FERDINAND PORSCHE
FERN FH

Vergleich von 802.1X und MAC based authentication (MBA) Authentifizierung zur Verbesserung der Netzwerksicherheit anhand des Beispiels Schrack Technik GmbH

Bachelorarbeit

eingereicht von: **Ahmed ALY**
Matrikelnummer: 52009258

im Fachhochschul-Bachelorstudiengang Wirtschaftsinformatik (0470)
der Ferdinand Porsche FernFH

zur Erlangung des akademischen Grades eines

Bachelor of Arts in Business

Betreuung und Beurteilung: **DI Eszter Geresics-Földi MSc, BSc**

Wiener Neustadt, 01.2024

Ehrenwörtliche Erklärung

Ich versichere hiermit,

1. dass ich die vorliegende Bachelorarbeit selbständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel benutzt habe. Alle Inhalte, die direkt oder indirekt aus fremden Quellen entnommen sind, sind durch entsprechende Quellenangaben gekennzeichnet.
2. dass ich diese Bachelorarbeit bisher weder im Inland noch im Ausland in irgendeiner Form als Prüfungsarbeit zur Beurteilung vorgelegt oder veröffentlicht habe.

Wien, 14.01.2024

Unterschrift

Die Kapitel 1 bis 3 der vorliegenden Bachelorarbeit wurden im Rahmen der Lehrveranstaltung „Bachelor Seminar 1“ eingereicht und am 10.10.2023 als Bachelorarbeit 1 angenommen.

Kurzzusammenfassung: Vergleich von 802.1X und MAC based authentication (MBA) Authentifizierung zur Verbesserung der Netzwerksicherheit anhand des Beispiels Schrack Technik GmbH

Die Bachelorarbeit handelt davon, welche Methode, 802.1X oder MAC-basierte Authentifizierung, für die Sicherheit des Netzwerks bei der Firma "Schrack Technik GmbH" besser geeignet ist. Ursprünglich dachte man, dass die MAC-basierte Methode besser ist, aber die Untersuchung mit Hilfe einer Umfrage zeigt, dass 802.1X in den meisten Bereichen besser abschneidet, vor allem bei der Sicherheit.

Die Analyse berücksichtigt Dinge wie Kompatibilität, Sicherheitsvorteile, wie leicht die Methode umzusetzen ist und das Preis-Leistungsverhältnis. Die Ergebnisse zeigen, dass 802.1X besser geeignet ist, die Sicherheitsanforderungen der Firma zu erfüllen. Das ist wichtig für Schrack Technik, um ihr Netzwerk gut zu schützen.

Die Schlussfolgerung ist also anders als gedacht, und das zeigt, wie wichtig es ist, genau zu prüfen, welche Methode am besten zu den speziellen Bedürfnissen eines Unternehmens passt. Die Arbeit hilft dabei, die richtige Entscheidung für die Netzwerksicherheit von Schrack Technik zu treffen und betont, dass es wichtig ist, immer auf dem neuesten Stand der Sicherheitsanforderungen zu bleiben.

Schlagwörter:

Netzwerksicherheit, Netzwerkzugangskontrolle, 802.1x, Mac-basierte Authentifizierung, Authentifizierung

Abstract: Comparison of 802.1X and MAC based authentication (MBA) authentication to improve network security using the example of Schrack Technik GmbH

The bachelor thesis is about which method, 802.1X or MAC-based authentication, is better for the security of the network at the company "Schrack Technik GmbH". Originally it was thought that the MAC-based method was better, but the survey shows that 802.1X performs better in most areas, especially security.

The analysis takes into account things like compatibility, security benefits, how easy the method is to implement and the price/performance ratio. The results show that 802.1X is better suited to meet the company's security requirements. This is important for Schrack Technik to protect their network well.

So the conclusion is different than expected, and this shows how important it is to carefully consider which method best suits a company's specific needs. The paper helps to make the right decision for Schrack Technik's network security and emphasizes the importance of staying up to date with the latest security requirements.

Keywords:

network security, network access control, 802.1x, Mac-based authentication, authentication

Inhaltsverzeichnis

1. Einleitung

1.1 Problemstellung/Motivation

In der aktuellen Zeit der fortschreitenden Digitalisierung spielen Unternehmensnetzwerke eine große und wichtige Rolle in der Geschäftsführung. Sie stellen die grundlegende Grundlage dar, auf der Informationen ausgetauscht werden, die Zusammenarbeit gefördert wird und Geschäftsprozesse reibungslos ablaufen können. Diese verstärkte Abhängigkeit von digitalen Netzwerken bringt jedoch auch eine erhöhte Anfälligkeit für potenzielle Bedrohungen mit sich. Cyberkriminelle sind ständig auf der Suche nach Schwachstellen, um in die Unternehmensnetzwerke einzudringen und somit an vertrauliche Daten zu kommen oder den Betrieb zu stören. (Engländer et al. 2021)

Die Firma Schrack Technik GmbH, wie so gut wie jedes andere Unternehmen, steht vor der Herausforderung, ihre Netzwerksicherheit auf höchstem Niveau zu bringen, um sich vor den verschiedensten Angriffsszenarien zu schützen. Die zunehmende Anzahl von Cyberangriffen in den letzten Jahren lehrt den Firmen die Dringlichkeit dieses Themas. Ein erfolgreicher Angriff auf das Firmennetz kann nicht nur finanzielle Verluste als Folge haben, sondern auch das Image des Unternehmens schädigen und dadurch das Vertrauen der Kunden beeinflussen.(Müller 2022)

Um diesen Herausforderungen entgegenzuwirken, hat die Firma Schrack Technik GmbH die Entscheidung getroffen, die Network Access Control (NAC) Authentifizierung in ihre Sicherheitsmaßnahmen zu integrieren. NAC ist eine Technologie, die dafür implementiert ist, den Zugriff auf das Unternehmensnetzwerk zu regeln und dadurch nicht gewünschten Zugriff zu verhindern. Dabei werden Verfahren eingesetzt, die sicherstellen, dass nur autorisierte Geräte und Benutzer Zugang zum Firmennetzwerk erhalten.(Ehsan et al. 2012)

Dies erklärt die Wichtigkeit der Wahl der richtigen Authentifizierungsmethode. Eine falsche Entscheidung könnte dazu führen, dass die Sicherheit des Netzwerks gefährdet wird oder dass die Implementierungskosten unnötig hoch sind. Aus diesem Grund steht Schrack Technik GmbH vor der Aufgabe, zwischen verschiedenen Authentifizierungsmethoden wählen zu müssen, wobei die beiden Hauptoptionen 802.1X und MAC-basierte Authentifizierung (MBA) sind. Die Wahl zwischen diesen beiden Methoden erfordert eine umfassende Analyse, um sicherzustellen, dass die gewählte Methode den spezifischen Anforderungen und Zielen des Unternehmens entspricht.

Diese Bachelorarbeit zielt darauf ab, diese Problemstellung anzugehen, indem sie eine gründliche Untersuchung der Authentifizierungsmethoden 802.1X und MBA durchführt. Sie beabsichtigt, anhand von wirtschaftlichen und technischen Kriterien die am besten geeignete Methode für die Firma Schrack Technik GmbH zu ermitteln und damit einen Beitrag zur Steigerung der Netzwerksicherheit des Unternehmens zu leisten.

1.2 Ziel der Bachelorarbeit

Die vorliegende Bachelorarbeit verfolgt das Ziel, die beiden Network Access Control (NAC) Authentifizierungsmethoden, nämlich 802.1X und MAC-based Authentication (MBA), eingehend zu vergleichen. Dieser Vergleich erfolgt anhand einer umfassenden Analyse, die sowohl wirtschaftliche als auch technische Kriterien berücksichtigt. Das Ziel ist es, die für die Firma Schrack Technik GmbH am besten geeignete Authentifizierungsmethode zu erkennen und damit die Netzwerksicherheit und Effizienz des Unternehmens verbessern zu können.

1.2.1 Forschungsinteresse

Das Forschungsinteresse dieser Arbeit ist der klaren Bedarf in der heutigen IT-Infrastruktur. Als Mitglied des Infrastrukturteams bei Schrack Technik GmbH steht die Sicherheit der Netzwerkinfrastruktur immer im Fokus. Vorangegangene Projekte wie die Implementierung von "Microsoft Defender for Endpoints" haben gezeigt, wie wichtig eine umfassende

Sicherheitsstrategie ist. Dabei fiel das Augenmerk auf Network Access Control als potenzielles Mittel, um den Zugriff auf das Netzwerk effektiver zu steuern.

Aufgrund meiner spezialisierten Kenntnisse im Bereich Netzwerktechnik, die ich während meiner schulischen Ausbildung erworben habe, habe ich mich entschieden, diese Thematik näher zu erforschen. Mein Forschungsinteresse liegt darin, die Frage zu klären, welche der beiden verfügbaren Authentifizierungsmethoden – 802.1X oder MAC-based Authentication – am besten den wirtschaftlichen und technischen Anforderungen und Möglichkeiten der Firma Schrack Technik GmbH entspricht.

