nicht erfolgreich zum Authentifizieren von Legacy-Geräten heranziehen.

Ein möglicher, aber nicht sehr praktikabler Workaround ist es, das gewünschte Geräte an einen 802.1X-authentifizierten Switch-Port anzustecken, sodass PacketFence die MAC-Adresse lernt. Anschließend kann im NAC unter der Registerkarte „Nodes“ bei der gewünschten MAC-Adresse die Rolle manuell zu MAB definiert werden. Wird anschließend das Legacy-Gerät neu angesteckt, funktioniert die Anmeldung und das spezifische VLAN wird zugewiesen.

6.4 Compliance-Check

Während WMI und OpenVAS bereits in der Setup-Phase ausgeschieden waren, konnte Tenable Nessus Essentials erfolgreich installiert werden. Allerdings konnte im Test Nessus als Schwachstellen-Scanner nicht erfolgreich in PacketFence eingebunden werden. Dies ist vor allem dem geschuldet, dass die Dokumentation hierfür sehr oberflächlich ausfällt.

Zusätzlich konnte im Test die Segmentierung für die Registrierung und Isolierung von Endgeräten nicht erfolgreich umgesetzt werden. War die Authentifizierung erfolgreich, so wurde dem Endgerät die spezifische Rolle (Standard-Client oder Admin-Client) bzw. dessen VLAN-ID zugewiesen. Falls die Anmeldung ungültig war, wurde generell der Zugriff verwehrt. Die Vermutung liegt nahe, dass diese Einschränkung mit einem Problem des VM-Hypervisors zusammenhängt. Es war praktisch nicht möglich, der virtuellen Maschine mehr als zwei virtuelle Netzwerkadapter zuzuweisen, da sonst willkürlich Netzwerkadapter bereits beim Starten deaktiviert wurden. PacketFence verlangt allerdings, dass der Zweck der vorhanden Netzwerkadapter in den Netzwerkeinstellungen (zum Beispiel Management, Registration oder Isolation) definiert wird.

6.5 Captive Portal

PacketFence bietet für die Integrierung von Gästen und MitarbeiterInnen (BYOD) ein sehr flexibles Gerüst an, um ein Captive Portal nach den eigenen Wünschen zu konfigurieren. Der Ablauf im Captive Portal wird dabei über einen Flow beschrieben, der in PacketFence unter „Portal Modules“ zu finden ist. Im Test konnte ein Captive Portal für Gäste, die die Nutzungsbedingungen akzeptieren müssen, und MitarbeiterInnen, die BenutzerInnen-Name und Passwort eingeben müssen, erfolgreich aufgesetzt werden. PacketFence ist hierbei so flexibel, dass der Flow aus mehreren Schritten bestehen kann. So kann ein Prozess aufgesetzt werden, der die Person im ersten Schritt nach den Zugangsdaten fragt und im zweiten Schritt die Bestätigung mit dem MFA auffordert. Dies kann grafisch auf der Weboberfläche dargestellt werden, wie es die Abbildung 6.2 zeigt.

Darüber hinaus können mehrere Captive Portals bzw. Flows angelegt werden, um so flexibel auf Anforderungen von unterschiedlichen Standorten eingehen zu können. Es werden diverse Methoden wie „Password of the Day“, E-Mail, SMS oder auch externe Identity-Provider wie Eduroam, Facebook, GitHub unterstützt, die im Captive Portal zur Authentifizierung eingebunden werden können.

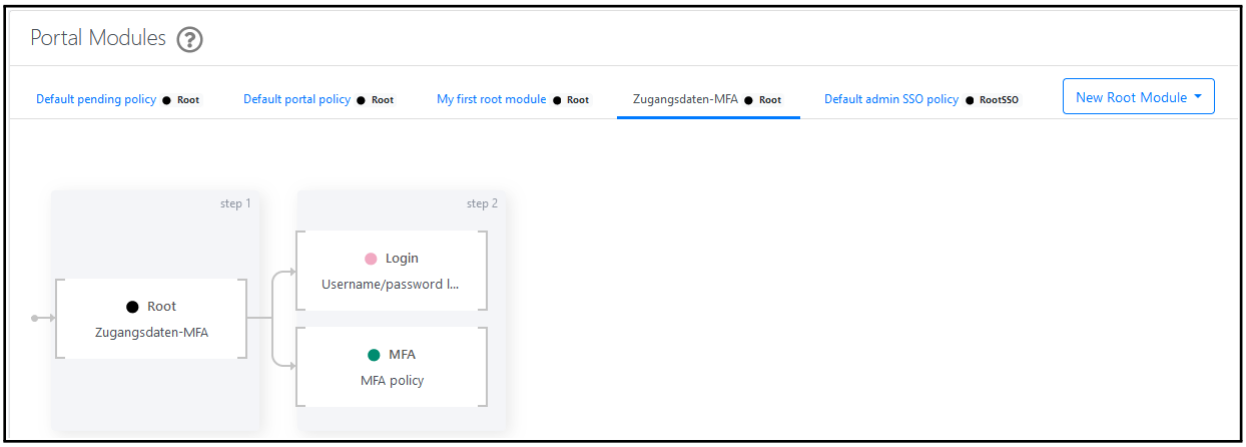


Abbildung 6.2: Grafische Darstellung des Captive Portal Flows

6.6 Inline

Mit dem Inline-Ansatz bietet PacketFence eine Möglichkeit, um Netzwerkgeräte in eine Netzwerkauthentifizierung einzubinden, die nicht 802.1Q bzw. 802.1X unterstützen. Im Test wurde ein dediziertes VLAN für diesen Zweck konfiguriert, wobei das zweite Netzwerkinterface von PacketFence als Gateway und DHCP-Server konfiguriert wurde. Sowohl im WLAN als auch im LAN konnte erfolgreich der Inline-Ansatz getestet werde, zur Authentifizierung steht allerdings nur das Captive Portal zur Verfügung. Ist die Anmeldung erfolgreich, schaltet die lokale Firewall von PacketFence den spezifischen Client frei bzw. sperrt die Kommunikation, wenn die vordefinierte Sitzungsdauer abgelaufen ist. Für die Kommunikation außerhalb des Subnetzes erfolgt entweder mit der eigenen IP-Adresse des Clients oder mit einer IP-Adresse, die PacketFence zur Verfügung (NAT) stellt.

6.7 Monitoring

PacketFence bietet eine Vielzahl an Informationen und Daten an, die einen Einblick zu Systemressourcen, Authentifizierungen und Endgeräten geben. Die Startseite ist hierbei in zwei Kategorien unterteilt – Statistiken zu registrierten Endgeräten und Informationen zur Auslastung des Servers. In Abbildung 6.3 ist ein Ausschnitt der Startseite zu sehen. Darüber hinaus bietet PacketFence eine Timeline zu den durchgeführten Authentifizierungen, ausgehändigte IP-Adressen mit dem integrierten DHCP-Server und der registrierten Endgeräte.

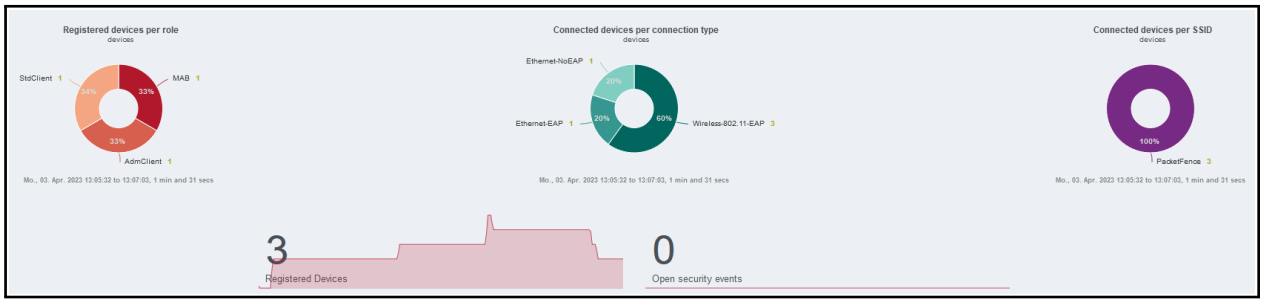


Abbildung 6.3: Statistiken zu den registrierten Clients

Zusätzlich existiert unter dem Menüpunkt „Auditing“ eine Übersicht zu erfolgreichen und fehlgeschlagenen RADIUS-Anmeldungen, wie die Abbildung 6.4 zeigt. Für jeden Versuch wird ein Logeintrag erstellt, der darüber hinaus viele nützliche Informationen zentral an einer Stelle bereitstellt und bei der Fehlersuche hilfreich ist. Die Logeinträge können gefiltert und die Spalten an eigene Bedürfnisse angepasst werden.

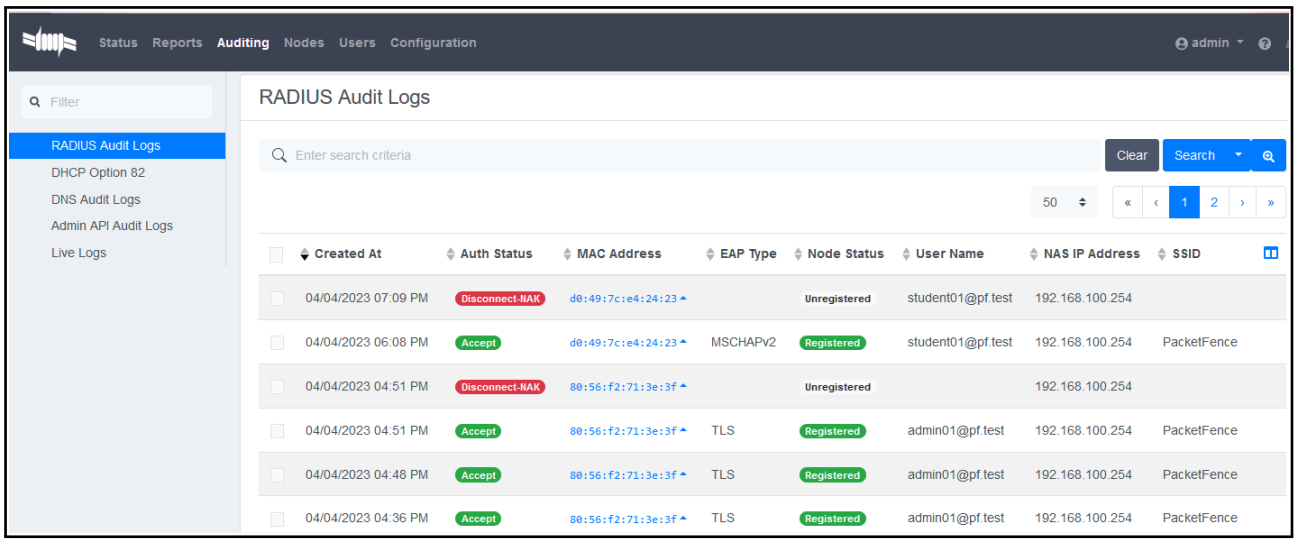


Abbildung 6.4: Übersicht zu erfolgreichen und fehlgeschlagenen RADIUS-Anmeldungen

PacketFence stellt mit der Integrierung von „Fingerbank“ eine Möglichkeit bereit, um Clients zu analysieren und deren Hersteller und Gerätetyp zu erkennen. Technisch wird hierzu die MAC-Adresse, der Browser-User-Agent und DHCP-Informationen beim Abrufen einer IP-Adresse analysiert. Vor allem die MAC-Adresse wird allerdings in Zukunft stark an Relevanz verlieren, weil die Betriebssysteme der Clients mittlerweile die MAC-Adresse zufällig generieren lassen können, und dies bei Android und iOS standardmäßig eingeschaltet ist. In der Praxis hat sich zusätzlich gezeigt, dass die Qualität dieser Analyse besser funktioniert, wenn das Captive Portal verwendet und somit die IP-Adresse von PacketFence verteilt wird. So konnte beim Captive Portal das genaue Handy-Modell und Betriebssystem eruiert werden, während bei der Authentifizierung mittels 802.1X nur der Hersteller sichtbar war. Abbildung 6.5 liefert eine Übersicht der registrierten Endgeräte inklusive einiger Informationen. Diese Ansicht kann zusätzlich nach „Switch Groups“ gefiltert werden, wodurch eine spezifische Einsicht und Visualisierung pro Standort umgesetzt werden kann. Darüber hinaus protokolliert PacketFence den Zeitpunkt von Anmeldungen bzw. den Wechsel zwischen den Rollen, und stellt diese als Timeline pro Endgeräte zur Verfügung.

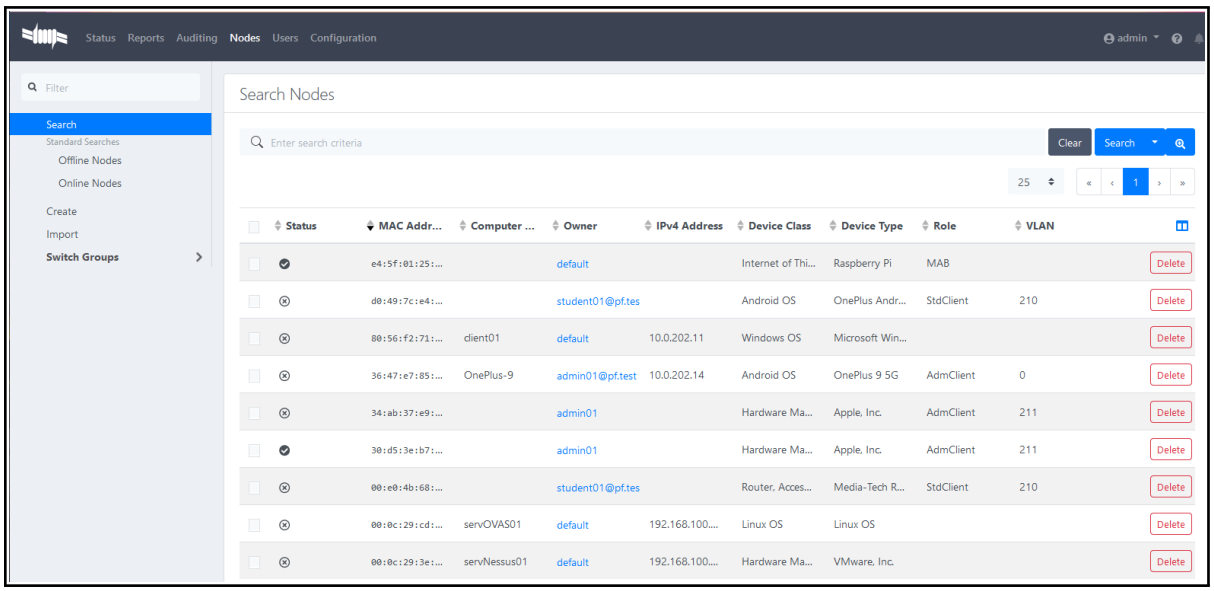


Abbildung 6.5: Übersicht der registrierten Clients

Der Menüpunkt „Users“ liefert eine zentrale Übersicht aller BenutzerInnen, die mit PacketFence interagiert haben. Dazu zählen lokal erstellte BenutzerInnen-Konten aber auch alle Konten, die über einen externen Identity-Provider eingebunden waren. Zusätzlich können im Captive Portal Felder wie E-Mail-Adresse oder Firma definiert werden, die bei der Anmeldung angegeben werden müssen und später in Übersicht dargestellt werden können. Des Weiteren bietet PacketFence eine Zusammenfassung aller Clients, die von einer spezifischen BenutzerIn verwendet wurde.

6.8 Fazit

Das Ergebnis des Concepts für PacketFence fällt sehr durchwachsen aus. Auf der einen Seite bietet das NAC eine Vielfalt an Funktionen, die teilweise einzigartig am Markt sind. Das Captive Portal bietet viele Einstellungen, um einen spezifischen Prozess der Anmeldung nach den eigenen Bedürfnissen abbilden zu können. Die Netzwerkauthentifizierung mit 802.1X wird ebenfalls gut unterstützt und es gibt viele Optionen, um möglichst flexibel spezifische Wünsche abdecken zu können. So lassen sich die Authenticator in Gruppen einteilen, wodurch Rollen an unterschiedlichen Standorten spezifischen VLAN-ID zugewiesen werden können. In der Weboberfläche von PacketFence werden viele Statistiken und Graphen zu diversen Kategorien wie Systemressourcen, RADIUS, BenutzerInnen oder registrierten Endgeräte angeboten.

Auf der anderen Seite ist PacketFence eine komplexe Anwendung, die fortgeschrittenes Know-how in den Bereichen Netzwerktechnik und Systemadministration erfordert. Wie das Beispiel mit der irreführenden Fehlermeldung in dem Abschnitt 6.3 „802.1X“ beweist, sind die Logeinträge nicht immer hilfreich und können in die Irre führen. Die Konfiguration von PacketFence mit einem X.509-Zertifikat für den RADIUS- und Webserver war ebenfalls herausfordernd und kann nur mit einem CSR durchgeführt werden, da andernfalls der Zertifikatsbaum nicht korrekt validiert werden konnte, obwohl die Weboberfläche die Validierung als valide anzeigt.

Im Test sind zudem viele kleine Fehler aufgetaucht, die allerdings keine einschneidenden Auswirkungen im Betrieb haben. So muss die Analyse von Endgeräten mit der Fingerbank-Integration manuell angestoßen werden, wenn die Anmeldung mit 802.1X durchgeführt wurde – mit dem Captive Portal wurde dies automatisch im Hintergrund erledigt. In den Netzwerkeinstellungen für den Inline-Netzwerkadapter soll laut der Dokumentation angegeben werden, dass das Captive Portal als Service aktiviert bzw. erreichbar (Additional listening daemon(s)) ist. Nach dem Speichervorgang verschwindet allerdings diese Einstellung wieder. Wie die Abbildung 6.6 zeigt, ist bei der „Traffic Shaping Policy“ ein Feld falsch benannt, welches vermutlich den Download beschreiben soll.

Die Vorgaben vom Hersteller bezüglich der Hardware-Anforderung sollten eingehalten werden, da beispielsweise ein zu geringer Arbeitsspeicher zu Instabilitäten führen kann, wodurch der Server sowohl über die CLI als auch über die Weboberfläche nur noch träge reagiert. Inverse inc. bietet diverse Dokumentationen an, die beim Betrieb von PacketFence maßgeblich helfen. Dies ist allerdings auch zwangsläufig notwendig, da abseits vom Hersteller kaum Anleitungen und Guides existieren. Im Alltag muss also auf die

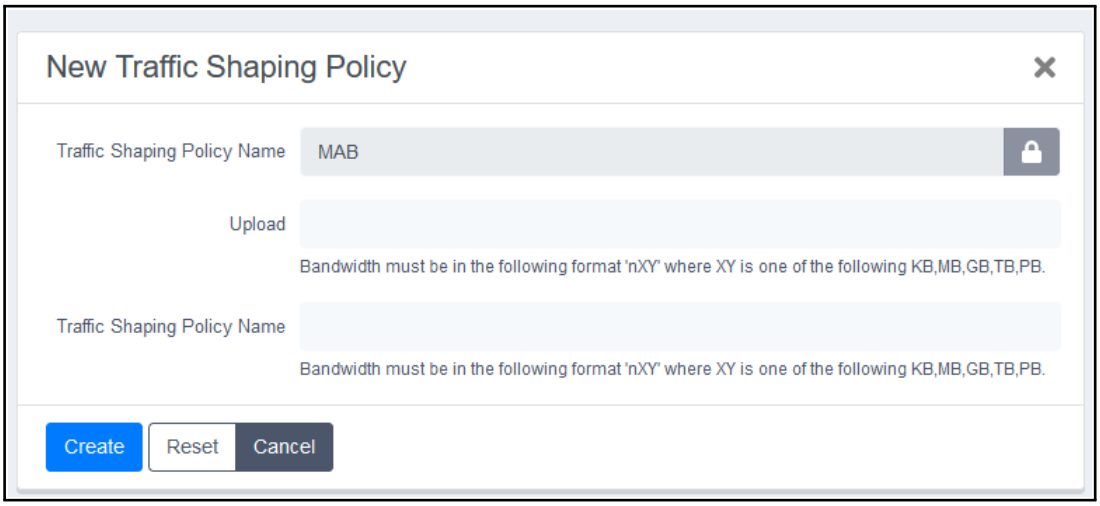


Abbildung 6.6: Felder in PacketFence falsch bezeichnet

Dokumentation von PacketFence vertraut werden, die aber selbst einige Einschränkungen bieten. So dürfte u.a. das Kapitel zur Einbindung von WMI und OpenVAS in PacketFence seit mindestens 2021 bzw. 2020 nicht mehr aktualisiert worden sein, da zu diesem Zeitpunkt die Unterstützung eingestellt wurde. Zusätzlich gibt es Ungenauigkeiten zwischen Text und Bild bei der Konfiguration des Captive Portals. So wird im Text ein Captive Portal ohne Anmeldung beschrieben, während die Abbildung die Konfiguration für ein Captive Portal mit einer Umfrage darstellt [85, p. 89].

Werden die Konfiguration von PacketFence geändert, so ist teilweise der Neustart von bestimmten Diensten notwendig. In der Dokumentation wird allerdings nur sehr inkonsistent darauf hingewiesen, ob und welcher Dienst neu gestartet werden muss. Im Test kam es mehrmals vor, dass der Server allgemein neu gestartet werden musste, damit die Änderungen wirksam wurden.
Im Proof-of-Concept war es nicht möglich, PacketFence für die Überprüfung von Richtlinien aufzusetzen. Entweder war die Methode entgegen der Dokumentation nicht mehr unterstützt oder die vorhandene Dokumentation war nicht ausreichend.

PacketFence bietet mit „Inline“ bzw. Port-Security und SNMP zwei alternative Möglichkeiten an, um eine Anmeldung im Netzwerk umzusetzen. Im Test konnten Endgeräte erfolgreich mit der Inline-Methode authentifiziert werden, wobei im Hintergrund ein Captive Portal benutzt werden musste. Der SNMP-Ansatz konnte nicht getestet werden, da auch hier die Dokumentation sehr gering ausfällt.

7 Evaluierung von On-Premises-Verzeichnisdiensten in Form eines All-in-one-Ansatzes

7.1 Einleitung

Microsoft stellt mit seinem Active Directory Domain Services (AD DS) einen De-facto-Standard für die Verwaltung von BenutzerInnen-Konten und Endgeräten bereit. Die zentrale Konfiguration von Clients mit Group Policy Objects (GPOs) ist ebenfalls möglich wie die Vergabe von Berechtigungen mit einer Gruppenzugehörigkeit. Viele Services bauen auf AD auf und verwenden dies zur Authentifizierung und Autorisierung. Die Komplexität nimmt allerdings stark mit der Anzahl der Windows Server-Rollen (Active Directory Federation Services, Active Directory Certificate Services, NPS, Fileserver, etc.) zu und es werden fachkundige Personen benötigt, die die Systeme warten und diese sicher halten. Dieser Aufwand mit den verbundenen Lizenzkosten ist für manche Firmen allerdings wirtschaftlich nicht sinnvoll bzw. finanzierbar, wodurch Alternativen zu Microsofts AD DS in Frage kommen, die in diesem Kapitel vorgestellt werden. Mit Samba 4 wird erstmals die Funktionalität eines Microsoft-kompatiblen Modus „Active-Directory Domain-Controller“ (AD DC) angeboten [97], die die Ausführung unter Linux möglich macht.

Ziel dieses Kapitels ist die Recherche und Evaluierung von potenziellen Alternativen zu Microsoft AD, wobei eine davon im Anschluss in einer praktischen Überprüfung näher untersucht wird. Hier liegt der Fokus auf ein System, welches eine möglichst sichere Anmeldung im Netzwerk für die MitarbeiterInnen und deren Endgeräte ermöglicht. Hier wird besonders das Zusammenspiel aus der Verwaltung von BenutzerInnen-Konten, der Konfiguration von Clients, dem RADIUS-Server und einer Infrastruktur für öffentliche Schlüssel (CA) überprüft. Um den administrativen und finanziellen Aufwand für Unternehmen möglichst klein zu halten, sollten diese Komponenten auf einem einzelnen Server (All-in-one) installiert sein, und mit einer zentralen Oberfläche administriert werden.

7.2 Definierung der Anforderungen

Bevor eine Lösung oder ein Produkt näher betrachtet werden kann, sollte vorab der Ist-Stand des Unternehmens in Bezug auf die Ausrichtung der IT näher analysiert werden. Es gibt keine Muster-Lösung, die zu allen Betrieben ideal passt. Daher sollte im Vorhinein die Stärken und Schwächen der eigenen IT-Assets näher betrachtet werden, um beispielsweise eine teure Migration zu einem Linux-basierten Produkt zu vermeiden, wenn die eigenen SystemadministratorInnen ausschließlich Erfahrung im Umgang mit Windows-Produkten haben. Die Unternehmen sollten sich die Fragen stellen, welche Anforderungen jetzt, in fünf bzw. zehn Jahren bestehen und wie viel Budget hierfür eingeplant werden muss. Dies sind wichtige Fragen, um ableiten zu können, wohin sich die IT entwickeln kann und muss.

Es gibt bereits viele Systeme auf Linux-Basis, die die komplexe Administration von Services wie AD DS und Co. über eine Weboberfläche komfortabel für Nicht-IT-Spezialisten ermöglicht. Allerdings bauen diese Produkte auf das Paket Samba 4 auf, die mit der Entwicklung von Microsoft Active Directory nicht mithalten kann und somit diverse Sicherheitsfunktionen und Features nicht anbieten kann. So kann ein Active Directory Domain Services auf Windows-Basis von Haus mit einer bidirektionalen Replizierung der Daten umgehen, während dies auf Samba 4-Basis nicht ohne Umwege umgesetzt werden kann.

