h_da
HOCHSCHULE DARMSTADT
UNIVERSITY OF APPLIED SCIENCES
fbi
FACHBEREICH INFORMATIK

Hochschule Darmstadt
- Fachbereich Informatik -

Analyse sicherheitsrelevanter Informationen in industriellen Netzwerken für den Einsatz eines SIEM Systems

Abschlussarbeit zur Erlangung des akademischen Grades
Master of Science (M.Sc.)

vorgelegt von

Niklas Breuer
727905

Referent:	Prof. Dr. Oliver Weissmann
Korreferent:	Jürgen Zorenc

Erklärung

Ich versichere hiermit, dass ich die vorliegende Arbeit selbstständig verfasst und keine anderen als die im Literaturverzeichnis angegebenen Quellen benutzt habe. Alle Stellen, die wörtlich oder sinngemäß aus veröffentlichten oder noch nicht veröffentlichten Quellen entnommen sind, sind als solche kenntlich gemacht. Die Zeichnungen oder Abbildungen in dieser Arbeit sind von mir selbst erstellt worden oder mit einem entsprechenden Quellennachweis versehen. Die Arbeit ist in gleicher oder ähnlicher Form noch bei keiner anderen Prüfungsbehörde eingereicht worden.

Darmstadt den 5. Juni 2018

Niklas Breuer

Abtract

Abstract formulieren

Todo list

Abstract formulieren IV
Mehr Kontext der Schutzziele einfügen 7
Schutzziele: Beispiel für Schutzziele formulieren 7
Log Management: Unterschied zwischen Log Management Systemen und SIEM Systemen herausstellen/formulieren 13
Log Management: Log Management Architektur einfügen? 14
Log Management: Beispiel für Log Management Architektur einfügen . . . 14
Kollektoren: Füge Definition für "Parsing"hinzu 15
Kollektoren: Zeige die Datenextraktion anhand eines Beispiels 15
Sicherheitsanforderungen (Zweck und grobe Beschreibung) formulieren . . 21
Bild für typische Enterprise Technical Architecture Infrastructure einfügen 22
Enterprise Kommunikation - VPN & Remote Access beschreiben 24
Kontext der industriellen Infrastruktur einfügen 27
Einfügen eines Bildes der Automatisierungspyramide 28
SCADA-Systeme, siehe Handbuch Quelle 28
Industrial Ethernet: Einsatz Feldbus vs. IE sinnvoll? 37
Industrial Kommunikationsprotokolle: Wird dieser Unterteil benötigt? (Abhängig von der Analyse und notwendigen Definitionen) 37
Tabelle der Kommunikationsschnittstellen einfügen, Name, Protokoll, Kurzbeschreibung 43
Gibt es Vorgaben welche Felder gefüllt werden müssen? Microsoft Dokumentation nochmal checken! 44
Bild für Windowslog Eventfelder einfügen zur Verdeutlichung 45
Windows Logs: Ggf. weitere Beispiele nennen, kurz beschreiben 49
Loggt das Betriebssystem Elemente aus diesem Bereich? Wie funktioniert die Anbindung der Logdateien an das Betriebssystem? 49
Beschreibe das Linux Auditing Framework um einen Überblick zu geben, wie Linux Auditing funktioniert und was überwacht wird 51

Dieser Abschnitt soll die Interaktion der Netzwerkteilnehmer beschreiben, gehört ggf. in den Architekturteil mit Bild 55
Dummypräsentation, Bilder von HTTP Request und Response müssen später eingefügt werden 55
Tabelle erstellen und Listen ersetzen 68
PROFIBUS Frage: Unterschiede zwischen Informationsmengen DP vs DPV1 bzgl. Status und Alarmmeldungen? 73
Stuxnet-Betrachtung und Informationen 79

Inhaltsverzeichnis

1 Einleitung **2**

2 Grundlagen **3**

2.1 Industrie 4.0 Konzept 4

2.1.1 Stand der IT-Sicherheit in industriellen Produktionsnetzwerken 4

2.1.2 Forschungsgebiete der IT-Sicherheit 5

2.2 IT Security Schutzziele 7

2.3 Risiko Management 8

2.4 Security Information and Event Management 9

2.4.1 SIEM Konzept und Zweck 9

2.4.2 SIM Log Management 12

2.4.3 Kollektoren 14

2.4.4 Event Verarbeitung 16

2.4.5 Security Event Management 17

2.4.6 Features & Gemeinsamkeiten von SIEM-System-Anbietern . . 18

2.5 Infrastruktur Office 19

2.5.1 Geräte 19

2.5.2 Architekturen & Anforderungen 22

2.5.3 Kommunikation 23

2.5.4 Bekannte Angriffsvektoren 24

2.6 Infrastruktur industrielle Produktionsnetzwerke 27

2.6.1 Architektur & Anforderungen 27

2.6.2 Geräte 30

2.6.3 Kommunikationstechnologien 34

2.6.4 Kommunikationsprotokolle 37

2.6.5 Bekannte Angriffsvektoren 37

3 Analyse der Informationsquellen in einer typischen Unternehmensstruktur 39
3.1 Verwendete Analysemethode . . . 39
3.2 Beschreibung der Unternehmensarchitektur (Model) . . . 42
3.3 Beschreibung der Systeme . . . 44
3.3.1 Windows . . . 44
3.3.2 Linux . . . 49
3.3.3 Applikationen . . . 51
3.3.4 Interaktionen der Systeme (und Anwender) . . . 55
3.3.5 Netzwerkprotokolle . . . 55
3.4 Analyse des Informationspools im Bezug auf Angriffsszenarien . . . 60
3.4.1 Betrachtung der Datenmenge . . . 61
3.4.2 Relevanz für die Sicherheitsbetrachung mit Hilfe von SIEM-Systeme . . . 62

4 Analyse der Informationsquellen in einem industriellen Produktionsnetzwerk 64
4.1 Beschreibung der Unternehmensarchitektur (Beispiel) . . . 65
4.1.1 Systeme . . . 66
4.1.2 Kommunikationsmedien . . . 69
4.2 Applikationen . . . 77
4.2.1 WinCC (SCADA / HMI) . . . 77
4.3 Analyse im Bezug auf typische Angriffsvektoren . . . 78
4.3.1 Betrachtung der Datenmenge . . . 79
4.3.2 Relevanz für die Sicherheitsbetrachung mit Hilfe von SIEM-Systeme . . . 79

5 Vergleich der Analysen 80
5.1 Vergleichsmetrik . . . 80
5.2 Vergleich . . . 80

6 Bewertung der Informationslücken 81
6.1 Bewertungsschema . . . 81
6.2 Bewertung . . . 81
6.3 Beschreibung existierender wissenschaftlichen Lösungsansätze . . . 81

7 Lösungsansatz zur Schließung der fokussierten Informationslücke 82
7.1 Tiefergehende Beschreibung der Informationslücke und bestehende Abhängigkeiten 82
7.2 Beschreibung des Lösungsansatz 82
7.3 Beschreibung des Versuchsaufbaus des Beweises 82
7.4 Beschreibung der Ergebnisse 82

8 Fazit 83

Literaturverzeichnis iv

Abbildungsverzeichnis v

Kapitel 1

Einleitung

TODO

Kapitel 2

Grundlagen

In diesem Kapitel sollen die Grundlagen vermittelt werden, die für das Verständnis der nachfolgenden Kapitel notwendig sind. Das folgende Bild zeigt die Struktur des Kapitels:

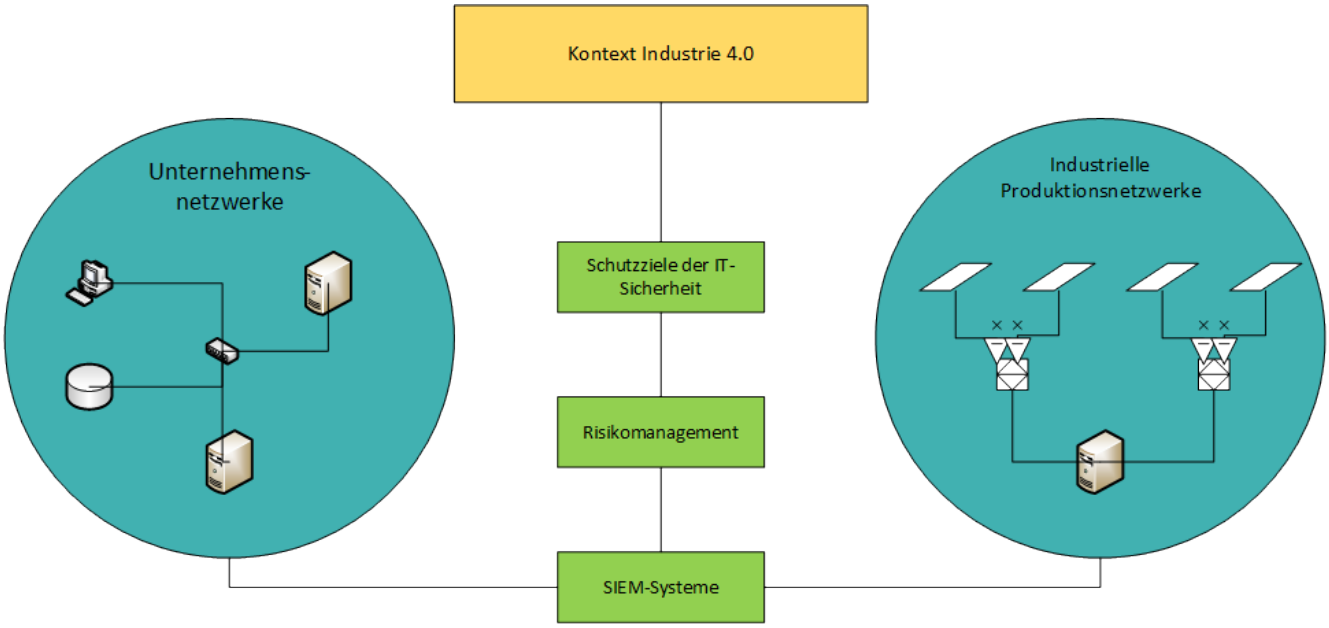

Abbildung 2.1: Aufbau des Grundlagenkapitels

Zunächst wird der Kontext der Industrie 4.0 beschrieben um ein Rahmenverständnis für den aktuellen Stand und die Idee der Vernetzung von Fertigungsanlagen zu vermitteln. Darauf folgend werden die grundlegenden Schutzziele der IT-Sicherheit definiert, welche die Basis für eine IT-Sicherheitsanalayse darstellen. Da eine Analyse aller relevanten Daten und Datenquellen auf Grund der limitierten Ressourcen eines SIEM-Systems nicht möglich ist, ist eine Risiko Management Strategie von fundamentaler Bedeutung. Aus diesem Grund werden die Grundlagen für