1.2.2 Konkrete wissenschaftliche Forschungsfrage

Die konkrete wissenschaftliche Forschungsfrage, die am Ende dieser Arbeit beantwortet sein wird, lautet: "Welche der beiden Authentifizierungsmethoden, nämlich 802.1X und MAC-based Authentication, erfüllt die wirtschaftlichen sowie technischen Anforderungen und Möglichkeiten der Firma 'Schrack Technik GmbH' passender?"

1.2.3 Hypothese

Auf Grundlage meines Vorwissen und meiner Analyse, komme ich zu dem Schluss, dass die Methode der MAC-based Authentication für das Beispiel der Firma Schrack Technik GmbH und deren spezifische wirtschaftlichen und technischen Kriterien die geeignetere Authentifizierungsmethode darstellt. Diese Annahme beruht auf einer groben Bewertung beider Methoden im Hinblick auf Sicherheit, Skalierbarkeit, Benutzerfreundlichkeit und Kosten.

Im Verlauf dieser Arbeit werde ich diese Hypothese weiter prüfen und die endgültige Schlussfolgerung auf Basis der gesammelten Daten und Ergebnisse ziehen.

1.3 Angestrebte Lösung

Die Hauptaufgabe dieser Bachelorarbeit besteht darin, eine umfassende und gut begründete Empfehlung für die Auswahl der optimalen Authentifizierungsmethode für die Firma Schrack Technik GmbH bereitzustellen. Es ist wichtig zu betonen, dass die Umsetzung dieser Empfehlung nicht unmittelbar Auswirkungen auf das Firmennetzwerk hat. Stattdessen dient die Arbeit als strategischer Leitfaden für künftige Entscheidungsprozesse bezüglich der Netzwerksicherheit und -effizienz.

Um dieses anspruchsvolle Ziel zu erreichen, setzt diese Arbeit auf eine sorgfältige und strukturierte Vorgehensweise, die auf dem bekannten Weighted Scoring Model basiert. Dieses Modell hat sich als äußerst effektiv erwiesen, insbesondere wenn es darum geht, zwischen verschiedenen Methoden oder Alternativen zu wählen und die Entscheidung auf einer Grundlage zu treffen.(Scholles 2018) Hier ist der schrittweise Ablauf dieser Vorgehensweise:

1. Formulierung der Anforderungen: Als erster Schritt werden klare und präzise Anforderungen an die Authentifizierungsmethoden definiert. Diese Anforderungen sind das Ergebnis einer gründlichen Analyse der Problemstellung (wie in Punkt 1.1 beschrieben) sowie des Forschungsinteresses (wie in Punkt 1.2 erwähnt). Ein entscheidender Aspekt hierbei ist die Gewichtung der einzelnen Anforderungen, da nicht alle von gleicher Wichtigkeit sind.
2. Bewertung der Methoden: Als nächstes erfolgt die systematische Bewertung der beiden Authentifizierungsmethoden, nämlich 802.1X und MAC-based Authentication, im Hinblick auf die definierten Anforderungen. Dabei werden objektive und messbare Kriterien herangezogen, um zu ermitteln, wie gut jede Methode diese Anforderungen erfüllt. Sowohl technische Anforderungen wie Sicherheit, Skalierbarkeit und Benutzerfreundlichkeit als auch wirtschaftliche Anforderungen wie Kosten werden in diese Bewertung einbezogen.
3. Gewichtete Bewertung: Im Anschluss werden die Bewertungen der Methoden mit den zuvor festgelegten Gewichtungen der Anforderungen multipliziert. Dadurch entsteht eine Gesamtbewertung für jede Methode. Es wird sichergestellt, dass die einzelnen Anforderungen aufgrund ihrer Gewichtung angemessen berücksichtigt wird.

4. Entscheidungsfindung: Schlussendlich dient die Gesamtbewertung als Entscheidungsbasis. Auf dieser Grundlage wird entschieden, welche der beiden Authentifizierungsmethoden am besten den eigenen Anforderungen und Zielen der Firma Schrack Technik GmbH entspricht.

Diese Vorgehensweise stellt sicher, dass die getroffene Entscheidung objektiv und auf die individuellen Anforderungen des Unternehmens ausgerichtet ist. Die Ergebnisse dieser Bachelorarbeit werden somit als Entscheidungsbasis für Schrack Technik GmbH dienen, wenn es darum geht, die Netzwerksicherheit durch eine Network Access Control Lösung zu stärken.

1.4 Leser*innenkreis

Die vorliegende Bachelorarbeit richtet sich an einen Leserkreis, der ein Interesse an den Herausforderungen der Netzwerksicherheit und der Auswahl geeigneter Authentifizierungsmethoden für Unternehmensnetzwerke hat.

Dieser Kreis umfasst:

1. Führungskräfte und Entscheidungsträger bei Schrack Technik GmbH: Die Ergebnisse dieser Arbeit werden für Führungskräfte und Verantwortliche bei Schrack Technik GmbH von entscheidender Bedeutung sein.
2. IT-Experten und Netzwerkadministratoren: Netzwerkexperten, Sicherheitsspezialisten und Administratoren bei Schrack Technik GmbH werden von den technischen Analysen und Erkenntnissen dieser Arbeit profitieren. Diese Leser werden in der Lage sein, die detaillierten Bewertungen der Authentifizierungsmethoden (wie in Punkt 1.2 beschrieben) zu nutzen, um technische Entscheidungen zu treffen und die Implementierung der ausgewählten Methode vorzubereiten.
3. Stakeholder und externe Interessengruppen: Neben internen Parteien bei Schrack Technik GmbH werden auch externe Stakeholder wie Kunden und Geschäftspartner ein Interesse an der Netzwerksicherheit des Unternehmens haben. Die Arbeit zeigt die

Absicht von Schrack Technik GmbH die Sicherheit im Unternehmensnetzwerk zu stärken, die für diese Gruppen von Interesse sein könnten.

Der Leserkreis dieser Arbeit zeigt, wie wichtig sie für die Netzwerksicherheits- und IT-Fachkräfte ist. Diese Bachelorarbeit verbindet die Problemstellung (Punkt 1.1), das Forschungsinteresse (Punkt 1.2) und das angestrebte Lösungsziel (Punkt 1.3), um einen Überblick über die Auswahl einer geeigneten Authentifizierungsmethode zu bieten. Diese Methode soll den wirtschaftlichen und technischen Anforderungen gerecht werden und somit dazu beitragen, die Netzwerksicherheit bei Schrack Technik GmbH zu stärken.

1.5 Strukturübersicht

Bachelorarbeit Teil I

Theorieteil: Themenaufbereitung, Literaturanalyse

- 1 - Einleitung
    - 1.1 Problemstellung/Motivation
    - 1.2 Ziel der Arbeit (Forschungsfrage, Hypothese)
    - 1.3 Angestrebte Lösung (Überblick der Methode, welche genutzt wird)
    - 1.4 Leser*innenkreis 1.5 Strukturübersicht

- 2 - Grundlagen und derzeitiger Stand von Wissenschaft und Technik
    - 2.1 Network Access Control
    - 2.2 Authentifizierung
        - 2.2.1 802.1X
        - 2.2.2 MAC based authentication (MBA)
    - 2.3 Stand der Wissenschaft
- 3 - Konzeptioneller Vorgehens- und Lösungsansatz
    - 3.1 Vorgehensmodell

- 3.2 Alternativen und deren Ausschlussgrund
- 3.3 Bewertung von Anforderungswichtigkeit (Wie habe ich vor die Wichtigkeit einer Anforderung zu bewerten)

Bachelorarbeit Teil II

Empirischer Teil: Experiment, Beantwortung der Forschungsfrage, Bewertung der Hypothese

- 4 - Aufstellung des Weighted Scoring Models
  - 4.1 Veranschaulichung der Netzwerkarchitektur
  - 4.2 Anforderungserfassung
  - 4.3 Gewichtungsvergabe
  - 4.4 Bewertungsmatrix

- 5 - Analyse der Ergebnisse
  - 5.1 Darstellung der Punktesumme pro Methode
  - 5.2 Ergebnis
  - 5.3 Erkenntnisse
- 6 - Schlussfolgerungen aus der Analyse und Beantwortung der Forschungsfrage
  - 6.1 Erinnerung an die Forschungsfrage und deren Nutzen
  - 6.2 Beantwortung der Forschungsfrage und Schlussfolgerung
- 7 - Zusammenfassung und Ausblick
- 8 – Literaturverzeichnis

Am Ende der Arbeit werden die Ergebnisse zusammengefasst und Schlussfolgerungen gezogen.