7.3 Einschränkungen von Samba 4

Samba bietet in der Version 4 eine kostenlose Alternative zu Microsofts Active Directory Domain Services, allerdings existieren auch einige Einschränkungen, die beachtet werden müssen. Grundsätzlich definiert Samba die Software als stabil für den Einsatz in einer produktiven Umgebung, obwohl auf Einschränkungen wie die fehlende native Sysvol-Replikation hingewiesen wird [98]. Es werden Workarounds für die unidirektionale [99] bzw. bidirektionale [100] Replikation angeboten, doch diese verlangen technisches Fachwissen und skalieren nicht besonders mit mehreren Servern.

Samba 4 setzt für die Bereitstellung eines Active Directory Domain Controller auf eine Gesamtstrukturfunktionsebene (Forest functional level) von Windows Server 2008 R2. Neue Funktionen und Sicherheitsverbesserungen, die auf Gesamtstrukturfunktionsebenen von Windows Server 2012, Windows Server 2012 R2 oder Windows Server 2016 bauen, fehlen somit bei der Linux-Implementierung. Für Windows Server 2019 oder Windows Server 2022 wurde keine neue Ebene erstellt, wobei die Zukunft ungewiss ist [101].

Bis Samba in der Version 4.10 wurde noch ein altes Datenbank-Format eingesetzt, wodurch hier die Einschränkung von max. 100.000 AD-Objekten besteht. Da Synology in ihrem Paket für AD DS noch die Version 4.10 einsetzt, muss diese Limitierung beim Einsatz eines Synology-Speichers mitberücksichtigt werden. Mit Samba 4.11 wird ein neues Datenbank-Format eingesetzt, die die Verwendung von mehr als 100.000 AD-Objekten erlaubt [102, p. 29].

Eine weitere Einschränkung besteht darin, dass ausschließlich eine einzelne Domäne in einer einzelnen Gesamtstruktur (Forest) verwendet werden kann. Mehrere Domänen in einer Gesamtstruktur oder generell mehrere Gesamtstrukturen werden nicht unterstützt [103].

Synology gibt bei ihren „AD DS“-Paket an, dass das Active Directory-Modul für Windows PowerShell nicht unterstützt wird. Zusätzlich funktionieren sekundäre Domänencontroller nur mit Domänen, die von dem Synology Directory Server erstellt wurden. Die Liste an BenutzerInnen-Konten, die an einem „Read Only Domain Controller“ (RODC) authentifiziert wurden, können nur angezeigt werden, wenn der RODC einer Windows AD-Domäne beigetreten ist. Ein Windows-basierter „Read Write Domain Controller“ (RWDC) synchronisiert die Informationen alle fünf Minuten zu den RODC [104].
Das Paket von Synology verwendet, wie viele Produkte von anderen Herstellern, im Hintergrund Samba 4 – die zuvor erwähnten Synology-spezifischen Einschränkungen können somit auch andere Produkte betreffen.

7.3.1 Sicherheitsüberlegungen für Samba 4

Wie bereits erwähnt verwendet Samba 4 eine Gesamtstrukturfunktionsebene von Windows Server 2008, wobei Windows Server 2016 die letzte Gesamtstrukturfunktionsebene ist, die eine Veränderung mitbringt. Somit fehlen Samba 4 drei Versionssprünge (Windows Server 2012, Windows Server 2012 R2 und Windows Server 2016), um die neuesten Funktionen und Sicherheitsverbesserungen zu verwenden [101]. Einige Verbesserungen werden in den nächsten Absätzen im Detail vorgestellt.

Mit der Gesamtstrukturfunktionsebene von Windows Server 2012 R2 wird die Security-Gruppe „Protected Users“ unterstützt, die u.a. eine Sicherheitsbaseline für BenutzerInnen-Konten im Umgang mit der Authentifizierung, der Speicherung der Sitzung und der Rechtevererbung festlegt [105]. Zusätzlich erhält ein neues Feature Einzug, welche Replizierungsfehler zwischen DCs reduziert, sollte einer der Domänencontroller aus einem Backup oder Snapshot wiederhergestellt werden. Dies wird mit einem fortlaufenden 128-Bit Wert (VM-GenerationID) realisiert, der den aktuellen Zustand der virtuellen Maschine repräsen-

tiert. Wird ein Server neu gestartet oder führt dieser Veränderungen im AD durch, so vergleicht dieser die VM-GenerationID mit der Kopie im AD und erkennt ein Rollback. Wird die Situation eines wiederhergestellten Servers nicht erkannt, können die notwendigen Maßnahmen für die Wahrung eines stabilen AD DS (beispielsweise die Löschung des aktuellen Relative-ID-(RID-)Pools am betroffenen DC) nicht umgesetzt werden, und es kommt zu Fehlern [106].

Mit Windows Server 2016 wird die Funktion von „Shielded VMs“ eingeführt, die die virtuellen Maschinen von kompromittierten oder böswilligen Administratoren schützt, indem der Zustand und die Festplatte des virtuellen Servers verschlüsselt wird. Mit „Windows Defender Credential Guard“ und „Remote Guard“ werden zusätzlich NTLM- und Kerberos-Zugangsdaten geschützt und Attacken wie „Pass-the-hash“ verhindert. Des Weiteren können bei „group managed service accounts“ (gMSAs) automatisch die Kennwörter von Service-Accounts geändert werden. Mit der Gesamtstrukturfunktionsebene Windows Server 2016 wurde das Kerberos-Protokoll verbessert, um eine Gruppenmitgliedschaft im Kerberos-Ticket Zeit-limitiert zu erlauben. Ist die vordefinierte erlaubte Zeit abgelaufen, werden die Rechte automatisch ungültig bzw. zurückgezogen [107].

7.4 Hersteller von NAS-Lösungen - Synology und QNAP

Diverse Hersteller von Network Attached Storage (NAS) bieten mit ihren Betriebssystemen nicht nur eine Möglichkeit zur Verwaltung ihrer Speicher-Produkte an, sondern erweitern ihr System darüber hinaus mit Services, die modular hinzugefügt oder entfernt werden können. Synology gilt als ein populärer Anbieter von NAS-Produkten und bietet mit seinen sogenannten Paketen wie Medien-Server oder Musik-Player bzw. mit E-Mail-Server oder „Virtual Machine Manager“ sowohl Lösungen für Endkunden als auch Businesskunden an. Für diese Forschungsarbeit sind allerdings die Pakete wie DNS-Server, „Directory Server“ [108] oder RADIUS-Server [109] besonders interessant, um so eine potenzielle Alternative zu Microsofts Active Directory anbieten zu können. Die Sicherung der Anwendungsdaten kann ebenfalls über die herstellereigene Lösung „Hyper Backup“ umgesetzt werden. Neben Synology bietet auch das Unternehmen QNAP ähnliche Anwendungen wie den RADIUS-Server [110] oder eine Alternative zu Microsofts Active Directory an [111].

Der erste Nachteil dieser Lösung ist, dass beide Hersteller kein Paket für die Installation einer Infrastruktur für öffentliche Schlüssel anbieten. Die Installation einer CA kann zwar virtualisiert über den Virtual Machine Manager betrieben werden, erhöht allerdings den Aufwand für kleine Firmen und widerspricht dem Ziel dieses Kapitels.

Der zweite Nachteil ist die Tatsache, dass zumindest Synology in der neuesten Betriebssystem-Version DSM 7.1 (Paket-Version 4.10.18-0387 Stand 18.02.2023) die veraltete Samba-Version 4.10 verwendet [104]. Laut dem Samba Wiki gilt diese Version seit 2020-09-22 als nicht mehr unterstützt (EOL) [17]. Ob die Software mithilfe der Backporting-Methode aktuell gehalten wird, wie es bei den Linux-Distribution Debian oder CentOS üblich ist, konnte nicht eruiert werden. Das Versionsschema des Pakets bzw. vereinzelten Berichte im Internet lassen zumindest auf den Einsatz der Linux-Variante Debian schließen, die allerdings stark auf deren Einsatzzweck angepasst wurde um somit kein vollwertiges Debian darstellt [112][113][114].

7.5 Zentyal

Das Unternehmen „Zentyal“ bietet mit dem gleichnamigen Produkt „Zentyal Linux Server“ eine „einfache Linux Alternative zu Windows Server“ an. Die abgedeckten Services umfassen dabei eine breite Palette von Active Directory Domain Services, über E-Mail-, RADIUS-, DNS-, DHCP-Server, bis hin zu einer CA oder Firewall. Die gesamte Liste an Funktionen ist auf der Webseite des Herstellers zu finden [115]. Die Verwaltung von diesen Services inklusive des Servers an sich erfolgt primär über eine Weboberfläche, die ebenfalls auf dem Server lokal betrieben wird.
Support wird in Form einer einmaligen oder jährlichen Bezahlung angeboten, wobei bei ersterem nur Software- und Sicherheitsupdates bis zum Ende der bezahlten Zentyal Version verfügbar sind, während bei letzterem zusätzlich die Upgrades auf neue Major Versionen und technischer Support inklusive sind. Es gibt bei beiden Support-Varianten die Auswahl aus vier Paketen, wobei hier die Unterschiede bei der Anzahl der verfügbaren BenutzerInnen-Konten und bei der jährlichen Bezahlung zusätzlich die Anzahl der inkludierten Tickets liegen. Sollte das Kontingent an Tickets nicht ausreichen bzw. die Lizenz auf einmaliger Bezahlung verwendet werden, so kann bei Bedarf Hilfe von Zentyal zusätzlich erworben werden. Neben der technischen Hilfe im Falle eines Problems wird auch die Unterstützung zur Ausbildung der eigenen MitarbeiterInnen mit Kursen und Zertifizierungen angeboten [116].

Der technische Unterbau basiert auf Ubuntu in der LTS-Variante, wobei die Major-Versionen von Zentyal mit den Ubuntu LTS-Versionen gekoppelt sind (Zentyal 7.x = Ubuntu LTS 20.04, Zentyal 6.x = Ubuntu LTS 18.04, usw.) und für einen Zeitraum von ca. 4,5 Jahren technische Unterstützung und Sicherheitsupdates zur Verfügung gestellt werden [117]. Zentyal setzt für einen Microsoft Active Directory kompatiblen Domain Controller auf das Linux-Paket „Samba“ in der Version 4.13.17, welches bereits im März 2022 das End-of-Life erreicht hat [17]. Allerdings wird mit Stand Februar 2023 die Version „2:4.13.17 dfsg-0ubuntu1.20.04.5“ eingesetzt, welche von Ubuntu weiterhin mit Sicherheitsupdates aktuell gehalten wird [118].

7.6 Linuxmuster

Linuxmuster ist eine umfassende Komplettlösung zum Betrieb schulischer IT-Infrastrukturen, die in über 200 Schulen mit ca. 25.000 Endgeräten und ca. 135.000 BenutzerInnen-Konten eingesetzt wird [119]. Die BenutzerInnen-Verwaltung erfolgt ebenfalls mit einem Active Directory auf Samba 4 Basis, wobei zusätzlich bereits ein Konzept für die Rollen SchülerInnen, LehrerInnen, Schul-AdministratorInnen und globalen AdministratorInnen mitgeliefert wird [119][120]. Das Selbstheilungssystem „LINBO“ hält die Rechner der SchülerInnen in einem „unterrichtstauglichen“ Zustand, in dem bei jedem Neustart alle Änderungen zurückgesetzt werden und somit das Risiko für eine fehlerhafte Konfiguration oder Schadsoftware am Endgerät stark reduziert wird. Des Weiteren können LehrerInnen den Zugriff auf Internet und Drucker für die SchülerInnen regulieren, Prüfungen oder die Verteilung von Unterrichtsmaterial über die Schulkonsole abwickeln, die eine Weboberfläche darstellt und somit bequem von diversen Endgeräten aufgerufen werden kann [121].

Der technische Unterbau besteht aus zwei Servern: OPNsense als Firewall und Ubuntu LTS 18.04 als Betriebssystem für den Server. Eine detaillierte Anleitung und Dokumentation inklusive vieler nützlicher Hinweise wird von Linuxmuster in deren Online-Dokumentation angeboten [122].
Das Projekt wird von einem gemeinnützigen Verein betrieben und bietet somit einen ziemlich eingeschränkten Support an [119]. So gibt es an einem Wochentag ein vier Stunden Fenster, in dem telefonischer Kontakt mit dem Support möglich ist. Darüber hinaus wird der Kontakt via E-Mail oder Forum angeboten, die relativ zügige Antworten liefern sollen [123]. Neben dem Support vom gemeinnützigen Verein haben sich mittlerweile einige private Unternehmen gefunden, die ebenfalls Unterstützung bei der Verwaltung der IT-Infrastruktur anbieten [124].

7.7 Manuell Linux Server aufsetzen

Pro forma möchten wird auf die manuelle Installation und Zusammenstellung der notwendigen Linux-Pakete hingewiesen, die ebenfalls eine Alternative darstellen kann. Wie Zentyal erklärt [116], basiert deren Produkt auf über 30 Open-Source-Komponenten, die händisch installiert und konfiguriert werden können. Eine detaillierte Anleitung zum manuellen Aufsetzen von Active Directory Domain Controller auf Samba-Basis wird hier [125] angeboten. Die Auswahl der passenden Linux-Distribution inklusive der einzelnen Pakete, die ebenfalls zusammenspielen müssen, kann allerdings aufwendig sein oder mit zusätzlichen Kosten für Support verbunden sein [126]. Abschließend sei erwähnt, dass diese Variante der Bereitstellung von Services explizit in den Zielen dieser Forschungsarbeit ausgeschlossen ist, da die Administration möglichst nicht von Fachpersonal durchgeführt werden soll.

7.8 Fazit

Mit Samba 4 wurde eine Möglichkeit geschaffen, ein AD DS ohne Lizenzkosten und Abhängigkeiten zu Microsoft zu betreiben. Im Vergleich zu einem „originalen“ Microsoft Active Directory existieren allerdings auch einige Einschränkungen, die auf die eigenen Anforderungen überprüft und abgewogen werden müssen. Viele Hersteller implementieren Samba 4 in ihre Produkte, die sie anschließend mit Support an Kunden vertreiben. Allgemein gibt es einige Produkte bzw. Hersteller, die einen großen Funktionsumfang anbieten und die Verwaltung davon mit einer grafischen Oberfläche realisieren. Dazu zählen auch Produkte wie „NethServer“, „Univention UCS“ oder Tirols „samba4box“, die alle individuelle Einschränkungen, wie eine fehlenden CA als Services, aufwiesen und somit nicht näher berücksichtigt werden konnten.

Hersteller von NAS-Produkten wie Synology oder QNAP bieten teilweise eine breite Vielfalt an Software an, um u.a. Active Directory, Datei- und E-Mail-Server zu betreiben. Dies kann bereits für einige Unternehmen ausreichend sein, um deren Anforderungen abdecken und eine effiziente Plattform für ihre Teams bereitstellen zu können. Allerdings wird in beiden Fällen keine Möglichkeit einer CA angeboten, wodurch dieser Ansatz für diese Forschungsarbeit uninteressant ist. Am Beispiel des „Synology Directory Server“ zeigt sich allerdings, dass die Version (Samba 4.10) der eingesetzten Software im Hintergrund nicht zwangsläufig aktuell sein muss, auch wenn Synology Updates bereitstellt. Hier wird stark empfohlen, dass die Software zuvor auf Aktualität und deren Support für Sicherheitsupdates bzw. Funktionsupdates überprüft werden sollte, bevor dies in einem produktiven Umfeld eingesetzt wird.

Mit Linuxmuster wurde eine ideale Plattform geschaffen, die für Lehreinrichtungen eine einfache und kostenlose Möglichkeit bietet, um die Anforderungen im Schulalltag abdecken zu können. Die Software wird von LehrerInnen entwickelt, um von LehrerInnen in Schulen eingesetzt zu werden, wodurch der Fokus und die zukünftige Entwicklung sehr eindeutig ist. Sollten dennoch Probleme auftreten, wird Hilfe über diverse Möglichkeiten angeboten, weswegen die Scheu für den Einsatz in der eigenen Schule reduziert wird. In Bezug auf diese wissenschaftliche Arbeit wird dieser Ansatz nicht weiterverfolgt, da Linuxmuster sich auf ein Angebot für den Schulbetrieb fokussiert und dies einem breiten Einsatz in Unternehmen widerspricht.

Der Betrieb eines händisch aufgesetzten Linux-Server mit der manuellen Installation der benötigten Komponenten bietet natürlich die größte Flexibilität, bringt allerdings eine hohe Komplexität im Alltag, und kann teilweise von vielen Unternehmen so nicht umgesetzt werden. Zusätzlich erfolgt die Administration an vielen Stellen über die Kommandozeile (CLI), und nicht über einen komfortablen Zugang, wie beispielsweise einer grafische Oberfläche (GUI), die eigentlich die Grundvoraussetzung für dieses Kapitel darstellt. Somit wird diese Variante nicht näher in Betracht gezogen.

Zentyal bietet das beste Gesamtkonzept aus den verfügbaren Services und der Bereitstellung von Support im Falle von technischen Problemen. Es werden alle Services wie RADIUS-Server, CA und AD DS angeboten, die für die Beantwortung der Forschungsfrage benötigt werden. Daher wird in Kapitel 8 „Proof-of-Concept - All-in-one-Ansatz“ das Produkt Zentyal für die praktische Untersuchung herangezogen.

8 Proof-of-Concept - All-in-one-Ansatz

8.1 Einleitung

Das Kapitel 7 „Evaluierung von On-Premises-Verzeichnisdiensten in Form eines All-in-one-Ansatzes“ hat sich ausgiebig mit diversen All-in-one-Produkten beschäftigt, und das Produkt Zentyal für die weiteren Tests ausgewählt.

8.2 Setup

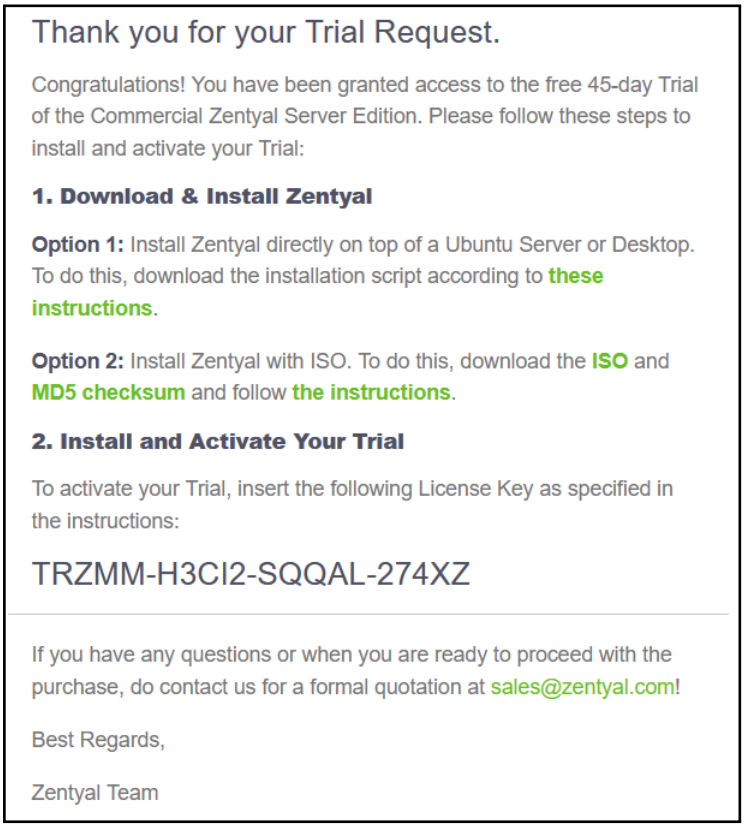
Bei den FAQ auf der Webseite des Herstellers wird für Zentyal eine geringe Hardware-Anforderung für den Betrieb genannt: ein Intel-Prozessor auf Basis eines Intel Core i5, 8GB Arbeitsspeicher und eine ungenaue Angabe der Festplattengröße. Des Weiteren wird angemerkt, dass eine zu Ubuntu kompatible Hardware (Ubuntu-certified hardware) eingesetzt werden soll [127]. Für die Ubuntu-Version LTS 20.04 gibt es Stand März 2023 insgesamt 364 kompatible Server, die somit eingesetzt werden dürfen [128].

ZENTYAL PROFILE	USERS	CPU	MEMORY	DISK	NETWORK CARDS
Gateway	<50	i3 or higher	2 GB	80 GB	2 or more
	50 or more	Xeon Dual core or higher	4 GB	160 GB	2 or more
Infrastructure	<50	i3 or higher	4 GB	80 GB	1
	50 or more	i3 or higher	8 GB	160 GB	1
Office	<50	I3 or higher	8 GB	500 GB	1
	50 or more	Xeon Dual core or higher	16 GB	1 TB	1
Communications	<50	i3 or higher	4 GB	500 GB	1
	50 or more	Xeon Dual core or higher	8 GB	1 TB	1

Abbildung 8.1: Hardware-Anforderungen basierend auf unterschiedlichen Einsatzgebieten [129]

Hingegen liefert der Hersteller im letzten Kapitel der Installationsanleitung für Zentyal eine für den Einsatz abgestimmte Liste an Hardware-Anforderungen. So wird zwischen den Einsatzgebieten als „Gateway“, „Infrastructure“, „Office“ und „Communications“ unterschieden [129]. Eine Übersicht über die Anforderungen basierend auf dem Einsatzszenario liefert die Abbildung 8.1.
Für die Untersuchung wird die kommerzielle Version anstatt der Community Version von Zentyal herangezogen, weil dies der Praxis vermutlich am ähnlichsten ist und darüber hinaus weitere Vorteile wie mehr Funktionen und eine bessere Update-Unterstützung bietet [127]. Der Hersteller stellt hierfür eine 45-tägige Testversion zur Verfügung, die über die Webseite im Austausch von Namen, E-Mail-Adresse und Land bezogen werden kann. Nachdem man die Anfrage für die Testphase abgeschickt hat, bekommt man, wie in Abbildung 8.2 angezeigt, eine E-Mail mit zwei möglichen Optionen für die Installation angeboten.

Für den Testlauf dieser wissenschaftlichen Arbeit wird auf die Option 2 bzw. die Installation mithilfe einer ISO-Datei zurückgegriffen. Damit sichergestellt werden kann, dass die ISO-Datei fehlerfrei heruntergeladen wurde, wird auch der passende MD5-Hash angeboten, welcher mit Tools wie „Get-FileHash -Algorithm MD5“ oder „md5sum“ auf Windows bzw. Linux überprüft werden kann.


Thank you for your Trial Request.

Congratulations! You have been granted access to the free 45-day Trial of the Commercial Zentyal Server Edition. Please follow these steps to install and activate your Trial:

1. Download & Install Zentyal

Option 1: Install Zentyal directly on top of a Ubuntu Server or Desktop. To do this, download the installation script according to **these instructions**.

Option 2: Install Zentyal with ISO. To do this, download the **ISO** and **MD5 checksum** and follow **the instructions**.

2. Install and Activate Your Trial

To activate your Trial, insert the following License Key as specified in the instructions:

TRZMM-H3CI2-SQQAL-274XZ

If you have any questions or when you are ready to proceed with the purchase, do contact us for a formal quotation at sales@zentyal.com!

Best Regards,

Zentyal Team

Abbildung 8.2: Anweisungen für die Installation von Zentyal

Die Installation für den Test erfolgt auf der Hardware, die bereits in Abschnitt 4.6 „Versuchsaufbau“ vorgestellt wurde. Zentyal wird als eine virtuelle Maschine auf Basis vom Zentyal Profile „Infrastructure“ mit vier CPU-Kernen, 4GB Arbeitsspeicher, zwei Netzwerkadaptern und einer 80GB Festplatte auf einer VMware ESXi-Plattform virtualisiert. Die Installation des Betriebssystems inklusive aller Zentyal-Komponenten erfolgt mit der vom Hersteller zur Verfügung gestellten Anleitung [129].

Im Anschluss beginnt die Konfiguration des Linux-Servers über die Weboberfläche, der automatisch den Browser Firefox startet und die URL „https://localhost:8443“ öffnet. Hier wird auch der Lizenzschlüssel benötigt, damit alle Funktionen zur Verfügung stehen.

Die folgenden Pakete wurden ausgewählt und installiert:

- Domain Controller and File Sharing
- DNS Server
- DHCP Server
- Firewall
- Certification Authority
- RADIUS
- HTTP Proxy
- Backup

Manche der bereitgestellten Pakete sind von anderen Paketen abhängig, wodurch sich die ausgewählte Software geringfügig ändern kann. Abbildung 8.3 bietet eine Übersicht der tatsächlich installierten Pakete.