Risiko Management in einer Sektion beschrieben. Aufbauend auf diesen Grundlagen erfolgt eine Beschreibung des SIEM-Systems- Konzepts, Komponenten und Funktionalitäten. Dies soll ein Grundverständnis für die zu betrachtenden Datenmengen schaffen, die ein SIEM-System in die Analyse und Korrelation der Daten benötigt. Schlussendlich sind Grundkenntnisse zu den Elementen sowohl von Unternehmensnetzwerken als auch industriellen Automatisierungsnetzwerken notwendig, weshalb eine grobe Beschreibung dieser Elemente hinzugefügt wurde.

2.1 Industrie 4.0 Konzept

Das Konzept der Industrie 4.0 stellt einen Ansatz zur Steigerung der Flexibilität und Effektivität der Wertschöpfungsketten. Dazu sollen verschiedene industrielle Anlagen innerhalb einer Wertschöpfungskette über das Internet (WAN) miteinander verbunden werden und sogenannte „Smart Factories“geschaffen werden, die sich besser auf die Wünsche der Kunden einstellen können. Wichtige Punkte dieses Konzeptes sind die horizontale und vertikale Integration. Zum aktuellen Zeitpunkt sind Unternehmens- und Industrienetzwerke voneinander getrennt und/oder durch eine Sicherheitsschicht voneinander getrennt, sodass keine Kommunikation zwischen Industrienetzwerk und Internet durchgeführt werden kann. Das Konzept der vertikalen Integration soll diesen Zustand verändern, sodass Produktionsverwaltung per Web Interface erfolgen kann. Gleichzeitig soll über das Konzept der horizontalen Integration eine stärkere Verknüpfung und Kommunikation der Elemente auf den verschiedenen Netzwerkebenen erreicht werden[9].

2.1.1 Stand der IT-Sicherheit in industriellen Produktionsnetzwerken

Industrielle Netzwerke wurden ursprünglich als isolierte Umgebungen entwickelt, sodass Sicherheitsmaßnahmen sich stärker auf den physischen Zugang zu den Anlagen als auf die Sicherung der IT Systeme konzentrierten [18].

Durch das Auftreten von Stuxnet auf das iranische Atomprogramm und andere Angriffe auf industrielle Anlagen ist die Sicherung der Kommunikation und des virtuellen Zugriffes auf die Komponenten verstärkt als wichtiger Punkt anerkannt worden [18]. Da in industriellen Netzwerken unterschiedliche Kommunikationstechniken existieren, die teilweise keinerlei Schutzmechanismen z.B. für die Verifizierung der Kommunikationspartner oder der Integritätsprüfung der ausgetauschten Informationen bieten, sind industrielle Netzwerke nach aktuellem Stand potentiell an-

fällig für Angriffe. Dementsprechend ist die Sicherung dieser Netzwerke eine hohe Priorität, da bei einer Verbindung mit dem Internet ein potentieller Angriffsweg für Angreifer geschaffen wird, die bisher auf physischen Zugang oder das Einschleusen kompromitierter Speicher, wie z.B. USB Sticks, angewiesen sind [18].

Neben den Schwachstellen der Kommunikationstechnologien ist die Sicherung bei gleichzeitiger Garantie der Verfügbarkeit eine weitere Herausforderung. So ist es nach aktuellem Stand nicht möglich, regelmäßige Sicherheitsupdates für SPSen aufzuspielen, da dies das Anhalten der Produktionsprozesse und damit signifikante Verzögerungen und finanzielle Verluste zur Folge hat. Darüber hinaus müssen Neuerungen an der SPS Firmware und/oder geladenen Programmen jeweils zertifiziert und überprüft werden um die Robustheit und Ausfallsicherheit zu garantieren. Dieser Zustand macht es schwierig gebräuchliche Sicherheitskonzepte aus Unternehmensnetzwerken in industriellen Netzwerken einzusetzen [18].

2.1.2 Forschungsgebiete der IT-Sicherheit

Um die IT-Sicherheit der industriellen Netzwerk zu erhöhen und eine Möglichkeit zu schaffen, die Konzepte der Industrie 4.0 sicher umsetzen zu können, wird an verschiedenen Themenfeldern geforscht um Erkenntnisse zu gewinnen und Lösungen zu entwickeln. Quelle [18] zeigt eine mögliche Klassifizierung dieser Felder. Die Autoren teilen die Forschung in die folgenden Themenfelder auf:

- Sichere Kontrolle
- Erkennung von Eindringungsversuchen
- Simulation und Modellierung
- Kommunikations- und Infrastruktursicherheit

Sichere Kontrolle („Secure Control“)

Unter diesem Begriff werden Forschungen zusammengefasst, welche sich mit dem Schutz von Informationen (d.h. Daten in der Speicherung und bei der Übertragung) befassen. Es gilt die Verfügbarkeit der Daten zu abzusichern, z.B. gegen Angriffe, die eine (langfristige) Störung als Ziel haben (Denial of Service (DoS)), sowie die Integrität und Vertraulichkeit der Informationen zu sichern (zur Vermeidung von fehlerhaften Ausführung und Täuschungen). Dabei spielt der Vertrauensgrad für die Korrektheit der übermittelten Daten („Veracity“) eine wichtige Rolle. Dabei sollen nicht nur Daten des IT-Bereichs, sondern auch Prozessdaten einbezogen werden.

Kernthemen sind etwa die sichere Identifizierung der Kommunikationsteilnehmer, Analyse von Entscheidungsmustern der Angreifer und damit verbundene Forschungen über die Robustheit bzw. die Anfälligkeit der Prozesses gegen Störungen.

Erkennung von Eindringungsversuchen

Wie in der klassischen IT-Sicherheit geht es bei diesem Gebiet darum herauszufinden in welcher Form industrielle Kontrollsysteme anfällig sind gegenüber Angreifern und die darauf basierende Entwicklung von Algorithmen und Maßnahmen um diese Angriffe zu erkennen und vorbeugende Maßnahmen zu treffen. Bereits entdecke Schwachstellen weisen u.a. unsichere Umsetzungen, aber auch Designfehler auf, die Angriffsmöglichkeiten eröffnen. Im Zuge dieses Themenfeldes haben sich Forscher auch u.a. mit dem Stuxnet-Programm beschäftigt, welches für die Manipulation des iranischen Atomprogramms verwendet wurde.

Simulation und Modellierung

Dieses Themenfeld beschäftigt sich hauptsächlich mit Fragen, die sich auf die Möglichkeit des Testens von IT-Sicherheitsmaßnahmen in industriellen Netzwerken beschäftigen. Die Grundproblematik teilt sich in zwei Elemente auf. Zum einen ist das Testen an realen Umgebungen sehr aufwendig, gefährlich und teuer, der Nachbau nicht öknomisch und aufwendig. Daher wird versucht mit sofware-basierten Frameworks zu arbeiten um die Arbeit eines automatisierten Fertigungssystems zu simulieren. Ein sehr wichtiger Punkt ist dabei die akkurate Simulation von physikalischen Prozessen und die fehlende Kompetenz/Fachwissen der Sicherheitsforscher in diesem Bereich. Andere Bereiche der Modellierung und Simulation beinhalten das (komplexe) Verhalten solcher Umgebungen und die Analyse von Kommunikationsmustern (Datenverkehr) innerhalb dieser Systeme.

Kommunikations- und Infrastruktursicherheit

Die Grundlage dieses Forschungsbereichs ist u.a. das Streben der Industrie nach einem einheitlichen Kommunikationsmedium in Form des Industrial Ethernets. Kernthemen sind dabei etwa die horizontale und vertikale Integration der Netzwerkteilnehmer und das Verpacken von Prozessdaten in Ethernet-Pakete und die damit verbundenen Herausforderungen der klassischen IT-Sicherheit. Hinzu kommt die wachsende Verzahnung und Abhängigkeiten der Teilsysteme und die Analyse von Risiken und Anforderungen für einen sicheren Betrieb. Forschungen dieses Bereichs richten sich damit u.a. auf Angriffsszenarien auf allen Hierarchieebenen des Netzwerkes von der

Unternehmensleitebene bis zur Feldebene, etwa Angriffsszenarien mit dem Ziel der Beschädigung oder Zerstörung des Fertigungssystems.

2.2 IT Security Schutzziele

In der IT-Sicherheit werden alle Ziele bezeichnet, die für die Sicherung von Systemen und Kommunikation zwischen Systemen sichergestellt werden müssen.