2. Grundlagen und derzeitiger Stand von Wissenschaft und Technik

2.1 Network Access Control (NAC)

Network Access Control (NAC) ist eine entscheidende Technologie, wenn es darum geht, die Sicherheit von Computernetzwerken zu gewährleisten. Denken Sie an Ihr Heimnetzwerk oder das Netzwerk in einem Unternehmen wie sehr viele digitale Straßen und Wege, über die Informationen fließen. Diese Informationen können sensible Unternehmensdaten, vertrauliche Kundendaten oder persönliche Informationen sein, die zu schützen sind. (Martinez, Stolfo, Keromytis 2008)

NAC handelt dabei wie ein „digitaler Sicherheitsdienst“. Es stellt sicher, dass nur diejenigen, die tatsächlich berechtigt sind, Zugang zu diesem Netzwerk bekommen. Dies ist entscheidend, um das Netzwerk vor Bedrohungen zu schützen, sei es von außen durch Hacker oder von innen durch menschliche Fehler.

Die Funktionsweise von NAC kann mit der eines Sicherheitsverantwortlichem an einem Eingangstor verglichen werden. Wenn Sie ein Gebäude betreten möchten, müssen Sie sich ausweisen. Das kann durch Vorzeigen eines Ausweises oder das Besitzen einer Eintrittskarte oder das Eingeben eines PIN-Codes erfolgen. Genauso verlangt NAC eine Überprüfung, um sicherzustellen, dass Benutzer und Geräte zugelassen sind, bevor sie Zugang zum Netzwerk erhalten.

Diese Überprüfung kann verschiedene Formen annehmen. Benutzer könnten aufgefordert werden, Benutzernamen und Passwörter einzugeben, die dann überprüft werden, ähnlich wie bei der Anmeldung bei einem E-Mail-Konto. Es ist wie die Verwendung eines Tickets, um Zugang zu einem Club zu erhalten.

In der Geschäftswelt ist die Sicherheit von Informationen von größter Bedeutung. NAC spielt eine zentrale Rolle dabei, sicherzustellen, dass nur diejenigen, die befugt sind, auf vertrauliche Daten zuzugreifen, dies auch tatsächlich können. Gleichzeitig hilft es, Cyberangriffe zu verhindern, indem es unerwünschte Gäste abwehrt. Daher ist NAC zu einem wesentlichen Bestandteil der Netzwerksicherheit in Unternehmen und Organisationen geworden. (Network Access Control 2007)

2.2 Authentifizierung

Die Authentifizierung ist ein Schlüsselkonzept, um die Identität von Benutzern und Geräten in einem Netzwerk sicherzustellen. Sie ist vergleichbar mit dem Identitätsnachweis, den Sie beim Betreten eines Sicherheitsgebäudes oder bei der Einreise benötigen. Authentifizierung bedeutet, dass Sie sich auf eine verlässliche Art und Weise gegenüber dem Netzwerk ausweisen müssen.

Hier sind zwei wichtige Methoden zur Authentifizierung:

2.2.1 802.1X Authentifizierung

Diese Methode ähnelt dem Entsperren Ihres Smartphones mit einem PIN oder Passwort. Wenn Sie sich in ein Netzwerk einloggen möchten, müssen Sie Ihren Benutzernamen und Ihr Passwort eingeben. Das Netzwerk prüft dann, ob diese Informationen korrekt sind, bevor es Ihnen Zugang gewährt. (Brown 2007)

2.2.2 MAC-basierte Authentifizierung (MBA)

Hier wird die einzigartige ID Ihres Geräts, die als MAC-Adresse bezeichnet wird, verwendet. Jedes Gerät hat seine eigene, eindeutige MAC-Adresse. MBA prüft, ob Ihre MAC-Adresse in einer Liste autorisierter Geräte steht. Wenn ja, erhalten Sie Zugang. Dies kann mit dem Überprüfen Ihres Namens auf der Gästeliste bei einer Veranstaltung verglichen werden.

Dies schützt nicht nur vertrauliche Informationen, sondern auch die Integrität des Netzwerks, indem es unautorisierten Zugang verhindert. Je nach den Anforderungen und Standards eines Unternehmens kann die tatsächliche Umsetzung und Komplexität dieser Authentifizierungsmethoden variieren. (Bicakci, Uzunay 2008)

2.3 Stand der Wissenschaft

Die Entwicklung der Informationstechnologie und die Vernetzung von Geräten haben in den letzten Jahren eine rasante Geschwindigkeit erreicht. Dies hat auch die Anforderungen an die Sicherheit von Netzwerken erheblich erhöht. Der Stand der Wissenschaft und Technik in Bezug auf Network Access Control (NAC) und Authentifizierungsmethoden unterliegt daher ständigen Neuangriffsmethoden und sicherheitstechnischem Fortschritt.

Die Digitalisierung hat unsere Welt vernetzter gemacht als je zuvor. Vom Internet der Dinge (IoT), bei dem Alltagsgegenstände miteinander kommunizieren(Wollert,Booke 2016), bis hin zu cloudbasierten Diensten, die in vielen Unternehmen genutzt werden, gibt es immer mehr Eintrittspunkte für mögliche Sicherheitsbedrohungen. Daher ist es von entscheidender Bedeutung, dass Sicherheitsprotokolle und Authentifizierungsmethoden ständig verbessert werden, um diesen wachsenden Herausforderungen entgegenwirken zu können.

Forscher und Experten auf dem Gebiet der Netzwerksicherheit sind stets bemüht, Wege zu finden, um Netzwerke sicherer zu machen. Dies umfasst die Entwicklung fortschrittlicherer und zuverlässigerer Authentifizierungsmethoden sowie die Verbesserung von NAC-Systemen.(Helmbrecht, Gneuß 2003)

Einige der aktuellen Entwicklungen im Bereich der Netzwerksicherheit und Authentifizierung sind folgende:

1. Biometrische Authentifizierung:
   Biometrische Merkmale wie Fingerabdrücke, Gesichtserkennung und Iris-Scan werden zunehmend als sichere Authentifizierungsmethoden eingesetzt. Diese Methoden bieten eine höhere Sicherheitsstufe, da sie auf einzigartigen körperlichen Merkmalen basieren. Diese zu fälschen ist unwahrscheinlich – und sie erraten/rausfinden wie Passwörter ist nicht möglich(Petermann, Sauter 2002)

2. Künstliche Intelligenz und maschinelles Lernen:
   Diese Technologien werden verwendet, um verdächtiges Verhalten und potenzielle Sicherheitsrisiken in Echtzeit zu erkennen. Sie ermöglichen eine proaktivere Reaktion auf Bedrohungen.(Schmidt 2020)

3. Blockchain-Technologie: Blockchain bietet die Möglichkeit, Identitätsdaten sicher zu speichern und zu verwalten. Dies kann die Authentifizierung und den Datenschutz verbessern.(Hasanova et al. 2019)

4. Zero Trust Security: Diese Herangehensweise geht davon aus, dass niemand im Netzwerk automatisch vertrauenswürdig ist, selbst wenn er bereits Zugang hat. Jeder Benutzer und jedes Gerät muss sich andauernd authentifizieren, um Zugang zu erhalten. (Flanigan 2018)

Die Netzwerksicherheitslandschaft ist dynamisch, und die besten Praktiken und Technologien ändern sich ständig. Es ist von entscheidender Bedeutung, dass Unternehmen und Organisationen auf dem neuesten Stand der Technik bleiben, um sicherzustellen, dass ihre Netzwerke gegen aktuelle und zukünftige Angriffsarten geschützt sind. Entwicklung in diesem Bereich ist daher von großer Bedeutung, um immer ein sicheres Netzwerk zu behalten – und gleichzeitig darf die Benutzerfreundlichkeit nicht verloren gehen.

Nun zum aktuellen Stand der Wissenschaft auf die von uns in dieser Arbeit gewählten Authentifizierungsmethoden. In diesem Punkt gehen wir genauer darauf ein, mit welchen Nachteilen hauptsächlich gerechnet werden muss bei den jeweiligen Methoden. Aber natürlich werden wir auch die Vorteile nennen und vergleichen.

Beginnend mit **MAC-basierter Authentifizierung:**

- Vorteile:
    1. Einfache Implementierung: MAC-basierte Authentifizierung ist einfach einzurichten und erfordert keine zusätzlichen Server oder komplexen Konfigurationen.
    2. Schnelle Identifizierung: Die Verwendung von MAC-Adressen zur Authentifizierung ermöglicht eine schnelle Identifizierung von Geräten im Netzwerk.
    3. Geeignet für kleine Netzwerke: Dieser Ansatz eignet sich gut für kleine Netzwerke, in denen die Verwaltung von Benutzern und Geräten weniger aufwendig ist.
- Nachteile:
    1. Mangelnde Sicherheit: MAC-Adressen können leicht gefälscht oder gespoofed werden, was die Sicherheit gefährden könnte. Als Vergleich die vorhin erwähnte Authentifizierungsmethode der biometrischen Authentifizierung – dort wäre dies nicht möglich bzw. sehr unrealistisch.
    2. Eingeschränkte Kontrolle: MAC-basierte Authentifizierung bietet eingeschränkte Kontrolle über den Netzwerkzugriff und die Berechtigungen, da sie auf der Identität des Geräts basiert und nicht auf Benutzerinformationen.
    3. Skalierbarkeitsprobleme: In größeren Netzwerken kann die Verwaltung der MAC-Adressen und deren Aktualisierung zeitaufwändig sein.

