

# | Vorstudie

## Anomalie Detection in Netzwerken

Ives Schneider

## Index

1. Management Summary .....	1
2. Projektinformationen .....	2
2.1. Projektauftrag .....	2
2.2. Problemstellung .....	2
2.3. Projektorganisation .....	2
2.4. Projektzeitplan .....	2
2.5. Ausgangslage .....	2
3. Projektziele .....	3
3.1. Muss Kriterien .....	3
3.2. Kann Kriterien .....	3
3.3. Zielgewichtung .....	3
4. Analysetechnik .....	4
4.1. Abgrenzung .....	4
4.2. Systemgrenzen .....	4
4.3. Analyse der Teilsysteme .....	4
4.4. Umsysteme .....	4
4.5. Schnittstellen .....	4
4.6. Systemgrenzen .....	4
5. Erhebung .....	5
5.1. IST-Zustand .....	5
5.2. Risiken .....	5
6. Würdigung .....	6
6.1. IST-Zustand .....	6
6.2. SWOT-Analyse .....	6
7. Lösungsvarianten .....	7
7.1. Log-Collector .....	7
7.2. Network Monitoring System .....	7
8. Weiteres Vorgehen .....	8
9. Freigabe .....	9
10. Darstellungsverzeichnis .....	10
11. Glossar .....	11



## 1. Management Summary



## **2. Projektinformationen**

### **2.1. Projektauftrag**

#### **2.1.1. Projektbeschreibung**

### **2.2. Problemstellung**

### **2.3. Projektorganisation**

### **2.4. Projektzeitplan**

### **2.5. Ausgangslage**



### **3. Projektziele**

#### **3.1. Muss Kriterien**

#### **3.2. Kann Kriterien**

#### **3.3. Zielgewichtung**



## **4. Analysetechnik**

### **4.1. Abgrenzung**

### **4.2. Systemgrenzen**

### **4.3. Analyse der Teilsysteme**

### **4.4. Umsysteme**

### **4.5. Schnittstellen**

### **4.6. Systemgrenzen**



## **5. Erhebung**

### **5.1. IST-Zustand**

### **5.2. Risiken**



## **6. Würdigung**

### **6.1. IST-Zustand**

### **6.2. SWOT-Analyse**





## **7. Lösungsvarianten**

### **7.1. Log-Collector**

#### **7.1.1. V0 | Null**

#### **7.1.2. V1 | Graylog**

#### **7.1.3. V2 | ELK-Stack**

### **7.2. Network Monitoring System**

#### **7.2.1. V0 | Null**

#### **7.2.2. V1 | PRTG**

#### **7.2.3. V2 | Nagios**



## **8. Weiteres Vorgehen**



## 9. Freigabe



## **10. Darstellungsverzeichnis**



## 11. Glossar