



**Oldenburgische**  
Industrie- und Handelskammer

Abschlussprüfung Sommer 2025

Dokumentation der betrieblichen Projektarbeit  
im Rahmen der Abschlussprüfung  
zum Fachinformatiker für Systemintegration

### **Einführung eines Monitoring Tools**

**Prüfungsbewerber:**

Luis Weber  
Bremer Straße 92  
27751 Delmenhorst  
Identnummer: 0001072602

# ATLAS

**Ausbildungsbetrieb:**

Atlas GmbH  
Atlasstraße 6  
27777 Ganderkesee

## Inhalt

1. Einleitung .....	1
1.1 Projektumfeld .....	1
1.2 Projektziel .....	1
1.3 Projektumfang .....	2
1.4 Projektabgrenzung .....	2
1.5 Projektverlauf .....	2
2. Analysephase .....	3
2.1 Ist-Zustand .....	3
2.2 Soll-Zustand .....	3
2.3 Rahmenbedingungen .....	3
2.4 Lösungsvergleich .....	4
2.5 Auswahl des Monitoring Tools .....	6
2.6 Wirtschaftlichkeit .....	7
3. Durchführung .....	8
3.1 Installation .....	8
3.2 Konfiguration .....	8
3.2.1 Zugriff auf die Weboberfläche .....	8
3.2.2 Lizenzaktivierung .....	9
3.2.3 Netzwerkerkennung .....	9
3.2.4 Gruppierung der Geräte .....	9
3.2.5 Sensoren .....	9
3.2.6 Einbindung von SNMP-Geräten .....	10
3.2.7 Einrichtung von Remote Probes .....	11
3.2.8 Benachrichtigungen und Alarmierung .....	12
4. Qualitätssicherung .....	13
4.1 Testphase .....	13
5. Abschluss .....	14
5.1 Soll-Ist-Vergleich .....	14
5.2 Fazit .....	15
5.3 Übergabe .....	15

# 1. Einleitung

## 1.1 Projektumfeld

Die Atlas GmbH ist ein Unternehmen, welches sich auf die Entwicklung, Produktion und den Vertrieb von Baumaschinen spezialisiert hat, genauer gesagt auf Krane und Bagger. Die Atlas GmbH verfügt über 3 Standorte in Deutschland und einen in Großbritannien, mit Hauptsitz in Ganderkesee.

Gegründet wurde das Unternehmen 1919 von Hinrich Weyhausen gegründet, wo zu Beginn landwirtschaftliche Geräte produziert wurden. Zurzeit verfügt das Unternehmen über rund 500 Mitarbeiter, verteilt über alle Werke. [REDACTED]

Die Standorte bestehen jeweils aus Produktion und Verwaltung. Die Standorte Ganderkesee, Delmenhorst und Vechta verfügen jeweils über ein Rechenzentrum. In diesen Rechenzentren laufen [REDACTED]

[REDACTED] Zurzeit liegt nur eine minimierte Überwachung dieser Systeme vor, was potenzielle Risiken im Bereich der Performance und der Ausfallsicherheit birgt.

Im Rahmen meiner Ausbildung zum Fachinformatiker für Systemintegration wurde mir das für das Projekt die Verantwortung für die Planung, Bewertung und Durchführung eines Monitoring Tools gegeben.

## 1.2 Projektziel

Ziel dieses Projekts ist die firmeninterne Netzwerküberwachung der Atlas GmbH standortübergreifend einzuführen und sowohl für die Überwachung der Server als auch der Infrastruktur dienen. Dadurch sollen Netzausfälle oder andere Störungen frühzeitig erkannt und proaktiv gehandelt werden, wodurch die Verfügbarkeit und Stabilität der IT-Infrastruktur erhöht werden.

Dazu muss das System folgende Anforderungen erfüllen, diese wurden im Vorfeld mit dem IT-Leiter abgesprochen:

- Benutzerfreundliche GUI, um eine einfache Bedienung zu gewährleisten
- Kosteneffizienz, um das Budget nicht unnötig zu belasten
- On-Premise-Installation, so dass alle Daten intern verwaltet werden
- Datenspeicherung innerhalb der Atlas GmbH, um Sicherheits- und Datenschutzrichtlinien zu erfüllen
- Unterstützung mehrerer Standorte
- Alarmierungs- und Benachrichtigungsfunktionen (z.B. per E-Mail) für eine schnelle Reaktion auf Vorfälle
- Kompatibilität mit bestehenden Systemen, um eine reibungslose Integration zu gewährleisten
- Skalierbarkeit, damit das System mit den Anforderungen des Unternehmens wachsen kann
- Ein anpassbares Dashboard, das an die individuellen Bedürfnisse angepasst werden kann

- Eine visuelle Darstellung der Netzwerktopologie, um einen besseren Überblick über das Netzwerk zu erhalten
- Einhaltung von Sicherheits- und Datenschutzstandards zur Erfüllung der Unternehmensrichtlinien

Durch die Umsetzung dieser Anforderungen soll ein zuverlässiges und leistungsfähiges Netzwerk-Monitoring geschaffen werden, das die IT-Infrastruktur der Atlas GmbH nachhaltig unterstützt und optimiert. Der Auftraggeber ist hierbei die Atlas GmbH selbst.

## 1.3 Projektumfang

Im Rahmen dieses Projekts wurde ein Monitoring Tool implementiert, welches die Überwachung der IT-Infrastruktur der drei Standorte in Deutschland der Atlas GmbH gewährleistet. Das Projekt beinhaltet die Analyse des Ist-Zustands, die Auswahl und Bewertung von Monitoring Tools, die Installation und Konfiguration des ausgewählten Tools, sowie die Abgabe, Dokumentation und Einweisung der IT-Abteilung.

## 1.4 Projektabgrenzung

Nicht Bestandteil des Projekts ist die Netzwerküberwachung des Werks in England, die Überwachung von Endgeräten (Computer der Mitarbeiter, Diensthandys) als auch Schulungen der Mitarbeiter außerhalb der IT-Abteilung.