802.1X-Authentifizierung:

- Vorteile:
    1. Hohe Sicherheit: 802.1X bietet eine höhere Sicherheit, da es auf Benutzeridentitäten basiert und die Verwendung von Zertifikaten oder anderen Authentifizierungsmethoden ermöglicht.
    2. Skalierbarkeit: 802.1X ist in größeren Netzwerken gut skalierbar und ermöglicht eine effiziente Verwaltung von Benutzern und Geräten.

- Nachteile:
    1. Komplexität: Die Implementierung von 802.1X erfordert zusätzliche Infrastrukturkomponenten wie RADIUS-Server und die Konfiguration von Netzwerkgeräten, was komplexer sein kann.
    2. Höhere Kosten: Die Implementierung von 802.1X kann kostspielig sein, insbesondere wenn zusätzliche Hardware und Softwarelizenzen benötigt werden.
    3. Benutzererfahrung: In einigen Fällen kann die Einrichtung von 802.1X dazu führen, dass Benutzer sich jedes Mal authentifizieren müssen, wenn sie sich mit dem Netzwerk verbinden, was zu einem potenziellen Benutzerfreundlichkeitsproblem führe könnte.

Die Netzwerksicherheit und Angriffsmuster sind ein sehr komplexes Thema, da es ein „never-ending“ Thema ist, welches eine große Rolle in IT-Infrastrukturen in Zukunft übernehmen wird. (Epah 2009)

Zusammenfassend können wir festhalten, dass der Stand der Wissenschaft im Bereich Network Access Control (NAC) und Authentifizierungsmethoden ständig voranschreitet, um den steigenden Sicherheitsanforderungen in vernetzten Umgebungen gerecht zu werden. Dies ist insbesondere angesichts der fortschreitenden Digitalisierung und des vermehrten Einsatzes von IoT-Geräten von großer Bedeutung.

Die Auswahl zwischen diesen beiden Authentifizierungsmethoden hängt von den spezifischen Anforderungen des Netzwerks ab. 802.1X bietet eine höhere Sicherheit und mehr Kontrolle,

erfordert jedoch mehr Aufwand bei der Implementierung. MAC-basierte Authentifizierung ist einfacher, aber weniger sicher. Die Wahl sollte also unter Berücksichtigung von Sicherheitsanforderungen, Budget und Benutzererfahrung getroffen werden.

3 Konzeptioneller Vorgehens- und Lösungsansatz

3.1 Vorgehensmodell

Im Rahmen der Bachelorarbeit wird das Weighted Scoring Modell angewendet, um eine Bewertung und Priorisierung von Lösungsalternativen durchzuführen. Dieses Modell ist insbesondere geeignet, um verschiedene Alternativen auf Basis definierter Kriterien zu analysieren und ihre Eignung für die speziellen Anforderungen zu bewerten. Die Anwendung des Weighted Scoring Modells umfasst mehrere Schlüsselschritte:

- Anforderungsfestlegung:
  Zunächst werden die relevanten Anforderungen identifiziert, die bei der Bewertung der Lösungsalternativen berücksichtigt werden sollen. Diese werden in enger Abstimmung mit den Zielen des Unternehmens Schrack Technik GmbH festgelegt.

- Gewichtung der Anforderungen: Wie die Anforderungen gewichtet werden, wird in Kapitel 3.2 genauer beschrieben.

- Bewertung der beiden Möglichkeiten: Die Lösungsalternativen werden anhand der zuvor festgelegten Anforderungen analysiert und bewertet. Dabei kann dies Kriterien wie Kosten, Ressourcenaufwand, Nutzerfreundlichkeit und Skalierbarkeit umfassen.

- Punktevergabe: Jede Lösungsalternative erhält Punkte basierend auf ihrer Erfüllung der einzelnen Kriterien. Diese Punkte werden unter Berücksichtigung der Gewichtung der Kriterien zusammengefasst, um einen Gesamtwert für jede Alternative zu erhalten.

Anhand der Gesamtwerte können die Lösungsalternativen miteinander werden. Dies ermöglicht es, diejenige Alternative zu identifizieren, die am besten geeignet ist, um die gestellten Anforderungen und Ziele zu erfüllen.

3.2 Bewertung von Anforderungswichtigkeit

Um eine Gewichtung der Anforderung festlegen zu können, muss dessen Wichtigkeit erstmal bewertet werden. Dies funktioniert wie folgt:

1. Kriterienauswahl: Zunächst definieren wir die Kriterien, anhand derer wir die Anforderungen bewerten. Diese Kriterien können beispielsweise Kundennutzen, Geschäftswert, technische Machbarkeit und Compliance-Anforderungen sein.

2. Gewichtung der Kriterien: Wir vergeben Gewichtungen für jedes Kriterium, um deren relative Bedeutung festzulegen. Dies erfolgt in enger Abstimmung mit den Stakeholdern und unter Berücksichtigung von Expertenmeinungen.

3. Bewertung der Anforderungen: Jede Anforderung wird anhand der definierten Kriterien bewertet und mit einem Nutzwert versehen.

4. Berechnung des Gesamtnutzwerts: Der Gesamtnutzwert für jede Anforderung ergibt sich durch die Multiplikation der einzelnen Nutzwerte mit den Gewichtungen der zugehörigen Kriterien und deren Summierung.

5. Priorisierung: Anhand der Gesamtnutzwerte werden die Anforderungen in absteigender Reihenfolge priorisiert. Anforderungen mit höheren Nutzwerten haben eine höhere Wichtigkeit für das Projekt.

Zusammenfassend ermöglicht die Anwendung des Weighted Scoring Modells in Verbindung mit der Bewertung von Anforderungswichtigkeit eine strukturierte und transparente Herangehensweise. Die folgenden Kapitel werden detailliert auf die Umsetzung dieser Methoden eingehen und zeigen, wie sie angewendet werden, um eine Entscheidungsgrundlage für die anstehenden Herausforderungen bei Schrack Technik GmbH zu schaffen.

4. Aufstellung des Weighted Scoring Models

Bei der Erstellung eines Weighted Scoring Models für die Auswahl von Authentifizierungsmethoden ist es von zentraler Bedeutung, sich mit den Netzwerkkomponenten vertraut zu machen. Diese bilden die Grundlage für Kriterien, die bei der Bewertung von Authentifizierungsoptionen eine Rolle spielen. In diesem Abschnitt wird die Erfassung von Anforderungen und die Gewichtung dieser Kriterien diskutiert, wobei das Ziel ist, die Authentifizierungsmethoden anhand von Erfüllung dieser Kriterien und jegliche anderen Anforderungen zu vergleichen. Dazu ist es nötig, die Netzwerkkomponenten zu identifizieren, um ein klares Verständnis für die Funktion und Interaktion zu haben. Danach müssen die Netzwerkanforderungen analysiert werden – ist es überhaupt möglich diese Authentifizierungsmethode zu integrieren, wie viel Aufwand steckt dahinter und wie viel Geld wird dieses Projekt kosten – all dies sind offene Fragen, die in dem folgenden Abschnitt dieser Bachelorarbeit beantwortet werden.

Da für das Weighted Scoring Model Anforderungen notwendig sind, anhand dessen die beiden Authentifizierungsmethoden verglichen werden, wurde wie in Kapitel 3.1 erwähnt, mit enger Abstimmung der Ziele des Unternehmens Schrack Technik GmbH vier Punkte festgelegt, anhand denen das Scoring Model aufgebaut wird. Diese sind:

- Kompatibilität (40%)
- Sicherheitsvorteile und bekannte Sicherheitslücken (40%)
- Implementierungsaufwand (10%)
- Preis-Leistungsverhältnis (10%)

Kompatibilität und Sicherheit haben die gleiche Gewichtung (40%), da das eine ohne dem anderem unbrauchbar wird – sei es ein kompatibles System mit einem höheren Sicherheitsrisiko oder einem sicheren System, welches in das Firmennetzwerk nicht integrierbar ist oder eine zu

große Umstellung erfordert. Der Implementierungsaufwand und die Kosten sind zweitrangig (10% jeweils), aber sollen bei einem Gleichstand ausschlaggebend sein.