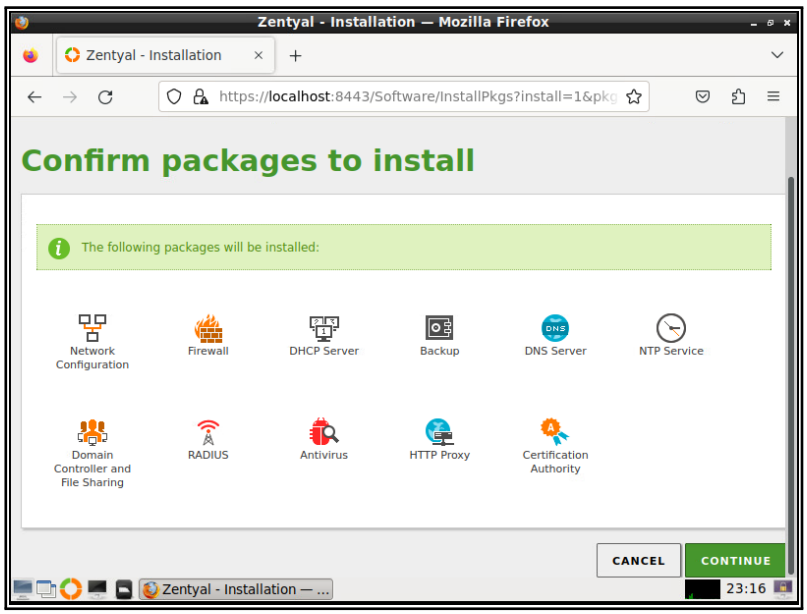


Abbildung 8.3: Übersicht der installierten Pakete

Die zwei virtuellen Netzwerkkarten werden beide für einen internen Einsatzzweck und mit statischen IP-Adressen konfiguriert. Während die eine Netzwerkkarte für die Administration des Zentyal-Servers dient, wird das zweite Netzwerk für die Endgeräte der AnwenderInnen benötigt. Die genauen Netzwerk-Einstellungen können den folgenden Zeilen entnommen werden:

Netzwerkadapter für Management

- IP-Adresse: 10.0.50.20
- Subnetzmaske: 255.255.255.0
- Gateway: 10.0.50.1
- Primäre DNS-Server: 1.1.1.2
- Sekundäre DNS-Server: 1.1.1.1

Netzwerkadapter für Endgeräte bzw. Clients

- IP-Adresse: 10.0.55.1
- Subnetzmaske: 255.255.255.0
- Gateway: 10.0.55.1
- Primäre DNS-Server: 10.0.55.1

Im letzten Schritt wurde der Typ des Domänencontrollers als „Standalone server“ ausgewählt, da es sich hier um eine neue Domäne „zentyal.test“ handelt.

8.3 Active Directory vorbereiten

Administrator-Konto anlegen

Im ersten Schritt wurde ein neues Konto mit dem Namen „admin01“ angelegt, dem die AD-Gruppe „Domain Admin“ zugeordnet wurde und somit als Domänen-Administrator fungiert.

Client der Domäne hinzufügen

Für diesen Schritt wurde zuvor ein PC mit Windows 10 in der Edition „Professional“ vorbereitet, wobei „Enterprise“ oder „Education“ ebenfalls geeignet wären. Der anschließende Prozess zum Hinzufügen des Endgerätes zu der Domäne unterscheidet sich nicht mit einer Domäne, die auf einen Windows Server betrieben wird. Der DNS-Servers des Clients muss auf den DC verweisen, und der tatsächliche „join“ erfolgt über den System-Dialog mit der Definierung des Computernamen und der Domäne.

Remote Server Administration Tools (RSAT) installieren

Die RSAT-Suite ist eine Kollektion von Programmen, die zur Verwaltung von Rollen und Features installiert auf einem Windows Server dienen. Die Anwendungen werden auf dem Windows Client (Windows 10 bzw. Windows 11) installiert, der zuvor der Domäne beigetreten ist. Die Suite an Programmen kann auf einem aktuellen Windows 10 am schnellsten über die „Optionalen Features“ installiert werden. Konkret wurden die folgenden RSAT-Kategorien installiert:

- RSAT: Tools für Active Directory Domain Services und Lightweight Directory Services
- RSAT: Tools für Active Directory-Zertifikatsdienste
- RSAT: Tools zur Gruppenrichtlinienverwaltung
- RSAT: DNS-Servertools

AD Struktur definieren

Um eine Übersicht und eine Struktur in dem AD-Baum zu bekommen, wurden die Organisationseinheiten (OU) „Groups“, „Clients“ und „Domain Users“ angelegt. Auf den letzteren zwei OUs wurden anschließend die Gruppenrichtlinienobjekte (Group Policy Object, GPOs) gebunden, die für die Verwaltung der Clients und der BenutzerInnen benötigt werden. In der Organisationseinheit „Groups“ wurde dann die AD-Gruppe „sec.pem.dot1x“ erstellt, die die Authentifizierung der Endgeräte bzw. der BenutzerInnen am RADIUS-Server steuert.

StandardbenutzerIn anlegen

Es wurde ein neues Konto „student01“ erstellt, der anschließend ein Mitglied der zuvor erstellten AD-Gruppe „sec.pem.dot1x“ wird. Dieses BenutzerInnen-Konto simuliert MitarbeiterInnen in einem Unternehmen.

8.4 802.1X vorbereiten

RADIUS-Server konfigurieren

Wurde der RADIUS-Server zuvor installiert, ist dieser in der linken Seite der Weboberfläche von Zentyal zu finden. Hier wurde anschließend jene AD-Gruppe definiert, die für die Authentifizierung über RADIUS berechtigt ist. In diesem konkreten Fall wurde die AD-Gruppe „sec.pem.dot1x“ hinterlegt. Zusätzlich wurde die Firewall bzw. der WLAN-Controller als RADIUS-Client mit einem Passwort (Shared Secret) konfiguriert, damit diese RADIUS-Anfragen an den Zentyal RADIUS-Server senden darf. Abbildung 8.4 liefert hierfür einen Überblick der konfigurierten Einstellungen.

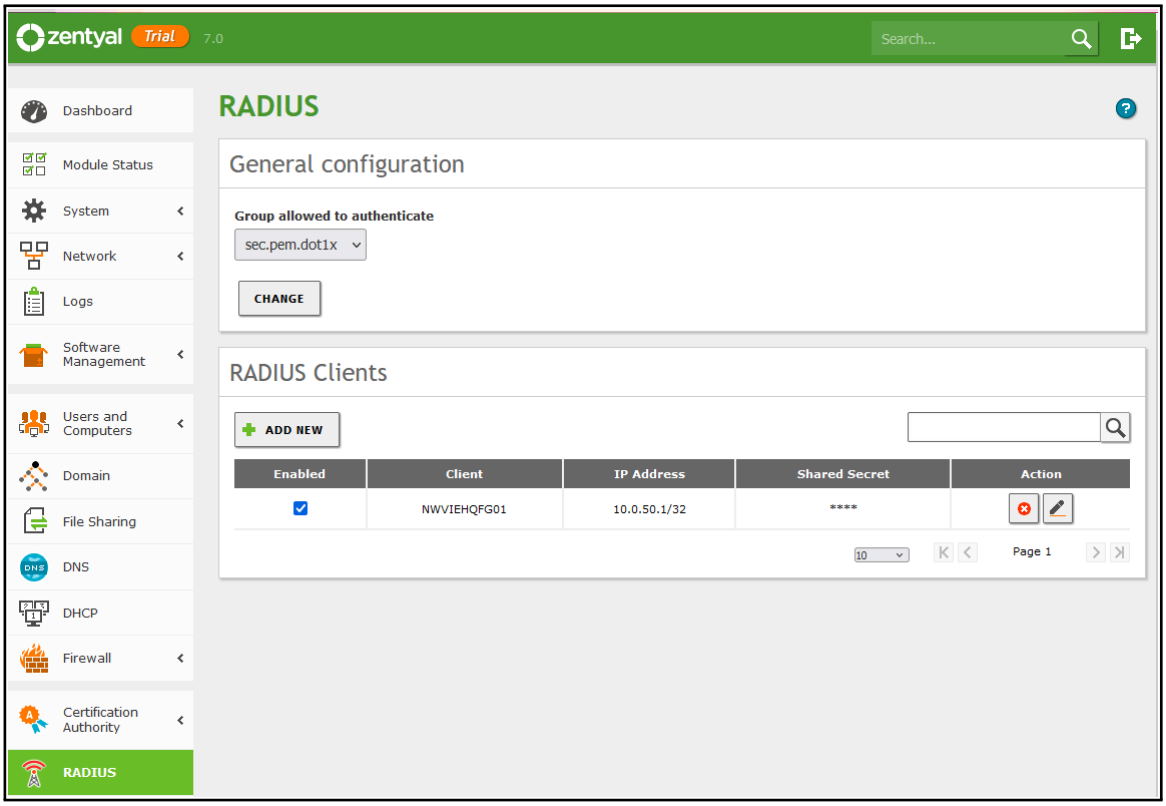


Abbildung 8.4: Übersicht der Konfiguration vom Zentyal RADIUS-Server

Die Funktionalität des RADIUS-Servers ist äußerst eingeschränkt und erfüllt das Minimum. Es kann ausschließlich eine einzelne AD-Gruppe herangezogen werden, die als Berechtigung für eine Netzwerkauthentifizierung dient. Eine Netzwerksegmentierung für Endgeräten mit unterschiedlicher Berechtigung ist daher nicht umsetzbar. Die Definierung der VLAN-ID erfolgt nicht dynamisch am RADIUS-Server, sondern muss am WLAN-Controller vorab konfiguriert werden.

Zertifizierungsstelle konfigurieren

Wenn das Paket „Certification Authority“ installiert und aktiviert ist, kann dieses über die Weboberfläche gestartet werden. Im ersten Schritt wurde eine Root-CA mit den folgenden Parametern erstellt:

- Organization Name: Zentyal-Lab
- Country Code: AT
- City: Vienna
- State: Vienna
- Days to expire: 3650

Die CA ist schnell eingerichtet, bietet allerdings im Wesentlichen auch keine Möglichkeit für Anpassungen oder Einstellungen an. Des Weiteren existiert nur eine Root-CA, die anschließend die Zertifikate für die Services ausstellt. Eine oder mehrere Sub-CAs werden nicht unterstützt, die, mit Fokus auf IT-Sicherheit, essenziell wären. Amazon beschreibt in deren Dokumentation [130] die Variante mit einer Root-CA und einer Sub-CA bzw. einer Root-CA und zwei Sub-CAs als üblich. Hingegen wird der Ansatz mit ausschließlich der Stammzertifizierungsstelle (1x Root-CA) als atypisch beschrieben und bevorzugt in Test-Umgebungen eingesetzt. Der Einsatz in einer produktiven Umgebung widerspricht den „Best Practices“ der Sicherheitsrichtlinien für Stammzertifizierungsstellen.

Zum Erstellen eines Zertifikats existieren ausschließlich die drei Felder „Common Name“, „Days to expire“ und „Subject Alternative Names“ (SAN), aber beispielsweise keine Möglichkeit zur Definierung der Schlüsselverwendung (Serverauthentifizierung, Clientauthentifizierung, etc.). Zusätzlich wird der Einsatz von Zertifikatssperrliste, weder in Form von Certificate Revocation List (CRL) oder Online Certificate Status Protocol (OCSP), nicht unterstützt bzw. die ausgestellten Zertifikate enthalten keine Informationen hierzu, wodurch hier die Sicherheit stark eingeschränkt wird. Grundsätzlich wird allerdings eine CRL unter dem Verzeichnis „/var/lib/zentyal/CA/crl“ abgelegt bzw. aktuell gehalten, sobald ein Zertifikat zurückgezogen wird. Die Veröffentlichung von gesperrten Zertifikaten über einen Webserver wäre somit machbar.

Zertifikate, die über Zentyal mit einem SAN für DNS erstellt werden, besitzen die Schlüsselverwendung „Serverauthentifizierung (1.3.6.1.5.5.7.3.1)“ und „Clientauthentifizierung (1.3.6.1.5.5.7.3.2)“, wodurch die Authentifizierung der Endgeräte über 802.1X möglich erscheint. Des Weiteren können die ausgestellten Zertifikate über die Weboberfläche heruntergeladen werden und stehen dabei in binärer (PKCS #12) und Base64-kodierten (PEM) Form zur Verfügung [131]. Für Windows-basierte Clients ist die PKCS #12-

Variante besonders interessant, da eine einzelne Datei alle wichtigen Komponenten mitbringt und einfach importiert werden kann.

Zentyal bietet die Möglichkeit über die Einstellungen für „Certification Authority > Services Certificates“ in der Weboberfläche ein Zertifikat für den RADIUS-Server zu konfigurieren. Hier existiert allerdings die Einschränkung, dass nur der Allgemeine Name (CN) bestimmt werden kann, allerdings nicht die Dauer der Gültigkeit. Das neue Zertifikat wird mit der gleichen Gültigkeitsdauer wie das Stammzertifikat ausgestellt.

In der Praxis zeigt sicher allerdings, dass das Zertifikat nur unzuverlässig geändert wurde. Während das Zertifikat für den RADIUS-Server mit einem Allgemeinen Namen (CN) von „RADIUS.zentyal.test“ konfiguriert wurde, wie die Abbildung 8.5 zeigt, wurde in der Praxis das Default-Zertifikat mit dem Allgemeinen Namen „Zentyal“ angeboten, wie die Abbildung 8.6a beweist. Im Laufe des Praxistests wurde allerdings das korrekte Zertifikat übernommen, wie die 8.6b zeigt. Dies ist dadurch aufgefallen ist, dass die Server Validierung, welche durch die Gruppenrichtlinie konfiguriert wurde, die Anmeldung im Netzwerk verweigert hat. In der Logdatei „/var/log/freeradius/radius.log“ wurden dazu Logeinträge mit dem Inhalt „eap_tls: TLS Alert read:fatal:access denied“ gefunden.

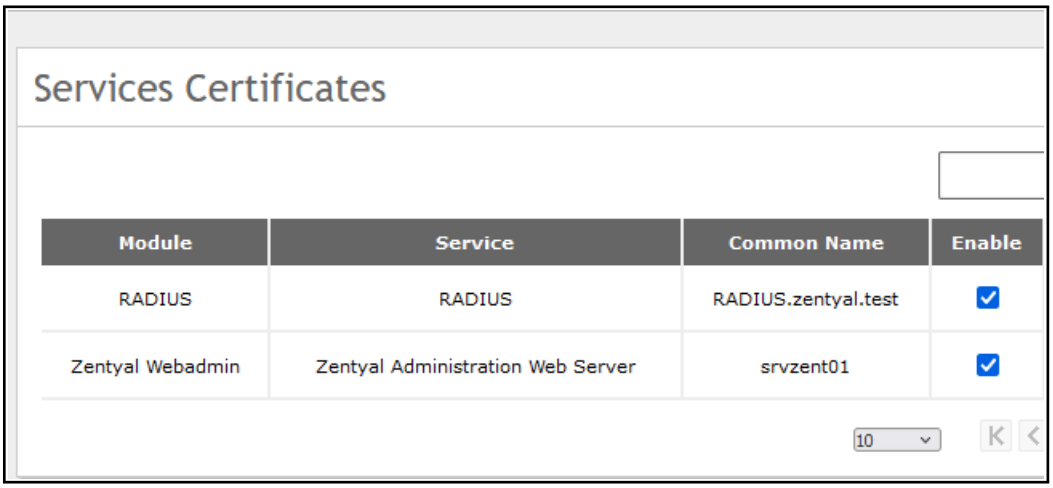
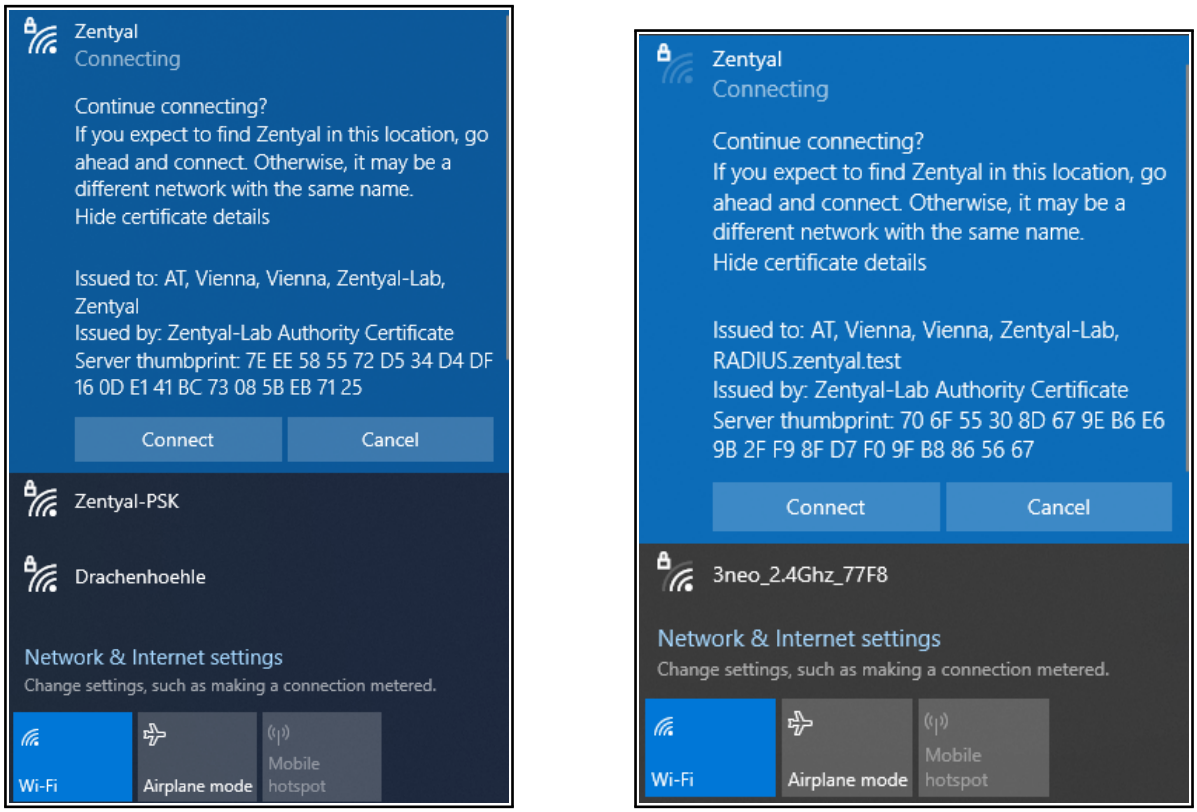


Abbildung 8.5: Übersicht der Service-Zertifikate



(a) Übersicht der Service-Zertifikate (b) Angebotenes Zertifikat vom RADIUS-Server für Endgeräte

Abbildung 8.6: Zertifikat für den RADIUS-Server anpassen

Gruppenrichtlinien konfigurieren

Konfiguration des Clients

Für die WLAN-Konfiguration der Endgeräte wurden im ersten Schritt der Dienst „WLAN AutoConfig“ so eingestellt, dass dieser mit Starttyp „Automatisch“ startet. Zusätzlich wurden die Einstellungen für die 802.1X-Konfiguration mit EAP-TLS, Server-Validierung und akzeptierten Root-Zertifikaten definiert.

Die benötigten Parameter sind unter den folgenden Pfaden zu finden:

- Computer Configuration > Policies > Windows Settings > Security Settings > System Services > WLAN AutoConfig
- Computer Configuration > Policies > Windows Settings > Security Settings > Wireless Network (IEEE 802.11) Policies

Die gesetzten Einstellungen in der Gruppenrichtlinie für 802.1X mit PEAP können der Abbildung 8.7 ent-

nommen werden.

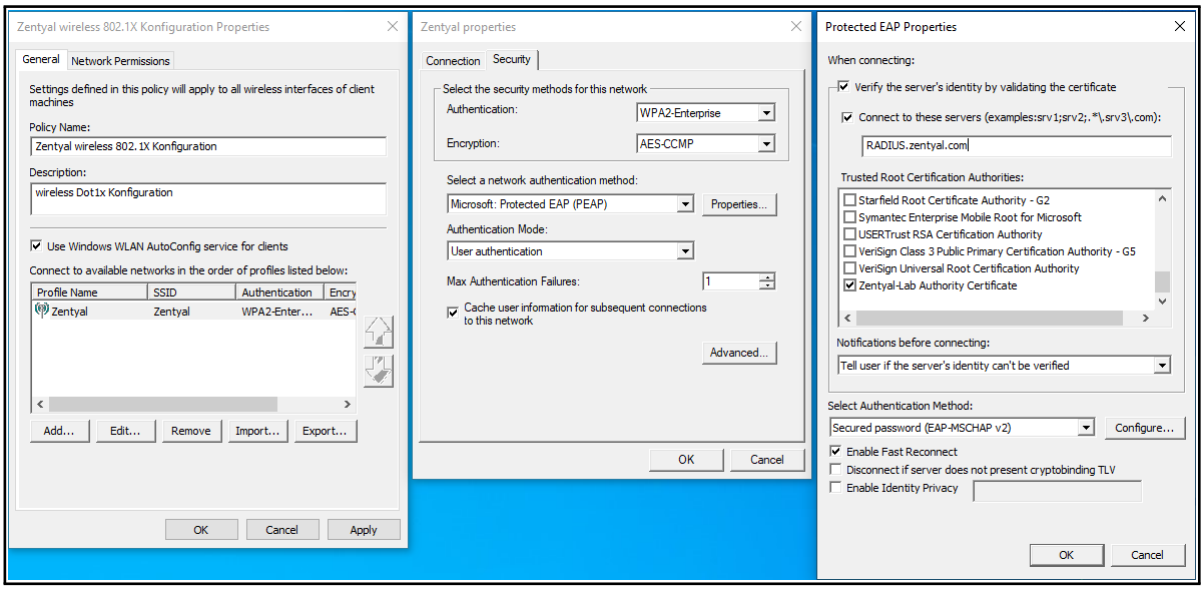


Abbildung 8.7: konfigurierte Gruppenrichtlinie für 802.1X mit PEAP

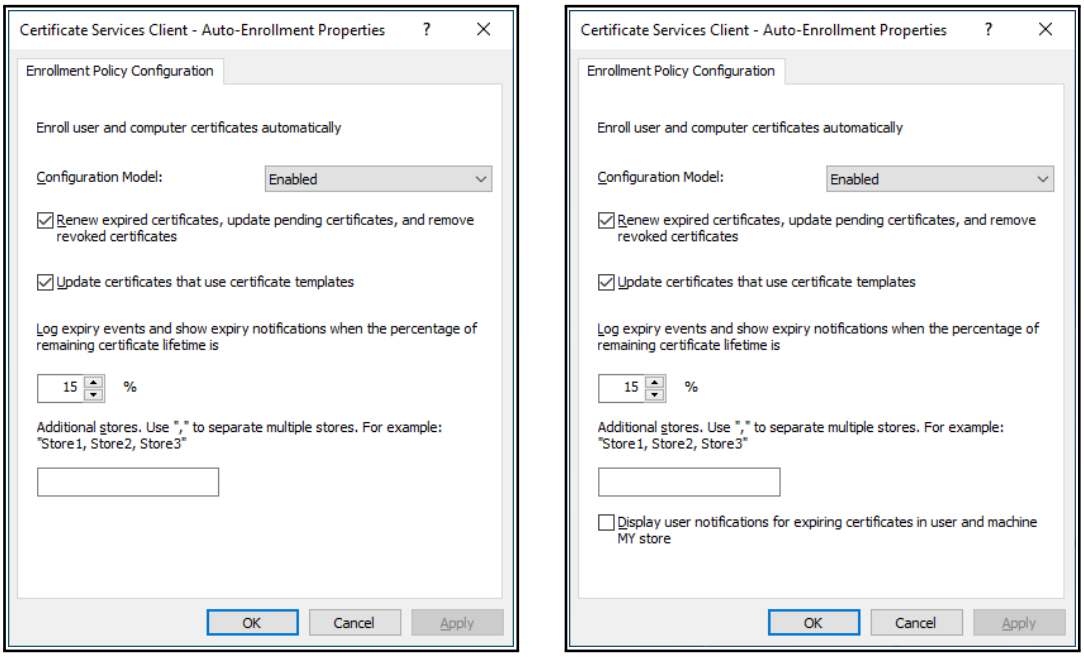
Verteilung der Zertifikate

Nachdem die Root-CA aufgesetzt wurde, wurde das Zertifikat heruntergeladen und über eine Gruppenrichtlinie an die Endgeräte verteilt. Dazu wurde eine neue GPO erstellt und unter dem Pfad „Computer Configuration > Policies > Windows Settings > Security Settings > Public Key Policies > Trusted Root Certification Authorities“ das Zertifikat der Stammzertifizierungsstelle importiert.

Das automatische Beziehen von Zertifikaten für Clients und BenutzerInnen-Konten wurde mit GPOs konfiguriert, die Einstellungen wurden in den folgenden Pfaden gesetzt:

- Computer Configuration > Policies > Windows Settings > Security Settings > Public Key Policies > Certificate Services Client - Auto-Enrollment Settings
- User Configuration > Policies > Windows Settings > Security Settings > Public Key Policies > Certificate Services Client - Auto-Enrollment Settings

Im Test haben diese Einstellungen nicht funktioniert und es wurden keine Zertifikate abgerufen. Die Zertifikate müssen somit manuell erstellt und auf den Endgeräten installiert werden. Die gesetzten Einstellungen können den Abbildungen 8.8a und 8.8b entnommen werden.



(a) Auto-Enrollment Computer (b) Auto-Enrollment User

Abbildung 8.8: Konfiguration für Zertifikat Auto-Enrollment

SSIDs am WLAN-Controller erstellen

Es wurden zwei SSIDs konfiguriert – eine für das Onboarding der Clients und die zweite SSID dient als Test für 802.1X. In beiden Fällen wird den Endgeräten statisch das VLAN 55 zugewiesen, falls die Authentifizierung erfolgreich war. Eine dynamische VLAN-Zuweisung kann über Zentyal nicht konfiguriert werden, wodurch es eine statische Konfiguration benötigt.

SSID 1

- SSID: Zentyal
- Traffic mode: Bridge/local Breakout
- Security Mode: WPA2-Enterprise mit RADIUS-Server
- statische VLAN-Zuweisung: VLAN 55

SSID 2

- SSID: Zentyal-PSK
- Traffic mode: Bridge/local Breakout
- Security Mode: WPA2-Personal mit PSK
- statische VLAN-Zuweisung: VLAN 55

8.5 Netzwerkauthentifizierung

PEAP mit MSCHAPv2

Nachdem Zentyal inklusive aller Pakete aufgesetzt bzw. konfiguriert wurde, konnten erfolgreich Netzwerkauthentifizierung der Endgeräte durchgeführt werden. Für die Anmeldung war allerdings die Kombination aus BenutzerInnen-Name und Passwort notwendig, die Übertragung der Zugangsdaten wurde mit PEAP und MS-CHAPv2 durchgeführt.