Mehr Kontext der Schutzziele einfügen

Dabei werden als Grundlage die folgenden Schutzziele betrachtet:

- Integrität: Bei der Kommunikation zwischen Systemen und der Speicherung bzw. dem Abruf von Daten auf einem System ist es wichtig, dass darauf vertraut werden kann, dass diese Daten nicht ohne Authorisierung verändert wurden. Daher befasst sich dieses Schutzziel mit der Korrektheit von Daten bzw. der korrekten Funktion eines Systems. Bei der Sicherstellung dieses Zieles geht es also darum die Veränderung von übertragenen oder gesicherten Daten und Software sicherzustellen.

- Vertraulichkeit: Innerhalb einer Infrastruktur oder auf einem System existieren verschiedene Arten von Daten, darunter auch sensible Daten, die von nichtauthorisierten Personen missbraucht werden können. Daher ist es notwendig den Zugriff zu Daten zu limitieren und dadurch diese Daten vor unauthorisiertem Zugriff zu schützen. Aktivitäten dieser Art werden dem Schutzziel Vertraulichkeit zugeordnet

- Verfügbarkeit: Diesem Schutzziel werden alle Aktivitäten zugeordnet, die den Betrieb von Systemen und die Erhaltung von Kommunikationswegen sicherstellen. Darunter fallen z.B. Maßnahmen, die den Zugriff von Kunden und/oder Mitarbeitern auf einen Webservice sicherstellen, auch im Falle eines Angriffes, der es zum Ziel hat die Erreichbarkeit des Services zu unterbinden.

Schutzziele: Beispiel für Schutzziele formulieren

Neben diesen Schutzzielen existieren auch noch weitere Schutzziele wie z.B. Authentizität, Nichtabstreitbarkeit, Zurechenbarkeit und Privatsphäre.

2.3 Risiko Management

Risiko Management bezeichnet einen Bereich bzw. eine Sammlung von Aktivitäten, die der Abschätzung, Planung und Vermeidung von Risiken für ein Unternehmen

bzw. eine Organisation dienen. Ein Risiko wird als Kombination aus der Eintrittswahrscheinlichkeit eines bestimmten Sicherheitsereignises und der damit verbundenen Konsequenzen definiert [24]. Nach der ISO27001 definiert ein Sicherheitsereignis laut Quelle [16] als eine Änderung eines Zustandes in der Informationsverarbeitung, welches mindestens theoretisch eine Auswirkung auf die Sicherheit haben kann. Die zentralen Begriffe für die Beschreibung eines Risikos sind „Schwachstelle“und „Bedrohung“. Eine Schwachstelle wird im Kontext der Informationstechnologie als eine potentiell ausnutzbare Schwäche bzw. Fehler in einem Asset bezeichnet. Der Begriff „Asset“beschreibt laut ISO27001 alles was für das Unternehmen bzw. die Organisation wertvoll ist, im Bezug auf Informationssysteme schließt dies u.a. Daten, Systeme, Anwendungen und Dienste (Services) ein. Unter einer Bedrohung wird widerum ein potentieller Auslöser für einen Sicherheitsvorfall verstanden, welcher Schaden am Unternehmen verursachen kann [16].

Daraus folgend wird das Risiko beschrieben durch die Wahrscheinlichkeit, dass eine Bedrohung konkrekt vorhanden ist und eine Schwachstelle ausnutzt.

Die Aktivitäten des Riskomanagement werden sowohl durch das NIST als auch durch den ISO27001 Standard in folgende Schritte zusammengefasst: Risikoabschätzung, Risikovermeidung, Risikoakzeptanz und Risikokommunikation.

Die Abschätzung potentieller Risiken ist der erste Schritt, der sich in verschiedene Unterpunkte gliedert. Dazu zählt zunächst die Identifikation potentieller Risiken und die Analyse der gefundenen Risiken. Von der Beschreibung eines Risikos, die aus der Analyse folgt, ist der Detailgrad sehr wichtig für die Präzision der Risiko Abschätzung [16]. So kann etwa die Risikoabschätzung für die potentielle Ausnutzung einer Schwäche an einem Systems innerhalb des Unternehmensnetzwerkes präziser geschätzt werden, wenn der konkrete Zugriffsweg des Angreifers präzise beschrieben wird. Einen weiteren Unterpunkt der Risikoabschätzung stellt die Risikoevaluation ein, die die Bewertung und Beurteilung eines Risikos beinhaltet. Dies beinhaltet neben der konkreten Einschätzung einer Eintrittswahrscheinlichkeit auch die Erarbeitung potentieller Gegenmaßnahmen [24].

Der zweite Schritt umfasst die Risikovermeidung. Diese schließt die Priorisierung bestimmter Risiken sowie die Umsetzung und Pflege der Maßnahmen zur Vermeidung der priorisierten Risiken ein.

Als dritter Schritt wird die Risikoakzeptanz genannt. In diesem Schritt werden die übrigen Risiken neu bewertet. An diesem Punkt können abhängig von der Entscheidung der Verantwortlichen weitere Gegenmaßnahmen eingeleitet oder aber auch Risiken als Restrisiko für das Unternehmen akzeptiert werden.

Die resultierende Risiko Management Strategie wird im letzten Schritt mit be-

troffenen Vertragspartnern kommuniziert [24].

2.4 Security Information and Event Management

2.4.1 SIEM Konzept und Zweck

Im Umgang mit Security Information and Event Management (SIEM) Systemen werden oft die Begriffe „Information“, „Ereignis“ und „Daten“ verwendet. Um eine Grundlage für die Verwendung dieser Begriff in der vorliegenden Thesis zu geben, werden im folgenden diese Begriffe wie folgt definiert:

- Ereignis (Event): Unter einem Ereignis ist in diesem Zusammenhang das Auftreten von systemrelevanten Aktionen zu verstehen. Dabei kann zwischen Systemereignissen, z.B. das Laden eines Programmes, und Benutzerereignissen, z.B. Anschläge auf der Tastatur, unterschieden werden.

- Daten: Daten sind die Bausteine aus denen Ereignisse zusammengesetzt werden. Daten sind z.B. der Name des geladenen Programms oder der Wert einer Benutzereingabe.

- Information: Eine Information ist in diesem Kontext die Interpretation verschiedener Ereignisse, die eine Aussage über den Zustand eines Systems ermöglicht.

Die IT Infrastruktur von Unternehmen umfasst eine große Menge an Elementen wie Server, Arbeitsstationen, Netzwerkgeräte, Sicherheitssysteme und mobile Endgeräte (z.B. Laptops und Mobilfunkgeräte). Um diese Infrastruktur zu schützen reicht es nicht diese hinter einem Schutzwall zu positionieren, es ist auch wichtig zu erfassen welche Aktionen von wem wie und von wo innerhalb des Netzwerkes ausgeführt werden. Daher ist es wichtig, dass es Informationsquellen gibt aus denen diese Informationen ausgelesen und bewertet werden können. In Unternehmens-netzwerken wird dies typischerweise von den Elementen selbst durchgeführt. So befinden sich z.B. auf einem Server mit den Betriebssystem Windows verschiedene Log-Dateien, die Informationen darüber speichern welcher Anwender sich zu welchem Zeitpunkt angemeldet hat, wie viele Versuche für die Eingabe des Passwortes verwendet werden und welche Prozesse von diesem Anwender ausgeführt wurden. Die Analyse dieser Log-Dateien kann fachkundigen Administratoren Aufschluss darüber geben welche Aktionen von dem Benutzer oder dem System durchgeführt wurden. Eine Herausforderung bei dieser Analyse ist die Bewältigung der schieren Menge an Informationen

und das Filtern relevanter Ereignisse. Selbst eine geringe Anzahl an Systemen kann eine große Menge an Daten produzieren welche von einem Administratorenteam ohne Hilfe von Werkzeugen nicht zu bewältigen sind. Mit Hilfe technischer Werkzeuge können die Daten in Log-Dateien gefiltert werden. Die Suche nach sicherheitsrelevanten Informationen kann dabei automatisiert werden und Administratoren können über Anomalien im Verhalten der Systeme informiert werden.

Allerdings bietet diese Vorgehensweise auch Nachteile. So ist die Definition der Regeln nach denen Werkzeuge Log-Dateien durchsuchen eine komplexe Aufgabe, denn diese Regeln müssen eng genug gefasst sein um die Anzahl der Sicherheitsmeldungen verwaltbar zu halten, aber auch weit genug um potentiell bedrohliche Situationen zu erkennen. Um eine bedrohliche Situation bewerten zu können müssen Administratoren nicht nur in der Lage sein die Meldungen des Werkzeuges zu verstehen, sondern diese auch im korrekten Kontext einordnen zu können. Diese Einordnung kann in komplexen Netzwerken sehr schwierig sein.

Um diese Einordnung zu vereinfachen und die Anzahl an Falschmeldungen („False Positives“) zu reduzieren ist es also notwendig nicht nur ein Element sondern verschiedene Elemente im Zusammenspiel zu betrachten und die Informationen dieser Netzwerkelemente zu verknüpfen, also einen Zusammenhang von Informationen von verschiedenen Elementen zu erfassen. Für die Unterstützung der Administratoren bei dieser Aufgabe wurden Security Information and Event Management (SIEM) Systeme entwickelt.

Ein SIEM System ist also ein System, welches Informationen aus verschiedenen Quellen extrahiert, die einzelnen Informationsquellen analysiert und die gewonnenen Informationen in einen Zusammenhang bringt. Durch Aggregation von ähnlichen Daten und Korrelation dieser Daten lassen sich einzelne Alarmmeldung in einen Zusammenhang setzen und neue Informationen über den Wert und den Kontext der Meldungen gewinnen. Dadurch ist es möglich den Zustand eines Netzwerkes und seiner Elemente über ein zentrales System zu überwachen und kritische Situationen zu erkennen, die durch das Betrachten einzelner Elemente nicht erkennbar sind. Das SIEM System bildet damit eine zentrale Verwaltungsschicht oberhalb der Netzwerkelemente.