4.1 Veranschaulichung der Netzwerkarchitektur

Um die Netzwerkkomponenten zu kennen, wird in diesem Punkt die Netzwerkarchitektur genauer beschrieben und anhand von Abbildungen veranschaulicht. Da es aus Sicherheitstechnischen Gründen nicht möglich ist, die genaue Netzwerkarchitektur darzustellen, wird dies verallgemeinert veranschaulicht. Dies reicht für die Veranschaulichung und Beantwortung unserer Forschungsfrage aus. Die Grundidee jedes Unternehmensnetzwerk ist sehr ähnlich, da dies Anforderungen an ein sicheres Netzwerk sehr ähnlich sind. Grob beschrieben sieht die Netzwerkarchitektur eines Unternehmens wie folgt aus:

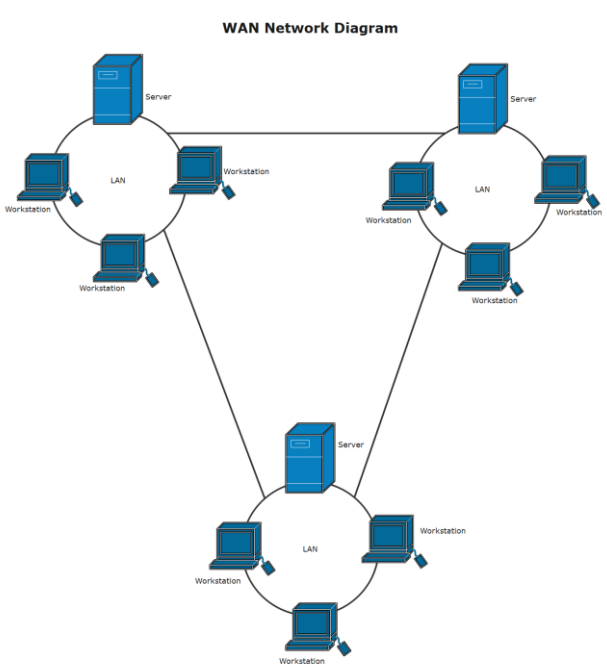
- Zentrales Rechenzentrum

  Hier befinden sich die zentralen Server und Ressourcen des Unternehmens. Firewall und Intrusion Detection/Prevention System (IDS/IPS) schützen den Datenverkehr. Dies kann aber muss nicht selbst betrieben werden, kann z.B. auch bei einem Datenzentrum „gemietet“ werden. Ob der Vermieter diese auch technisch betreut oder die Firma selbst, kann meist selbst entschieden werden.

- WAN (Wide Area Network)

  Da es sich um eine Firma mit vielen Standorten handelt, ist ein WAN (Wide Area Network) natürlich notwendig, um die verschiedenen Standorte des Unternehmens miteinander zu verbinden. Um sich das ganze vorstellen zu können, nachfolgend die Skizze.

Ein WAN ist nur notwendig, wenn mehrere LAN (Local Area Network) miteinander kommunizieren müssen (in unserem Fall die verschiedenen Standorte).



Jeder Standort hat lokale Server und Ressourcen, die für spezifische Aufgaben benötigt werden.

- **Router und Switches**

  Leiten den Datenverkehr zwischen den Standorten und dem zentralen Rechenzentrum. Quality of Service (QoS) wird implementiert, um die Priorisierung von Datenverkehr sicherzustellen.

- **Firewalls**

  Jeder Standort verfügt über eine Firewall für lokale Sicherheit und um den Verkehr zu überwachen. VPN (Virtual Private Network) für sichere Kommunikation über unsichere Netzwerke.

- **Internetzugang**

  Jeder Standort hat einen sicheren Internetzugang über Firewalls. Content-Filtering und Malware-Schutz sind implementiert.

- **Wireless LAN (WLAN)**

  Drahtlose Netzwerke für mobile Geräte und flexible Arbeitsplatzgestaltung. Sicherheit durch WPA3-Verschlüsselung und Authentifizierung.

- **Monitoring und Management**

  Einsatz von Netzwerkmanagement-Tools zur Überwachung der Netzwerkperformance und zur Fehlerbehebung.

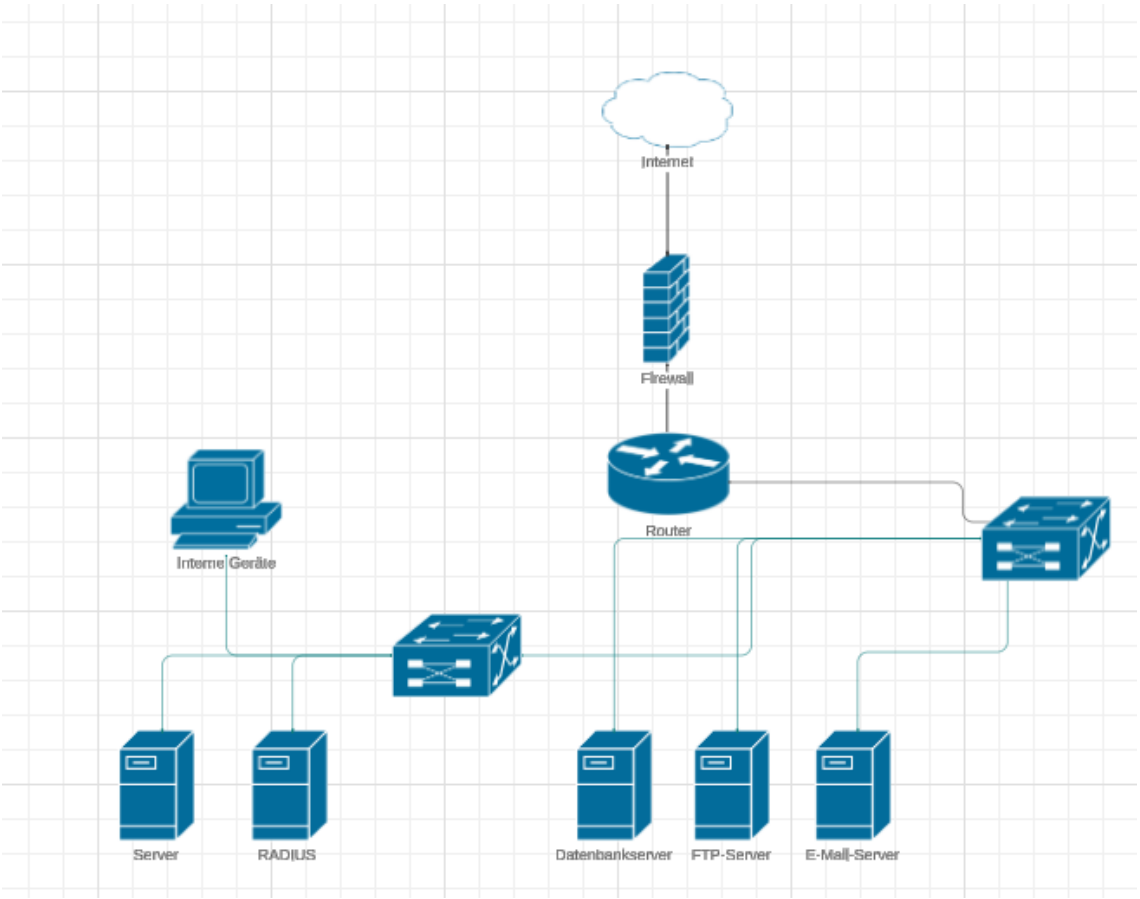
- **Backup und Disaster Recovery**

  Regelmäßige Datensicherungen an den Standorten und im zentralen Rechenzentrum. Notfallwiederherstellungspläne für kritische Systeme.

- **Clients**

  Natürlich nicht zu vergessen und auch eine sehr wichtige Anforderung. Geräte wie Notebooks, Drucker usw. die für das tägliche Arbeiten der Mitarbeiter unverzichtbar sind.

Um sich das Ganze vorstellen zu können, wurde eine Demoskizze angefertigt, wie das Ganze aussehen könnte.



Diese Skizze soll einen sehr einfachen Aufbau eines Netzwerkes darstellen – mit den üblichen notwendigen Komponenten sei es in diesem Fall Clients, Server, Switche, Router oder Firewalls.

4.2 Anforderungserfassung

Beide Authentifizierungsmethoden haben gewisse Anforderungen, um implementiert werden zu können. Da überprüft werden muss, ob die Netzwerkarchitektur dies zulässt – musste eine Recherche zu den Anforderungen der Authentifizierungsmethoden durchgeführt werden.

4.2.1 Kompatibilität

MAC-basierte Authentifizierung:

- Whitelist-Management:
  Dient dazu, autorisierten Geräten den Zugriff zu ermöglichen und unbefugte Geräte auszuschließen.

- Sicherheitsmechanismen:
  Implementierung zusätzlicher Sicherheitsmechanismen, um MAC-Spoofing und andere Manipulationsversuche zu erkennen und zu verhindern.

802.1X-Authentifizierung:

- Radius-Server Integration:
  Integration mit einem Radius-Server für die zentrale Verwaltung von Authentifizierungsinformationen und -richtlinien.

- Zertifikatsinfrastruktur (PKI):
  Implementierung einer Zertifikatsinfrastruktur (Public Key Infrastructure, PKI) für die sichere Übertragung von Authentifizierungsinformationen und um Vertrauenswürdigkeit sicherzustellen.