## 1.5 Projektverlauf

Phase	Zeit
<b>Analyse</b>	<b>4h</b>
• Besprechung des Projektumfangs	1h
• Analyse des Ist-Zustands	2h
• Definition des Soll-Zustands	1h
<b>Entwurf</b>	<b>6h</b>
• Konzeption eines Netzwerkplans	2h
• Erstellung der Lösungsvorschläge	4h
<b>Kalkulation und Abnahme</b>	<b>6h</b>
• Kosten/Nutzenanalyse der Alternativen	4h
• Kalkulation des ganzen Projekts	1h
• Vorstellung / Präsentation beim IT-Leiter	1h
<b>Implementierung inkl. Tests</b>	<b>19h</b>
• Installation der Software	3h
• Konfiguration der Software	13h
• Überprüfung und Fehlerbehebung der Funktion der Software	3h
<b>Dokumentation und Einweisung</b>	<b>5h</b>
• Erstellung einer Administrationsdokumentation	2h
• Einweisung der Administratoren	1h
• Erstellen einer Systemdokumentation	2h

Tabelle 1: Projektverlauf

## 2. Analysephase

### 2.1 Ist-Zustand

Die IT-Infrastruktur der Atlas GmbH ist über die drei Standorte Ganderkesee, Delmenhorst und Vechta verteilt und verfügt jeweils über ein Rechenzentrum. Zusätzlich gibt es ein Werk in England, welches jedoch für dieses Projekt nicht berücksichtigt wird.

In den Rechenzentren befinden sich:



Die IT-Infrastruktur ist über die Jahre historisch gewachsen und wurde nur minimal überwacht. Ein Monitoring-System, das alle Standorte, Server und Netzwerkkomponenten überwacht, ist nicht vorhanden. Die Fehlerbehebung erfolgt derzeit eher reaktiv. Alarmierungen bei Systemausfall oder Komponentenausfall erfolgen bei uns zurzeit nur über "Fujitsu ServerView", welches jedoch nur bei Servern von Fujitsu funktioniert, was zurzeit jedoch kein Problem darstellt, da wir nur Server von Fujitsu einsetzen. Spezifische Programme oder Datenbanken, die auf den Servern ausgeführt werden, sind von der Überwachung ausgeschlossen. Zusätzlich ist bei der Namensgebung der Server meistens ein Kürzel für den Standort des Servers eingetragen worden, einige Standorte sind davon jedoch nicht mehr aktuell, wodurch die Übersicht des Systems erschwert wird.

### 2.2 Soll-Zustand

Nach dem abgeschlossenen Projekt soll ein Monitoring-System, welches standortübergreifend die IT-Infrastruktur überwacht, implementiert worden sein. Ziel ist die Transparenz zu schaffen und vor allem den aktuellen Zustand der Geräte bzw. der Systeme frühzeitig zu erkennen und dadurch die Reaktionszeit unsererseits deutlich zu verkürzen.

Die Systemzustände, sowie die Systeme an sich sollen benutzerfreundlich und grafisch dargestellt werden und Alarmierungen automatisch versendet werden. Langfristig sollen so die Ausfallzeiten minimiert werden, den administrativen Aufwand reduzieren und die Verfügbarkeit gewährleisten. Zudem soll das System einfach skalierbar bzw. erweiterbar sein.

### 2.3 Rahmenbedingungen

- **Zeitlicher Rahmen:** Die gesamte Projektlaufzeit beträgt 40 Stunden und darf diese nicht überschreiten.
- **Ressourcen:** Es steht ein Server bzw. eine Arbeitsstation zur Verfügung, auf der das Monitoring Tool installiert als auch konfiguriert wird. Zusätzlich stehen 2 weitere Rechner für eine Instanz in den anderen Werken und die Serverlandschaft und Netzwerkinfrastruktur zur Verfügung
- **Budget:** Es steht ein Budget von 10.000€ zur Verfügung. Damit soll die Implementation, zusätzliche Hardwarekosten und die Lizenzkosten für 1 Jahr abgedeckt werden.

- **Vorgaben:** Das Monitoring-System muss On-Premise installiert werden, kompatibel mit unserer Infrastruktur und skalierbar sein.

## 2.4 Lösungsvergleich

Um die Umsetzung des Projekts zu gewährleisten, wurden drei verschiedene Monitoring Tools betrachtet und miteinander verglichen. Diese entsprechen wirtschaftlich als auch funktional den Anforderungen und wären geeignete Kandidaten für die Atlas GmbH. Während der Entwurfsphase wurden die Lösungen CheckMK, PRTG und Nagios anhand vorher definierter Kriterien verglichen.

Im Vergleich stellt sich heraus, dass PRTG sehr benutzerfreundlich ist und eine Auto-Discovery Funktion bietet, was den Einrichtungsaufwand erheblich senkt. Durch die Unterstützung von Remote Probes können die verteilten Standorte zentral eingebunden werden, ohne alles auf einen Server laufen zu lassen. Die Software lässt sich ohne Probleme integrieren und bietet ein benutzerfreundliches, individuell anpassbares Dashboard.

CheckMK überzeugt vor allem durch ein gutes Preis-Leistungs-Verhältnis, bringt jedoch einen höheren manuellen Aufwand mit sich. Die verschiedenen Standorte lassen sich ebenfalls einrichten.

Nagios ist als Open-Source-Produkt zwar das günstigste Produkt, kann jedoch nicht in den Punkten Benutzerfreundlichkeit, Skalierbarkeit und der Visualisierung mithalten. Die Konfiguration erfordert tiefgehende technische Kenntnisse und die Bereitstellung der erforderlichen Funktionen erfolgt über Plugins von Drittanbietern.

Die Tools CheckMK, PRTG und Nagios wurden in folgender Tabelle miteinander verglichen.