Um diese Funktion auszuführen sind verschiedene Schritte notwendig. Die Aufgaben teilen sich dabei in zwei Bereiche auf: Security Information Management (SIM) und Security Event Management (SEM). SIM ist eine Unterkategorie des Log Management Feldes, das heißt es umfasst Erfassung, Extraktion, Transfer und Sicherung von sicherheitsrelevanten Informationen in Log-Dateien. SEM umfasst Funktionen für die Analyse und Verknüpfung von Ereignissen in Echtzeit.

Der erste Schritt ist die Extraktion der Daten von den Netzwerkelementen. Dies kann entweder durch Anbindung einer geeigneten Schnittstelle durchgeführt werden (z.B. Meldungen von Sicherheitssystemen wie einer Firewall oder einem Intrusion Detection System (IDS)) oder durch Extraktion der Informationen über Kollektoren in Form von Software Agents. Der zweite Schritt betrifft die Übertragung der extrahierten Informationen. Diese muss sicherstellen, dass die Informationen vollständig und unverändert übertragen werden, da veränderte Informationen die Informationsgrundlage verändern auf der das SIEM System seine Analyse durchführt.

Da nicht jedes System gleich ist und auch Log-Dateien und -Formate sich deutlich unterscheiden können, müssen die vom SIEM empfangenen Informationen vorverarbeitet und in ein einheitliches Format umgewandelt werden. Dieser Schritt wird als „Normalisierung“ bezeichnet. Die normalisierten Daten können dann zentral gespeichert und für statistische Langzeitanalysen und statistische Verwertungen gespeichert werden. Dabei ist es wichtig darauf zu achten, dass die abgelegten Daten nicht verändert werden können und das Änderungen nachvollziehbar sind. Da die Datenmenge abhängig von der Größe und Komplexität sehr groß sein kann und die Ressourcen des SIEM Systems für die Analyse und Bewertung begrenzt sind, werden ähnliche Daten in einem Zwischenschritt zusammengefasst, sodass die zu analysierende Menge an Daten deutlich reduziert wird. Man spricht dabei von der Aggregation der Daten. Die Aggregation kann z.B. dadurch erfolgen, dass Ereignisse desselben Ursprungs und desselben Inhalts als eine Meldung zusammengefasst und mit einem Zähler versehen werden, der die Anzahl der Meldungen wiederspiegelt. Im nächsten Schritt werden die aggregierten Daten dann durch ein Regelwerk analysiert. Dieses Regelwerk wird manchmal auch als „Rule Correlation Engine“ bezeichnet. Dabei werden verschiedene Meldungen mit Regeln abgeglichen. Wird eine Regel als erfüllt angesehen, wird eine Alarmmeldung an verantwortliche Administratoren ausgegeben, sodass weitere Maßnahmen ergriffen werden können. Die Bewertung ob eine Regel erfüllt wurde hängt von der verwendeten Korrelationstechnik ab. So müssen z.B. eine Reihe von Bedingungen erfüllt werden, damit eine Regel als erfüllt angesehen wird. So könnte z.B. eine Regel beinhalten, dass ein Alarm ausgegeben wird, wenn mehrere nicht-erfolgreiche Anmeldungsversuche von einem inaktiven Account von einer nicht-registrierten IP-Adresse protokolliert wurden. Die Bildung solcher Regelwerke kann sehr komplex sein und durch verschiedene Techniken gebildet werden.

In der Praxis werden SIEM Systeme u.a. in Security Operations Center (SOC) eingesetzt. Das SIEM hilft in diesem Kontext nicht nur den Administratoren für die Verwaltung, sondern ersetzt auch die Verwaltung und Analyse über verschiede-

nen UIs unterschiedlicher Sicherheitsprodukte (z.B. von Firewalls, IDSs, Anti-Virus Software). Hier zeigen sich neben den Vorteilen von SIEM Systemen auch aktuelle Grenzen. So kann ein SIEM nur auf der Informationsbasis operieren, die in der jeweiligen Umgebung zur Verfügung steht. So kann sich das Fehlen von Informationen zum Kontext der Meldungen auf die Auswertung auswirken, da fehlende Informationen zu ungenauen Analysen oder False Positives bzw. False Negatives (kritische Meldungen, die als harmlos klassifiziert werden) führen können. Eine andere Limitierung sind Abfragezeiten von gespeicherten Langzeitdaten für die Echtzeitanalyse durch die entweder die Analyse oder die Menge der Daten begrenzt wird. Auf der technischen Seite ergeben sich zudem Herausforderungen entlang der Funktionskette eines SIEM Systems bei der Datenextraktion aus proprietären Formaten, der effektiven und sicheren Speicherung der Daten sowie der Analyse und Erstellung von Korrelationsregeln in komplexen Systemen.

2.4.2 SIM Log Management

Security Information Management (SIM) bezeichnet die Verwaltung von Log-Dateien im SIEM Kontext und bildet damit eine Untermenge des Log Management. Sicherheitsrelevant sind in diesem Falle alle Log-Dateien, die Auskunft über den Zustand eines Systems oder einer Kommunikation zwischen Netzwerkelementen geben können. Dazu zählen sowohl Log-Dateien von Betriebssystemen und Programmen als auch von Netzwerkswitches und anderen Elementen, die den Datenverkehr zwischen Teilnehmern im Netzwerk aufzeichnen. Eine Log-Datei besteht aus Ereignissen, die Daten zu Aktionen (u.a. Zeitpunkt, ausführender Benutzer, ausführender Prozess (ID), ...) enthalten. Diese Daten können interpretiert werden und liefern Informationen über den Zustand des Systems zum bestimmten Zeitpunkt.

Log Management umfasst die Sammlung, Übertragung, Normalisierung, Zentralisierung und Aufbewahrung der Menge an Log-Dateien. In großen Unternehmen kann diese Menge mehrere hundert Gigabyte umfassen. Das Verwalten der Log-Dateien wird aus mehreren Gründen in Unternehmen als außerordentlich wichtig angesehen. Zum einen beinhalten Log-Dateien Informationen über den Zustand der Umgebung und können damit Rückschlüsse auf potentiell schädliche Aktionen zulassen, zum anderen können durch diese Informationen auch die Einhaltung von geltenden Richtlinien und Anforderungen gegenüber Kunden und Institutionen belegt werden. Daraus folgt, dass sichergestellt werden muss das die Informationen nicht nur korrekt aus den verschiedenen Quellen extrahiert werden können, sondern auch die Umwandlung und ggf. Veränderung der Daten dokumentiert werden muss um die Integrität der Informationen zu gewährleisten. Dies spielt u.a. für die Sicherheits-

analyse eine wichtige Rolle, da nur mit den richtigen Informationen die korrekten Rückschlüsse auf die Sicherheit der Umgebung geschlossen werden können. So lassen sich u.a. mit forensische Analysen rückwirkend Aktionsketten, die zu einer Richtlinienverletzung oder eines nicht-authorisierten Eindringens in das System geführt haben, rekonstruieren. Darüber lassen sich aus den Informationen Grundlagen für den Normalzustand eines Systems ablesen und entsprechende Regeln formulieren.

Log Management: Unterschied zwischen Log Management Systemen und SIEM Systemen herausstellen/formulieren

Log-Dateien können aus fast jedem System gewonnen werden. Dazu zählen u.a.

- Anti-Malware und Anti-Virus Systeme
- Intrusion Detection Systems / Intrusion Prevention Systems
- Remote Access Software
- Web Proxieserver
- Vulnerability Management Software
- Network Access Control (NAC) Server
- Firewalls
- Router

Eine interessantes Thema in diesem Zusammenhang ist die Frage welche Log-Dateien und Event-Daten sicherheitsrelevant sind. Moderne und komplexe IT-Umgebungen produzieren mehrere hundert Gigabyte an Event-Daten auf einer täglichen Basis. Daher ist die Definition sicherheitskritischer Elemente (Systeme, Kommunikationspfade, Applikationen, ...) eine wichtige Aufgabe. Dazu können unter anderem diese Elemente gehören:

- Logs der Security Controls (z.B. Firewalls, Intrusion Detection SystemIntrusion Prevention System, Data Loss Protection)
- Logs der Netzwerk Infrastruktur (z.B. Domain Name Service (DNS) Server, Dynamic Host Configuration Protocol (DHCP) Server, VPN Logs)
- Informationen über die Infrastruktur aus anderen Quellen (z.B. Informationen zu Systembestand und Netzwerksegment eines Elements)
- Informationen über das Unternehmen

Log Management: Log Management Architektur einfügen?

Log Management: Beispiel für Log Management Architektur einfügen

Eine große Herausforderung des Log Management ist das Schaffen einer Balance zwischen limitierten, verfügbaren Ressourcen für das Verwalten der Log-Dateien und der Menge an zu verarbeitenden Log-Dateien pro Zeiteinheit. Dabei spielen nicht nur die potentiell große Menge an Dateien in einer komplexen Umgebung eine Rolle, sondern auch der Umgang mit Inkonsistenzen zwischen vergleichbaren Logs (etwa in Bezug auf den Zeitstempel), der Umwandlung aus verschiedenen Formaten und das Wachstum an Daten mit dem Hinzufügen von weiteren Systemen in die Umgebung.