- Client-Zertifikate:
  Es wird benötigt, dass die Geräte gültige "Ausweis"-Zertifikate besitzen, um sich im Netzwerk anmelden zu können.

- Benutzer-Authentifizierung:
  Dadurch besteht die Möglichkeit, die Identität der Benutzer zu prüfen, um den Zugriff auf Netzwerkdienste je nach Position/Rechten zu steuern.

4.2.2 Sicherheit

MAC-basierte Authentifizierung:

Sicherheitsvorteile:

- Eindeutige Geräteidentifikation:
  MAC-basierte Authentifizierung ermöglicht die Identifikation von Geräten anhand ihrer eindeutigen MAC-Adressen. Dies erleichtert die Erkennung und Autorisierung von bekannten Geräten im Netzwerk.

Sicherheitslücken**:**

- MAC-Spoofing:
  Ein potenzielles Risiko besteht in der Möglichkeit des MAC-Spoofing, bei dem ein Angreifer versucht, die MAC-Adresse eines autorisierten Geräts zu kopieren.

- Manuelle Whitelist-Verwaltung:
  Die manuelle Verwaltung von MAC-Adressen-Whitelists kann zu Sicherheitslücken führen, wenn sie nicht aktualisiert und überwacht wird.

- Fehlende Benutzeridentifikation:
  Da die Authentifizierung ausschließlich auf der MAC-Adresse basiert, erfolgt keine Benutzeridentifikation. Ein einmal autorisiertes Gerät hat unter Umständen uneingeschränkten Zugriff, unabhängig vom Benutzer.

802.1X-Authentifizierung:

Sicherheitsvorteile:

- Starke Authentifizierung:
  802.1X bietet eine starke Authentifizierung durch das Einsetzen von Benutzer- und Gerätezertifikaten, was eine höhere Sicherheit im Vergleich zur MAC-basierten Authentifizierung ermöglicht.

- Dynamische Re-Authentifizierung:
  Die Möglichkeit zur dynamischen Re-Authentifizierung sorgt dafür, dass Geräte während einer laufenden Sitzung regelmäßig überprüft werden, um sicherzustellen, dass sie weiterhin den Sicherheitsrichtlinien entsprechen.

- Benutzerbasierte Zugriffskontrolle:
  Durch die Integration von Benutzeridentitäten wird es möglich, den Zugriff auf Ressourcen sehr genau anhand der Benutzerprofile zu steuern.

- Zentrale Verwaltung mit Radius-Server:
  Die Verwendung eines Radius-Servers ermöglicht eine zentrale Verwaltung von Authentifizierungsinformationen und -richtlinien.

Sicherheitslücken:

- Benutzerfreundlichkeit:
  Die Notwendigkeit von Benutzerzertifikaten kann viel Arbeit erzeugen, insbesondere in Umgebungen mit vielen Endbenutzern.

- Potenzielle Angriffe auf den Radius-Server:
  Ein Radius-Server ist ein kritischer Punkt in der 802.1X-Infrastruktur, und ein Angriff darauf könnte die gesamte Umgebung gefährden.

In vielen Fällen wird eine Kombination beider Methoden als sinnvoll erachtet, um die Vorzüge beider Ansätze zu nutzen und potenzielle Schwächen zu minimieren.

4.2.3 Implementierungsaufwand

MAC-basierte Authentifizierung:

- Einfache Konfiguration:
  Die MAC-basierte Authentifizierung ist eine einfache Konfiguration auf Netzwerkgeräten wie Switches oder Access Points. Es müssen lediglich die MAC-Adressen der autorisierten Geräte in eine Whitelist eingetragen werden.

- Geringe Infrastrukturanforderungen:
  Im Vergleich zu 802.1X erfordert die MAC-basierte Authentifizierung weniger komplexe Infrastrukturelemente. Es ist keine Zertifikatsinfrastruktur (PKI) oder ein Radius-Server notwendig.

802.1X-Authentifizierung:

- Infrastrukturanforderungen:
  Die Implementierung von 802.1X erfordert eine sorgfältige Planung und die Bereitstellung zusätzlicher Infrastrukturelemente wie eines Radius-Servers und einer Zertifikatsinfrastruktur (PKI).

- Radius-Server Integration:
  Die Integration eines Radius-Servers ist ein sehr wichtiger Schritt. Dies erfordert die Konfiguration des Servers selbst sowie die Synchronisation mit dem Active-Directoy (Benutzerdatenbank) des Unternehmens.

- Zertifikatsverwaltung:
  Die Einführung von Zertifikaten für Geräte und Benutzer erfordert eine Zertifikatsverwaltung – welche die Ausstellung, Verteilung und Aktualisierung von Zertifikaten übernimmt.

- Schulungsaufwand:
  Da die Implementierung komplexer ist, erfordert die 802.1X-Authentifizierung mehr Schulungsaufwand für das IT-Personal.

Insgesamt kann gesagt werden, dass die MAC-basierte Authentifizierung aufgrund ihrer Einfachheit und geringeren Anforderungen an die Netzwerkinfrastruktur schneller implementiert werden kann. 802.1X hingegen bietet eine höhere Sicherheitsstufe, erfordert jedoch einen höheren Implementierungsaufwand und Ressourceneinsatz.

4.2.4 Kosten

MAC-basierte Authentifizierung:

- Hardwarekosten:
  MAC-basierte Authentifizierung erfordert keine zusätzliche Hardware außer den vorhandenen Netzwerkgeräten wie Switches oder Access Points.

- Lizenzkosten:
  Es fallen keine Lizenzkosten für spezielle Authentifizierungssoftware an, da die Netzwerkgeräte der Firma diese Funktionen standardmäßig besitzen.

- Schulungskosten:
  Schulungskosten können minimal sein, da die Implementierung relativ einfach ist und Administratoren bereits mit den grundlegenden Netzwerkkonfigurationen vertraut sind.

- Sicherheitslücken:
  Der potenzielle Schaden durch Sicherheitslücken, insbesondere durch MAC-Spoofing, könnte zu höheren Kosten führen, wenn zusätzliche Sicherheitsmaßnahmen implementiert oder Vorfälle behandelt werden müssen.

802.1X-Authentifizierung:

- Hardwarekosten:
  802.1X erfordert zusätzliche Hardwarekomponenten wie einen Radius-Server. Dies ist mit Hardware- und Lizenzkosten verbunden.

- Softwarelizenzen:
  Die Implementierung eines Radius-Servers und einer Zertifikatsinfrastruktur verursacht Lizenzkosten für die entsprechende Software.

- Zertifikatsinfrastruktur (PKI):
  Die Einrichtung einer PKI für die Verwaltung von Zertifikaten kann zusätzliche Kosten für Hardware, Software und Schulung mit sich bringen. In unserem Fall existiert bereits eine PKI, diese muss lediglich erweitert werden.

- Schulungskosten:
  Aufgrund der Komplexität der Implementierung sind Schulungskosten für IT-Personal höher. Aber auch dies sollte nicht sehr hohe Kosten in unserem Fall verursachen, da die Mitarbeiter mit den meisten Themen schon bei anderen Projekten zu tun hatten.

Im Allgemeinen lassen sich die Kosten für die MAC-basierte Authentifizierung oft als geringer einschätzen. Dies resultiert aus einem geringeren Bedarf an spezieller Hardware und Software. Im Gegensatz dazu sind die Gesamtkosten für die Implementierung von 802.1X höher. Dies liegt an den komplexeren Anforderungen an die Infrastruktur. Dies wird auch in dem Fall der Firma Schrack Technik GmbH nicht anders sein, jedoch bewegt sich das Ganze in einem angemessenem Rahmen. Konkrete Zahlen können nicht genannt werden, da diese erst bei einer offiziellen Angebotsanfrage genannt werden.

4.3 Bewertung

Um nun schlussendlich Daten zu erfassen, mit denen das Model aufgestellt werden kann, wurde Teil 4 dieser Bachelorarbeit dem Netzwerkteam (bestehend aus drei Mitarbeitern) und zwei Systemadministratoren mit Security-Kenntnissen vorgelegt. Warum genau diese Personen befragt wurden ist einfach zu erklären – denn die folgenden Fragen für diesen speziellen Fall zu beantworten, ist ohne ein Verständnis zu dem Unternehmensnetzwerk und der IT-Infrastruktur nicht möglich. Bei einer einzigen Frage, nämlich der des Implementierungsaufwandes, wurde ein externer Partner, welcher dies aufgrund seiner Arbeit an mehreren ähnlichen Projekten besser einschätzen kann, einbezogen. Nun zu den Fragen:

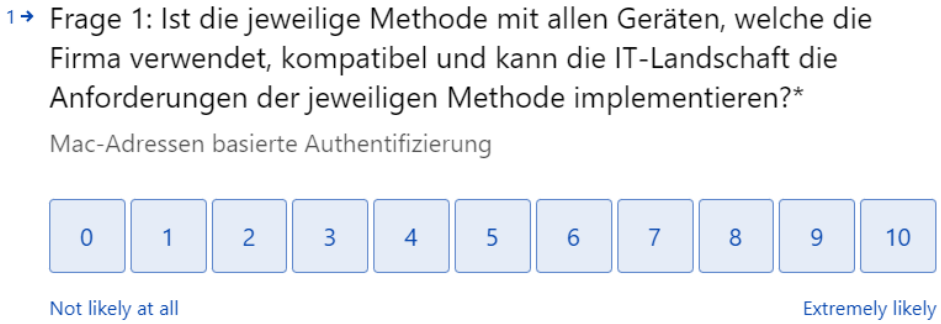
1. **Frage 1**: Ist die jeweilige Methode mit allen Geräten, welche die Firma verwendet, kompatibel und kann die IT-Landschaft die Anforderungen der jeweiligen Methode implementieren?