Kriterium	CheckMK	PRTG	Nagios
GUI	Übersichtlich, aber verschachtelte Menüführung	Sehr benutzerfreundlich, übersichtlich, Gruppierungen möglich, Gerätebaum-Ansicht (Diagramm)	Alt, überholt, standardmäßig wenig modern
Installationsaufwand	<b>Gering:</b> Linux-basiert, Installationsanleitung auf der Webseite. Mit 5 Befehlen kann ein Server aufgesetzt werden.	<b>Gering:</b> Windows-basiert, Installationsprogramm muss nur ausgeführt werden.	<b>Aufwändig:</b> Linux-basiert. Pakete müssen manuell installiert werden.
Konfigurationsaufwand	Hoch: Hosts (Geräte) müssen einzeln angelegt werden. Netzwerktopologie muss manuell gepflegt werden. Verknüpfte Geräte (Switch zu Server)	Mittel: Auto-Discovery erkennt das Netzwerk automatisch. Erste Gruppierung erfolgt automatisch. Empfohlene Sensoren für Geräte werden vorgeschlagen.	Sehr hoch: Hosts und Services müssen manuell angelegt werden. Sensoren müssen ebenfalls individuell definiert werden.

	müssen händisch eingetragen werden. Agenten müssen manuell installiert werden. Nach der Installation schlägt CheckMK automatisch Services (Sensoren) vor.	Manuelles Feintuning über Drag & Drop möglich.	
Preis	2.100 €/Jahr für 3.000 Services (Netto)	6.099 €/Jahr für 2.500 Services (Netto)	Gratis (Nagios Core) / 299\$ einmalig (Nagios XI) (Netto)
On-Premise	Ja	Ja	Ja
Daten liegen beim Unternehmen	Ja	Ja	Ja
Mehrere Standorte abbilden	Ja, über verteilte Instanzen	Ja, über Remote Probes	Nicht direkt möglich, erfordert Drittanbieter-Erweiterungen
Benachrichtigung / Alarmierung	E-Mail, SMS, Skripte, Webhooks, Slack, Microsoft Teams	E-Mail, SMS, Push-Benachrichtigung (App), Webhooks	E-Mail, SMS, Skripte (individuell anpassbar, aber manuell einzurichten)
Skalierbarkeit	Möglich, aber manuell aufwendig (100 neue Server = 100 neue Hosts müssen angelegt werden)	Skaliert gut, Auto-Discovery erleichtert das Wachstum. Viele Hosts sind kein Problem, aber zu viele Sensoren können problematisch werden.	Sehr eingeschränkt ohne Erweiterungen
Kompatibilität	Alle Netzwerkgeräte werden erkannt (SNMP, Agenten)	Alle Netzwerkgeräte werden erkannt (SNMP, WMI, NetFlow)	Nur Basis-SNMP, viele Plugins erforderlich für moderne Systeme
Dashboard	Flexibel, aber komplizierter einzurichten	Sehr benutzerfreundlich, individuelle Dashboards über Web-GUI	Basis-Dashboard, oft durch Plugins erweitert
Darstellung Netzwerktopologie	Muss händisch angelegt werden	Wird durch Gruppen dargestellt, keine automatische Netzwerktopologie-Darstellung	Nicht nativ vorhanden, nur mit Erweiterungen möglich
Sicherheits- und Datenschutzkonform	Ja, DSGVO-konform	Ja, DSGVO-konform	Ja, aber nur mit zusätzlicher Absicherung

Wartung/Updates	Manuelle Updates nötig, jedoch mit ausführlicher Dokumentation. Logs vorhanden, Debugging einfach möglich.	Automatische Updates, geringster Wartungsaufwand	Manuelle Updates, oft aufwendig, mögliche Konflikte mit bestehenden Plugins
-----------------	--	--	---

Tabelle 2: Monitoring-Vergleich

## 2.5 Auswahl des Monitoring Tools

Um besser zu einer Entscheidung zu finden und um die Monitoring Tools besser bewerten zu können, wurde eine Nutzwertanalyse durchgeführt. Dabei wurden die vorher ausgewählten Kriterien mit Gewichtungen versehen, die von 1 bis 5 gehen. Für jedes Kriterium konnten Punkte von 1 bis 3 vergeben werden, die mit den entsprechenden Gewichten multipliziert wurden.

Besonders wichtige Kriterien wie die Benutzeroberfläche (GUI), der Konfigurationsaufwand oder die Kompatibilität wurden dabei höher gewichtet, während andere Kriterien wie die Darstellung der Netzwerktopologie eine niedrigere Gewichtung erhielten.

Kriterium	Gewichtung	CheckMK		PRTG		Nagios	
		P	Pg	P	Pg	P	Pg
GUI	5	2	10	3	15	1	5
Installationsaufwand	4	2	8	3	12	1	4
Konfigurationsaufwand	5	2	10	3	15	1	5
Preis	4	2	8	1	4	3	12
On-Premise	5	3	15	3	15	3	15
Daten liegen beim Unternehmen	5	3	15	3	15	3	15
Mehrere Standorte abbilden	4	3	15	3	12	1	4
Benachrichtigung / Alarmierung	2	3	6	3	6	2	4
Skalierbarkeit	3	2	6	3	9	1	3
Kompatibilität	5	3	15	3	15	2	10
Dashboard	2	2	4	3	3	1	2
Darstellung Netzwerktopologie	1	2	2	3	3	1	1
Sicherheits- und Datenschutzkonform	5	3	15	3	15	2	10
Wartung/Updates	4	2	8	3	12	1	4
<b>Gesamtpunkte</b>		<b>34</b>	<b>137</b>	<b>40</b>	<b>151</b>	<b>23</b>	<b>94</b>

Tabelle 3: Nutzwertanalyse

\* P = Punkte, Pg = Punkte (gewichtet)

- PRTG erreicht **151** Punkte und erfüllt damit die Anforderungen am besten.
- CheckMK erreicht **137** Punkte und bietet damit eine gute Alternative, zeigt jedoch noch in den Punkten Benutzerfreundlichkeit und dem Konfigurationsaufwand Schwächen

- Nagios erreicht **94** Punkte und liegt damit weit hinter den Alternativen. Die altmodische GUI und der hohe Konfigurationsaufwand machen dieses Tool eher ungeeignet.