Trotz dieser relativ einfachen Konfiguration mit BenutzerInnen-Name und Passwort gab es im Test Schwierigkeiten mit der Anmeldung. Wird ein Endgerät auf Windows-Basis mittels Gruppenrichtlinie angewiesen sich mit PEAP-MSCHAPv2 an einer SSID zu authentifizieren, so wird dies mit dem Schema <Domain>\<Benutzername> beim BenutzerInnen-Name durchgeführt. Der RADIUS-Server von Zentyal akzeptiert allerdings nur den Namen des Accounts (weder Domäne vor oder nach dem Namen). Interessant ist, dass bei Android 13 die Domäne ein Pflichtfeld ist, diesen allerdings laut Log nicht mitschicken dürfte.

Nachstehend sind die Einstellung und die Ergebnisse der Authentifizierungen basierend auf unterschiedliche Betriebssysteme aufgelistet:

iOS 16.3.1

- Identität: student01
- Passwort: <Passwort student01>
- Modus: automatisch
- Authentifizierung: Erfolgreich
- Referenz im Log: Position 1 (Abbildung 8.9)

iOS 16.3.1

- Identität: zentyal\student01 oder student01@zentyal.test
- Passwort: <Passwort student01>
- Modus: automatisch
- Authentifizierung: Fehlgeschlagen
- Referenz im Log: Position 2 und 3 (Abbildung 8.9)

Android 13

- EAP-Methode: PEAP
- Phase 2-Authentifizierung: MSCHAPv2
- CA-Zertifikat: Zentyal-Lab (wurde zuvor importiert)
- Online-Zertifikatsstatus: Zertifikatsstatus erforderlich
- Domäne: zentyal
- Identität: student01
- Passwort: <Passwort student01>
- Authentifizierung: Erfolgreich
- Referenz im Log: Position 4 (Abbildung 8.9)

Android 13

- EAP-Methode: PEAP
- Phase 2-Authentifizierung: MSCHAPv2
- CA-Zertifikat: Zentyal-Lab (wurde zuvor importiert)
- Online-Zertifikatsstatus: Zertifikatsstatus erforderlich
- Domäne: <leer>
- Identität: zentyal\student01 oder student01@zentyal.test
- Passwort: <Passwort student01>
- Authentifizierung: Fehlgeschlagen
- Referenz im Log: Position 5 bis 8 (Abbildung 8.9)

Windows manuell

- Identität: student01
- Passwort: <Passwort student01>
- Authentifizierung: Erfolgreich
- Referenz im Log: Position 9 (Abbildung 8.9)

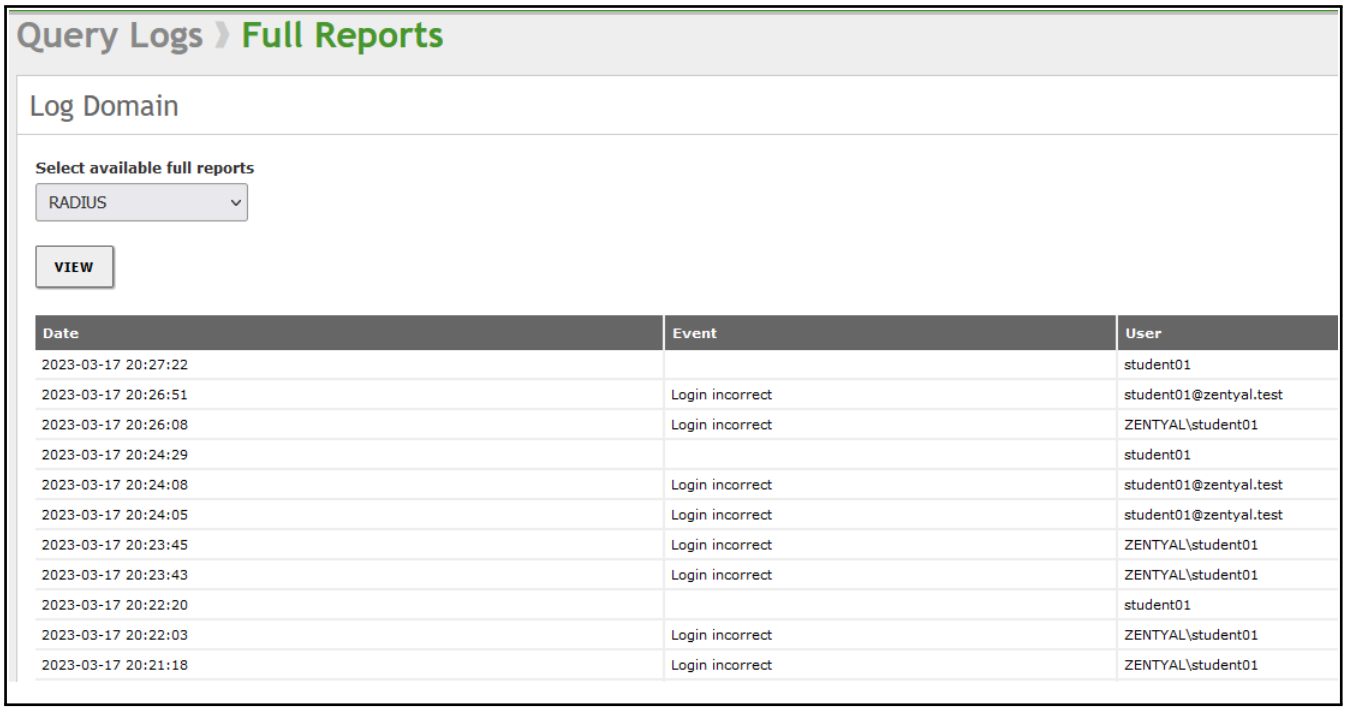
Windows manuell mit „Mein Windows-Benutzerkonto verwenden“

- Identität: zentyal\student01
- Passwort: <Passwort student01>
- Authentifizierung: Fehlgeschlagen
- Referenz im Log: Position 10 (Abbildung 8.9)

Windows mit GPO

- Identität: zentyal\student01
- Passwort: <Passwort student01>
- Authentifizierung: Fehlgeschlagen
- Referenz im Log: Position 11 (Abbildung 8.9)

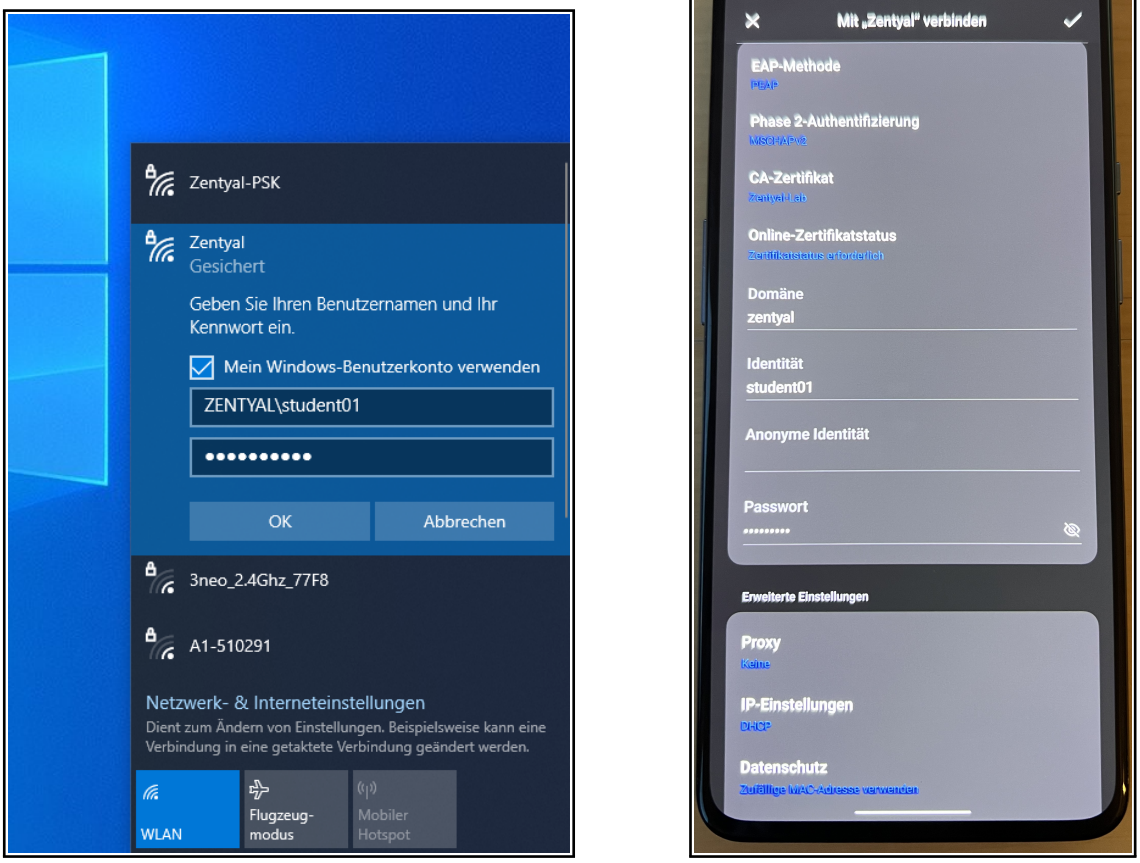
Ist die GPO zur Konfiguration der Endgeräte für 802.1X mit PEAP/MSCHAPv2 aktiv, funktioniert die Anmeldung nicht, da wie bei der manuellen Konfiguration mit „use my Windows user account“ der BenutzerInnen-Name mit dem Schema <Domain>\<Benutzername> übertragen wird. Dieses Ergebnis wird in den Logs bzw. in der 8.9 dargestellt. Die Abbildung wurde zwar grafisch verändert, damit diese weniger Platz in Anspruch nimmt – das Ergebnis wurde allerdings nicht verfälscht.



Date	Event	User
2023-03-17 20:27:22		student01
2023-03-17 20:26:51	Login incorrect	student01@zentyal.test
2023-03-17 20:26:08	Login incorrect	ZENTYAL\student01
2023-03-17 20:24:29		student01
2023-03-17 20:24:08	Login incorrect	student01@zentyal.test
2023-03-17 20:24:05	Login incorrect	student01@zentyal.test
2023-03-17 20:23:45	Login incorrect	ZENTYAL\student01
2023-03-17 20:23:43	Login incorrect	ZENTYAL\student01
2023-03-17 20:22:20		student01
2023-03-17 20:22:03	Login incorrect	ZENTYAL\student01
2023-03-17 20:21:18	Login incorrect	ZENTYAL\student01

Abbildung 8.9: RADIUS-Logs für erfolgreiche und fehlgeschlagene Netzwerkauthentifizierungen

In den Abbildungen 8.10a und 8.10b werden die manuelle Konfiguration für Windows und Android dargestellt, die für die Anmeldung im Netzwerk angewendet wurde.



(a) Konfiguration für Windows

(b) Konfiguration für Android

Abbildung 8.10: Konfiguration für Windows- und Android-basierte Endgeräte

Wie bereits oben beschrieben funktioniert die Anmeldung im Netzwerk mit PEAP-MSCHAPv2 für die Endgeräte nur eingeschränkt bzw. für Windows mit Gruppenrichtlinien nicht ohne weitere Anpassungen. Laut einem alten Foreneintrag [132] gibt es den Ansatz die Datei „/etc/freeradius/3.0/mods-available/mschap“ zu adaptieren. Für diese Änderungen bedarf es allerdings weitgehendes Wissen in Linux, Samba und FreeRadius, wodurch dies nicht näher verfolgt wird. Ob diese Einstellungen darüber hinaus Updates von Zentyal bzw. des Servers beständig sind, ist ebenfalls unsicher.

EAP-TLS

Obwohl Zentyal standardmäßig nicht EAP-TLS unterstützt, kann dies mit wenig Aufwand nachgeholt werden. Hier setzt sich der Trend von vorher fort, dass nur der BenutzerInnen-Name verwendet werden darf, und die Domäne keine Rolle spielt. Dies ist bei der Ausstellung der Zertifikate für die Accounts essenziell, da sonst die Anmeldung über RADIUS nicht erfolgreich ist. In der Praxis war nur die User-Authentication erfolgreich, bei der Computer-Authentication hingegen scheitert es daran, dass bei der Anmeldung die Domäne mitgeschickt wird (host/pc01.zentyal.test).

Zertifikat der Stammzertifizierungsstelle verschieben

Im ersten Schritt muss das Zertifikat der Root-CA an einen bestimmten Platz kopiert werden. Schlussendlich muss das Zertifikat unter dem Pfad „/etc/ssl/certs/ca-certificates.crt“ zu finden sein. Der Versuch den Pfad in der Konfigurationsdatei anzupassen war nicht erfolgreich, da beim Neustart des RADIUS-Servers ein Fehler auftritt (systemctl restart freeradius.service). Das Zertifikat der neuen Root-CA wurde lokal auf der Festplatte nicht gefunden, wodurch der Download über die Weboberfläche als Workaround eingesetzt wurde.

Konfigurationsdatei des RADIUS-Servers anpassen

In diesem Schritt wird die Konfigurationsdatei „/etc/freeradius/3.0/mods-available/eap“ für den Einsatz von EAP-TLS angepasst. Zuerst ist es allerdings sinnvoll die Konfigurationsdatei zu sichern, falls der Originalzustand wiederhergestellt werden möchte. Die folgenden Änderungen wurden anschließend durchgeführt:

- Zeile 27: (-) default_eap_type = md5; (+) default_eap_type = tls
- (Zeile 197: Hier kann der Pfad zum Zertifikat der Root-CA angepasst werden.)
- Zeile 250: Auskommentieren von „random_file = /dev/urandom“
- (Zeile 281: Hier kann die CRL-Überprüfung aktiviert werden.)
- Zeile 330: Die Cipher-Liste von „Default“ auf „High“ härten

Ob diese Konfiguration eine persistente Änderung bietet, oder ob diese Adaptierung regelmäßig nach Updates erneut durchgeführt werden muss, kann nicht beantwortet werden. Für die gesetzten Änderungen wurde ein Guide von Alpine Linux herangezogen [133].

Gruppenrichtlinie vorbereiten

Die Einstellungen in der Gruppenrichtlinie wurden an den folgenden zwei Pfaden durchgeführt.

- Computer Configuration > Policies > Windows Settings > Security Settings > System Services > WLAN AutoConfig
- Computer Configuration > Policies > Windows Settings > Security Settings > Wireless Network (IEEE 802.11) Policies

Die gesetzten Einstellungen in der Gruppenrichtlinie für 802.1X mit EAP-TLS können der Abbildung 8.11 entnommen werden.

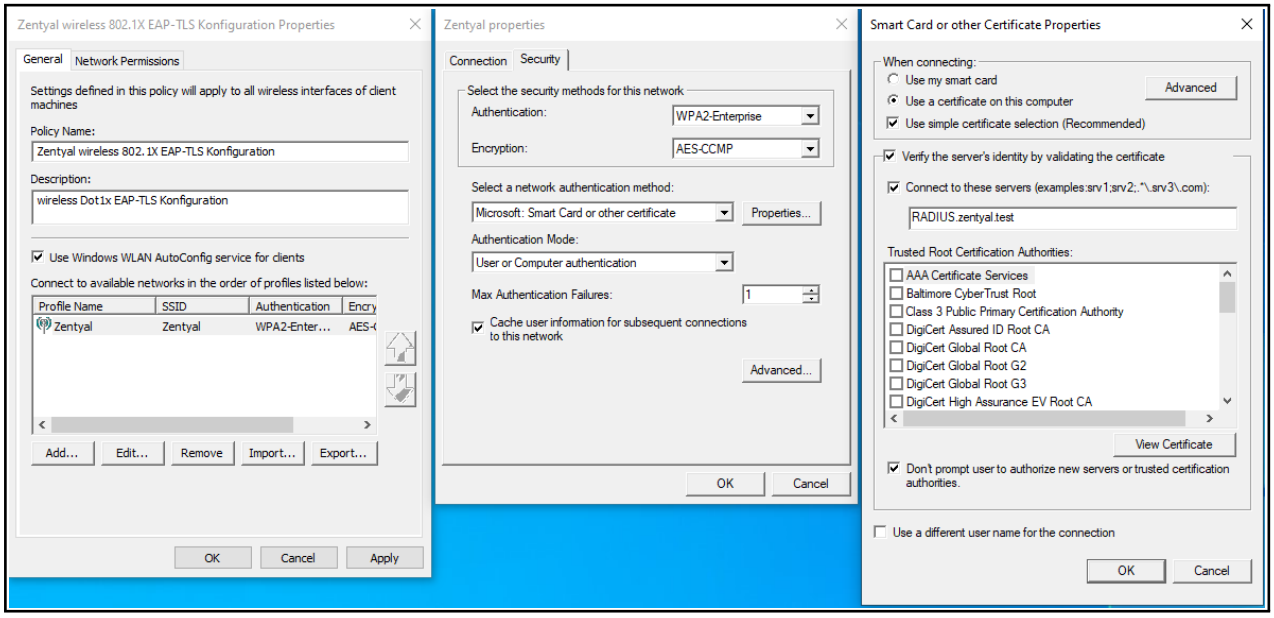


Abbildung 8.11: konfigurierte Gruppenrichtlinie für 802.1X mit EAP-TLS

Zertifikate ausstellen und installieren

Wie bereits erwähnt, funktioniert das automatische Abrufen von Zertifikaten für BenutzerInnen und Endgeräten mit den Gruppenrichtlinien nicht. Daher müssen die Zertifikate manuell ausgestellt und verteilt bzw. auf den Endgeräten installiert werden. Die Ausstellung erfolgt über die Weboberfläche, wobei nur der Allgemeine Name (CN) wie zum Beispiel „student01“ und die Dauer der Gültigkeit benötigt wird. Das Zertifikat kann anschließend exportiert, auf das gewünschte Gerät kopiert und installiert werden.

8.6 Probleme

Zentyal bietet viele Funktionen und punktet vor allem mit einer intuitiven Weboberfläche, die zur Konfiguration sämtlicher Services dient. Wenn Änderungen getätigt wurden, sind diese nicht sofort aktiv und müssen zuerst mit „SAVE CHANGES“ bestätigt werden. Im Test hat sich gezeigt, dass diese zusätzliche Bestätigung nicht zuverlässig funktioniert bzw. ab einem bestimmten Moment hängen bleibt. Ab diesem Zeitpunkt bleibt der Dialog zum Speichern bei der letzten Aufgabe hängen und schließt sich nicht. Es werden die neuen Einstellungen übernehmen, ob allerdings alle Änderungen sauber abgespeichert werden, konnte nicht eindeutig eruiert werden.

Im Verlauf dieser Arbeit wurden mehrere Zentyal-Server aufgesetzt, und nicht immer war die Installation von Updates über die Weboberfläche reibungslos. Hier war es notwendig auf die CLI zu wechseln und die Updates manuell über die Ubuntu-Tools wie „apt“ einzuspielen. In Abbildung 8.12 ist der Fehler bei einem neu aufgesetzten Zentyal-Server zu sehen.

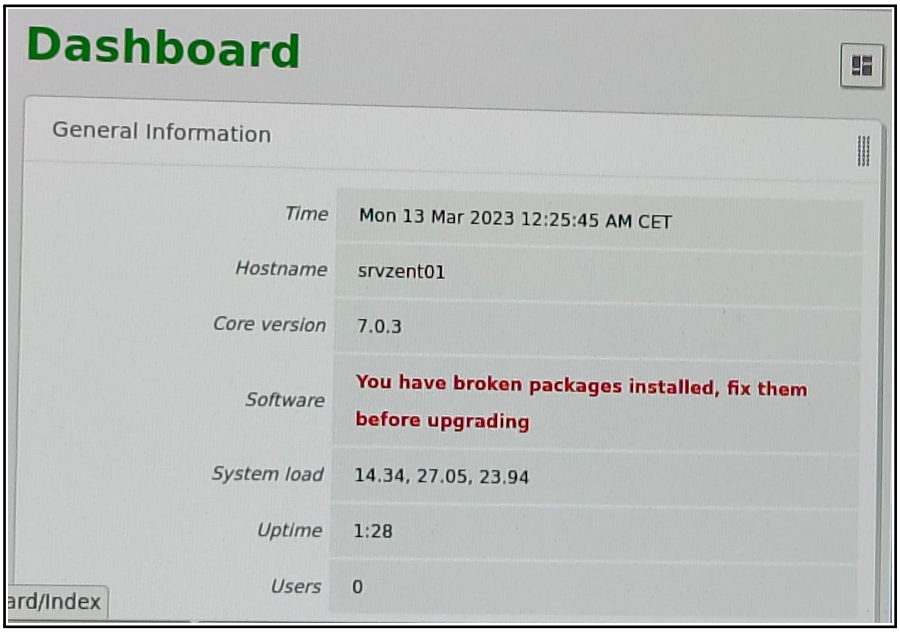


Abbildung 8.12: Probleme mit Software-Komponenten bei Zentyal

Das Anlegen von neuen Gruppenrichtlinienobjekten war initial auch nicht möglich und wurde mit einer Fehlermeldung „Access is denied“ verweigert. Einem Eintrag in dem Zentyal-Forum [134] zufolge, tritt dieser Fehler nicht selten auf und kann mit dem Kommando „samba-tool ntacl sysvolreset“ behoben werden. Der Befehl setzt die Access Control List (ACL) der AD-Daten (Sysvol) auf den Standardwert zurück [135].

Dieser Lösungsansatz wurde durchgeführt und anschließend konnten GPOs erstellt und konfiguriert werden. Des Weiteren trat im Praxistest eine Fehlermeldung auf, die auf einen Konflikt mit unterschiedlichen Sprachen bei der Gruppenrichtlinienobjekten hindeutet. Nach dem Updaten der administrativen Vorlagen (ADMX) war das Problem behoben. Die Fehlermeldung wird in Abbildung 8.13 dargestellt.

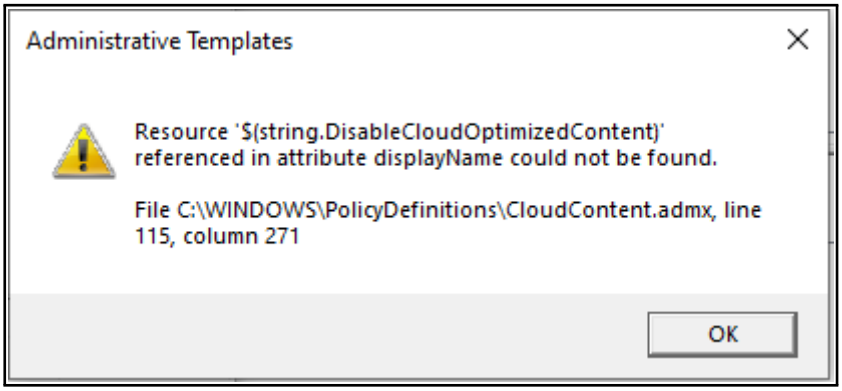


Abbildung 8.13: Fehlermeldung für ein Problem mit den administrativen Vorlagen

Zusätzlich war die initiale Einrichtung zwischen WLAN-Controller und RADIUS-Server herausfordern, da das „Secret“ keine Sonderzeichen enthalten darf. Hier hat Zentyal keine hilfreichen Logdateien zur Verfügung gestellt, um rasch das Problem lösen zu können. Die Logdaten, die Zentyal für RADIUS in der Weboberfläche darstellt, greift im Hintergrund auf die Logdatei „/var/log/freeradius/radius.log“ zu und liest die erfolgreichen und fehlgeschlagenen Anmeldeversuche aus, wie die Abbildung 8.9 zeigt. Diese Logdatei hilft darüber hinaus beim Troubleshooten von gescheiterten Anmeldeversuchen, muss dafür allerdings über Linux-Bordmittel wie der CLI ausgelesen werden.

8.7 Fazit

Zentyal bietet ein solides Paket zur Verwaltung von Endgeräten und BenutzerInnen-Konten an. Die Administration funktioniert mit den RSAT-Werkzeugen von Microsoft sehr gut und im Test gab es kaum merkbare Einschränkungen. Während Active Directory auf Samba 4-Basis somit überzeugt, enttäuschen hingegen die Zertifizierungsstelle und der RADIUS-Server. Mit Fokus auf der Netzwerkauthentifizierung kann hier kein idealer Prozess für Verteilung und anschließender Anmeldung mit Zertifikaten umgesetzt werden. In beiden Fällen muss im Hintergrund die Konfiguration der Linux-Pakete (OpenSSL, FreeRadius, WinBind) angepasst werden, um ein akzeptables Level an Sicherheit und Usability gewährleisten zu können.

Zentyal bietet am Dashboard eine schnelle und einfache Übersicht über ausstehende Updates, wie die Abbildung 8.12 zeigt. Zusätzlich gibt es die Option Updates automatisch zu einer vordefinierten Zeit einspielen zu lassen. Darüber hinaus werden viele Services von Zentyal angeboten, allerdings sind deren Funktionalitäten stark eingeschränkt und bildet das absolute Minimum für den Betrieb. So bietet der RADIUS-Server mit einer AD-Gruppe eine nur sehr eingeschränkte Möglichkeit Zugriff für das Netzwerk zu definieren. Eine dynamische Zuweisung von VLANs und die damit einhergehende Berechtigungssteuerung ist somit auch nicht möglich.

Die Zertifizierungsstelle unterstützt nur eine Stammzertifizierungsstelle ohne Zwischenzertifizierungsstelle, die wiederum nicht den Sicherheitsrichtlinien für Stammzertifizierungsstellen entspricht. Des Weiteren wird keine Möglichkeit zum Blockieren von gesperrten Zertifikaten unterstützt, die die Sicherheit von Zertifizierungsstellen stark in Frage stellt. Das automatische Beziehen von Zertifikaten für Clients oder BenutzerInnen mithilfe einer Gruppenrichtlinie, wie es Microsoft AD DS anbietet, wird nicht unterstützt.