2. **Frage 2:** Wie hoch schätzt man den Sicherheitsstandard der jeweiligen Methode in Betracht des IT-Netzwerkes?

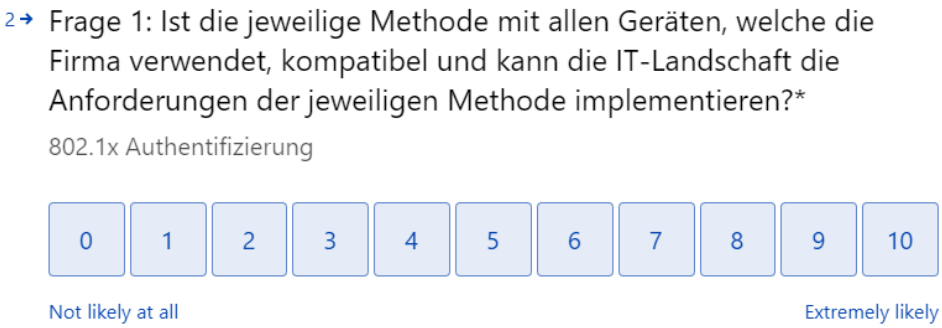
3. **Frage 3:** Bewerten Sie das Preis-Leistungsverhältnis der beiden Methoden, indem die dafür notwendigen Anforderungen (Radius-Server usw.) in Kosten abgeschätzt werden. Die Leistung kann durch die Antwort auf Frage 1 und 2 gemessen werden.

Für die Beantwortung dieser Fragen wurde ein Punktesystem verwendet. Als zulässige Antwort können die Punkte 0-10 vergeben werden, wobei 0 für trifft überhaupt nicht zu und 10 für trifft sehr zu steht.

Für die Umfrage wurde das kostenlose Online-Tool Type form verwendet. Die Umfrage wurde erstellt und dann per Link an unsere 4 Teilnehmer versendet. Folgend sieht man einen Ausschnitt aus der Umfrage.



Jede Frage gab es selbstverständlich für Mac-based Authentifizierung sowie für 802.1x Authentifizierung.



Nachdem die Teilnehmer an der Umfrage teilgenommen haben, konnte das Ergebnis aus dem „Creator-Portal“ angeschaut werden. Dabei sind folgende Werte gewählt worden.

Frage 1: Ist die jeweilige...	Frage 1: Ist die jeweilige...	Frage 2: Wie hoch schätzt...	Frage 2: Wie hoch schätzt...	Frage 3: Bewerten Sie...	Frage 3: Bewerten Sie das Preis-Leistungsverhältnis der beiden Methoden,...
10	9	3	10	7	9
10	8	2	9	6	7
10	8	4	10	7	9
10	6	5	9	9	7

Frage 1 – MBA → 10,10,10,10

Frage 1 – 802.1x → 9,8,8,6

Frage 2 – MBA → 3,2,4,5

Frage 2 – 802.1x → 10,9,10,9

Frage 3 – MBA → 7,6,7,9

Frage 3 – 802.1x → 9,7,9,7

Um das Ganze nochmal zu verdeutlichen, folgende Kriterien wurden in Punkt 4 für das Model herangezogen:

- Kompatibilität (40%)
- Sicherheitsvorteile und bekannte Sicherheitslücken (40%)
- Implementierungsaufwand (10%)
- Preis-Leistungsverhältnis (10%)

Frage 1 diente dazu den Punkt „Kompatibilität“ zu bewerten -> Je höher die Punkte, desto mehr ist die Methode kompatibel

Frage 2 diente dazu den Punkt „Sicherheitsvorteile und bekannte Sicherheitslücken“ zu bewerten – desto höher die Punkte, desto höher der Sicherheitsgrad.

Frage 3 diente dazu den Punkt „Preis-Leistungsverhältnis“ zu bewerten -> desto höher die Punkte, desto besser das Preis-Leistungsverhältnis.

Um zu guter Letzt den fehlenden Punkt bewerten zu können, wurde einem externen Partner der Firma Schrack Technik GmbH die Frage gestellt, wie hoch der Implementierungsaufwand in dem Firmennetzwerk der Firma Schrack Technik sei, wobei die möglichen Antworten ebenfalls 0-10 sind. Diesmal stand 0 für sehr hoch und 10 für sehr gering. Daher bedeutet auch in diesem Fall, desto höher die Punkte, desto besser. Es kamen dabei folgende Ergebnisse zustande:

MBA (Mac-based Authentifizierung) → 7

802.1x Authentifizierung → 5

5. Analyse der Ergebnisse

In diesem Punkt werden die erzielten Ergebnisse nochmals mithilfe einer Tabelle präsentiert und schlussendlich analysiert und interpretiert.

5.1 Darstellung der Punktesumme pro Methode und Ergebnisse

In der Tabelle sieht man alle Antworten der Teilnehmenden sowie die Antwort des externen Spezialisten nochmal übersichtlich angeführt.

Um den Aufbau der Tabelle zu verstehen, kann diese wie folgt verstanden werden: Es wurde von jedem Teilnehmer jede Frage beantwortet, daher werden links alle Teilnehmer in Zeilen genannt. In den jeweiligen Spalten sind die Fragen, welche ihnen gestellt wurden, jede Frage zwei Mal – da jede Frage für beide Methoden gestellt wurde. Die Teilnehmer konnten die Punkte 0-10 vergeben.

	Frage 1 (MBA)	Frage 1 (802.1X)	Frage 2 (MBA)	Frage 2 (802.1X)	Frage 3 (MBA)	Frage 3 (802.1X)	Frage 4 (MBA)	Frage 4 (802.1x)
Teilnehmer1	10	9	3	10	7	9		
Teilnehmer2	10	8	2	9	6	7		
Teilnehmer3	10	8	4	10	7	9		
Teilnehmer4	10	6	5	9	9	7		
Teilnehmer5(ext. Partner)							7	5

Um daraus nun ein Ergebnis ableiten zu können, ist die nachfolgende Tabelle erstellt worden. Hier wurde in den Zeilen nochmal die Kriterien herangeholt, welche in Kapitel 4 festgelegt worden sind. Da wir vergleichen, stellen wir die beiden Methoden in den Spalten gegenüber. Um nun zu Ergebnissen in Sachen Kompatibilität, Sicherheitsvor- und – Nachteile, Implementierungsaufwand und Preis/Leistungsverhältnis zu kommen, wurden die Summe der Punkte für das jeweilige Kriterium gebildet und dann durch die Anzahl der Teilnehmer dividiert.

Kriterium (Gewicht)	Methode1 (MBA)	Methode2 (802.1x)
Kompatibilität (40%)	(10+10+10+10)/4	(9+8+8+6)/4
Sicherheitsvorteile - und Lücken (40%)	(3+2+4+5)/4	(10+9+10+9)/4
Implementierungsaufwand (10%)	7	5
Preis-Leistungsverhältnis (10%)	(7+6+7+9)/4	(9+7+9+7)/4

Nun wird das Gewicht jedes Kriteriums mit dem erreichten Durchschnittspunktewert multipliziert und danach alle Kriterien Ergebnisse addiert. Dies sieht dann wie folg aus:

Methode1 (MBA) → (10*0,4) + (3,5*0,4) + (7*0,1) + (7,25*0,1) = 4 + 1,4 + 0,7 + 0,725 = **6,825**

Methode2 (802.1x) → (7,75*0,4) + (9,5*0,4) + (5*0,1) + (8*0,1) = 3,1 + 3,8 + 0,5 + 0,8 = **8,2**

5.2 Erkenntnisse

Die Ergebnisse des Weighted Scoring Models deuten darauf hin, dass die 802.1X-Authentifizierung im Vergleich zur MAC-basierten Authentifizierung in mehreren Schlüsselbereichen überlegen ist. Insbesondere zeigt sich eine deutliche Überlegenheit in Bezug auf Sicherheitsaspekte. Hier sind die Hauptpunkte:

- Kompatibilität:
  Die MAC-basierte Authentifizierung erzielt einen höheren Score von 4 im Vergleich zu 3,1 für 802.1X. Dies deutet darauf hin, dass die MAC-basierte Authentifizierung besser mit bestehenden Geräten und Systemen kompatibel ist.