Besonders positiv hervorzuheben sind die automatische Netzwerkerkennung (Auto-Discovery), das intuitive Dashboard sowie die einfache Integration mehrerer Standorte über sogenannte Remote Probes. Diese Vorzüge resultieren in einem erheblich geringeren Einrichtungs- und Wartungsaufwand im Vergleich zu alternativen Lösungen.

Trotz höherer Lizenzkosten bleibt PRTG mit Blick auf das Projektbudget von 10.000 Euro wirtschaftlich vertretbar. Durch die Einsparung von Zeit und Ressourcen bei der Konfiguration und späteren Wartung bietet PRTG langfristig den größten Nutzen für das Unternehmen. Zudem ist PRTG nicht Linux-basiert und lässt sich als Windows-Anwendung nahtlos in unsere bestehende Systemlandschaft integrieren, insbesondere, da unser IT-Team ausschließlich mit Windows-Systemen arbeitet und keine Linux-Spezialkenntnisse vorhanden sind.

Auf Grundlage dieser Bewertung wurde PRTG als Monitoring-Lösung für die Atlas GmbH ausgewählt.

## 2.6 Wirtschaftlichkeit

Bezeichnung	Anzahl	Preis (Brutto)	Gesamtbetrag (Brutto)
<b>Lizenzen für das Monitoring Tool</b>			
PRTG 2500	1	7.257,81€ /Jahr	7.257,81€ /Jahr
<b>Personal (in Stunden)</b>			
Luis Weber (Auszubildender)	40	60,00€	2.400,00€
<b>Jährliche Kosten (Brutto)</b>			<b>7.257,81€</b>
<b>Kosten für das erste Jahr (Brutto)</b>			<b>9.657,81€</b>

Tabelle 4: Kostenkalkulation

*\* Hardwarekosten wurden nicht weiter berücksichtigt, da für die Umsetzung auf vorhandene Infrastruktur zurückgegriffen wurde.*

Die Gesamtkosten dieses Projekts setzen sich einmal aus den Lizenzkosten des Monitoring Tools und den Personalkosten des Auszubildenden zusammen. Zusätzliche Kosten für Hardware wurden nicht berücksichtigt, da auf bereits vorhandene Hardware bzw. die Infrastruktur zurückgegriffen wurde.

Die anfänglichen Kosten beliefen sich auf 2.400,00€, da ein externer Stundensatz von 60€ berechnet wurde. Diese Kosten fallen lediglich bei der Implementierung an.

Die jährlichen Lizenzkosten für das Monitoring Tool PRTG (2.500 Sensoren) belaufen sich auf 7.257,81€.

Fazit: Das Projekt bleibt mit den Kosten für das erste Jahr (9.657,81€) im Budget für 10.000€. Die Investition ist aufgrund des geringeren Konfigurationsaufwand, der verbesserten Netzwerküberwachung und der Möglichkeit, proaktiv bei Fehlern zu handeln, wirtschaftlich.

## 3. Durchführung

### 3.1 Installation

Die Installation erfolge auf einem bereits vorhandenem Windows 11 PC im Werk Ganderkesee. Dieser dient als Core-Server für das Monitoring.

Für die Nutzung der PRTG-Version mit bis zu 2.500 Sensoren gelten laut Hersteller folgende empfohlene Systemanforderungen:

- 8 GB RAM
- 4 CPU-Kerne
- 750 GB Speicherplatz
- Microsoft .NET Framework ab Version 4.7.2

Unser genutzter PC erfüllt diese Voraussetzungen bis auf den Speicherplatz. Da jedoch keine größeren Daten dauerhaft gespeichert werden und Backups vorgesehen sind, ist der Speicherplatz nicht von hoher Bedeutung. Die übrige Ausstattung erfüllt die Anforderungen:

- Intel Core i5-9400T CPU (6 Kerne)
- 32 GB RAM
- 250 GB SSD

Anschließend wurde das Installationspaket von der offiziellen Seite des Herstellers ([www.paessler.com](http://www.paessler.com)) heruntergeladen. Dabei wurde im Vorfeld sichergestellt, dass das erforderliche .NET-Framework installiert ist. Das Installationssetup wurde als Administrator ausgeführt und unter dem folgenden Pfad installiert: C:\Program Files (x86)\PRTG Network Monitor. Die Installation verlief ohne Probleme und das Programm konnte erfolgreich gestartet werden und es automatisch ein Webserver aufgesetzt.

## 3.2 Konfiguration

### 3.2.1 Zugriff auf die Weboberfläche

Nach der Installation konnte die Weboberfläche von PRTG intern über die URL [REDACTED] erreicht werden. Der erste Zugriff erfolgte dann mit diesen vorgegeben Anmeldedaten:



Anschließend wurde man aus Sicherheitsgründen dazu aufgefordert das Standardkennwort zu ändern, dies wurde getan und zusätzlich [REDACTED] unserer IT-Abteilung im Administratorbenutzer hinterlegt und in unserem Passwortmanager vermerkt.

### 3.2.2 Lizenzaktivierung

Nach dem erstmaligen Zugriff auf die Weboberfläche wurde die Lizenz für PRTG aktiviert. Die Atlas GmbH nutzt die kommerzielle Version mit bis zu 2.500 Sensoren.

Die Aktivierung erfolgte über das Menü „Konfiguration“ → „PRTG Status“ → „Lizenzinformationen“ → „Lizenzschlüssel ändern“, wo der bereitgestellte Lizenzschlüssel eingetragen wurde. Im Anschluss erfolgte die Online-Validation der Lizenz mit dem Paessler-Lizenzserver. Nach erfolgreicher Aktivierung stand der volle Funktionsumfang der Software zur Verfügung.