2.4.3 Kollektoren

Die Extraktion, oder auch Sammlung, der Daten von den Elementen des Netzwerkes bildet die Grundlage auf der das SIEM System (und ein Log Management System) funktioniert. Die Daten werden von vielen verschiedenen Geräten extrahiert, die eine gewisse gemeinsame Grundmenge an Daten bieten, darüber hinaus aber auch weiteren Kontext abhängig von Applikation, Betriebssystem oder Gerät selbst. Daher muss eine Schnittstelle geschaffen werden, die diese proprietären Datenformate mit Hilfe eines Parsers auszulesen und zu einem einheitlichen Format umwandeln [4]. Dies ist die Aufgabe der Kollektoren. Eine weitere Aufgabe des Kollektors ist zudem die eines Filters für relevante Ereignisse.

Ein Kollektor ist demnach ein Service, oder auch Software Agent, der diese Aufgabe übernimmt. Dabei sind verschiedene Elemente zu betrachten, wie die verfügbaren Daten, Ressourcen der Datenquelle, Kommunikation zwischen Datenquelle, Kollektor und SIEM System sowie der Ansatz für einen bestimmten Gerätetyp. So stellt etwa das Protokoll, das für die Kommunikation mit der Datenquelle genutzt wird, eine Art Sprache dar, in der die Kommunikationspartner miteinander kommunizieren. Diese Kommunikationsform muss vorher vereinbart worden sein und dabei kann auf eine große Variation an Kommunikationsprotokollen zurückgegriffen werden. Der Kollektor für den entsprechenden Geräte-, Betriebssystem- oder Applikationstyp muss natürlich dieses Protokoll unterstützen. Alternativ dazu können Daten auch in weit verbreiteten Formaten wie etwa im „syslog“ Format abgelegt und durch den Kollektor oder eine Schnittstelle übermittelt werden.

Bei dem Ansatz der Datensammlung kann bzgl. SIEM Kollektoren zwischen dem Agent-basierten und dem Agent-losen Ansatz unterschieden werden. Der Agent-basierte Ansatz wird durch die Installation der Kollektoren auf den jeweiligen Netzwerkelementen aufgebaut. Dadurch ergibt sich eine dezentrale Verarbeitung, die zum

einen Ressourcen des SIEM System spart, zum anderen aber auch einen erhöhten Verwaltungsaufwand für Kollektoren auf den verschiedenen Elementen des Netzwerkes bedeutet. Der Agent-lose Ansatz hingegen nutzt Kollektoren als Schnittstelle, die vom zentralen SIEM System aus mit den Komponenten über Schnittstellen kommuniziert. Hier wird die Verwaltung der Kollektoren erleichtert, aber es muss auch die Netzwerklast berücksichtigt werden, die durch die Kommunikation zwischen den SIEM Kollektoren und den Datenquellen erzeugt wird. Zudem muss über die entsprechenden Schnittstellen sichergestellt werden, dass Daten nicht auf der Datenquelle selbst oder während der Übertragung verändert werden.

Orientiert an den Aussagen aus der Industrie wird mehr und mehr zum dezentralen Ansatz tendiert, da die Agenten zusätzliche Funktionalitäten bieten können sowie Herausforderungen im Bereich der Regelung von Remote-Administrations Rechten, Security Compliance, Ressourcenmanagement und der Speicherung von hoch privilegierten Zugriffsdaten zu verschiedenen Systemen auf einer zentralen Instanz. Allerdings ist der Einsatz von Agenten auf Elemente mit einem entsprechenden Betriebssystem beschränkt. Hardware-Elemente mit proprietären Betriebssystemen wie etwa Netzwerk-Geräte unterstützen den Agenten-basierten Ansatz nicht und müssen daher selbst die Informationen in einem für das SIEM verständlichen Format zu der SIEM Instanz schicken oder eine Schnittstelle für den administrativen Remote-Zugriff bieten.

Kollektoren: Füge Definition für "Parsing"hinzu

Kollektoren: Zeige die Datenextraktion anhand eines Beispiels

Herausforderungen auf Basis von Log Dateien

Unabhängig von der Wahl des Ansatzes bestehen für die Analyse der Logs einige Herausforderungen, die auch oder im Speziellen Kollektoren betreffen. Da Logdateien pro System oder gar pro Anwendung in unterschiedlichen Formaten und mit unterschiedlichen Strukturen angelegt werden, muss ein Kollektor in der Lage sein, sowohl das Format, die Struktur als auch gängige Konstrukte zu erkennen und auszulesen. So muss ein Kollektor pro System, auf die systemspezifischen Schnittstellen und/oder Logdateien zugreifen können. Die Logdateien auf dem System können abhängig von der Systemart und/oder dem Betriebssystem bspw. als Textdatei, XML-Datei oder in einem binären Format abgelegt werden. Die Einträge innerhalb der Log-Dateien können einzeilig oder mehrzeilig gespeichert werden. Ein Kollektor muss in der Lage sein, diese Informationen zu erkennen und in den Lese- und Verarbeitungsprozess einfließen zu lassen [14].

Neben diesen formalen Herausforderungen besteht zudem die Möglichkeit der Korruption von Logdateien sowie das Vorkommen von Inkonsistenzen. Ein Kollektor muss also in der Lage sein, den Lese- und Verarbeitungsprozess trotz fehlerhafter Einträge fortzuführen. Die Erkennung von Inkonsistenzen kann eine weitere Herausforderung im Bezug auf wiedersprüchliche Einträge, sofern dies Teil der Filterungsaufgabe des Kollektors ist. In diesem Bezug spielt natürlich auch die Performanz des Kollektors bei der Verarbeitung eine Rolle. So ist z.B. die Frage zu stellen, inwiefern bestimmte Logdateien einen sogenannten „Performance Overhead“erzeugen basierend auf der Formatierung und der Menge des Inhalts [14].

2.4.4 Event Verarbeitung

Durch die hohe Anzahl an Daten und Logquellen ist es notwendig relevante Einträge herauszufiltern und weiter zu verarbeiten, sodass die gewonnenen Informationen für die Überwachung und Analyse der Organisation verwendet werden können.

Die Ereignisdaten, die aus den Logs gewonnen werden, müssen daher zusammengefasst und auf Grund der Diversität der Logquellen vereinheitlicht werden. Aus diesem Grund können Logeinträge von den Kollektoren ausgelesen und sofern möglich die Daten in neue Logdateien mit einheitlichen Feldern transferiert werden. Im Kontext der SIEM Systeme gibt es verschiedene Begriffe und Ebenen für die Zusammenführung unterschiedlicher Datensätze zu einem einheitlichen Datensatz, im Bezug auf die Vereinheitlichung von Logeinträgen wird in diesem Fall der Begriff „Normalisierung “verwendet. Dabei werden Logeinträge (Ereignisse) in verschiedene Kategorien unterteilt und die Daten in entsprechend strukturierten Datensätzen gespeichert [22].

Diese kann, abhängig von der Menge an unterschiedlichen Logdateien und -quellen, auf Grund der notwendigen Vorarbeit für die Erarbeitung eines geeigneten Datenbank Schemas komplex oder sehr schwierig sein [33].

Die zweite Aktivität im Bezug auf die Verarbeitung von Logeinträgen ist die Aggregation. Bei der Aggregation werden ähnliche Ereignisse, meist basierend auf bestimmten Feldern wie etwa Quell-IP, Ziel-IP und Event-ID, zu einem Ereignis zusammengefasst. Diese Methodik hilft dabei die Analyse der eingehenden Daten und kann damit die benötigte Menge an technischen und zeitlichen Ressourcen reduzieren. Auch kann sie ggf. bei der Vorverarbeitung helfen die Menge der zu übertragenden Informationen, und damit die Netzwerklast, deutlich reduzieren. Zu guter Letzt können durch die Reduzierung der Datenmenge diese Daten formatiert schneller und mit geringerem Speicherverbrauch gespeichert und abgerufen werden. Die Verwendung von Aggregationsmethoden kann jedoch auch dazu führen, dass

ggf. wichtige Daten nicht zur Verfügung stehen. Daher ist es in der Praxis wichtig, die Aggregationsmethodik bzw. -regeln abhängig von bestimmten Faktoren wie etwa der Häufigkeit oder Bedeutung im Bezug auf den Sicherheitskontext [23].

Diese Aufgaben können durch das zentrale System oder verteilte Agenten durchgeführt werden.

2.4.5 Security Event Management

Security Event Management befasst sich mit der Echtzeit-Analyse von normalisierten Events, der Korrelation dieser Events sowie der Benachrichtigung von Sicherheitsadministratoren und der Darstellung relevanter Informationen. Man kann in diesem Zusammenhang auch von kontext-bewusster Überwachung sprechen.

Bei der Echtzeit-Analyse werden die extrahierten, normalisierten Events auf ihre Bedeutung untersucht. Dabei werden die Events einzeln für sich betrachtet und basierend auf den Daten(feldern) Informationen gewonnen. Diese Informationen werden bei der Korrelation der Events verwendet um einen Zusammenhang herzustellen. Dabei werden u.a. zusätzliche Informationen hinzugezogen, z.B. die Quelle der Informationen und Informationen zu der entsprechenden Quelle. Dies ist notwendig um die Herstellung falscher Zusammenhänge zu minimieren. Die Herstellung der Korrelation basiert auf den verwendeten Techniken. So können Regelwerke auf verschiedene Art und Weisen hergestellt werden. Die Spannweite der Korrelationsregeln reicht dabei von simplen Wertevergleichen über Regeln mit verschiedenen Bedingungen hin zu der Erzeugung komplexer Szenarien durch Machine Learning und Big Data Ansätze. Wird eine Korrelationsregel erfüllt wird ein Alarm ausgegeben. Diese Alarme können abhängig von ihrer Priorität und Häufigkeit widerum durch Aggregationsregeln zusammengefasst werden.