- Sicherheitsvorteile und bekannte Sicherheitslücken:
  Die 802.1X-Authentifizierung zeigt einen signifikant höheren Score von 3,8 im Vergleich zu 1,4 für die MAC-basierte Authentifizierung. Dies unterstreicht die wahrgenommene Überlegenheit der 802.1X-Authentifizierung in Bezug auf Sicherheitsaspekte und potenzielle Sicherheitsrisiken.

- Implementierungsaufwand:
  Der Implementierungsaufwand ist geringfügig niedriger für 802.1x(Score von 0,5) im Vergleich zu MAC-basierte Authentifizierung (Score von 0,7). Dies bedeutet bei unserer Skala jedoch, dass der Implementierungsaufwand für 802.1x höher ist als jener von MBA, da ein höheres Rating in diesem Fall bedeutet, dass die Implementierung einfacher ist.

- Preis-Leistungsverhältnis:
  Die 802.1X-Authentifizierung weist einen höheren Score von 0,8 auf im Vergleich zu 0,725 für die MAC-basierte Authentifizierung. Dies lässt darauf schließen, dass 802.1X als kostengünstiger betrachtet wird.

Gesamtbetrachtung:

Die kumulierten Ergebnisse legen nahe, dass die 802.1X-Authentifizierung als insgesamt vorteilhafter für die Netzwerksicherheit betrachtet wird.

Trotz einer höheren Bewertung in der Kategorie Kompatibilität für die MAC-basierte Authentifizierung könnten die überlegenen Sicherheitsmerkmale und andere Vorteile der 802.1X-Authentifizierung für Schrack Technik von größerer Bedeutung sein, abhängig von den spezifischen Anforderungen und Prioritäten des Unternehmens.

6. Schlussfolgerungen aus der Analyse und Beantwortung der Forschungsfrage

Im Rahmen der Forschungsfrage, welche der beiden Authentifizierungsmethoden (802.1X und MAC-basierte Authentifizierung) besser den wirtschaftlichen und technischen Anforderungen der Firma "Schrack Technik GmbH" entspricht, ergeben die vorliegenden Daten eine klare Tendenz. Die Evaluierung der gewichteten Scores für die definierten Kriterien - Kompatibilität, Sicherheitsvorteile und bekannte Sicherheitslücken, Implementierungsaufwand sowie Preis-Leistungsverhältnis - zeigt, dass die 802.1X-Authentifizierung in den meisten Aspekten überlegen ist. Insbesondere im Bereich der Sicherheit, einem essenziellen Faktor für Schrack Technik, erzielt die 802.1X-Authentifizierung deutlich höhere Werte im Vergleich zur MAC-basierten Authentifizierung. Der Implementierungsaufwand ist minimal unterschiedlich, und das Preis-Leistungsverhältnis zeigt keine signifikanten Unterschiede. Daher lässt sich schlussfolgern, dass die 802.1X-Authentifizierung besser geeignet ist, die Sicherheitsanforderungen von Schrack Technik zu erfüllen.

Entgegen der vorab formulierten Hypothese, die postulierte, dass die MAC-basierte Authentifizierung die geeignetere Methode für die spezifischen wirtschaftlichen und technischen Kriterien von Schrack Technik sei, ergibt die Datenauswertung eine abweichende Schlussfolgerung. Die 802.1X-Authentifizierung scheint besser geeignet, die Sicherheitsanforderungen von Schrack Technik zu erfüllen. Dies unterstreicht die Notwendigkeit einer detaillierten Analyse, um die spezifischen Anforderungen des Unternehmens umfassend zu verstehen und eine fundierte Entscheidung zu treffen. Diese Arbeit sollte einen essenziellen Beitrag dazu leisten.

7. Zusammenfassung und Ausblick

Die eingehende Analyse der Authentifizierungsmethoden, MAC-basierte Authentifizierung und 802.1X, im Kontext der wirtschaftlichen und technischen Anforderungen der Firma "Schrack Technik GmbH", zeigt deutlich, dass die 802.1X-Authentifizierung überlegen ist, insbesondere in Bezug auf Sicherheitsaspekte. Obwohl die MAC-basierte Authentifizierung in Bezug auf Kompatibilität höhere Scores erzielte, unterstreichen die höheren Sicherheitswerte der 802.1X-Authentifizierung deren Eignung für die Netzwerksicherheit von Schrack Technik. Diese Erkenntnisse werfen ein neues Licht auf die anfängliche Hypothese, die die MAC-basierte Authentifizierung als geeignetere Methode für Schrack Technik postulierte.

Ausblick:

Um eine fundierte Entscheidung zu treffen, ist es ratsam, einen weiteren Blick in die Zukunft zu werfen. Hierbei empfehle ich, eine detaillierte Analyse der Bedürfnisse von Schrack Technik durchzuführen, um die spezifischen Anforderungen besser zu verstehen. Diese Analyse könnte auch eine Bewertung der aktuellen Netzwerkinfrastruktur und möglicher zukünftiger Entwicklungen einschließen. Es wäre sinnvoll, Gespräche mit IT-Sicherheitsexperten zu führen und möglicherweise kleinere Testimplementierungen (Pilotimplementierungen) in Betracht zu ziehen. Ein umfassender Blick auf die langfristigen strategischen Ziele von Schrack Technik im Bereich Netzwerksicherheit wird dazu beitragen, die am besten geeignete Methode zur Authentifizierung auszuwählen. Diese Methode sollte nicht nur den aktuellen Anforderungen gerecht werden, sondern auch für zukünftige Entwicklungen gut gerüstet sein.

Literaturverzeichnis

Müller Marion.2022."Unternehmen erleiden hohe Schäden durch Datendiebstahl" Die Aktiengesellschaft, 01.Dezember

Engländer Jacques, Kaminski Lars, Majchrzak Anna, Bülskämper Martin .2021. "Cybersicherheit und Schwachstellen in produzierenden Unternehmen." Whitepaper,FIR e.V. an der RWTH Aachen, Aachen.

Ehsan Amiri, Elham Afshar, Hamid Reza Naji, Mahdi Maleknasab Ardekani. 2012. "Survey on network access control technology in MANETs" International Conference on Innovation Management and Technology Research, pp.367-372.

Scholles Frank .2018. "Bewertungs- und Entscheidungsmethoden" ARL – Akademie für Raumentwicklung in der Leibniz-Gemeinschaft, Hannover, S.118

Frias-Martinez V., Stolfo S.J., Keromytis A.D., 2008. Behavior-Based Network Access Control: A Proof-of-Concept. In: Information Security. Berlin, Heidelberg. https://doi.org/10.1007/978-3-540-85886-7_12

Network Access Control.2007.Rivier Academic Journal.

https://www2.rivier.edu/journal/ROAJ-Fall-2007/J105-Sood.pdf

Brown, Edwin.2007. 802.1X Port-Based Authentication.Auerbach Publications.New York

https://books.google.at/books?hl=de&lr=&id=nlbrC3KLvCAC&oi=fnd&pg=PP1&dq=802.1+x+authentication&ots=2zbhZYnnw8&sig=VO29PKFUHx4slIY-3kgbn7vIyls&redir_esc=y#v=onepage&q=802.1%20x%20authentication&f=false

Bicakci Kemal, Uzunay Yusuf.2008."Pushing the Limits of Address Based Authentication: How to Avoid MAC Address Spoofing in Wireless LANs".World Academy of Science,Engineering and Technology.

Wollert Jörg, Booke Andreas.2016."IoT von der Stange". Elektroniknet.de. Aachen

https://opus.bibliothek.fh-aachen.de/opus4/frontdoor/deliver/index/docId/7912/file/Wollert_EK_504_cd_2016-21.pdf

Helmbrecht Udo, Gneuß Carina. 2003. "IT-Sicherheit als Managementaufgabe". Bundesamt für Sicherheit in der Informationstechnik. Bonn

Petermann Thomas, Sauter Arnold.2002."Biometrische Identifikationssysteme" Sachstandsbericht.TAB

https://www.itas.kit.edu/pub/v/2002/pesa02a.pdf

Schmidt, T. Künstliche Intelligenz in der Cybersicherheit – zwischen Hype und Notwendigkeit. Wirtsch Inform Manag 12, 70–74 (2020). https://doi.org/10.1365/s35764-020-00244-4

Hasanova Huru, Baek Ui-jun,Shin Mu-gon,Cho Kyunghee.2019."A survey on blockchain cybersecurity vulnerabilities and possible countermeasures".

https://doi.org/10.1002/nem.2060

Flanigan John. 2018. "Zero Trust Network Model".

https://www.cs.tufts.edu/comp/116/archive/fall2018/jflanigan.pdf

Epah Michael. 2009. "Network Access Control". Darmstadt.

https://dl.gi.de/server/api/core/bitstreams/bcfef3b4-7cc4-48df-9ce8-0818ec20841d/content