Standardmäßig bietet Zentyal nur die Netzwerkauthentifizierung mit PEAP-MSCHAPv2 an, also die Kombination aus BenutzerInnen-Name und Passwort. Die Anmeldung mit Zertifikaten, also EAP-TLS, lässt sich manuell realisieren, indem die Konfigurationsdateien des darunterliegenden RADIUS-Servers modifiziert wird. Ob diese Änderungen tatsächlich langfristig bestehen bleiben, oder ob diese durch Updates überschrieben werden, kann nicht beantwortet werden. Die Anmeldung mit Zertifikaten bietet eine höhere Sicherheit und eine Verbesserung in der Usability für die AnwenderInnen, reduziert aber auch stark die Kontrolle über Neu-Anmeldungen. In der Tabelle 8.1 werden die Möglichkeiten für die Zugriffskontrolle übersichtlich dargestellt.

	Zertifikat zurückgezogen	kein Mitglied der AD-Gruppe	BenutzerInnen-Konto abgelaufen	BenutzerInnen-Konto deaktiviert
EAP-TLS	Zugriff	kein Zugriff	Zugriff	Zugriff
PEAP	-	kein Zugriff	kein Zugriff	kein Zugriff

Tabelle 8.1: Übersicht der Möglichkeiten für die Zugriffskontrolle

Bedeutet als Ergebnis, dass sobald ein Zertifikat ausgegeben wurde, gibt es keine Möglichkeit dieses auch wieder zu sperren und somit den Zugriff zu unterbinden. In Kombination mit der Tatsache, dass keine Zwischenzertifizierungsstelle unterstützt wird, bedeutet das, dass wenn ein Zertifikat von Clients oder BenutzerInnen kompromittiert wird, muss die gesamte Stammzertifizierungsstelle neu erstellt werden.

Hingegen funktioniert bei beiden Authentifizierungsmethoden, dass tatsächlich nur jene BenutzerInnen Zugriff ins Netzwerk bekommen, die auch Mitglied der AD-Gruppe „sec.pem.dot1x“ sind. Mit PEAP werden zusätzlich abgelaufene oder deaktivierte BenutzerInnen-Konten von der Verbindung mit dem Netzwerk abgelehnt, wie die Logeinträge „The referenced account is currently disabled and cannot be logged on to.“ und „The user account has expired.“ in der Logdatei „/var/log/freeradius/radius.log“ beweisen.

Die Validierung des Zertifikats vom RADIUS-Server ist eine wichtige Sicherheitsfunktion, die einfach und effektiv schützt. In der Praxis war die Definierung des Zertifikats nur unzuverlässig möglich. Die Konfiguration der Endgeräte auf Windows-Basis erfolgt über Gruppenrichtlinien, wie sie oben im Kapitel zu finden sind. Wie bereits oben beschrieben, kann die GPO für PEAP nicht ohne weiteres eingesetzt werden. Daher kann die Server-Validierung für PEAP nicht verwendet werden, für EAP-TLS hingegen schon.

Das zweite Netzwerkinterface bzw. einige Pakete wurden nicht aktiv im Praxistest benötigt, machen allerdings für eine produktive Umgebung Sinn. Da Zentyal auch Services wie DHCP, Firewall, Traffic Shaping, etc. anbietet, kann diese als zentrale Anlaufstelle für Administratoren konfiguriert werden.
Abschließend sei erwähnt, dass Zentyal für den sicheren Einsatz von EAP-TLS überarbeitet und optimiert werden muss. Funktionen wie ein CRL-Check oder die einfache Verteilung von Zertifikaten können in weiterführenden Arbeiten bearbeitet werden.

9 Evaluierung von Cloud-basierter Netzwerkauthentifizierung

9.1 Einleitung

Die Netzwerkauthentifizierung für Endgeräte und deren Vorteile wurde ausgiebig in dem Kapitel 1 „Einleitung“ und Kapitel 2 „Grundlagen“ dargelegt. Allerdings ist die Implementierung dieses Prozesses in einem Unternehmen nicht trivial und benötigt fachkundiges Personal. Daher liegt in diesem Kapitel der Fokus auf der theoretischen Ausarbeitung von möglichst einfachen und sicheren Lösungen, mit denen eine Netzwerkauthentifizierung durchgeführt bzw. die eigenen Endgeräte und MitarbeiterInnen vor Unbefugten geschützt werden können. Dieser Ansatz bedient sich vor allem den Vorteilen, die die Systeme in der Cloud besitzen. Dies bietet vor allem kleineren Firmen Vorteile wie eine bessere Kostenübersicht und eine einfachere Verwaltung. Dieser Ansatz richtet sich weniger an SystemadministratorInnen, die die Services bis ins kleinste Detail optimieren möchten und viel mehr an fortgeschrittene IT-BenutzerInnen mit geringen Anforderungen.

Aufgrund dieser „simplen“ Systeme müssen teilweise Kompromisse akzeptieren werden, und nicht alle Features wie in einer komplexen Umsetzung können angeboten werden. Es existieren von vielen Herstellern Cloud-basierte Identitätsanbieter (engl. Identity Provider, IdP) wie Microsofts „Azure AD“, Okta oder Googles „Cloud Identity“. Für dieses Kapitel wurde primär Microsoft Azure AD für die theoretische Kompatibilität mit den nachstehend beschriebenen Lösungen ausgewählt, da dieses laut Gartner einer der führenden Produkte am Markt ist [136]. In vielen Fällen werden allerdings die Lösungen von Okta oder Google ebenfalls unterstützt.

Dieser Teil der Diplomarbeit wird mit einer theoretischen Recherche umgesetzt und die Ergebnisse werden in den folgenden Absätzen vorgestellt. Abgerundet wird dieses Kapitel mit einem Fazit und einer Empfehlung.

9.2 Definierung des Schutzbedarfs

Bevor eine Lösung in Betracht gezogen werden kann, sollte im Vorhinein der gewünschte Schutzbedarf evaluiert und ausgearbeitet werden. Dabei ist wichtig festzustellen, welche Kategorien von Assets geschützt werden sollen, um eine möglichst realistische Einschätzung des Bedarfs treffen zu können. Basierend darauf, ob nur die Clients im Netzwerk, oder auch die lokal zur Verfügung gestellten Services geschützt werden sollen, ergibt sich hierdurch eine angepasste Schutzanforderung mit unterschiedlichen Lösungen, um diese auch umzusetzen. Aufgrund vieler Faktoren wie Vorwissen, Branche und zukünftige Trends ist die Entscheidung des Schutzbedarfs für jedes Unternehmen sehr individuell und verlangt eine genaue Planung. Teilweise können bestehende Lösungen in Betrieb bleiben und um weitere Ansätze ergänzt werden, erfordern aber womöglich insgesamt einen Mehraufwand und bringen unerwartete Probleme in der Praxis im Vergleich zu einer erstmaligen Umsetzung.

9.3 Lösung 1 - Isolierung der Endgeräte

Besteht das eigene Netzwerk nur aus einem einzelnen Subnetz mit wenigen Clients, die ausschließlich eine Kommunikation zu Cloud-Services und einen allgemeinen Internet-Zugang benötigen, könnte sich die Isolierung der Endgeräte anbieten. Dieser Ansatz ist besonders einfach und schnell bei Netzwerkgeräten umgesetzt, die auch diese Funktion unterstützen. Ist diese Sicherheitsmaßnahme aktiviert, können Clients im gleichen Subnetz nicht mehr untereinander kommunizieren, und sind somit vor Attacken wie MitM und Lauschangriffen geschützt. Die Konnektivität ins Internet bleibt davon unberührt, und gewährleistet eine sichere Verbindung zu Microsoft Azure und Co.

Dieses Feature wird sowohl im LAN als auch WLAN von hochpreisigen als auch kostengünstigen Herstellern wie u.a. von AVM, Meraki [137], Cisco [138] oder HP Aruba [1] angeboten. Die einzige Herausforderung besteht darin, diese Funktion in den Einstellungen des Netzwerkgerätes zu finden, da diese von Hersteller zu Hersteller unterschiedlich betitelt wird. Während dies bei einer AVM FRITZ!Box „Die unten angezeigten aktiven WLAN-Geräte dürfen untereinander kommunizieren“ benannt wird, heißt es bei einer Fortinet FortiGate „Block intra-SSID traffic“.
Abbildung 9.1 und 9.2 zeigen die Einstellungen für die Isolierung der Clients für eine AVM FRITZ!Box und eine Fortinet FortiGate (grüner Block).

[1] HP Aruba dürfte das Feature nicht auf allen Geräten unterstützen, es gibt allerdings mit „Portfilter“ [139] oder „isolate-list“ [140] Möglichkeiten um ein ähnliches Ergebnis zu erzielen.

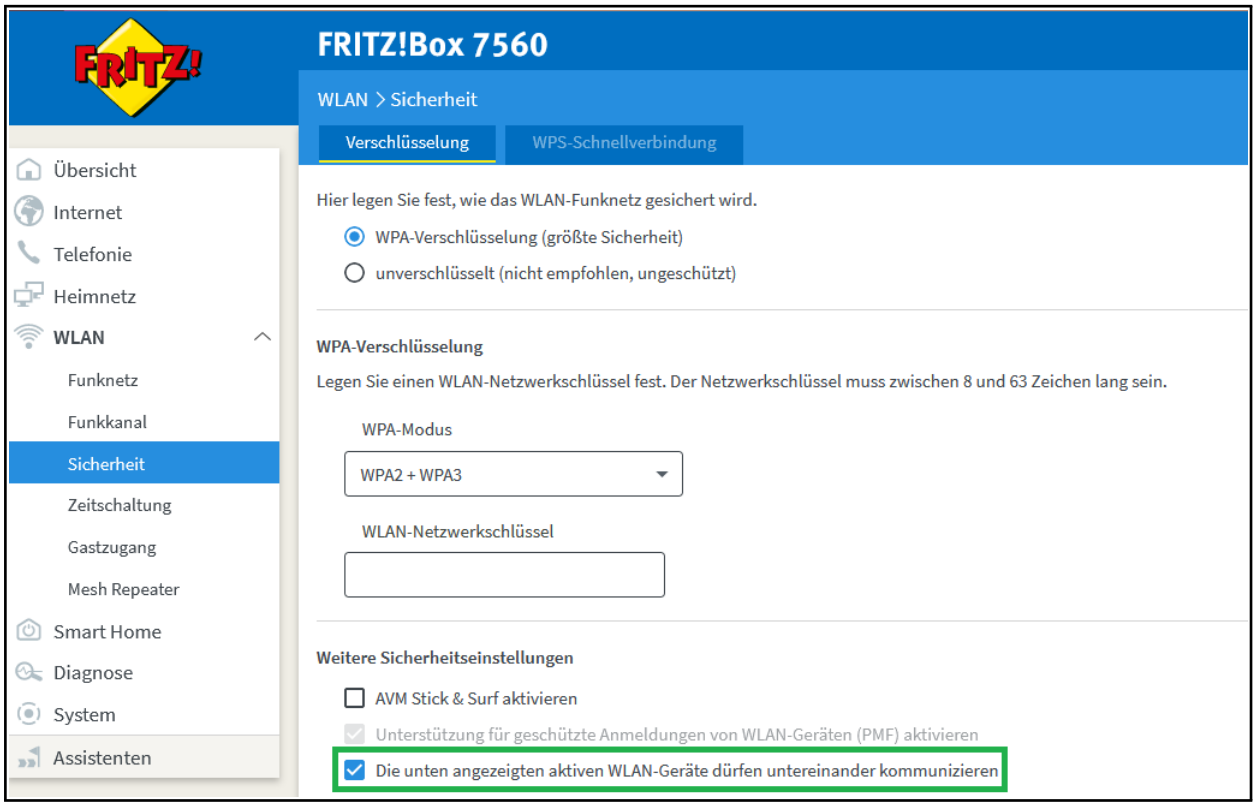


Abbildung 9.1: Client-Isolierung bei einer AVM FRITZ!Box

Bei diesem Ansatz muss allerdings beachtet werden, dass damit sämtliche Kommunikation zwischen Clients unterbunden wird, wodurch Geräte wie Drucker nicht mehr direkt angesprochen werden können. Eine Alternative für Drucker stellt das sogenannte Cloud Printing da, wodurch der Druckauftrag von Clients über das Internet bzw. Cloud zu dem jeweiligen Drucker übermittelt wird. Mit dem Google-Dienst „Google Cloud Print“ war ein sehr bekannter Service ca. zehn Jahre lang verfügbar, wird aber seit dem 1. Jänner 2021 nicht mehr unterstützt [141]. Abseits von Google bieten auch diverse Drucker-Hersteller wie Konica Minolta, Lexmark, Xerox oder HP eine Cloud Printing Plattform an [142].

Wie bereits angemerkt ist die Kommunikation zwischen Clients nicht möglich, wodurch die Angriffsfläche im Netzwerk drastisch reduziert wird. Es besteht allerdings nach wie vor das Risiko, dass die internen IPv4-Adressen (RFC 1918) der Endgeräte von MitarbeiterInnen und Angreifern auf die gleiche externe IPv4-Adresse übersetzt wird (NAT/PAT) und dadurch eine IP-Adressen-basierte Freischaltung umgangen und die Reputation der Firmen-IP-Adresse geschädigt werden kann. Mit IPv6 wird die NAT-Funktion nicht mehr benötigt, wodurch das Teilen einer externen IP-Adresse bei IPv6-Clients hinfällig wird, das Problem verschiebt sich allerdings hin zu den Subnetzen bzw. der Netz-ID.

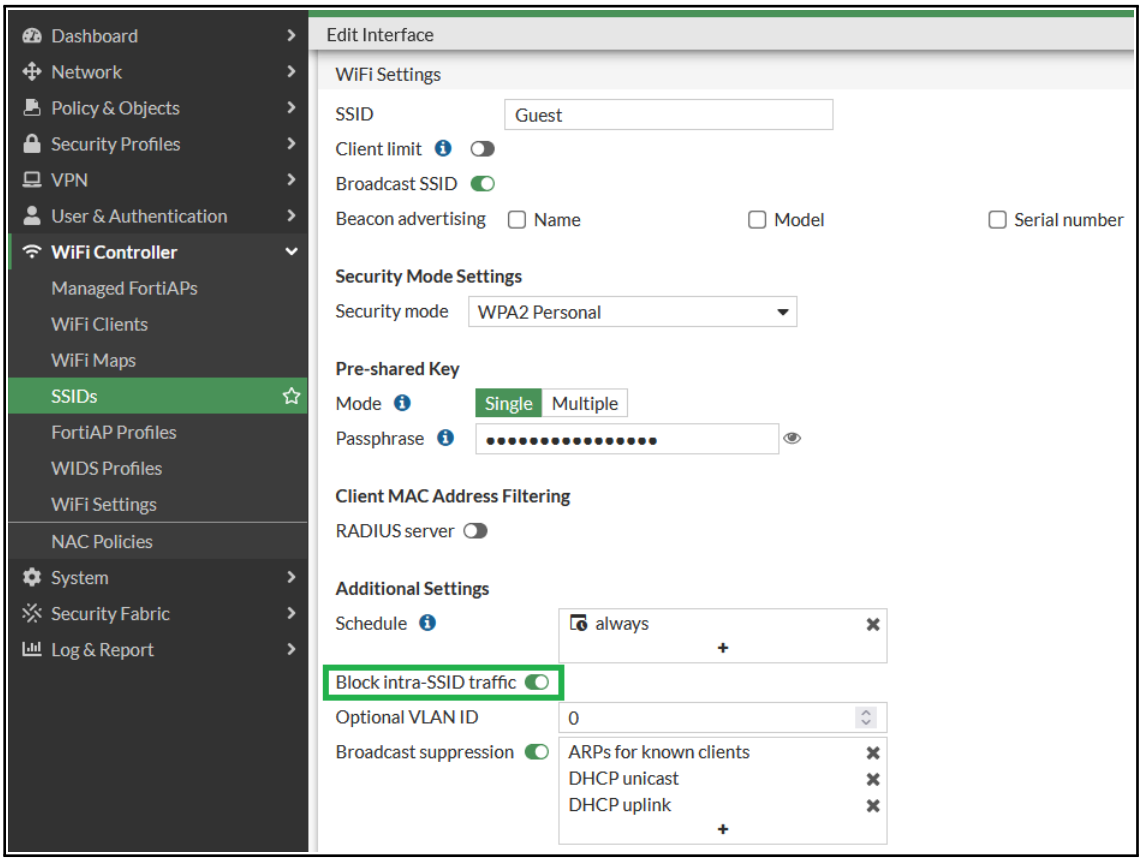


Abbildung 9.2: Client-Isolierung bei einer Fortinet FortiGate

9.4 Lösung 2 - Captive Portal

Ein weiterer Ansatz wäre die Kombinierung von einem Captive Portal zur Authentifizierung der AnwenderInnen und Opportunistic Wireless Encryption (OWE) zur Absicherung der drahtlosen Kommunikation. Mit OWE [143] besteht seit dem Jahr 2017 die Möglichkeit eine verschlüsselte drahtlose Verbindung mit einem AP, ohne einer Schlüsseleingabe einzugehen [144]. In diesem Fall wird keine Authentifizierung mit einem PSK oder 802.1X für die Verschlüsselung benötigt.

Für die Anmeldung der AnwenderInnen dient ein Captive Portal, welches sowohl lokal als auch extern betrieben werden kann. Zur Anmeldung können sowohl lokale Konten [145] dienen, die zum Beispiel am Captive Portal bzw. auf der Firewall hinterlegt sind, als auch Identitätsanbieter (IdP), die beispielsweise mittels LDAP abgefragt werden können. Die vermutlich eleganteste Lösung wäre allerdings die Einbindung von Azure AD, welche unter anderem von Fortinet [146] und Palo Alto [147] unterstützt wird. Der große Vorteil liegt daran, dass Azure AD mithilfe von Primary Refresh Token (PRT) als SSO verwendet werden

kann [148], wodurch die AnwenderInnen bei „Azure AD joined“-Geräten im Captive Portal automatisch angemeldet werden.

Wie bereits erwähnt, kann das Captive Portal auch extern in der Cloud betrieben werden. Firmen wie „Cloudi-Fi“ [149] oder „IronWiFi“ [150] bieten externe Captive Portals an, die im Hintergrund diverse Identitätsanbieter wie Azure AD, Google oder allgemein SAML ansprechen können [151][152]. IronWiFi liefert darüber hinaus eine Liste mit unterstützten Herstellern [153], bei denen die Funktionalität mit dem externen Captive Portal bestätigt wird, und Schritt-für-Schritt-Anleitungen, um diese einzubinden.

Da die Clients ohne Authentifizierung bei einem Captive Portal für gewöhnlich keine generelle Internet-Freischaltung besitzen, müssen spezifische Domains für die Identitätsanbieter erlaubt werden (Walled Garden). Für Azure AD liefert Cloudi-Fi eine Liste von Domänen, die für die Clients auch im unauthentifizierten Zustand erreichbar sein müssen [154].
Mithilfe von Single Sign-on (SSO) und der Modifizierung der Dauer (Lifetime) einer authentifizierten Sitzung kann die Usability verbessert werden, da der Aufwand bzw. die Anzahl der Anmeldungen für die AnwenderInnen verringert wird [155].

9.5 Lösung 3 - Zscaler

Zscaler bietet mit dem „Zscaler Internet Access“ [156] und „Zscaler Private Access“ [157] eine Technologie an, bei dem die Kommunikation zwischen Endgeräten und den Services über einen Tunnel stattfindet und der Zugriff mit dem Zero-Trust-Modell gesteuert wird. Die Services umfassen sowohl externe Dienste wie der Internetzugriff oder Saas-Anbieter wie „Microsoft 365“ oder „Salesforce“, als auch interne Anwendungen in der Private Cloud oder On-Premises. Die gewünschten Anwendungen sind nur für jene AnwenderInnen sichtbar, die auch hierfür die Berechtigungen für den Zugriff besitzen und sind daher auch nicht den öffentlichen Angriffen exponiert.

Für gewöhnlich wird der Netzwerkverkehr vom Endgerät in die Cloud zu Zscaler getunnelt, wo dieser analysiert und mit diversen Sicherheitsmechanismen wie URL Filtering, SSL Inspection, etc. überprüft wird, um anschließend die Kommunikation basierend auf Richtlinien weiterzuleiten oder zu unterbinden. Eine Liste aller Sicherheitsfunktionen bietet Zscaler auf deren Webseite an. Das Backbone nennt Zscaler „Zero Trust Exchange“ und entscheidet basierend auf zuvor festgelegten Richtlinien, welche AnwenderInnen auf welche Dienste zugreifen dürfen. Mithilfe des Zero-Trust-Modells können hierbei die Berechtigungen sehr feingranular für einzelne MitarbeiterInnen konfiguriert werden, und somit das Least-Privilege-Prinzip umgesetzt werden.
In Abbildung 9.3 wird das Konzept von Zscaler dargestellt [156].

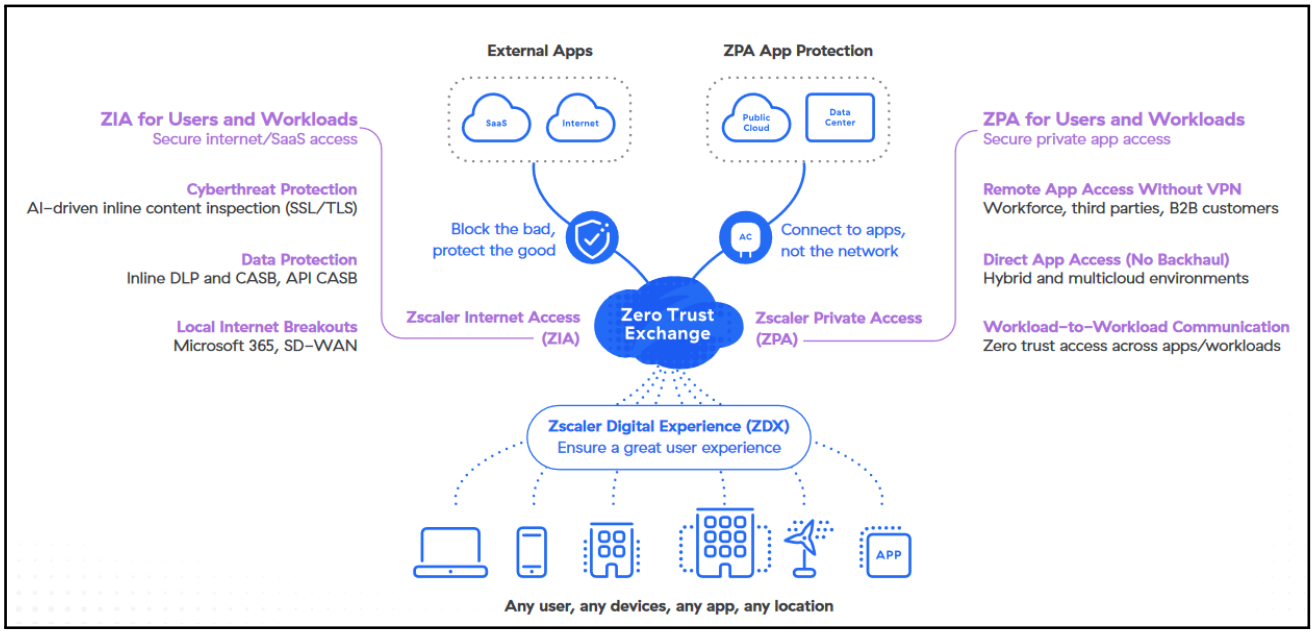


Abbildung 9.3: The Zero Trust Exchange [156]

9.5.1 Komponenten

Die Technologie von Zscaler baut auf vier wesentliche Komponenten auf:

Zscaler Client Connector

Der „Zscaler Client Connector“ ist ein Programm, welches auf den Endgeräten installiert wird und das den Netzwerkverkehr der AnwenderInnen zu dem nächstgelegenen Zscaler Service Edge weiterleitet. Dies betrifft sowohl den Zugriff auf öffentliche Ressourcen wie das Internet, als auch private Anwendungen, die über das „Zero Trust Exchange“ zur Verfügung gestellt werden. Zusätzlich besteht die Möglichkeit, dass ein Teil des Datenverkehrs (z.B. Zugriff auf bestimmte Domänen IdP-URLs) den Tunnel umgeht und direkt auf die herkömmliche Art ins Internet geleitet wird (Split Tunnel). Mit „iOS 9 oder höher“, „Android 5 oder höher“, „Windows 7 oder höher“, „Mac OSX 10.10 oder höher“, „CentOS 8“ und „Ubuntu 20.04“ wird eine breite Palette an Systemen unterstützt [158]. Die Integrierung von Zscaler erfolgt beispielsweise beim Betriebssystem Windows über die Installation eines dedizierten virtuellen Netzwerkadapters, über den die Kommunikation zu Zscaler erfolgt [159].

Zscaler Agentless Access

Für die Fälle, bei denen die Installation eines Programms auf den Endgeräten nicht möglich ist, beispielsweise weil diese in die Kategorie „BYOD“ fällt, bietet Zscaler mit einem webbasierten Ansatz auch eine Alternative an, in der der Zugriff via Web, RDP und SSH möglich ist.
Zudem wird mit „Browser Isolation“ [160] eine noch restriktivere Möglichkeit angeboten, in welcher der Zugriff zu den Anwendungen in einer isolierten Umgebung virtuell stattfindet, und ausschließlich der Bildstream an die AnwenderInnen übertragen wird. Hierdurch werden die MitarbeiterInnen daran gehindert, die darin enthaltenen sensiblen Daten herunterzuladen, zu kopieren, einzufügen oder zu drucken.

ZPA App Connector

Der „ZPA App Connector“ ist wie der Client Connector eine Anwendung, die die eigenen Dienste im On-Premises Rechenzentrum oder in der Cloud für Zscaler erreichbar macht. Die Anwendung baut hierfür eine Verbindung vom internen Netzwerk nach außen zu Zscaler auf, wodurch die Services nicht öffentlich exponiert sind [157].