Die durch die Korrelationsregeln ausgelösten Alarme helfen den Analysten in einer Organization kritische Situationen zu erkennen. Sie dienen dabei als Indikator für eine Kompromitierung (IoC, Indicator of Compromise). In größeren Organisationen sind die Analysten Teil eines „Security Operation Centers“. In diesem Zentrum arbeiten Analysten mit verschiedenen Qualifikationen. So werden Indikatoren etwa zunächst von einem Analyst der Stufe 1 auf einen potentiell fälschlich ausgelösten Alarm (False Positive) untersucht und bei Feststellung eines Problems an Analysten der Stufe 2 weitergegeben. Diese Struktur dient zur effektiven Bewältigung der ausgelösten Alarme [2].

2.4.6 Features & Gemeinsamkeiten von SIEM-System-Anbietern

Für die allgemeine Betrachtung von SIEM Systemen kann es nützlich sein, die Gemeinsamkeiten und Unterschiede gebräuchlicher SIEM Anbieter zu kennen. Nach den Quellen [26, 20, 5] gehören zu dieser (nicht vollständigen) Liste AlienVault, HP Enterprise, IBM, LogRythm, RSA, Solar Winds und Splunk.

Die Produkte dieser Anbieter bieten jeweils ein Minimum an grundlegenden Funktionen eines SIEM Systems zusammen. Dazu zählt die Möglichkeit der Sammlung von Logs von vielen typischen Quellen, die Archivierung und Analyse der erhobenen Daten, sowie die Korrelation und Echtzeit-Überwachung der Quellen (d.h. Server, Netzwerkgeräte, Sicherheitslösungen, Anwendungen, etc.). Zusätzlich setzen die Produkte sogenannte „Threat Intelligence Feeds“ein um (Kontext-)Informationen zu neuen Schwachstellen und/oder Bedrohungen zu erhalten.

Die Unterschiede ergeben sich in der Architektur als auch in der Spezialisierung auf die Größe einer Organisation. Bzgl. der Architektur ergeben sich prinzipiell drei unterschiedliche Modelle: Cloud-basierte Lösungen, hardware-basierte Lösungen und anwendungsbasierte Lösungen. Cloud-basierte Lösungen bieten SIEM Funktionalitäten ausgelagert als einen Service an, der die Log-Quellen einer Organisation sammelt und analysiert. Hardware- und anwendungs-basierte Lösungen werden innerhalb der Infrastruktur der Organisation installiert und von dieser Organisation konfiguriert und gepflegt. Die Größe der Organisation kann dabei von sogenannten „SMBs“(Small to Middle Sized Businesses) bis zu sehr großen und komplexen Infrastrukturen reichen.

Die Spezialisierungen der einzelnen Produkte können nach verschiedenen Kriterien festgelegt werden. Nach Studie der Quellen ergeben sich die folgenden Kategorien für Spezialisierungspunkte:

- Möglichkeiten der Erschließung von Logquellen - Dies kann entweder durch eine größere Menge an unterstützten Logquellen erfolgen oder durch eine flexiblere Anpassungsmöglichkeit (mit höherem administrativen Aufwand)(s. Splunk)
- Möglichkeiten der Korrelation unter Einbeziehung der Logdaten sowie weiterer externer Quellen für die Integrierung von Kontextdaten wie etwa Threat Intelligence Feeds
- Zusätzliche Fähigkeiten wie etwa „Deep Packet Inspect“oder „User Behavior Analytics“
- Möglichkeiten der Visualisierung des Status von Datenströmen und Netzwerken

- Schwierigkeitsgrad der Installation und Einrichtung

Bei dieser Kategorisierung sein angemerkt, dass diese Liste keinesfalls vollständig ist oder sein kann. Nach den Einschätzungen der oben genannten Quellen muss für jede Organisation individuell geprüft werden, welche Fokuspunkte notwendig sind. Diese Kategorien geben lediglich grundlegende Elemente an. Quelle [27] etwa kategorisiert nach sieben grundlegenden Fragen: grundlegenden Unterstützung von Logquellen und -format, Möglichkeiten der zusätzlichen Protokollierung von zusätzlichen, relevanten Daten, die Nutzung und Qualität von Threat Intelligence Feeds, Möglichkeiten für forensische Analysen, zusätzliche Möglichkeiten für die Analyse und Examinierung von Daten, Qualität von automatischen Reaktionsmaßnahmen und Unterstützung für die Erfüllung von Industriestandards.

2.5 Infrastruktur Office

Für den Vergleich zwischen Unternehmensnetzwerk und industriellem Netzwerk ist es notwendig beide Netzwerke zu kennen. Dieser Abschnitt stellt eine Fundament zur Verfügung auf dessen Basis die Analyse des Models eines Unternehmensnetzwerkes gestartet werden kann. Das Ziel ist es einen guten Überblick über die allgemeinen Elementtypen in solchen Netzwerkinfrastrukturen zu geben und ihre Kerncharakteristiken zu beschreiben und ihre Anordnung über Architekturtypen in den Kontext zu setzen. Neben den Netzwerkelementen als Quelle der Daten muss zudem die Kommunikation bzw. die verwendeten Kommunikationsschnittstellen in Form der Netzwerkprotokolle berücksichtigt werden, da die versendeten Pakete ebenfalls wichtige Daten enthalten um das Verhalten der System zu verstehen. Zuletzt soll noch eine grobe Übersicht über potentielle Angriffsszenarien bzw. -techniken gegeben werden. Die Kenntnis dieser Szenarien ermöglicht es später in der Analyse einen Bezug zu der Bedeutung der verfügbaren Daten des Netzwerkes herzustellen.

2.5.1 Geräte

Ein Unternehmensnetzwerk kann aus vielen verschiedenen Elementen bestehen. Dies beinhaltetet (verteilte) Anwendungen und Dienste, die auf der Basis von verschiedenenen, teils spezialisierten, Betriebssystemen installiert werden. Im Bezug auf physische Geräte können die Elemente jedoch in drei Basiskategorien unterteilt werden:

- Endgeräte (PCs, Laptop, Handy, ...)
- Server

- Netzwerkgeräte (Switches, Router, Firewalls, Sicherheitselemente (z.B. Intrusion Detection Systems))

Um Unternehmensprozesse durchzuführen werden verschiedene Server-Elemente benötigt. Ein Server ist ein zentrales Computerelement, welches mit mehreren anderen Elemente verbunden werden kann und entsprechenden Zugriff von diesen Elementen erlaubt. Zudem verfügen Server oft über leistungsfähigere Hardware und Speicherressourcen als ein Endgerät. Server werden benutzt um zentrale Applikationen bereitzustellen und zu verwalten. Dazu zählen neben Applikationen und (zugehörigen) Datenbanken auch Benutzerverwaltungssysteme und Sicherungscluster (Cluster := eine Menge an Servern, die durch eine zusätzliche Virtualisierungsschicht zu einem Element verknüpft werden). Zu den üblichen Serverarten zählen Webserver, Datenbankserver, Anwendungsserver, Proxyserver und Dateiablagesysteme, auf die über eine Netzwerkschnittstelle zugegriffen werden kann.

Ein Webserver stellt über das Netzwerkprotokoll HTTP (Hypertext Transport Protocol) bzw. HTTPS erreichbare Dienste wie etwa Webseiten oder Webdienste zur Verfügung. Zu den typischerweise verwendeten Webservern zählen Microsofts IIS sowie Apache Webserver (meistens auf Basis eines Linux-basierten Servers wie etwa Ubuntu, CentOS oder RedHat). Ein Datenbankserver stellt den Zugriff auf eine strukturierte Menge von Daten in Form einer Datenbank über das Netzwerk zur Verfügung. Das verwendete Netzwerkprotokoll ist abhängig von dem installierten Datenbanktyp. Typische Datenbanken sind etwa Microsoft SQL Server, Oracle Database oder MySQL. Ein Anwendungsserver ist meist ein dedizierter Server für eine spezielle Anwendung, die einen Dienst für das interne Netzwerk bereitstellt. Beispiele sind etwa VPN-Server, Email-Server oder Sicherheitszugänge zu speziell geschützten Resourcen des Netzwerkes. Dateiablagen (FTP Server) nutzen die File Transfer Protocol Schnittstelle um den Zugang zu auf dem Server gespeicherten Daten (z.B. Dokumente verschiedenen Typs) über das Netzwerk verfügbar zu machen. Proxyserver schließlich dienen als Zwischenpunkt zu einem anderen Netzwerk. Proxyserver werden z.B. benutzt um sonst vom WAN/Internet abgeschotteten Servern oder Endgeräten den kontrollieren Zugang zum Internet zu ermöglichen.

Netzwerkgeräte dienen der Verbindung und/oder Überwachung der Kommunikation zwischen den einzelnen Netzwerkelementen. Diese lassen sich typischerweise in Router und Switche unterteilen. Router dienen der Verknüpfung mehrerer lokaler Netzwerke. Typischerweise existieren in Unternehmensnetzwerken eine Vielzahl an unterschiedlichen lokalen Netzwerken (auch Netzwerksegmente genannt), die es zu verbinden gilt. Daher kann im Rahmen dieser Netzwerken von zwei Routertypen gesprochen werden: „Edge-Router“und „Core-Router“. Der Typ Edge-Router

bezeichnet Router, die an den Grenzen des Unternehmensnetzwerkes zum WAN/Internet platziert sind, d.h. sie stellen die Verbindung zum Internet her. Core-Router widerum dienen dazu, die verschiedenen Netzwerksegmente innerhalb des Unternehmensnetzwerk miteinander zu verbinden. Diese Geräte existieren widerum, je nach Hierarchiestufe, in unterschiedlichen Fertigungen und sind angepasst für die jeweilige Aufgabe und Position im Netzwerk.