Es wurden folgende Punkte bei der Lizenzüberprüfung berücksichtigt:

- Gültige Sensoranzahl (2.500)
- Lizenzinhaber (Atlas GmbH)
- Lizenzlaufzeit (1 Jahr)

Die Aktivierung verlief ohne Probleme und die Software war damit betriebsbereit.

### 3.2.3 Netzwerkerkennung

Nach der Aktivierung der Lizenz wurde als nächstes die Netzwerkerkennung durch die integrierte Auto-Discovery-Funktion durchgeführt, um die benötigten Netzwerkgeräte automatisch zu erkennen. Dabei wurde die Auto-Discovery-Funktion durchgeführt und alle aktiven Geräte innerhalb unseres Netzes wurden erkannt. Da die Server und Netzwerkkomponenten wie Switches dauerhaft laufen wurden diese auch gefunden und mit dem vom DNS vergebenen Namen inklusive IP-Adresse angezeigt. Im Nachgang wurden dann erstmal alle übrigen bzw. nicht relevanten Geräte, wie z.B. mobile Endgeräte und Drucker entfernt, da diese nicht dauerhaft aktiv sind und dadurch nur unnötige Fehlermeldungen senden. Für den Fall, dass ein Netzwerkgerät nicht gefunden wurde, wurden die bereits erkannten Geräte, mit denen in unserem Active-Directory verglichen. Es wurden jedoch alle benötigten Geräte vorher erkannt.

### 3.2.4 Gruppierung der Geräte

Im Anschluss an den Netzwerkskan erfolgte die Gruppierung der Geräte, um eine schnelle Feststellung des Standorts und der Art des Geräts zu ermöglichen. Die Gruppierung erfolgte zunächst standortbasiert für die Werke Ganderkesee, Delmenhorst und Vechta. Innerhalb der Standorte wurde eine weitere Unterteilung zwischen Server und Infrastruktur vorgenommen.

Diese Unterteilung spielt eine zentrale Rolle, da PRTG bei einem Gerätefehler nicht nur das betroffene Gerät, sondern auch alle zugehörigen Gruppierungen rot markiert. Dadurch wird auf einen Blick ersichtlich, zu welchem Standort das Gerät gehört und um welche Gerätekategorie es sich handelt.

### 3.2.5 Sensoren

In PRTG wird jedes überwachte Element als Sensor bezeichnet, dabei misst ein Sensor immer einen bestimmten Aspekt eines Gerätes, sei es die CPU-Auslastung oder die Antwortzeit eines Pings. Jedes Gerät kann jedoch unbegrenzt viele Sensoren haben, dadurch kann z.B. auch jeder Port eines Netzwerkswitches einzeln überwacht werden.

Die nicht benötigten Sensoren, welche durch die Auto-Discovery-Funktion hinzugefügt wurden, mussten bei jedem Gerät manuell entfernt werden. Darunter fallen Sensoren für z.B. die CPU-Last bei Fileserver oder die SSL-Sicherheitsüberprüfung bei Servern ohne Webanwendungen oder welche die nur intern erreichbar sind.

Wichtige Sensoren mussten ebenfalls manuell und gezielt hinzugefügt werden, wenn diese nicht durch die Auto-Discovery-Funktion erkannt wurden. Darunter fallen hauptsächlich:

- **Ping-Sensoren:** Diese überprüfen, ob ein Gerät über das Netz erreichbar ist (Server, Router, Switches)
- **CPU- und RAM-Sensoren:** Diese überwachen die Auslastung auf Servern, um frühzeitig Überlastungen zu erkennen
- **HTTP-/HTTPS-Sensoren:** Diese kontrollieren die Erreichbarkeit von Webservern, sowie Webanwendungen
- **SNMP Traffic-Sensoren:** Diese überwachen die Portauslastung auf Netzwerkswitchen
- **SNMP Datenträgerspeicher:** Überprüft den freien Speicherplatz auf den jeweiligen

### 3.2.6 Einbindung von SNMP-Geräten

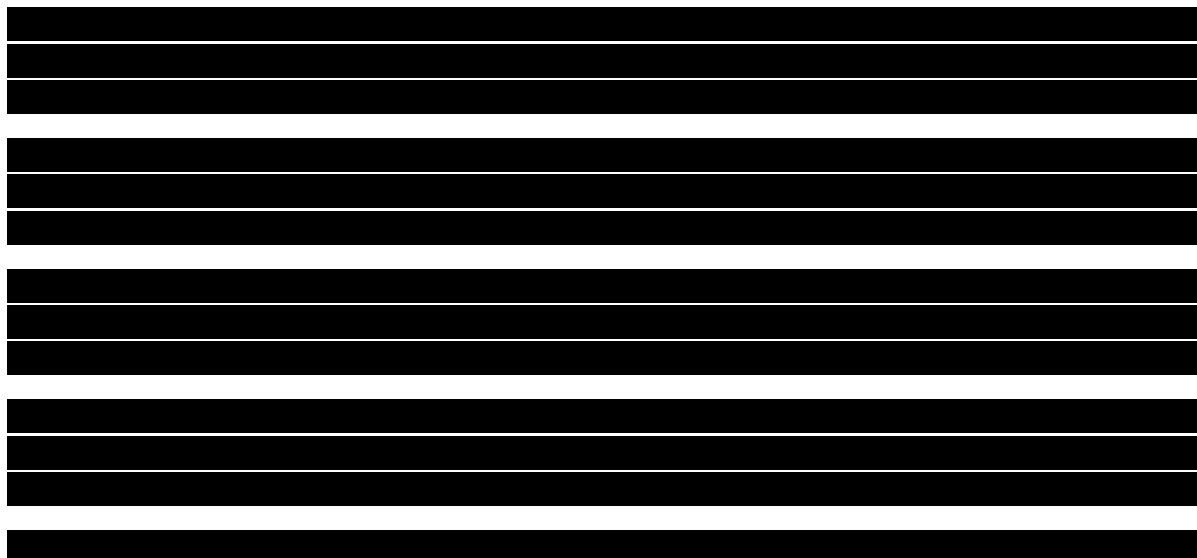
Vorab muss erstmal geklärt werden, was SNMP überhaupt ist. Es steht für Simple Network Management Protocol und ist ein Netzwerkprotokoll, welches zur Überwachung und Verwaltung von Netzwerkgeräten dient. Dadurch ist es Monitoring-Tools wie PRTG möglich, Informationen über den Zustand der Geräte abzurufen. Dazu zählen beispielsweise der Portstatus, die Bandbreite, die Temperatur oder die Speicherbelegung.