ZPA Service Edges

Der „ZPA Service Edge“ nimmt die Verbindung vom Client Connector und dem App Connector entgegen, und verknüpft diese, sollten die Richtlinien die Kommunikation zulassen. Hierdurch wird die Anfrage einer autorisierten AnwenderIn zu der gewünschten Applikation weitergeleitet. Neben dem Zugriff auf interne Anwendungen wird auch der Internetverkehr über diese Server geleitet und entsprechend Sicherheitsrichtlinien überprüft.

Für gewöhnlich stellt Zscaler die Service Edges an 150 Standorten auf der ganzen Welt zur Verfügung, sie können allerdings auch On-Premises betrieben werden. Der Vorteil ist, dass die Latenzen minimiert werden können und der Netzwerkverkehr so nicht den eigenen Perimeter verlassen muss. Diese Server werden auch vom Hersteller verwaltet, wodurch Mitarbeiterressourcen geschont werden [157].

9.6 Lösung 4 - Cloud-RADIUS - All-in-one-Lösung

Die bisher beschriebenen Lösungen versuchen Alternativen zu der Netzwerkauthentifizierung mit RADIUS-Server und Authenticator zu identifizieren. Der Hersteller „SecureW2“ bietet mit seinen Produkten die Möglichkeit einer Cloud-basierten Netzwerkauthentifizierung nach dem 802.1X-Schema an, wobei Authentication Server und Identity-Provider nicht On-Premises betrieben werden.

Zu den Produkten gehört ein RADIUS-Server und eine Zertifizierungsstelle (CA), welche in der Cloud von SecureW2 zur Verfügung gestellt werden. Zusätzlich werden Schnittstellen zu vielen Herstellern wie Microsoft, Okta oder Google als Identity-Provider angeboten, um so den Aufwand für die Verwaltung der BenutzerInnen-Konten der eigenen MitarbeiterInnen möglichst gering zu halten. Die Konfiguration der Endgeräte kann wahlweise über ein Mobile Device Management (MDM) [161] oder mittels der Onboarding Software von SecureW2 „JoinNow MultiOS“ [55] durchgeführt werden. Neben der Konfiguration kann mit der Anwendung auch ein Zertifikat bezogen werden [162], welche für die Authentifizierung via EAP-TLS Voraussetzung ist. Die Anmeldung in der Onboarding Software kann mit SSO und Azure AD umgesetzt werden, dass den Onboarding Prozess beschleunigt und weniger fehleranfällig realisiert werden kann [163]. In Abbildung 9.4 wird die Integration der zahlreichen Hersteller übersichtlich dargestellt [164].

Bei dieser Methode der Netzwerkauthentifizierung wird im Hintergrund weiterhin das Protokoll RADIUS gesprochen, obwohl der tatsächliche RADIUS-Server virtualisiert in der Cloud betrieben wird. Das bedeutet aber auch, dass die eingesetzten Verschlüsselungsalgorithmen bei RADIUS nach wie vor veraltet sind und eine Übertragung über einen unsicheren Kommunikationskanal wie dem Internet schwerwiegende Folgen haben kann. Um dieses Problem entgegenzutreten, gibt es bereits mit dem RFC 6614 [43] bzw. RadSec und RFC 7360 [44] Lösungen, die von beiden Seiten am Authenticator und dem Authentication Server unterstützt werden muss. SecureW2 unterstützt bei dem Cloud-basierten RADIUS-Server mit RadSec eine Möglichkeit, um die Datenübertragung abzusichern [46].

In Abbildung 9.5 wird der Ablauf einer Authentifizierung von einem Endgerät dargestellt [165]. Im ersten Schritt übermittelt der Client sein Zertifikat, welches zuvor über MDM oder über die Onboarding Software installiert wurde. In Schritt 2 nimmt SecureW2 die Infos aus dem Zertifikat wie die ID oder Name des Endgerätes bzw. der MitarbeiterIn und prüft beim Identity-Provider, ob die Berechtigung vorhanden ist und der Zugriff gewährt werden darf. Schritt 3 liefert die Antwort auf Schritt 2 zurück an SecureW2. Mit Schritt

Abbildung 9.4: SecureW2 Integration [164]

4 wird die Anmeldung beendet, und der Client erhält bzw. erhält keinen Zugriff auf das Netzwerk.

Zusätzlich wird bei jeder Anmeldung überprüft, ob das Objekt des Clients bzw. der MitarbeiterInnen noch aktiviert ist.

Die Firma SecureW2 beschreibt ihren RADIUS-Server als eine neue Generation von AAA-Servern und bezeichnet diesen als „Dynamic (Cloud) RADIUS“. Der Dynamic RADIUS baut auf den Funktionen eines RADIUS-Server auf, und erweitert den Funktionsumfang um dynamische Überprüfungen während der Laufzeit. So soll bei jeder Anmeldung eines Clients bzw. einer AnwenderIn neben der Überprüfung des Zertifikats zusätzlich deren Konto auf Gültigkeit abgefragt werden. Grundsätzlich sollte bei dem Austritt von MitarbeiterInnen oder bei Verlust das BenutzerInnen-Konto und/oder die Zertifikate gesperrt werden. Die

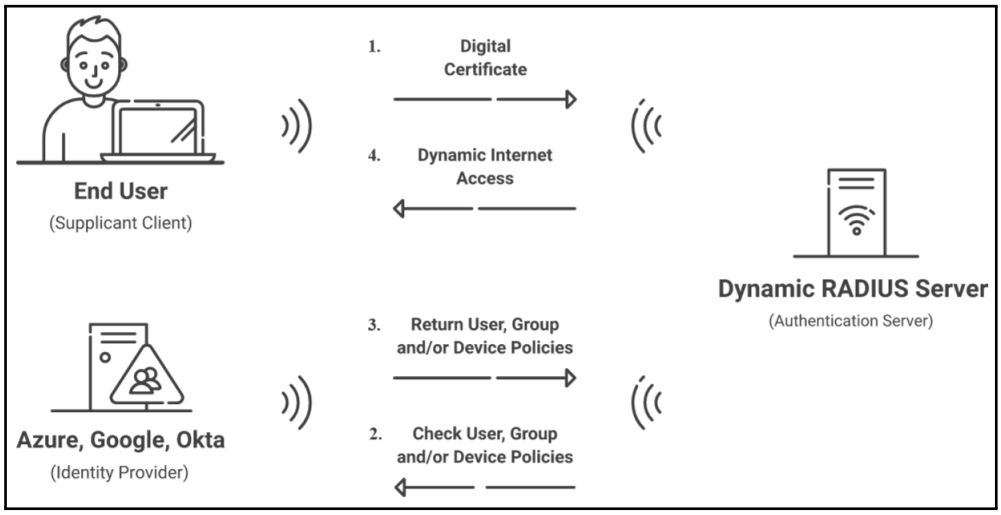


Abbildung 9.5: Authentication Flow bei SecureW2 Cloud RADIUS-Server [165]

CRL sollte anschließend um das gesperrte Zertifikat ergänzt worden sein. Es kann aber aufgrund menschlichen Versagens bzw. zeitlicher Überschneidungen zu Situationen kommen, wo der Zugriff, gänzlich oder zeitlich begrenzt, weiterhin bestehen bleibt. So kann ein zu hohes Aktualisierungsintervall der CRL oder mehrere Zertifikate pro MitarbeiterIn, von denen beim Austritt alle widerrufen werden müssen, zu Risiken im Betrieb führen. Dieses Risiko kann mit den Vorteilen eines „Dynamic (Cloud) RADIUS“ stark reduziert und schneller reagiert werden.

Das CA/Browser Forum (CA/B Forum) empfiehlt (Stichwort „shall“) in „Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates“ die Aktualisierung der CRL einer Zertifizierungsstelle zumindest alle 7 Tage, bei Zwischenzertifizierungsstelle (Intermediate CA) innerhalb von 24 Stunden nachdem ein Zertifikat widerrufen wurde [166]. Eine weitere Funktion ist die dynamische Überprüfung der Berechtigungen für die jeweiligen MitarbeiterInnen, wodurch eine entfernte Berechtigung über ein gesperrtes BenutzerInnen-Konto schneller als mit einer CRL überprüft werden kann [167].

Neben der Vielfalt an Produkten und Lösungen bietet SecureW2 einige Anleitungen an, mit denen die eigene Hardware für den Einsatz vorbereitet und eine Migration so möglichst einfach umgesetzt werden kann. So gibt es auf der Webseite von SecureW2 Guides für die Integration von EAP-TLS mit ihren Cloud-Lösungen für diverse (Hardware-)Hersteller wie Cisco [168], Meraki [169], Aruba [170], Ubiquiti [56] oder Microsoft [171].

9.7 Lösung 5 - Cloud-RADIUS mit Diversität

Während in der vorhergehenden Lösung sämtliche Services online von SecureW2 betrieben werden, soll mit diesem Ansatz der Fokus auf die Diversität und der Vermeidung eines Vendor Lock-ins thematisiert werden. So können verschiedene Anbieter aus den unterschiedlichen Kategorien eingesetzt werden und bleibt dabei möglichst flexibel. Mit der Flexibilität gehen allerdings auch Einschränkungen wie die Reduzierung von Funktionsumfang und eine erhöhte Komplexität bei der Wartung einher. Mit dieser Lösung ist auch möglich, gewisse Services wie ein Zertifizierungsstelle (CA) lokal im Unternehmen zu betreiben und nur Teile der Netzwerkauthentifizierung in die Cloud auszulagern. Welche Funktionen tatsächlich in der Praxis eingesetzt werden können, sind von der genauen Zusammensetzung der eingesetzten Produkte abhängig und kann pauschal nicht beantwortet werden. So können Inkompatibilitäten und Einschränkungen zwischen Cloud-Providern bzw. zwischen Cloud-Provider und Hardware On-Premises bestehen.

Die Konfiguration und die Installation von Zertifikaten auf den Endgeräten wird mit einem MDM stark empfohlen. Es gibt teilweise Möglichkeiten, dies auch manuell durchzuführen, skaliert allerdings selbst bei einer geringen Anzahl an Clients schlecht und unterscheidet sich zwischen den unterschiedlichen Betriebssystemen stark. Mit Simple Certificate Enrollment Protocol (SCEP), Enrollment over Secure Transport (EST) und Automatic Certificate Management Environment (ACME) existieren offene Protokolle für die Beziehung von X.509-Zertifikaten, welche gänzlich oder teilweise von den populärsten Betriebssystemen unterstützt werden. Der Cloud-Anbieter SecureW2 liefert eine Übersicht, wie diese Konfigurationen auf den Endgeräten manuell umgesetzt werden kann [172]. Um eine skalierbare und weniger fehleranfällige Lösung zu bauen, kann Microsofts Intune für die Verteilung der Konfiguration inklusive der Installation von X.509-Zertifikaten via SCEP eingesetzt werden [173]. Ein Video vom Youtube-Kanal „Intune Training“ zeigt diesen Prozess in einem praktischen Beispiel [174].

Es gibt einige Anbieter von Cloud-RADIUS-Server wie Jumpcloud [175] oder Portnox [176], die durch eine kurze Internetrecherche schnell gefunden werden. Hier sollte aber darauf geachtet werden, dass die Verbindung zwischen Authenticator und Authentication Server verschlüsselt, und somit mit RadSec abgesichert ist. Teilweise bieten Anbieter wie Jumpcloud auch Möglichkeiten zum Testen ihrer Produkte an, wodurch der praxisnahe Einsatz in der eigenen Umgebung ausgiebig getestet werden kann.

9.8 Fazit

Bevor eine Lösung in ein Unternehmen integriert werden kann, sollte im Vorhinein der Schutzbedarf definiert werden. Basierend auf den eigenen Anforderungen kann die Isolierung von Endgeräten den eigenen Sicherheitsbedürfnissen genügen. Dies ist eine schnell umgesetzte Lösung, wenn die vorhandene Hardware diese Funktion bereits unterstützt. Am Markt existieren viele Service-Anbieter für „Cloud Radius“ oder „RADIUS-as-a-Service“, die auch mit einer Vielfalt an Funktionen punkten wollen. Vor der Implementierung ins Unternehmen wird ein Testaufbau sehr empfohlen, um auch die Versprechen der Hersteller in der Praxis überprüfen zu können.

Sollte die Wahl auf einen Cloud-RADIUS-Server fallen, so bietet die ineinander abgestimmten Lösungen von Securew2 eine gute Basis. Mit der Palette an Funktionen, die Dynamic-RADIUS-Server bereitstellt, existieren unter Umständen zusätzliche Kontrollmöglichkeiten, die es bei anderen Anbietern so nicht gibt.

Teilweise werden Sorgen zum Aufsetzen eines Cloud-RADIUS-Servers stark reduziert, indem an vielen Stellen virtuelle Assistenten und Checklisten eingebaut wurden, und somit den AnwenderInnen unter die Arme gegriffen werden kann. Beispielsweise wird an einer Stelle des Konfigurationsprozesses der Administrator gefragt, mit welcher Quell-IP die RADIUS-Pakete zu erwarten sind. Hier wird die Möglichkeit „Are you currently located where you want RADIUS¿‘ angeboten, die die IP-Adresse des Büros übernimmt, wenn man sich zum Zeitpunkt der Konfiguration dort aufhält.

In Abbildung 9.6 zeigt der Anbieter Jumpcloud, wie man den Administrator bei der Konfiguration unterstützen kann. Im ersten Schritt wird abgefragt, für welchen Service Interesse besteht, um im zweiten Schritt passende Checklisten zu erstellen und den aktuellen Stand des Prozesses übersichtlich darzustellen.

Die Netzwerkkontrolle mit einem Captive Portal in Verbindung mit der Authentifizierung über Azure AD könnte vor allem bei Endgeräten, die mit Microsofts Cloud-Lösung verwaltet werden, in Situationen mit geringen Anforderungen eine bequeme Alternative zu 802.1X sein.
Mit Zscaler existiert eine Lösung, die sich im Vergleich mit einem AAA-Konzept grundlegend unterscheidet. Während bei letzterem die Authentifizierung und Autorisierung vor Ort erfolgt, führt dies Zscaler in einer seiner vielen Rechenzentren durch. Da hier auf dem Zero-Trust-Modell aufgebaut wird, können somit die Zugriffe auf interne und externe Ressourcen viel genauer gesteuert werden.

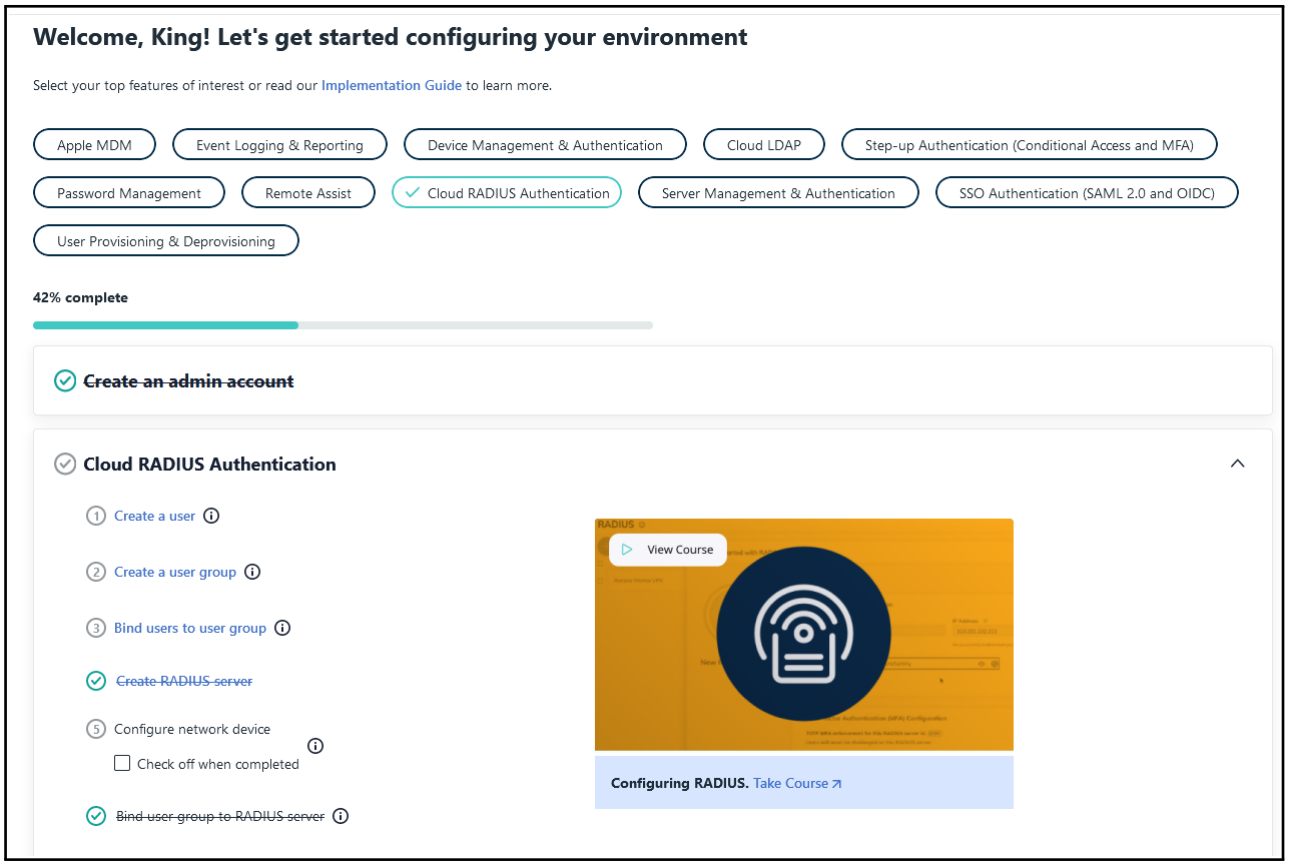


Abbildung 9.6: Checklisten beim Anbieter Jumpcloud

10 Vergleich der Ansätze

Jeder der drei Ansätze hatte als Basis eine andere Zielgruppe, dennoch sollen diese nun miteinander verglichen und die Vor- und Nachteile hervorgehoben werden, um eine Entscheidungsgrundlage für die LeserIn anbieten zu können. Zusätzlich soll erwähnt sein, dass die Ergebnisse für den Cloud-basierten Ansatz auf einer theoretischen Ausarbeitung aufbauen und keine Einschätzung für einen Einsatz in der Praxis getroffen werden kann.

Wird die Funktionsvielfalt der Netzwerkauthentifizierung zwischen den Ansätzen verglichen, zeigt sich, dass die NAC-Lösung klar gewinnt. Mit einem System können sowohl interne als auch externe Clients über unterschiedliche Methoden authentifiziert werden. PacketFence bietet an vielen Stellen Möglichkeiten der spezifischen Anpassungen, wodurch eigenen Wünsche und Anforderungen umgesetzt werden können. Im Cloud-Ansatz werden Produkte vorgestellt, die alle einen spezifischen Fokus haben – teilweise können mehrere Produkte kombiniert werden. Mit der eingebauten Monitoring-Funktionen werden viele Informationen gesammelt und übersichtlich dargestellt. Der All-in-one-Ansatz mit Zentyal bietet hingegen nur die Authentifizierung mittels 802.1X an, die wiederum selbst wenig Anpassungsmöglichkeiten (nur PEAP) unterstützt. Es ist möglich, dass Zertifikate ausgestellt und für die Authentifizierung (EAP-TLS) verwendet werden – hierdurch entstehen allerdings weitere Einschränkungen, die nicht endgültig geklärt werden konnten.

Der NAC- und Cloud-Ansatz lassen sich großteils in bestehende Prozesse integrieren und an vielen Stellen automatisieren. Zscaler stellt bei der Integrierung eine Ausnahme dar, da hier ein neuer Ansatz im Zugriffsschutz verfolgt wird. Bei Zentyal ist an vielen Stellen manuelles eingreifen erforderlich, wie die Ausstellung und Verteilung von x.509-Zertifikaten sowie der Konfiguration von Clients. Während der All-in-one-Ansatz ein aufeinander abgestimmtes und abgeschottetes System ist, bieten die anderen Ansätze die Einbindung von Partner-Produkte an.

PacketFence hat eine lange Liste an unterstützten Funktionen und Herstellern, und bietet viele Anpassungsmöglichkeiten, wodurch die Administration und Verwaltung komplex sein kann und erfahrene bzw. ausgebildete MitarbeiterInnen erfordert. Zentyal wird primär über eine Weboberfläche komfortabel verwaltet, allerdings müssen Funktionen wie EAP-TLS aufwendig mithilfe der Kommandozeile konfiguriert werden. Diverse Anbieter von Cloud-Produkten unterstützen bei der Einrichtung und im Betrieb mit Guides und Checklisten, wobei die Einbindung von Cloud und On-Premises-Hardware möglicherweise nicht trivial ist.

Der Einsatz einer Cloud-Lösung erfordert eine stabile Internetverbindung, um die Authentifizierungsanfragen zu dem jeweiligen Provider übertragen zu können. Ist die Verbindung zum Cloud-Anbieter unterbrochen, können keine neuen Anmeldungen durchgeführt werden – diese Tatsache muss unbedingt in der Business Continuity Disaster Recovery (BCDR) berücksichtigt werden. PacketFence und Zentyal benötigen im Betrieb nicht zwangsläufig eine Internetverbindung, wobei es beim NAC von der Konfiguration und der benötigten Funktionen abhängt. Während PacketFence und die Cloud-Ansätze einen detaillierten Einblick zu den Anmeldungen und den verbundenen Clients geben können, kann Zentyal nur erfolgreiche und fehlgeschlagene Authentifizierungsversuche ohne Details darstellen.

Fazit

Der Ansatz mit den meisten Funktionen und Anpassungsmöglichkeiten ist eindeutig PacketFence, wobei die Komplexität in der Verwaltung nicht unterschätzt werden sollte. Die Cloud-Produkte bieten flexible Möglichkeiten der Netzwerkauthentifizierung, erfordern allerdings eine stabile Internetverbindung. Mit Zentyal konnte im Proof-of-Concept die Verwaltung der Clients und die Anmeldung im Netzwerk erfolgreich getestet werden, sollte allerdings nicht in der Praxis aufgrund der Sicherheitseinschränkungen, wie fehlender CRL-Check und der ungewissen EAP-TLS-Nachrüstung, eingesetzt werden. In Tabelle 10.1 werden die Einschätzungen der Ansätze übersichtlich dargestellt.

	Open Source NAC	All-in-one-Ansatz	Cloud-Ansatz
Netzwerkauthentifizierung	+	-/∼	+
Automatisierung	+	-/∼	+/∼
Integrierung	+	-	+
Komplexität	-/∼	-	+/∼
Konnektivität	+	+	-
Reporting & Monitoring	+/∼	-/∼	+/∼

Tabelle 10.1: Vergleich der Ansätze

11 Conclusio

Ziel dieser Arbeit war die Evaluierung von Lösungen zur Netzwerkauthentifizierung mit Fokus auf KMUs. Hierzu wurden drei unterschiedliche Ansätze ausgearbeitet und anschließend untersucht, ob hierfür passende Lösungen am Markt zu finden sind. Zwei der Ansätze wurden zusätzlich in einem Proof-of-Concept näher beleuchtet, um die Erfahrungen von praktischen Tests für die Beantwortung der Forschungsfragen mit einfließen lassen zu können.

Wie in Kapitel 5 „Evaluierung von Open Source NAC-Produkten“ beschrieben, existieren nicht viele kostenlose NAC-Lösungen im Vergleich zu den zahlreichen kommerziellen Produkten von Cisco, Aruba, ForeScout und Co. Einzig mit PacketFence ist ein NAC-Produkt verfügbar, welches Open Source ist und ähnliche Funktionen wie die Marktführer unterstützt. Kapitel 6 „Proof-of-Concept - Open Source NAC“ zeigt, dass PacketFence die Netzwerkauthentifizierung mittels 802.1X und Captive Portal sehr umfangreich und mit vielen Anpassungsmöglichkeiten unterstützt. Darüber hinaus werden Methoden angeboten, die die Einbindung von Legacy-Netzwerkgeräten ermöglicht. Die Dokumentation des Herstellers ist die einzig verlässliche Informationsquelle, diese ist allerdings teilweise veraltet und enthält Fehler. Zusätzlich werden Themen wie die Überprüfung von Richtlinien (Endpoint Compliance) in der Dokumentation stark vernachlässigt, wodurch diese Funktion im Proof-of-Concept nicht getestet werden konnte.

Wie die Recherche in Kapitel 7 „Evaluierung von On-Premises-Verzeichnisdiensten in Form eines All-in-one-Ansatzes“ zeigt, existiert mit Samba 4 eine Alternative zum De-facto-Standard Active Directory von Microsoft. Mit Zentyal wurde nur ein Produkt gefunden, welches die Funktion von AD, CA und RADIUS-Server in einem System vereint und somit für einen Proof-of-Concept interessant ist. Mit dem Experiment in Kapitel 8 „Proof-of-Concept - All-in-one-Ansatz“ konnte gezeigt werden, dass Zentyal viele Funktionen anbietet, und diese komfortabel über die Weboberfläche verwaltet werden können. Im Test hat sich allerdings gezeigt, dass viele Einschränkungen bestehen, wodurch der produktive Einsatz nicht zu empfehlen ist. So kann ohne Modifizierung von Zentyal über die Kommandozeile nur eine Anmeldung im Netzwerk

mithilfe von BenutzerInnen-Name und Passwort erreicht werden. Darüber hinaus kann keine Autorisierung vorgenommen und die ausgestellten x.509-Zertifikate können beispielsweise bei einer Kompromittierung nicht zurückgezogen werden.