Die Netzwerksegmente werden aus Sicherheitsgründen oft bestimmten Zonen zugewiesen (dazu später mehr im Abschnitt Ärchitekturtypen"). Die Verbindungen, die durch Core-Router hergestellt werden, werden typischerweise durch Firewalls abgesichert. Firewalls stellen eine Art vorkonfigurierten Filter dar, der abhängig von den konfigurierten Regeln und Parametern nur Datenverkehr mit bestimmten Netzwerkprotokollen aus und zu bestimmten Teilen des Netzwerkes zulassen. Zusätzlich zu Firewalls werden außerdem Sicherheitselemente benötigt um den Datenverkehr zwischen den Netzwerkelementen zu überwachen. Diese Elemente werden Intrusion Detection Systems (IDS) bzw. Intrusion Prevention Systems (IPS) genannt. Ein IDS kann an einer bestimmten Stelle im Netzwerk platziert werden und ein Netzwerkpaket bzw. eine Sequenz von Netzwerkpaketen mitlesen und auf verdächtige Inhalte untersuchen. Für die Untersuchungsmethodik wird typischerweise eine Kombination aus der Suche nach bekannten Mustern im Datenverkehr als auch nach anomalen Datenpaketen oder -sequenzen verwendet. Ein IPS ist prinzipiell ein Gegenstück zu einer Firewall. Die Aufgabe des IPS ist es den Datenverkehr zu analysieren und nach vorkonfigurieten Regeln Datenpakete von spezifizierten Netzwerkprotokollen aus spezifizierten Teilen des Netzwerkes zu blockieren. Es existieren noch weitere potentielle Sicherheitselemente (wie etwa ein hardware-basierendes SIEM System), die jedoch in ihrer Grundfunktion auf Basis eines Server fungieren und daher hier nicht näher erläutert werden.

Endgeräte werden von Mitarbeitern und Gästen des Unternehmens verwendet als Zugangswerkzeug zum Unternehmensnetzwerk. Basierend auf den Richtlinien und Sicherheitsvorgaben sind diese Geräte deutlich eingeschränkt. Die Benutzer auf den Endgeräten werden üblicherweise in eine Domäne eingebunden um eine zentrale Benutzerverwaltung zu ermöglichen. Endgeräte können sowohl stationär als Arbeitsstation als auch mobil in Form von Laptops, Tablets oder Mobiltelefonen existieren.

Sicherheitsanforderungen (Zweck und grobe Beschreibung) formulieren

2.5.2 Architekturen & Anforderungen

Unter „Unternehmensarchitekturen“bzw. dem Design dieser Architekturen versteht man eine Sammlung an Architekturen aus verschiedenen Perspektiven. Diese definieren die verschiedenen Sichten und Schichten die ein Unternehmen definieren. Im speziellen wird der Begriff Unternehmensarchitektur definiert als eine zusammenhängendes Ganzes von Privilegien, Methoden und Modellen, die genutzt werden im Design und der Umsetzung von organisatorischen Unternehmensstrukturen, Unternehmensprozessen, Informationssystemen und -Infrastrukturen [19]. Im Kontext der Betrachtung von Informationsquellen für SIEM Systemen wird hier nur die Infrastruktur der technischen, sicherheitsbezogenen Architektur betrachtet. Das Ziel ist es eine grobe Übersicht zu vermitteln um einen Kontext für die Realtionen der Netzwerkelemente zu vermitteln.

Während die Architekturdetails, oder genauer definiert die Infrastrukturelemente, abhängig von anderen Modellen und Perspektiven gestaltet werden, lassen sich folgende grundlegende Kommunikations-Bereiche definieren: Extranet (Zugang zum globalen Netzwerk), demilitarisierte Zone (Zugangsbereich zum Unternehmen) und Intranet (internes Netzwerk des Unternehmens), ggf. mit weiteren Unterteilungen [31].

Bild für typische Enterprise Technical Architecture Infrastructure einfügen

Zunächst besteht eine Verbindung zum Internet (Extranet), diese wird durch gesicherte Gateways ermöglicht. Damit allerdings keine direkte Verbindung von diesen Gateways in das interne Netzwerk gewährt wird, wird eine zusätzliche Netzwerkzone zwischen das Gateway und das interne Netzwerk geschaltet. Diese Zone wird de-militarisierte Zone (DMZ) genannt. Innerhalb der DMZ werden Server angebunden, die aus dem Internet erreichbar sein sollen. Dies umfasst u.a. Webserver, die einen oder mehrere Webservices beherbergen oder Sprungserver (z.B. für eine VPN-Verbindung). Diese Server werden im Bezug auf ihre Kommunikationsfähigkeit limitiert, sodass keine Netzwerkverbindung von diesen Servern in das interne Netzwerk hergestellt werden kann, nur in umgekehrter Richtung ist die Herstellung einer Verbindung möglich. Das interne Netzwerk widerum kann in viele verschiedene weitere Netzwerkzonen und Domänen unterteilt sein. Diese Segmentierung dient der Strukturierung des Netzwerkes und eröffnet zusätzlich die Möglichkeit weitere Sicherheitsschichten in die Umgebung einfließen zu lassen. Das interne Netzwerk beherbergt Endgeräte von Mitarbeitern, Server mit Firmendaten, Datenbankserver und Datensicherungscluster. Alle Elemente in einer solchen Umgebung sowie die Kommunikation zwischen diesen Elementen können von verschiedenen Sicherheits-

systemen überwacht werden.

2.5.3 Kommunikation

In Unternehmensnetzwerken kommunizieren die Elemente auf Basis der Ethernet-Technologie und dem Internet Protocol (IP). Der zugehörige TCP/IP Stack bestimmt die grundlagen der Kommunikation durch die Zuweisung einer eindeutigen IP Adresse. Die Zuweisung dieser IP Adresse kann fest zugeordnet werden (z.B. für Server), manuell erfolgen oder automatisch über das Dynamic Host Configuration Protocol (DHCP) erfolgen, welches einem neuen Netzwerkelemente automatisch eine freie IP Adresse aus einem Adressenpool zuweist. Die meisten Elemente in einem Netzwerk werden einer sogenannten Domäne zugeordnet. Eine Domäne ist eine Zusammenstellung verschiedener Netzwerkelemente, die eine zentrale Benutzerverwaltung für die zugehörigen Elemente erlaubt. Zu einem der wichtigsten Netzwerkdienste zählt der „Domain Name Service“(DNS). Dieser Netzwerkdienst erlaubt es den Namen einer Domäne einer oder mehreren IP-Adressen zuzuordnen und übernimmt die Beantwortung von Anfragen zur Namensauflösung. Die Namensauflösung wandelt einen Domänennamen in eine zugehörige IP-Adresse um, die von dem anfragenden Gerät genutzt werden kann um eine Verbindung herzustellen. Dies ermöglicht menschlichen Benutzern die Möglichkeit eine bestimmte Domäne (z.B. „google.de“) über ihren Namen anzufragen anstatt über das Wissen um die korrekte IP-Adresse (die sich ggf. ändern kann) verfügen zu müssen. Die Ausführung der Anfrage und Empfang der Antwort wird von einem lokal installierten „DNS-Resolver“übernommen. Der DNS ist ein hierarchischer Verzeichnisdienst, das bedeutet, dass die Administration und Namensauflösung über ein hierarchisches Netz bestehend aus Namensservern durchgeführt wird. Der Namensraum des Internets wird dabei in einem hierarchischen Baum zunächst in sogenannte „Top-Level Domains“(z.B. „de“) unterteilt, die widerum in weitere Subdomänen unterteilt werden. Der von rechts nach links zusammengesetzt Pfad ergibt den Namen der Domäne. Dieser hierarchische Aufbau ermöglicht den strukturierten Aufbau der Namen und eine umgekehrt hierarchische Abfragemöglichkeit für die Namensauflösung. Diese Konzept kann nicht nur im Internet, sondern auch lokal innerhalb eines Unternehmensnetzwerkes verwendet werden [28]. Basierend auf der IP-Adresse kann eine verbindungsorientierte Kommunikation per Transmission Control Protocol (TCP) oder eine verbindungslose Kommunikation per User Datagram Protocol (UDP) erfolgen. Ist es eine Priorität, dass eine Nachricht vollständig und in richtiger Reihenfolge übertragen wird, wird z.B. TCP verwendet. Auf weiteren zusätzlichen Schichten können weitere Funktionalität wie etwa eine kryptografische Verschlüsselung erfol-

gen. Die verschiedenen Schichten sind u.a. im OSI-7-Schichtenmodel festgehalten. Das OSI-Modell bietet eine herstellunabhängige Grundlage für das Design von Kommunikationsprotokollen und Computernetzwerken. Das OSI-Modell unterteilt die Kommunikation in sieben Schichten:

- Schicht 7: Anmeldung - Funktionen und Anwendung
- Schicht 6: Darstellung - Umwandlung von Daten in ein systemunabhängiges Format
- Schicht 5: Kommunikation - Steuerung des Datenaustausches (Sessions)
- Schicht 4: Transport - Zuordnung von Datenpaketen zu einer Anwendung
- Schicht 3: Vermittlung - Routing
- Schicht 2: Sicherung - Segmentierung der Pakete
- Schicht 1: Bitübertragung - Umwandlung für die physikalische Übertragung

Jede Schicht fügt den vorherigen Schichten neue Elemente hinzu um die Kommunikation um zusätzliche Funktionalitäten und Eigenschaften zu erweitern [17].
Enterprise Kommunikation - VPN & Remote Access beschreiben

2.5.4 Bekannte Angriffsvektoren

Für das Risiko Management wie auch für die Implementierung von Verteidigungsmaßnahmen ist es notwendig die gebräuchlichen Angriffsvektoren zu kennen, die ein potentieller Angreifer nutzen kann um unberechtigterweise auf Komponenten in einem Unternehmensnetzwerk zuzugreifen.