Damit die SNMP-Sensoren genutzt werden können, ist zunächst die Auswahl einer SNMP-Version in PRTG erforderlich. Es wurde sich für SNMPv2c (Simple Network Management Protocol Version 2 Community), da dies gegenüber den anderen Protokollen einige Vorteile bietet:

- **Kompatibilität:** Ein Großteil unserer Netzwerkgeräte unterstützte SNMPv2 standardmäßig, was die Integration erleichtert.
- **Geringerer Konfigurationsaufwand:** SNMPv3 bietet weitere Sicherheitsfunktionen, wie Authentifizierung und Verschlüsselung, jedoch ist der Aufwand bei der Konfiguration deutlich höher. Da wir uns jedoch in einem geschlossenen Firmennetzwerk befinden reicht das Sicherheitsniveau von SNMPv2c aus.
- **Leistungsfähiger:** SNMPv1 unterstützt keine Bulk-Requests (mehrere Anfragen auf einmal), wodurch die Daten effizienter abgefragt werden können. Beispielsweise werden bei einem Switch mit 24 Ports bei SNMPv1 24 Anfragen gesendet und bei SNMPv2c nur eine.
- **Community-String-Prinzip:** Die Netzwerkgeräte und das Monitoring Tool verwenden den gleichen String, welcher den Zugang untereinander ermöglicht und ähnlich wie ein gemeinsamer Schlüssel funktioniert. Auf den Netzwerkgeräten werden dann ausschließlich Leseberechtigungen erteilt, um ungewollte Aktionen zu verhindern.




Alles in allem bietet SNMPv2c den besten Kompromiss zwischen Aufwand, Kompatibilität und Sicherheit. Da das Monitoring ausschließlich im internen Netzwerk stattfindet, ist auch das Sicherheitsniveau ausreichend.

Die folgenden Einstellungen wurden hier vorgenommen:



*Abbildung 1: Zugangsdaten für SNMP-Systeme*

Damit PRTG jetzt über SNMP Daten abrufen kann, müssen die Netzwerkgeräte SNMP unterstützen und zusätzlich auch auf den jeweiligen Netzwerkgeräten Einstellungen vorgenommen werden.

- SNMP muss aktiviert werden.
- Eine SNMP-Community muss eingerichtet werden:
- Der Community-String muss identisch mit dem von PRTG sein   

- Lese-Zugriffsrechte müssen aktiviert werden
- Die IP-Adresse des PRTG-Servers als vertrauenswürdigen Host muss eingetragen werden 

Da manche Netzwerkgeräte nicht SNMP-Fähig waren, musste auf andere Sensoren wie z.B. Ping ausgewichen werden, um diese zu überwachen.

### 3.2.7 Einrichtung von Remote Probes

Um den zentralen Core-Server in Ganderkesee zu entlasten, wurden pro Standort je ein „Remote Probe“ installiert und konfiguriert. Dies ermöglicht eine dezentrale Überwachung der lokalen Netzwerke, während die Daten zentral auf dem PRTG Core Server zusammenlaufen. Dadurch wird auch der Datenverkehr zwischen den Standorten deutlich reduziert und das System kann einfacher skaliert werden.

Die Vorgehensweise war wie folgt:

Zunächst wurde an den Standorten Delmenhorst und Vechta jeweils ein Windows 11 PC installiert. Anschließend wurden auf der Weboberfläche des Core-Servers unter dem Menü „Konfiguration“ → „Systemverwaltung“ → „Server und Probes“ die IP-Adressen der Remote Probes (Windows 11 PCs) und des Core-Servers unter den zugelassenen IP-Adressen eingetragen und die Option „Alle auf diesem Computer verfügbaren IP-Adressen“ ausgewählt.

Anschließend konnte man ebenfalls über das Webinterface unter dem Menüpunkt „Konfiguration“ → „Optionale Downloads“ → „Remote Probes“ den Installer für eine Remote Probe herunterladen und anschließend ausführen und installieren.

Nach der ersten Verbindung wurde man aufgefordert, die Remote Probe zu bestätigen und hatte die Auswahl „Abbrechen“, „Bestätigen“ und „Bestätigen und automatische Suche durchführen“. Da die benötigten Geräte vorher gescannt und gruppiert wurden, konnte man auf die automatische Suche verzichten und die vorher gruppierten Standorte den jeweiligen Remote Probes zuordnen.

Durch die Remote Probes konnte die Auslastung des Core-Servers deutlich reduziert werden. Zudem wurde die Netzwerkabfrage der Standorte logisch voneinander getrennt.