In Kapitel 9 „Evaluierung von Cloud-basierter Netzwerkauthentifizierung“ konnten Cloud-basierte Lösungen zur Netzwerkanmeldung vorgestellt werden, die nicht von einem On-Premises Identity-Provider abhängig sind. Stattdessen können Cloud-basierte Identitätsanbieter wie Microsoft „Azure AD“, Okta oder Googles „Cloud Identity“ für die Authentifizierung eingebunden werden. Die vorgestellten Methoden reichen von einem RADIUS-Server in der Cloud, über ein Captive Portal mit Einbindung von Cloud-Identity-Provider bis hin zu Zscaler, der mit dem Zero-Trust-Modell eine andere Philosophie verfolgt.

11.1 Weiterführende Arbeiten

Zentyal bietet bereits eine gute Plattform für KMUs, um ihre Endgeräte mit AD zu verwalten. Allerdings ist die Implementierung der CA und des RADIUS-Servers aus Sicht der IT-Security mangelhaft. In Abschnitt 8.5 „Netzwerkauthentifizierung“ konnte bereits demonstriert werden, dass die Netzwerkauthentifizierung mit EAP-TLS nachträglich implementiert werden konnte. Allgemein bietet Zentyal Potential für Verbesserungen, um in weiterer Folge in einer produktiven Umgebung eingesetzt werden zu können. In einem Langzeittest sollte zusätzlich überprüft werden, welche Anpassungen von Zentyal persistent sind und nach Updates bzw. Upgrades bestehen bleiben.

Hersteller eines NAS wie Synology oder QNAP bieten bereits eine Suite an Tools für die Zusammenarbeit im Team und der Verwaltung von IT-Assets an, die womöglich den Anforderungen vieler KMUs genügen. In einer weiterführenden Arbeit könnte beleuchtet werden, welche Anforderungen gedeckt werden können, und welche Wünsche von anderen Produkten erfüllt werden müssen.

Abbildungsverzeichnis

Tabellenverzeichnis

Glossar

2FA	Zwei-Faktor-Authentisierung
AAA	Authentication Authorization Accounting
ACL	Access Control List
ACME	Automatic Certificate Management Environment
AD	Active Directory
AD DC	Active Directory Domain Controller
AD DS	Active Directory Domain Services
AP	Access Point
API	Application Programming Interface
Authentifizierung	Ein System überprüft die von NutzerInnen vorgelegten Daten zur Authentisierung auf ihre Gültigkeit und authentifiziert diese [177].
Authentisierung	BenutzerInnen authentisieren sich an einem System mittels eindeutiger Anmeldeinformationen wie einem Passwort oder Chipkarte [177].
AV	AntiVirus
BSI	Bundesamt für Sicherheit in der Informationstechnik
BYOD	Bring your own device
CA	Certificate Authority
Captive Portal	Ein Captive Portal ist eine Webseite, auf die automatisch umgeleitet wird, wenn sich ein neuer WLAN-Gast an einem öffentlichen WLAN oder WLAN-Hotspot angemeldet hat. Über das Captive Portal werden die Gäste typischerweise auf Anwendungsebene authentifiziert. Zum Beispiel um die Nutzung zu begrenzen, abzurechnen oder zu protokollieren [144].
CESG	Communications Electronics Security Group

CLI	Command Line Interface
Cloud	Der Begriff Cloud beschreibt im IT-Umfeld die Bereitstellung von Speicherplatz, Rechenleistung und ausführbare Software in einer räumlich entfernten IT-Infrastruktur. Der englische Begriff trägt der Tatsache Rechnung, dass der dafür genutzte Server für die Nutzer nicht direkt sichtbar, sondern wie hinter einer Wolke verborgen ist [178].
CRL	Eine Zertifikatssperrliste oder Certificate Revocation List (CRL) beinhaltet eine Liste an ungültigen Zertifikaten, die u.a. aufgrund Sperrung oder Widerruf ihre Gültigkeit verlieren.
CSR	Certificate Signing Request
CSV	Comma-separated values
Dashboard	In der IT handelt es sich bei Dashboards um grafische Benutzeroberflächen, also eine Anordnung verschiedener grafischer Elemente, die der Visualisierung von Daten oder der Verwaltung von Systemen dienen [179].
DC	Domain Controller
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DSGVO	Datenschutz-Grundverordnung
DTLS	Datagram Transport Layer Security (DTLS) basiert auf dem Protokoll TLS, mit dem Unterschied, dass hier das Transportprotokoll UDP für die Übertragung verwendet wird [180].
EAP	Extensible Authentication Protocol
EAPOL	Extensible Authentication Protocol over LAN
ECC	Elliptic Curve Cryptography

EOL	End of Life
EST	Enrollment over Secure Transport
GPO	Group Policy Object
GUI	Graphical User Interface
HA	High Availability
HP	Hewlett Packard
HPE	Hewlett Packard Enterprise
IaaS	Infrastructure-as-a-Service
IANA	Internet Assigned Numbers Authority
Identity-Provider	Ein Identitätsanbieter oder Identity-Provider (IdP oder IDP) speichert und verwaltet die digitalen Identitäten von BenutzerInnen. Sie können sich einen IdP wie eine Gästeliste vorstellen, jedoch nicht für Veranstaltungen, sondern für digitale und Cloud-gehostete Anwendungen. Ein IdP kann Benutzeridentitäten beispielsweise anhand von Kombinationen aus BenutzerInnen-Namen und Passwort verifizieren. [181].
IEEE	Institute of Electrical and Electronic Engineering
IoT	Internet of Things
IP	Internet Protocol
IRC	Internet Relay Chat
ISE	Identity Services Engine
ISMS	Information Security Management System
ISO	International Organization for Standardization
IT	Information Technology
KMU	kleine und mittlere Unternehmen

LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
MAB	MAC Authentication Bypass
MD5	Message Digest 5
MDM	Ein Mobile Device Management (MDM) übernimmt die zentrale Verwaltung der Endgeräte von MitarbeiterInnen, um beispielsweise Sicherheitsrichtlinien vorzugeben, allg. Einstellungen zu definieren, oder diese aus der Ferne zu sperren bzw. zu löschen.
MITM	Machine-in-the-Middle
NAC	Network Access Control
NAP	Network Access Protection
NAS	Network Attached Storage
NAT	Network Address Translation
NIST	National Institute of Standards and Technology
NPS	Network Policy Server
OCSP	Online Certificate Status Protocol
OSI-Modell	Das OSI-Modell (Open Systems Interconnection Model) ist ein konzeptionelles Framework, das zur Beschreibung der Funktionen eines Netzwerksystems dient. Das OSI-Modell beschreibt Datenverarbeitungsfunktionen in Form eines universellen Satzes von Regeln und Anforderungen, um Interoperabilität zwischen verschiedenen Produkten und Software zu unterstützen. Im OSI-Referenzmodell wird die Kommunikation innerhalb eines Datenverarbeitungssystems in sieben Abstraktionsschichten unterteilt: Bitübertragung, Sicherung, Vermittlung, Transport, Sitzung, Darstellung und Anwendung [182].

OT	Operational Technology
OTP	One-Time Password
OU	Organizational Unit
OWE	Opportunistic Wireless Encryption
PaaS	Platform-as-a-Service
PAT	Port Address Translation
Pay as you go	Der Begriff „Pay as you go“ beschreibt ein Bezahlsystem für Cloud Computing, wo nur die tatsächliche Nutzung bezahlt wird. So werden keine Kosten und Ressourcen verschwendet im Gegensatz zu Bezahlmethoden, wo ein Kontingent bezahlt wird [183].
PKI	Public Key Infrastructure
PM	Passwort-Manager
PoC	Proof of Concept
PRT	Primary Refresh Token
RADIUS	Remote Authentication Dial-in User Service
RFC	Request for Comments
RID	Relative Identifier
RSA	Rivest–Shamir–Adleman
SaaS	Software-as-a-Service
SAN	Subject Alternative Names
SCEP	Simple Certificate Enrollment Protocol
SLAAC	Stateless Address Autoconfiguration
SMB	Server Message Block
SME	Small and medium-sized enterprises
SoH	Statement of Health
SSH	Secure Shell

SSID	Service Set Identifier
SSL	Secure Socket Layer
SSO	Single Sign-on
SUS	System Usability Scale
TLD	Top-Level-Domain
TLS	Transport Layer Security oder TLS ist ein Protokoll zum Schutz persönlicher Daten bei der Kommunikation zwischen Endgerät und Anwendung im Internet. Im Alltag trifft man regelmäßig auf TLS, da der Großteil der Webseiten via HTTPS erreichbar ist. TLS ist der Nachfolger von SSL und existiert mittlerweile in der Version TLS 1.3 [184].
TOTP	Time-based One-Time Password
USB	Universal Serial Bus
Vendor Lock-in	Ein Vendor Lock-in beschreibt die Situation, bei dem die Kosten für den Wechsel zu einem anderen Anbieter so hoch sind, dass der Kunde im Wesentlichen an den ursprünglichen Anbieter gefangen ist [185].
Walled Garden	Im Internet kontrolliert ein Walled Garden in der Regel den Zugang zu Webinhalten und -diensten. Der Walled Garden beschränkt den Internetzugriff der NutzerInnen innerhalb spezifischer Netzwerke, um den Zugang zu einer Auswahl von Websites zu ermöglichen oder den Zugang zu anderen Websites zu verhindern. [186].

WLAN	Wireless Local Area Network
WLC	Wireless LAN Controller
WMI	Windows Management Instrumentation
WPA	Wi-Fi Protected Access
WPA2-Enterprise	WPA2 steht für die Abkürzung „Wi-Fi Protected Access 2“ und beschreibt einen Standard aus dem Jahr 2004 für die Authentifizierung und Verschlüsselung von WLAN-Netzwerken. Während WPA2-Personal sich auf private Haushalte fokussiert und ein einzelnes Passwort zur Anmeldung nutzt, wird WPA2-Enterprise in Firmenumgebungen mit einer 802.1X-Infrastruktur eingesetzt. Mittlerweile wurde der WPA2-Standard durch den WPA3-Standard ersetzt, der weitere Sicherheitsfunktionen und größere Schlüssellängen unterstützt [187].

Literatur

[1] Chloe Biscoe. “ISO 27001 certification figures increase by 20%”. last accessed August 5, 2022. (Sep. 2017), Adresse: https://www.itgovernance.co.uk/blog/iso-27001-certification-figures-increase-by-20.

[2] International Organization for Standardization, *THE ISO SURVEY OF MANAGEMENT SYSTEM STANDARD CERTIFICATIONS – 2020 – EXPLANATORY NOTE*. International Organization for Standardization, 2021, last accessed August 5, 2022.

[3] IT Governance Europe Ltd. “Vorteile der ISO 27001 Zertifizierung”. last accessed August 5, 2022. (), Adresse: https://www.itgovernance.eu/de-de/iso-27001-benefits-de.

[4] ISMS.online. “ISO 27001 – Annex A.9: Access Control”. last accessed September 25, 2022. (), Adresse: https://www.isms.online/iso-27001/annex-a-9-access-control.

[5] ISMS.online. “ISO 27001 – Annex A.13: Communications Security”. last accessed September 25, 2022. (), Adresse: https://www.isms.online/iso-27001/annex-a-13-communications-security.

[6] Gartner. “IT Budget”. last accessed March 25, 2023. (2023), Adresse: https://www.gartner.com/en/information-technology/glossary/it-budget.

[7] Louis Columbus. “Benchmarking your cybersecurity budget in 2023”. last accessed March 25, 2023. (Feb. 2023), Adresse: https://venturebeat.com/security/benchmarking-your-cybersecurity-budget-in-2023/#:~:text=On%20average%20in%202022%2C%20enterprises,manufacturing%20sectors%20spend%20on%20cybersecurity..

[8] Wirtschaftskammer Österreich. “Klein- und Mittelbetriebe in Österreich”. last accessed November 20, 2022. (), Adresse: https://www.wko.at/service/zahlen-daten-fakten/KMU-definition.html.

[9] EU-Kommission, *EMPFEHLUNG DER KOMMISSION vom 6. Mai 2003 betreffend die Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen (2003/361/EG)*, Amtsblatt der Europäischen Union, last accessed November 20, 2022, Mai 2003. Adresse: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=celex:32003H0361.

[10] RedHat. "Vergleich von IaaS, PaaS und SaaS". last accessed November 27, 2022. (Aug. 2022), Adresse: https://www.redhat.com/de/topics/cloud-computing/iaas-vs-paas-vs-saas.

[11] IONOS. "On-Premises: Das Lizenzmodell für serverbasierte Software". last accessed November 27, 2022. (Sep. 2020), Adresse: https://www.ionos.at/digitalguide/server/knowhow/was-ist-on-premises.

[12] IONOS. "PaaS: platform as a service at a glance". last accessed November 28, 2022. (Juni 2019), Adresse: https://www.ionos.com/digitalguide/server/know-how/paas-platform-as-a-service.

[13] Christo Petrov. "52 Gmail Statistics To Show How Big It Is In 2022". last accessed November 28, 2022. (Nov. 2022), Adresse: https://techjury.net/blog/gmail-statistics.

[14] TheBoardishTeam. "Average IT Budget by Company Size". last accessed March 25, 2023. (2023), Adresse: https://www.boardish.io/average-it-budget-by-company-size/.

[15] JAnger. "Main Page". last accessed February 27, 2023. (Feb. 2023), Adresse: https://wiki.samba.org/index.php/Main_Page.

[16] SambaWiki. "Setting up Samba as an Active Directory Domain Controller". last accessed October 24, 2022. (Sep. 2022), Adresse: https://wiki.samba.org/index.php/Setting_up_Samba_as_an_Active_Directory_Domain_Controller.

[17] JAnger. "Samba Release Planning". last accessed February 18, 2023. (Feb. 2023), Adresse: https://wiki.samba.org/index.php/Samba_Release_Planning.

[18] Samba. "Samba Vendors". last accessed February 27, 2023. (2023), Adresse: https://www.samba.org/samba/vendors.

[19] Samba. "Samba Support". last accessed February 27, 2023. (2023), Adresse: https://www.samba.org/samba/support.

[20] Scott McBrien. “What is backporting, and how does it apply to RHEL and other Red Hat products?” last accessed February 27, 2023. (Feb. 2020), Adresse: https://www.redhat.com/en/blog/what-backporting-and-how-does-it-apply-rhel-and-other-red-hat-products.

[21] ThiagoPezzo. “Backports”. last accessed February 27, 2023. (Jan. 2023), Adresse: https://wiki.debian.org/Backports.

[22] ddstreet. “UbuntuBackports”. last accessed February 27, 2023. (Jan. 2022), Adresse: https://help.ubuntu.com/community/UbuntuBackports.

[23] ZOHO Corp. “Active Directory Objects List”. last accessed April 07, 2023. (2023), Adresse: https://www.windows-active-directory.com/active-directory-objects-list.html.

[24] Peter Schmitz Dipl.-Ing. (FH) Stefan Luber. “Was ist ein Zero-Trust-Modell?” last accessed April 07, 2023. (Okt. 2018), Adresse: https://www.security-insider.de/was-ist-ein-zero-trust-modell-a-752389.

[25] Okta. “Identification & Authentication: Similarities & Differences”. last accessed November 30, 2022. (Juni 2022), Adresse: https://www.okta.com/identity-101/identification-vs-authentication.

[26] Tori Taylor. “Hacking-Related Data Breaches Leverage Compromised Passwords”. last accessed November 30, 2022. (Mai 2021), Adresse: https://www.securelink.com/blog/81-hacking-related-breaches-leverage-compromised-credentials/.

[27] Microsoft. “Considerations when using Windows Defender Credential Guard”. last accessed November 30, 2022. (Aug. 2022), Adresse: https://learn.microsoft.com/en-us/windows/security/identity-protection/credential-guard/credential-guard-considerations.

[28] Elektronik-Kompendium. “VLAN - Virtual Local Area Network / IEEE 802.1q”. last accessed November 30, 2022. (2022), Adresse: https://www.elektronik-kompendium.de/sites/net/0906221.htm.

[29] Werner Fischer. “VLAN Grundlagen”. last accessed November 30, 2022. (2022), Adresse: https://www.thomas-krenn.com/de/wiki/VLAN_Grundlagen.

[30] NetworkLessons. “AAA and 802.1X Authentication”. last accessed December 5, 2022. (Dez. 2022), Adresse: https://networklessons.com/cisco/ccie-routing-switching/aaa-802-1x-authentication.

[31] SecureW2. “What is 802.1X? How Does it Work?” last accessed December 3, 2022. (Dez. 2022), Adresse: https://www.securew2.com/solutions/802-1x.

[32] Ian Brown Kevin Dooley. “Logging System Events”. last accessed April 07, 2023. (2023), Adresse: https://www.oreilly.com/library/view/cisco-ios-cookbook/0596527225/ch04s07.html.

[33] ArubaNetworks. “What Is AAA?” last accessed December 5, 2022. (Dez. 2022), Adresse: https://www.arubanetworks.com/techdocs/ClearPass/6.7/Aruba_DeployGd_HTML/Content/802.1X%20Authentication/About_AAA.htm.

[34] Dipl.-Ing. (FH) Stefan Luber / Peter Schmitz. “Wie funktioniert RADIUS?” last accessed December 5, 2022. (Dez. 2022), Adresse: https://www.security-insider.de/wie-funktioniert-radius-a-613266.

[35] Brenna Lee. “What is the RADIUS Protocol?” last accessed December 5, 2022. (Mai 2022), Adresse: https://jumpcloud.com/blog/what-is-the-radius-protocol.

[36] Wikipedia. “Remote Authentication Dial-In User Service”. last accessed December 5, 2022. (Jan. 2020), Adresse: https://de.wikipedia.org/wiki/Remote_Authentication_Dial-In_User_Service.

[37] O’Reilly. “TACACS+ Packet Encryption”. last accessed December 9, 2022. (Dez. 2022), Adresse: https://www.oreilly.com/library/view/network-security-principles/1587050250/1587050250_ch17lev1sec4.html.

[38] C. Rigney; A. Rubens; W. Simpson; S. Willens, “Remote Authentication Dial In User Service (RADIUS)”, RFC Editor, RFC RFC2058, Jan. 1997, last accessed December 9, 2022. Adresse: https://www.rfc-editor.org/rfc/rfc2058.

[39] P. Calhoun C. Rigney W. Willats, “RADIUS Extensions”, RFC Editor, RFC RFC2869, Jan. 2000, last accessed December 9, 2022. Adresse: https://www.rfc-editor.org/rfc/rfc2869.

[40] Roman Cinkais. “802.1X and Digital Certificates”. last accessed December 5, 2022. (Dez. 2022), Adresse: https://www.3key.company/802-1x-and-digital-certificates/.

[41] Cisco. “What Is Network Access Control?” last accessed December 9, 2022. (Dez. 2022), Adresse: https://www.cisco.com/c/en/us/products/security/what-is-network-access-control-nac.html.

[42] Alacrinet. “Network Access Control (NAC)”. last accessed March 31, 2023. (2023), Adresse: https://www.alacrinet.com/security-solutions/nac.

[43] S. Winter; M. McCauley; S. Venaas; K. Wierenga, “Transport Layer Security (TLS) Encryption for RADIUS”, RFC Editor, RFC RFC6614, Mai 2012, last accessed December 16, 2022. Adresse: https://www.rfc-editor.org/rfc/rfc6614.

[44] A. DeKok, “Datagram Transport Layer Security (DTLS) as a Transport Layer for RADIUS”, RFC Editor, RFC RFC7360, Sep. 2014, last accessed December 16, 2022. Adresse: https://www.rfc-editor.org/rfc/rfc7360.

[45] S. Farrell K. Moriarty, “Deprecating TLS 1.0 and TLS 1.1”, RFC Editor, RFC RFC8996, März 2021, last accessed December 16, 2022. Adresse: https://www.rfc-editor.org/rfc/rfc8996.

[46] Sam Metzler. “How to Configure RADIUS over TLS (RadSec)”. last accessed December 17, 2022. (Dez. 2022), Adresse: https://www.cloudradius.com/how-to-configure-radius-over-tls-radsec.

[47] Cisco. “Configuring RadSec”. last accessed December 16, 2022. (Dez. 2022), Adresse: https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9300/software/release/16-10/configuration_guide/sec/b_1610_sec_9300_cg/configuring_radsec.pdf.

[48] Aruba. “Enabling RADIUS Communication over TLS (RadSec)”. last accessed December 16, 2022. (Dez. 2022), Adresse: https://www.arubanetworks.com/techdocs/Instant_83_WebHelp/Content/Instant_UG/Authentication/ConfiguringRadSec.htm.

[49] Juniper. “RADIUS over TLS (RADSEC)”. last accessed December 16, 2022. (Juni 2022), Adresse: https://www.juniper.net/documentation/us/en/software/junos/user-access/topics/task/radsec-configuring.html.

[50] Fabian Mauchle Stig Venaas. “radsecproxy - a generic RADIUS proxy with RadSec support”. last accessed December 17, 2022. (Dez. 2022), Adresse: https://radsecproxy.github.io.

[51] SecureW2. “Server Certificate Validation”. last accessed December 17, 2022. (Dez. 2022), Adresse: https://www.securew2.com/solutions/server-certificate-validation.

[52] Patrick Grubbs. “What is RadSec?” last accessed December 17, 2022. (Dez. 2022), Adresse: https://www.securew2.com/blog/what-is-radsec.

[53] Amanda Tucker. “Android 13 Server Certificate Validation”. last accessed December 17, 2022. (Dez. 2022), Adresse: https://www.securew2.com/blog/android-13-server-certificate-validation.

[54] Sam Metzler. “WPA3: The Ultimate Guide”. last accessed April 06, 2023. (2023), Adresse: https://www.securew2.com/blog/wpa3-the-ultimate-guide.

[55] SecureW2. “JoinNow MultiOS: Simple Self-Service Onboarding for All Your Unmanaged Devices”. last accessed February 4, 2023. (2023), Adresse: https://www.securew2.com/products/joinnow.

[56] SecureW2. “How to Set Up Passwordless RADIUS Authentication with an Ubiquiti Unifi Access Point”. last accessed February 4, 2023. (2023), Adresse: https://www.securew2.com/solutions/wi-fi-integrations/how-to-eap-tls-ubiquiti-unifi/.

[57] Nicolae Tomai u. a., “Particularities of security design for wireless networks in small and medium business (SMB)”, *Informatica Economica*, Jg. 44, Nr. 11, S. 93–98, 2007.

[58] Cornelius Diekmann, Johannes Naab, Andreas Korsten und Georg Carle, “Agile network access control in the container age”, *IEEE Transactions on Network and Service Management*, Jg. 16, Nr. 1, S. 41–55, 2018.

[59] Jon Matias, Jokin Garay, Alaitz Mendiola, Nerea Toledo und Eduardo Jacob, “FlowNAC: Flow-based network access control”, in *2014 third European workshop on software defined networks*, IEEE, 2014, S. 79–84.

[60] Pedro Moreno Sanchez, Rafa Marin Lopez und Antonio F Gomez Skarmeta, “PANATIKI: a network access control implementation based on PANA for IoT devices”, *Sensors*, Jg. 13, Nr. 11, S. 14 888–14 917, 2013.

[61] Juuso Mattila, “Network Access Control-järjestelmän valinta ja käyttöönotto”, 2019.

[62] Jarrod Schafer, “Unified Endpoint Management Software for a Small Company”, 2021, last accessed March 6, 2023. Adresse: https://www.theseus.fi/bitstream/handle/10024/510474/Schafer_Jarrod.pdf?sequence=2.

[63] Alexandru Enaceanu, Gabriel Garais u. a., "Cost Effective RADIUS Authentication for Wireless Clients", *Database Systems*, Jg. 27, 2010, last accessed March 6, 2023. Adresse: http://dbjournal.ro/archive/2/3_Enaceanu_Garais.pdf.

[64] Hendra Supendar, "Penerapan Linux Zentyal Sebagai Filtering Dan Bandwidth Management Pada Jaringan Pt. Anta Citra Arges", *Jurnal Teknik Komputer AMIK BSI*, Jg. 2, Nr. 1, S. 22–30, 2016, last accessed March 6, 2023. Adresse: https://ejournal.bsi.ac.id/ejurnal/index.php/jtk/article/viewFile/359/268.

[65] Olubodunde Agboola, "Installation of Zentyal; LINUX Small Business Server", 2014, last accessed March 6, 2023. Adresse: https://scholarworks.bgsu.edu/cgi/viewcontent.cgi?article=1013&context=ms_tech_mngmt.

[66] Alejandro Castiblanco Bernal, César Alfonso Barbosa Serrato, Jose Uriel Joya u. a., "Servicios de infraestructura zentyal 6.0", last accessed March 6, 2023. Adresse: https://repository.unad.edu.co/bitstream/handle/10596/23184/jujoya.pdf?sequence=1.

[67] Toomas Ristola, "Pilvipohjainen langaton verkko: Ruckus Cloud", 2021.

[68] Dominic Zeni. "Cisco ISE: Wired and Wireless 802.1X Network Authentication". last accessed October 11, 2022; unclear creation date - chosen date is a assumption based on the comments. (Juni 2017), Adresse: https://www.lookingpoint.com/blog/ise-series-802.1x.

[69] A. Panitz D. Eastlake. "Reserved Top Level DNS Names". last accessed October 23, 2022. (Juni 1999), Adresse: https://www.rfc-editor.org/rfc/rfc2606.html.

[70] Meraki. "Configuring Microsoft NPS for MAC-Based RADIUS - MS Switches". last accessed October 16, 2022. (Okt. 2020), Adresse: https://documentation.meraki.com/MS/Access_Control/Configuring_Microsoft_NPS_for_MAC-Based_RADIUS_-_MS_Switches.

[71] ughisthisnametaken. "NPS (Radius) with MAB on Cisco Switch." last accessed April 07, 2023. (Nov. 2019), Adresse: https://www.reddit.com/r/sysadmin/comments/dwei0n/comment/f7iynre/?context=3.