### 3.2.8 Benachrichtigungen und Alarmierung

PRTG kategorisiert folgende Status bei den Sensoren:

- **OK:** Sensor funktionier einwandfrei (grün)
- **Ungewöhnlich:** Werte sind außerhalb des Normalbereichs, es liegt jedoch noch kein Fehler vor (orange)
- **Warnung:** Es liegt ein potenzielles Problem vor (gelb)
- **Fehler:** Sensor meldet ein kritisches Problem (rot)
- **Pausiert:** Sensor wurde pausiert und fragt keine Informationen ab (blau)

Bei kritischen Ereignissen, wie beispielsweise der Ausfall eines Servers oder überlasteten Ressourcen soll eine automatische E-Mail-Benachrichtigung an die IT-Abteilung gesendet werden. Dadurch kann schnell auf Vorfälle reagiert und Ausfallzeiten verkürzt werden. Jeder Sensor lässt sich individuell anpassen und es können individuelle Grenzwerte definiert werden, ab wann ein Sensor seinen Status ändert. Die Grenzwerte wurden für jede Geräte eingestellt bzw. angepasst.

Die E-Mail-Benachrichtigung lässt sich durch einen SMTP-Relay-Server versenden. Dafür haben wir in PRTG folgende Einstellungen angewandt:

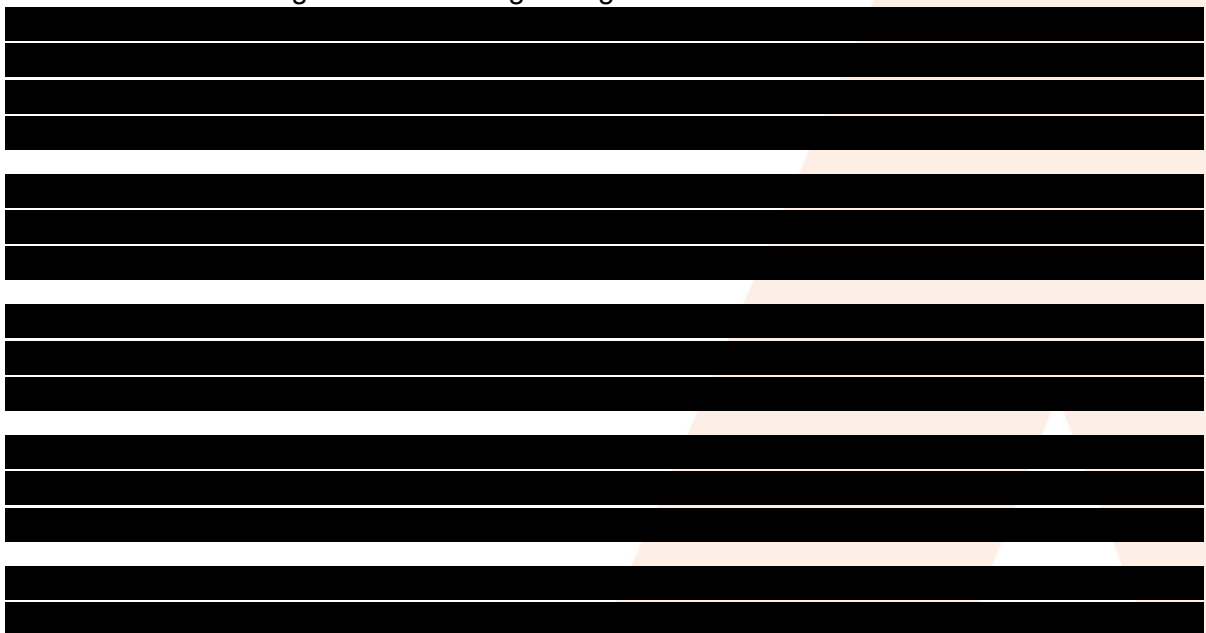
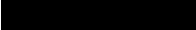


Abbildung 2: Versand per SMTP

Nun mussten noch Regeln definiert werden, unter welchen Bedingungen eine E-Mail-Benachrichtigung versendet werden soll. Hierfür gibt es die Kategorie „Trigger für Benachrichtigungen“, in der dies eingestellt werden kann. Es wurde eine Standardvorlage erstellt, die bei einem „Fehler“ automatisch eine E-Mail an den Administrator  sendet.



Trigger für Benachrichtigungen	
Typ ^	Regel
Zustands-Trigger (ID: 1)	Wenn der Sensor für mindestens 600 Sekunden im Zustand Fehler ist, führe @ E-Mail-Benachrichtigung an Administrator  aus.
	Wenn der Sensor für mindestens 900 Sekunden im Zustand Fehler ist, führe keine Benachrichtigung aus und wiederhole dies alle 0 Minuten.
	Wenn der Sensor nicht mehr im Zustand Fehler ist, führe @ E-Mail-Benachrichtigung an Administrator  aus.

Abbildung 3: Trigger für Benachrichtigungen

## 4. Qualitätssicherung

### 4.1 Testphase

Nach der Installation und Konfiguration sollte sichergestellt werden, dass das System zuverlässig funktioniert und die wichtigsten Funktionen überprüft wurden. Um sicherzustellen, dass der Ping-Sensor korrekt funktioniert, wurde ein aktiver Server, der überwacht wird, kurzzeitig vom internen Netzwerk getrennt. Nach kurzer Zeit meldete PRTG einen Fehlerzustand, der auch im Dashboard angezeigt wurde.

Die CPU- und RAM-Auslastung wurde durch einen Testserver künstlich erhöht, indem ein Benchmark gestartet wurde. Zuvor wurden die Grenzwerte für Fehlerzustände auf eine Auslastung von 30% gesetzt, da diese durch einen Benchmark in jedem Fall erreicht wird. Auch hier trat die Zustandsänderung in PRTG auf.

Um die Speicherplatzüberwachung zu testen, wurde der freie Speicherplatz auf einem Fileserver künstlich verringert, bis er den vorgegebenen Grenzwert überschritt. Der Statuswechsel in PRTG war ebenfalls erfolgreich.

Zur Überprüfung der Traffic-Überwachung an den Ports der Netzwerk-Switches wurde ein Laptop per LAN-Kabel direkt an einen Switch-Port angeschlossen. Anschließend wurde überprüft, ob der zugehörige Sensor den Traffic an diesem Port korrekt erfasst und anzeigt. Auch dies war erfolgreich.