[72] Lawrence Orans. "Magic Quadrant for Network Access Control". last accessed March 28, 2023. (Dez. 2013), Adresse: http://emailing.aquastar-consulting.com/2013/Infra/Newsletters/2014/Janvier/Magic-Quadrant-for-Network-Access-Control.pdf.

[73] ALACRINET. “Network Access Control (NAC)”. last accessed March 28, 2023. (2023), Adresse: https://www.alacrinet.com/security-solutions/nac.

[74] thomas. “ACS vs ISE Comparison”. last accessed March 28, 2023. (Nov. 2015), Adresse: https://community.cisco.com/t5/security-knowledge-base/acs-vs-ise-comparison/ta-p/3649661.

[75] SaintEvn. “PAN node and PSN node in Distributed Deployment”. last accessed March 28, 2023. (Nov. 2020), Adresse: https://community.cisco.com/t5/network-access-control/pan-node-and-psn-node-in-distributed-deployment/td-p/4190117.

[76] Alexander S. Gillis. “Cisco Identity Services Engine (ISE)”. last accessed March 28, 2023. (Mai 2022), Adresse: https://www.techtarget.com/searchmobilecomputing/definition/Cisco-Identity-Services-Engine-ISE.

[77] Paul Tablan. “What is Aruba ClearPass? How Does it Protect Your Network?” last accessed March 31, 2023. (Sep. 2022), Adresse: https://www.kelsercorp.com/blog/what-is-aruba-clearpass-and-how-does-it-protect-your-network.

[78] Hewlett Packard Enterprise. “ARUBA CLEARPASS POLICY MANAGER”. last accessed March 31, 2023. (2022), Adresse: https://www.arubanetworks.com/assets/ds/DS_ClearPass_PolicyManager.pdf.

[79] Forescout. “Homepage”. last accessed March 31, 2023. (2023), Adresse: https://forescout.de.

[80] Thomas Seiler Sean Boran. “FreeNAC”. last accessed March 28, 2023. (2023), Adresse: https://github.com/Boran/freenac.

[81] Open Cloud Factory. “OpenNAC is no longer available here”. last accessed March 28, 2023. (2023), Adresse: https://opennac.opencloudfactory.com/.

[82] Inverse inc. “Overview”. last accessed March 29, 2023. (2023), Adresse: https://www.packetfence.org/about.html.

[83] Inverse inc. “Administration Guide”. last accessed March 31, 2023. (Dez. 2013), Adresse: https://www.packetfence.org/downloads/PacketFence/doc/PacketFence_Administration_Guide-4.1.0.pdf.

[84] msatranjr alvinashcraft msatranjr. “Netzwerkzugriffsschutz”. last accessed March 31, 2023. (Sep. 2022), Adresse: https://learn.microsoft.com/de-de/windows/win32/nap/network-access-protection-start-page.

[85] Inverse inc. “Installation Guide”. last accessed March 31, 2023. (März 2023), Adresse: https://www.packetfence.org/downloads/PacketFence/doc/PacketFence_Installation_Guide.pdf.

[86] Enlyft. “Companies using PacketFence”. last accessed March 31, 2023. (2023), Adresse: https://enlyft.com/tech/products/packetfence.

[87] extrafu. “Missing WMI tab in new admin”. last accessed April 03, 2023. (Juli 2021), Adresse: https://github.com/inverse-inc/packetfence/issues/4357.

[88] Greenbone AG. “Greenbone Community Containers 22.4”. last accessed April 03, 2023. (2023), Adresse: https://greenbone.github.io/docs/latest/22.4/container/index.html.

[89] ffund. “GVM 20 install and setup”. last accessed April 03, 2023. (Feb. 2022), Adresse: https://gist.github.com/ffund/f9c06f77569a3865e9ca92b9455bd90c.

[90] immauss. “A Greenbone Vulnerability Management docker image”. last accessed April 03, 2023. (2023), Adresse: https://immauss.github.io/openvas/.

[91] Lukas. “The Greenbone Vulnerability Manager service is not responding”. last accessed April 03, 2023. (Aug. 2021), Adresse: https://forum.greenbone.net/t/the-greenbone-vulnerability-manager-service-is-not-responding/9817.

[92] Dexus. “The Greenbone Vulnerability Manager service is not responding.” last accessed April 03, 2023. (Juli 2021), Adresse: https://github.com/Secure-Compliance-Solutions-LLC/GVM-Docker/issues/126.

[93] Inverse inc. “Network Devices Configuration Guide”. last accessed April 02, 2023. (März 2023), Adresse: https://www.packetfence.org/downloads/PacketFence/doc/PacketFence_Network_Devices_Configuration_Guide.pdf.

[94] Arnab Roy. “Insufficient Space to Store Pair string”. last accessed April 02, 2023. (Okt. 2017), Adresse: https://lists.freeradius.org/pipermail/freeradius-users/2017-October/089271.html.

[95] Fabrice Durand. "[PacketFence-users] sql_reject: Insufficient space to store pair string". last accessed April 02, 2023. (Jan. 2020), Adresse: https://www.mail-archive.com/packetfence-users@lists.sourceforge.net/msg18053.html.

[96] Docs Team. "Example for Configuring NAC (PacketFence as the Authentication Server)". last accessed April 03, 2023. (Aug. 2020), Adresse: https://docs.pica8.com/pages/viewpage.action?pageId=29852722%5C&ia=web.

[97] noisefloor. "Samba4-Server als Active-Directory Domain-Controller". last accessed February 18, 2023. (Jan. 2022), Adresse: https://wiki.ubuntuusers.de/Archiv/Howto/Samba4-Server_als_Active-Directory_Domain-Controller/.

[98] Mjt. "Is Samba as an Active Directory Domain Controller Stable Enough for an Production Environment?" last accessed February 28, 2023. (Feb. 2022), Adresse: https://wiki.samba.org/index.php/FAQ#Is_Samba_as_an_Active_Directory_Domain_Controller_Stable_Enough_for_an_Production_Environment.3F.

[99] Dmulder. "Rsync based SysVol replication workaround". last accessed February 28, 2023. (Okt. 2021), Adresse: https://wiki.samba.org/index.php/Rsync_based_SysVol_replication_workaround.

[100] Hortimech. "Bidirectional Rsync/Unison based SysVol replication workaround". last accessed February 28, 2023. (Mai 2020), Adresse: https://wiki.samba.org/index.php/Bidirectional_Rsync/Unison_based_SysVol_replication_workaround.

[101] Microsoft. "Forest and Domain Functional Levels". last accessed February 28, 2023. (Feb. 2021), Adresse: https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/active-directory-functional-levels.

[102] Stefan Kania, *Samba 4: Das Handbuch für Administratoren*. Carl Hanser Verlag GmbH Co KG, 2021, last accessed March 6, 2023. Adresse: https://api.pageplace.de/preview/DT0400.9783446469785_A42298231/preview-9783446469785_A42298231.pdf.

[103] Zentyal. "Domain Controller and Directory Services". last accessed March 6, 2023. (2023), Adresse: https://doc.zentyal.org/en/directory.html#know-limitations.

[104] Synology. “Synology Directory Server”. last accessed February 18, 2023. (2023), Adresse: https://www.synology.com/de-de/dsm/7.1/software_spec/synology_directory_server.

[105] Microsoft. “Protected Users Security Group”. last accessed March 7, 2023. (Aug. 2021), Adresse: https://learn.microsoft.com/en-us/windows-server/security/credentials-protection-and-management/protected-users-security-group.

[106] Sean Deuby. “Virtualization-Safe Active Directory in Windows Server 2012”. last accessed March 7, 2023. (Juli 2012), Adresse: https://www.itprotoday.com/identity-management-and-access-control/virtualization-safe-active-directory-windows-server-2012.

[107] Sean Deuby. “Should you upgrade to Active Directory 2016... or stay where you are?” last accessed March 7, 2023. (Sep. 2018), Adresse: https://www.semperis.com/blog/should-you-upgrade-to-active-directory-2016or-stay-where-you-are/.

[108] Synology. “Synology Directory Server”. last accessed February 13, 2023. (2023), Adresse: https://www.synology.com/de-de/dsm/feature/active_directory.

[109] Synology. “RADIUS Server”. last accessed February 13, 2023. (2023), Adresse: https://kb.synology.com/de-de/DSM/help/RadiusServer/rad_desc?version=7.

[110] QNAP. “So nutzen Sie das QNAP-NAS als RADIUS-Server”. last accessed February 13, 2023. (März 2021), Adresse: https://www.qnap.com/de-de/how-to/tutorial/article/so-nutzen-sie-das-qnap-nas-als-radius-server.

[111] QNAP. “Domänencontroller aktivieren”. last accessed February 13, 2023. (2023), Adresse: https://docs.qnap.com/operating-system/qts/4.4.x/de-de/GUID-EE5D8534-FCA0-484F-A367-D6D1926D7D1E.html.

[112] John. “Is Synology’s Software Built on Linux? (Answers and More!)” last accessed February 25, 2023. (2023), Adresse: https://techguidecentral.com/is-synologys-software-built-on-linux-answers-and-more.

[113] Gerrit. “Synology NAS Exkurs: Die Basis des Diskstation Managers”. last accessed February 25, 2023. (Nov. 2019), Adresse: https://curius.de/2019/11/synology-nas-exkurs-die-basis-des-diskstation-managers.

[114] eccitaze. “what distribution of Linux is synology using ?” last accessed February 25, 2023. (Aug. 2019), Adresse: https://www.reddit.com/r/synology/comments/cn9qnd/what_distribution_of_linux_is_synology_using.

[115] Zentyal. “Features”. last accessed February 25, 2023. (2023), Adresse: https://zentyal.com/features.

[116] Zentyal. “Zentyal Support Customer Guide”. last accessed February 26, 2023. (Jan. 2021), Adresse: https://zentyal.com/Zentyal_Support_Customer_Guide.pdf.

[117] Zentyal. “Release Policy”. last accessed February 25, 2023. (2023), Adresse: https://zentyal.com/release-policy.

[118] UbuntuUpdates. “Package samba”. last accessed February 26, 2023. (2023), Adresse: https://www.ubuntuupdates.org/package/core/focal/main/security/samba.

[119] Netzint GmbH. “Education linuxmuster.net”. last accessed February 26, 2023. (2023), Adresse: https://www.netzint.de/education/linuxmuster.

[120] cweikl. “Lehrer-Passwörter zurücksetzen¶”. last accessed February 26, 2023. (Okt. 2022), Adresse: https://docs.linuxmuster.net/de/latest/user-management/change-teacher-passwords/index.html.

[121] cweikl. “Prüfungs-/Klassenarbeitsmodus, austeilen und einsammeln”. last accessed February 26, 2023. (Okt. 2022), Adresse: https://docs.linuxmuster.net/de/latest/classroom/exam-and-transfer.html.

[122] MachtDochNix cweikl. “Installationablauf”. last accessed February 26, 2023. (Okt. 2022), Adresse: https://docs.linuxmuster.net/de/latest/installation/overview.html.

[123] Linuxmuster. “Über”. last accessed February 26, 2023. (2023), Adresse: https://www.linuxmuster.net/de/ueber.

[124] Linuxmuster. “Dienstleister / Händler”. last accessed February 26, 2023. (2023), Adresse: https://www.linuxmuster.net/de/support-de/haendler/.

[125] noisefloor. “Samba4-Server als Active-Directory Domain-Controller”. last accessed February 27, 2023. (Jan. 2022), Adresse: https://wiki.ubuntuusers.de/Archiv/Howto/Samba4-Server_als_Active-Directory_Domain-Controller.

[126] OpenLogic. “How Much Does Red Hat Licensing Cost Compared to CentOS Licenses?” last accessed February 26, 2023. (2023), Adresse: https://www.openlogic.com/resources/red-hat-licensing-centos.

[127] Zentyal. “FAQ”. last accessed March 12, 2023. (2023), Adresse: https://zentyal.com/faq.

[128] Canonical Ltd. “Ubuntu certified servers”. last accessed March 12, 2023. (März 2023), Adresse: https://ubuntu.com/certified/servers?q=%5C&limit=364%5C&release=20.04+LTS.

[129] Zentyal. “Zentyal installation from the installer”. last accessed March 12, 2023. (2023), Adresse: https://doc.zentyal.org/en/installation.html#installation-on-top-of-ubuntu-20-04-lts-server-or-desktop.

[130] Amazon AWS. “Designing a CA hierarchy”. last accessed March 15, 2023. (2023), Adresse: https://docs.aws.amazon.com/privateca/latest/userguide/ca-hierarchy.html.

[131] Tobi. “Zertifikate – Ein Überblick der verschiedenen Formate”. last accessed March 15, 2023. (März 2017), Adresse: https://www.antary.de/2017/03/11/zertifikate-ein-ueberblick-der-verschiedenen-formate.

[132] King Michael. “with_ntdomain_hack”. last accessed March 17, 2023. (Mai 2006), Adresse: https://freeradius-users.freeradius.narkive.com/nJ3zj8qB/with-ntdomain-hack.

[133] Dngray. “FreeRadius EAP-TLS configuration”. last accessed March 19, 2023. (Juni 2021), Adresse: https://wiki.alpinelinux.org/wiki/FreeRadius_EAP-TLS_configuration.

[134] Kevinsky86. “[SOLVED] Zentyal 7, can’t create or edit GPO’s”. last accessed March 17, 2023. (Feb. 2021), Adresse: https://forum.zentyal.org/index.php?topic=35157.0.

[135] Tranquil IT. “Introducing the SysvolSync Utility”. last accessed April 07, 2023. (2021), Adresse: https://samba.tranquil.it/doc/en/samba_advanced_methods/samba_tis_sysvolsync.html#introducing-the-sysvolsync-utility.

[136] Eric Sachs. “Microsoft named a Leader in 2022 Gartner® Magic Quadrant™ for Access Management for the 6th year”. last accessed February 4, 2023. (Nov. 2022), Adresse: https://www.microsoft.com/en-us/security/blog/2022/11/04/microsoft-named-a-

leader-in-2022-gartner-magic-quadrant-for-access-management-for-the-6th-year/.

[137] Cisco Meraki. “Restricting Traffic with Isolated Switch Ports”. last accessed December 20, 2022. (Dez. 2022), Adresse: https://documentation.meraki.com/MS/Port_and_VLAN_Configuration/Restricting_Traffic_with_Isolated_Switch_Ports.

[138] Cisco. “Port Isolation Configuration”. last accessed December 20, 2022. (Dez. 2022), Adresse: https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst_pon/software/configuration_guide/olt_port/b-gpon-config-olt-port/port_isolation_configuration.pdf.

[139] Emil_G. “How to do Port Isolation in Aruba CX 6000 switch?” last accessed December 20, 2022. (Jan. 2022), Adresse: https://community.arubanetworks.com/community-home/digestviewer/viewthread?MessageKey=816d97ed-2fcd-4ada-b178-2260a1cefb52%5C&CommunityKey=22dc38ea-a1e1-4059-b55e-a622fedecf32%5C&tab=digestviewer%5C&bm=816d97ed-2fcd-4ada-b178-2260a1cefb52#bm816d97ed-2fcd-4ada-b178-2260a1cefb52.

[140] Subhashini. “Port Isolation (Wired Guest Network)”. last accessed December 20, 2022. (März 2017), Adresse: https://community.arubanetworks.com/community-home/digestviewer/viewthread?MID=12268.

[141] Google. “Google Cloud Print”. last accessed December 20, 2022. (Dez. 2022), Adresse: https://www.google.com/intl/de_ALL/cloudprint/learn/.

[142] Elke Witmer-Goßner Dr. Dietmar Müller. “Die besten Alternativen für Google Cloud Print”. last accessed December 20, 2022. (Nov. 2020), Adresse: https://www.cloudcomputing-insider.de/die-besten-alternativen-fuer-google-cloud-print-a-3846ec80bf52588a8284ebfeec6e017c/.

[143] Ed. D. Harkins Ed.; W. Kumari, “Opportunistic Wireless Encryption”, RFC Editor, RFC RFC8110, Mai 2017, last accessed December 26, 2022. Adresse: https://www.rfc-editor.org/rfc/rfc8110.

[144] Elektronik-Kompendium. “WLAN-Authentifizierung”. last accessed December 26, 2022. (Dez. 2022), Adresse: https://www.elektronik-kompendium.de/sites/net/1101181.htm.

[145] Fortinet. “Configuring security”. last accessed December 26, 2022. (Dez. 2022), Adresse: https://docs.fortinet.com/document/fortiap/6.4.3/fortiwifi-and-fortiap-configuration-guide/908404/configuring-security.

[146] Fortinet. “Outbound firewall authentication with Azure AD as a SAML IdP”. last accessed December 26, 2022. (Dez. 2022), Adresse: https://docs.fortinet.com/document/fortigate/6.4.8/administration-guide/33053/outbound-firewall-authentication-with-azure-ad-as-a-saml-idp.

[147] Microsoft. “Tutorial: Azure Active Directory integration with Palo Alto Networks Captive Portal”. last accessed December 26, 2022. (Nov. 2022), Adresse: https://learn.microsoft.com/en-us/azure/active-directory/saas-apps/paloaltonetworks-captiveportal-tutorial.

[148] Microsoft. “Azure Active Directory Seamless Single Sign-On”. last accessed December 26, 2022. (Aug. 2022), Adresse: https://learn.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sso.

[149] Cloudi-Fi. “Captive portal”. last accessed December 27, 2022. (2021), Adresse: https://www.cloudi-fi.com/technology/captive-portal.

[150] IronWifi. “Captive Portals”. last accessed December 27, 2022. (Dez. 2022), Adresse: https://www.ironwifi.com/help/captive-portals.

[151] Cloudi-Fi. “SAML For Sponsors with Azure”. last accessed December 27, 2022. (Dez. 2022), Adresse: https://help.cloudi-fi.com/en/articles/6138052-saml-for-sponsors-with-azure.

[152] IronWifi. “Authentication Providers”. last accessed December 27, 2022. (Dez. 2022), Adresse: https://www.ironwifi.com/help/authentication-providers.

[153] IronWifi. “List of Supported Vendors”. last accessed December 27, 2022. (Dez. 2022), Adresse: https://www.ironwifi.com/list-of-supported-vendors.

[154] Cloudi-Fi. “SAML for Guests with Azure”. last accessed December 27, 2022. (Dez. 2022), Adresse: https://help.cloudi-fi.com/en/articles/6078638-saml-for-guests-with-azure.

[155] Damien. “Duration of an account”. last accessed December 27, 2022. (2022), Adresse: https://help.cloudi-fi.com/en/articles/2926317-duration-of-an-account.

[156] Zscaler. “Zscaler Internet Access”. last accessed January 25, 2023. (2022), Adresse: https://www.zscaler.com/resources/data-sheets/zscaler-internet-access.pdf.

[157] Zscaler. “Zscaler Private Acces”. last accessed January 25, 2023. (2023), Adresse: https://www.zscaler.com/resources/data-sheets/zscaler-private-access.pdf.

[158] Zscaler. “Zscaler Client Connector”. last accessed January 31, 2023. (2021), Adresse: https://www.zscaler.de/resources/data-sheets/zscaler-mobile-app.pdf.

[159] Zscaler. “What is Zscaler Client Connector?” last accessed January 31, 2023. (2023), Adresse: https://help.zscaler.com/z-app/what-zscaler-app.

[160] Jacob Serpa. “What You Need to Know to Secure BYOD and Overcome Reverse Proxy Headaches”. last accessed January 25, 2023. (Juni 2022), Adresse: https://www.zscaler.de/blogs/product-insights/what-you-need-know-secure-byod-and-overcome-reverse-proxy-headaches.

[161] SecureW2. “Third-Party CA SCEP Integration with Microsoft Endpoint Manager: Intune”. last accessed February 4, 2023. (2023), Adresse: https://www.securew2.com/solutions/managed-devices/scep-ca-integration-with-microsoft-intune.

[162] SecureW2. “How To Configure WPA2-Enterprise With Microsoft Azure AD”. last accessed February 4, 2023. (2023), Adresse: https://www.securew2.com/solutions/configure-wpa2-enterprise-microsoft-azure.

[163] Microsoft. “Tutorial: Integrate SecureW2 JoinNow Connector with Azure Active Directory”. last accessed February 4, 2023. (Nov. 2022), Adresse: https://learn.microsoft.com/en-us/azure/active-directory/saas-apps/securejoinnow-tutorial.

[164] SecureW2. “Homepage”. last accessed February 4, 2023. (2023), Adresse: https://www.securew2.com/.

[165] SecureW2. “Role Based Access Control”. last accessed February 4, 2023. (2023), Adresse: https://www.securew2.com/solutions/role-based-access-control.

[166] CA/Browser Forum. “Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates”. last accessed February 5, 2023. (Apr. 2022), Adresse: https://cabforum.org/wp-content/uploads/CA-Browser-Forum-BR-1.8.4.pdf.

[167] Patrick Grubbs. “What is Dynamic RADIUS?” last accessed February 5, 2023. (2023), Adresse: https://www.securew2.com/blog/dynamic-radius.

[168] SecureW2. “Setting Up EAP-TLS WPA2-Enterprise with Cisco Wireless LAN Controller”. last accessed February 5, 2023. (2023), Adresse: https://www.securew2.com/solutions/wi-fi-integrations/setting-up-eap-tls-wpa2-enterprise-with-cisco-wireless-lan-controller.

[169] SecureW2. “How to Set Up EAP-TLS WPA2-Enterprise With Meraki”. last accessed February 5, 2023. (2023), Adresse: https://www.securew2.com/solutions/wi-fi-integrations/how-to-setup-eap-tls-with-meraki-access-points.

[170] SecureW2. “How to Set Up EAP-TLS with Aruba Instant Access Points”. last accessed February 5, 2023. (2023), Adresse: https://www.securew2.com/solutions/wi-fi-integrations/how-to-set-up-eap-tls-with-aruba-instant-access-points.

[171] SecureW2. “Integrating EAP-TLS Authentication With Microsoft NPS”. last accessed February 5, 2023. (2023), Adresse: https://www.securew2.com/solutions/radius-aaa-solutions/integrating-eap-tls-authentication-with-microsoft-nps.

[172] SecureW2. “What is 802.1X? How Does it Work?” last accessed February 5, 2023. (2023), Adresse: https://www.securew2.com/solutions/802-1x.

[173] Microsoft. “Add partner certification authority in Intune using SCEP”. last accessed February 5, 2023. (Sep. 2022), Adresse: https://learn.microsoft.com/en-us/mem/intune/protect/certificate-authority-add-scep-overview.

[174] Intune Training. “S03E18 - Deploying SCEP Certificates to Android Devices (I.T)”. last accessed February 5, 2023. (Nov. 2021), Adresse: https://www.youtube.com/watch?v=f4vGqKzs5ns.

[175] JumpCloud. “Cloud RADIUS”. last accessed February 6, 2023. (2023), Adresse: https://jumpcloud.com/platform/cloud-radius.

[176] Portnox. “RADIUS-as-a-Service”. last accessed February 6, 2023. (2023), Adresse: https://www.portnox.com/portnox-clear/radius-as-a-service.

[177] BSI. “Zwei-Faktor-Authentisierung für höhere Sicherheit”. last accessed May 14, 2020. (), Adresse: https://www.bsi-fuer-buerger.de/BSIFB/DE/DigitaleGesellschaft/OnlineBanking/Zwei_Faktor_Authentisierung/Zwei-Faktor-Authentisierung_node.html.

[178] IONOS. “Was ist eine Cloud?” last accessed February 28, 2023. (Jan. 2023), Adresse: https://www.ionos.at/digitalguide/server/knowhow/was-ist-eine-cloud.

[179] weclapp. “Dashboard”. last accessed February 28, 2023. (2023), Adresse: https://www.weclapp.com/de/lexikon/dashboard.

[180] Dipl.-Ing. (FH) Stefan Luber. “Was ist DTLS (Datagram Transport Layer Security)?” last accessed March 2, 2023. (Apr. 2020), Adresse: https://www.ip-insider.de/was-ist-dtls-datagram-transport-layer-security-a-903b5df4f4c79da30d226dbf1b1feb67.

[181] Cloudflare. “Was ist ein Identitätsanbieter (Identity Provider oder IdP?)” last accessed December 26, 2022. (Dez. 2022), Adresse: https://www.cloudflare.com/de-de/learning/access-management/what-is-an-identity-provider/.

[182] Forcepoint. “Definition des OSI-Modells”. last accessed February 28, 2023. (2023), Adresse: https://www.forcepoint.com/de/cyber-edu/osi-model.

[183] Erin Sullivan Stephen J. Bigelow. “pay-as-you-go cloud computing (PAYG cloud computing)”. last accessed February 28, 2023. (Okt. 2022), Adresse: https://www.techtarget.com/searchstorage/definition/pay-as-you-go-cloud-computing-PAYG-cloud-computing.

[184] ComputerWeekly. “Transport Layer Security (TLS)”. last accessed March 2, 2023. (Apr. 2014), Adresse: https://www.computerweekly.com/de/definition/Transport-Layer-Security-TLS.

[185] Cloudflare. “What does ’vendor lock-in’ mean?” last accessed February 5, 2023. (2023), Adresse: https://www.cloudflare.com/learning/cloud/what-is-vendor-lock-in.

[186] Aruba Networks. “Creating Walled Garden Access”. last accessed December 27, 2022. (Dez. 2022), Adresse: https://www.arubanetworks.com/techdocs/ArubaOS_63_Web_Help/Content/ArubaFrameStyles/Captive_Portal/Creating_Walled_Garden_A.htm.

[187] Elektronik-Kompendium. “WPA2 - Wi-Fi Protected Access 2 / IEEE 802.11i”. last accessed February 28, 2023. (2023), Adresse: https://www.elektronik-kompendium.de/sites/net/0907111.htm.