Zur Überprüfung der E-Mail-Benachrichtigung wurde ein Server heruntergefahren und 10 Minuten gewartet, da dies in den Triggern für Benachrichtigungen so eingestellt war. Danach kam auch die E-Mail-Benachrichtigung mit einer Fehlermeldung und war somit ebenfalls erfolgreich.

## 5. Abschluss

### 5.1 Soll-Ist-Vergleich

Der Vergleich der geplanten und tatsächlichen Zeiten zeigt, dass das Projekt im Allgemeinen gut im Zeitplan geblieben ist, jedoch hat sich die Zeitverteilung in einigen Phasen anders entwickelt. Besonders deutlich wurde dies bei der Konzeption: der geplante Netzwerkplan wurde erstmal nicht erstellt, da sich bei der Konzeption der verschiedenen Lösungen herausstellte, dass dieser auch in zwei der ausgewählten Tools erstellt werden konnte. Daher gab es auch hier eine Abweichung in der Reihenfolge und es wurde zunächst abgewartet, welches Monitoring-Tool verwendet wird, um sich diesen Schritt eventuell zu sparen und dies beiläufig im Monitoring Tool zu erstellen. Dies war auch der Fall, da die Wahl auf PRTG fiel, wo genau diese Funktion mit der Gruppierung gegeben war.

Leichte Abweichungen gab es auch in der Implementierungsphase. Die Installation der Software verlief deutlich schneller als erwartet, da hier die Voraussetzungen erfüllt waren und nur ein Setup durchgeführt werden musste und anschließend das Monitoring Tool installiert wurde. Die Konfiguration der Software und die Testphase nahmen jedoch deutlich mehr Zeit in Anspruch, da die Konfiguration der Sensoren auf den einzelnen Geräten deutlich anspruchsvoller war als zuvor angenommen. Zudem war SNMP auf fast allen Netzwerkschichten deaktiviert und musste auf jedem Gerät manuell über das Webinterface aktiviert werden. Auch die Erstellung der Administrationsdokumentation nahm etwas mehr Zeit in Anspruch als geplant.

Phase	Soll	Ist	Differenz
<b>Analyse</b>	<b>4h</b>	<b>4h</b>	
• Besprechung des Projektumfangs	1h	1h	
• Analyse des Ist-Zustands	2h	2h	
• Definition des Soll-Zustands	1h	1h	
<b>Entwurf</b>	<b>6h</b>	<b>5h</b>	<b>- 1h</b>
• Konzeption eines Netzwerkplans	2h	0h	- 2h
• Erstellung der Lösungsvorschläge	4h	5h	+ 1h
<b>Kalkulation und Abnahme</b>	<b>6h</b>	<b>6h</b>	
• Kosten/Nutzenanalyse der Alternativen	4h	4h	
• Kalkulation des ganzen Projekts	1h	1h	
• Vorstellung / Präsentation beim IT-Leiter	1h	1h	
<b>Implementierung inkl. Tests</b>	<b>19h</b>	<b>19h</b>	
• Installation der Software	3h	0,5h	- 2,5h
• Konfiguration der Software	13h	15h	+ 2h
• Überprüfung und Fehlerbehebung der Funktion der Software	3h	3,5h	+ 0,5h
<b>Dokumentation und Einweisung</b>	<b>5h</b>	<b>6 h</b>	<b>+ 1h</b>
• Erstellung einer Administrationsdokumentation	2h	3h	+ 1h
• Einweisung der Administratoren	1h	1h	
• Erstellen einer Systemdokumentation	2h	2h	

Tabelle 5: Soll-Ist-Vergleich

## 5.2 Fazit

Trotz all dieser Verschiebungen gab es keine Auswirkungen auf den Gesamtzeitplan. Alle Phasen konnten erfolgreich abgeschlossen werden und ich habe in diesem Projekt viele Erfahrungen gesammelt. Vor allem im Umgang mit unerwarteten Ereignissen und Herausforderungen. Ich nehme auch mit, dass eine flexible Planung wichtig ist, um auf Veränderungen im Projektverlauf reagieren zu können. Durch die Umsetzung konnte ich mein technisches Wissen im Bereich der Netzüberwachung erweitern und vor allem meine organisatorischen Fähigkeiten deutlich verbessern.

Das Monitoring-Tool weist für die Zukunft noch Ausbaupotenzial auf. Darüber hinaus besteht die Möglichkeit, weitere Netzwerkkomponenten zu überwachen oder die Alarmierungen in andere IT-Systeme zu integrieren. Bei bestimmten Fehlern oder Warnungen könnten auch automatisierte Skripte zum Einsatz kommen. Diese könnten beispielsweise einen Dienst neu starten. Es besteht zudem die Möglichkeit, eine direkte Anbindung an unser Ticketsystem zu realisieren. Dieses erstellt automatisch ein Ticket und leitet es an den zuständigen Mitarbeiter weiter. Generell wurde hier nur der Grundstein für das Monitoring gelegt.

## 5.3 Übergabe

Da es sich hierbei um ein internes Projekt handelt, erfolgte die Übergabe an die IT-Abteilung der Atlas GmbH. Damit der Betrieb dieses Monitoring Tools auch in Zukunft sichergestellt werden kann wurden zwei Dokumentationen erstellt:

- Administrationsdokumentation: Hier sind alle Informationen zur Verwaltung und Administration des Monitoring Tools dokumentiert, wie z.B. das Hinzufügen von Geräten und Sensoren, Gruppierungen und Alarmierungen.
- Systemdokumentation: Diese richtet sich an die Anwendung des Systems, darunter wird z.B. der Aufbau der Gruppen, das Interpretieren der Sensoren und das Bewerten von Fehlern dokumentiert.

Die Übergabe erfolgte durch eine Einweisung der IT-Abteilung, wo alle Dokumente übergeben und die grundlegende Bedienung von PRTG erklärt wurde.