Ein Angriffsvektor ist eine Technik, durch die ein Angreifer ein Netzwerk oder Netzwerkelemente angreifen oder ausnutzen kann. Angriffsvektoren helfen dabei Schwachstellen der angegriffenen Komponente, inklusive dem menschlichen Benutzern, auszunutzen. Eine Schwachstelle kann ein programmierter Fehler in einer Anwendung sein, ein Fehler in der Prozesskette einer Anwendung, Schnittstelle oder eines Netzwerkprotokolles oder eine Lücke in der Absicherung der Komponente [32].

Da es viele verschiedene Komponenten in einem Unternehmensnetzwerk gibt in vielen verschiedenen Versionen und mit vielen verschiedenen Abhängigkeiten, Kommunikationsprozederen und Anwendungsarten, ist es nicht möglich sich hundertprozentig for Angriffen zu schützen. Jedoch ist es möglich durch Kenntnis von

bekannten Angriffsvektoren Schwachstellen zu schließen und somit das Risiko eines erfolgreichen Angriffes zu verringern und diesen zu erschweren.

Für Unternehmensnetzwerke lassen sich Angriffsvektoren grob in die folgenden Kategorien unterteilen [3]

- „Malware“
- „Denial-of-Service“
- „Angriffsvektoren auf Webinhalte “

Malware

Malware, auch Schadsoftware, ist der Überbegriff für Programme, die auf einem Computersystem mit bösartiger Absicht ausgeführt werden. Eine Malware kann etwa dazu benutzt werden um über den infizierten Host auf Informationen und andere Komponenten des Netzwerkes zuzugreifen, die Resourcen des Hosts in Form von Rechenleistung, Netzwerkbandbreite, o.ä. zu nutzen oder den Host zu kontrollieren. Eine populäre Methode um Malware auf einem Ziel auszuführen ist die Versendung als Anhang von gefälschten E-Mail, etwa in der Form von Spam-Emails oder Phishing-Emails (personalisierte E-Mails für den entsprechenden Benutzer) oder auch Spear-Phishing (speziell angepasste E-Mails nach Hintergrundrecherchen der Zielperson). Der Angreifer versucht in diesem Falle den Benutzer dazu zu bringen etwa einen Link zu einer gefälschten Webseite anzuklicken, über die der Schadcode im Hintergrund auf den Computer des Ziels heruntergeladen wird, oder einen modifizierten Anhang zu öffnen, durch den der Schadcode auf dem Computer installiert wird. Gängige Malwaretypen sind trojanische Pferde, Computerviren, Computerwürmer, „Rootkits“, logische Bomben und Spionageprogramme[3].

Die Unterscheidung dieser Typen ist wichtig, da die Funktionalität und Operation der verschiedenen Typen Auskunft über potentielle Indikatoren geben kann. Aus diesem Grund werden die verschiedenen Typen im Folgenden kurz beschrieben. Ein Computervirus ist ein Programm, welches im Programmcode eines modifzierten Programmes oder einer modifizierten Datei versteckt ist. Wie der biologische Virus benötigt dieser Malware-Typ einen Host, also anderes Programm oder einen Prozess, um sich weiter zu verbreiten. Ein Computerwurm hingegen ist eine unabhängige Anwendung und kann sich unabhängig von seinem Host der Ressourcen des Hosts bedienen um sich weiterzuverbreiten. Sowohl Computerviren als auch Computerwürmer werden genutzt um weitere Computer im Einflussbereich des infizierten Hosts zu infizieren und den Einfluss des Angreifers auszuweiten. Ein Rootkit wird

verwendet oft in diesem Zusammenhang verwendet um seine eigene Ausführung und die Ausführung anderer Malware zu verbergen, etwa durch das Verbergen der Prozess im Windows Task Manager oder durch Blockierung des Benutzerzugriffes auf sein Quellenverzeichnis. Dafür wird das Rootkit oft als Folgeschritt der Infizierung eines Hosts von einer Quelle heruntergeladen und mit administrativen Privilegien installiert um Zugriff auf die Betriebssystemkomponente zu erlangen. Eine weitere Malware-Art ist das sogenannte „trojanische Pferd“. Diese Art von Malware ermöglichen die Ausführung von Kommandos auf dem infizierten Host ohne das Wissen des Benutzers und können unabhängig von den Operationen des Hosts ausgeführt werden. Trojanische Pferde ermöglich u.a. die Öffnung von Hintertüren, die dem Angreifer den Zugriff auf das kompromitierte System ermöglichen. Diese Technik wird oft für die Erstellung oder Erweiterung von Botnetzen verwendet. Botnetze bestehen aus einer Sammlung kompromitierter Systeme, die von einem „Command& Control-Server“gesteuert werden können. Dieser Server (Botmaster) ermöglicht die Versendung von Befehlen an die kompromitierten Systeme (Bots) zur Ausführung dieser Befehle auf den Systemen. Logische Bomben sind eine Malware-Art, die auf ein System heruntergeladen, deren Ausführung jedoch verzögert wird bis eine vordefinierte Bedingung bzw. eine Sammlung von Bedingungen erfüllt werden. Dies kann von einem bestimmten Zeitpunkt (Datum) bis zu komplexen Abhängigkeiten von Versionen installierter Software, Patches oder anderer Systemvariablen reichen. Unter „Spyware“versteht man eine Malware, die Informationen des kompromitierten Systems an den Angreifer übermittelt. Dies können z.B. Tastatureingaben (Key Logger), Screenshots (Screen grabber) oder auch Videostreams vom aktuellen Bildschirm sein[3].

Denial-of-Service

Neben dem Ziel Informationen zu stehlen oder System zu kontrollieren kann ein Angreifer auch das Ziel haben die Erreichbarkeit (s. Schutzziele) eines Webservers oder eines Webdienstes zu unterbinden, etwa um finanziellen Schaden oder rufschädigende Auswirkungen zu erzielen. Dieser Angriffsvektor wird als „Denial-of-Service “bezeichnet. Die Unterbindung der Erreichbarkeit wird durch das Aufbrauchen einer notwendigen Resource erreicht, etwa Bandbreite, Anzahl der maximalen Verbindungen zum Server oder Rechenleistung. Um dieses Ziel zu erreichen wird üblicherweise eine hohe Anzahl an Systemen benötigt, die gemeinsam den Angriff ausführen. Aus diesem Grund werden z.B. die beschriebenen Botnetze verwendet um parallel eine große Anzahl an Anfragen an einen Server zu senden um die Bandbreite auszulasten. Durch die verteilte Natur dieses Angriffes werden diese Angriffe als „Distributed

Denial-of-Service“Angriffe bezeichnet[3].

Angriffsvektoren auf Webinhalte

Bei diesem Angriffsvektor werden Schwachstellen von Webinhalten ausgenutzt, die den Zugang zu Informationen oder das Ausführen von Schadcode auf dem unterliegenden Webserver ermöglichen. Dieser Vektor lässt sich weiter unterteilen in „Active Content“Angriffe und „Content Injection“Angriffe. Als Active Content werden Webinhalte bezeichnet, die Funktionalitäten zu Webseiten hinzufügen. Dazu zählen etwa JavaScript, PHP, Adobe Flask, Perl, HTML5 und Java. Oft bringen diese Inhalte vollständige Programmierumgebungen mit sich, die eigene Schwachstellen und ausnutzbare Fehler enthalten können. So kann etwa durch das Ausnutzen einer Schwachstelle JavaScript Code in eine Webseite integriert werden, der ausgeführt wird, wenn ein anderer Benutzer diese Webseite aufruft um bspw. Malware auf den Computer des Benutzers herunterzuladen. Der Vektor Content Injection wird meistens durch fehlende Überprüfungsroutinen einer Webanwendung geöffnet. Durch das Einfügen von spezifischen Eingaben, die von den gewollten Eingabewerten abweichen wird etwa das Abrufen von Benutzerdaten einer Datenbank über ein Login-Feld oder die Möglichkeit des Stehlens von Cookies der Benutzersitzung über „Cross-Site Scripting“(XSS) ermöglicht, welches die Möglichkeit der Impersonifizierung des Benutzers gegenüber der Webanwendung eröffnet[3].

2.6 Infrastruktur industrielle Produktionsnetzwerke

Kontext der industriellen Infrastruktur einfügen

2.6.1 Architektur & Anforderungen

Die Architektur eines industriellen Netzwerkes ist darauf ausgelegt, einen Fertigungsprozess zu kontrollieren. Dementsprechend existiert eine hierarchische Struktur, welche die Kontrolle des Prozesses von der Aufgabenannahme bis hin zur Kontrolle der einzelnen Schritte durch SPSen, Aktoren und Sensoren. Zu diesem Zweck wird auf die Disziplin der Prozesskontrolle zurückgegriffen. Die Prozesskontrolle ist eine Ingenieursdisziplin, die sich auf Architekturen, Mechanismen und Algorithmen für die Aufrechterhaltung der Funktionalität eines Prozesses beschäftigt. Allgemein spricht man bei Elementen innerhalb der Prozesskontrolle von industriellen Kontrollsyste-

men. Diese Kontrollsysteme können in verschiedenen Architekturen abgebildet werden.

Die Automatisierungspyramide

Um das Zusammenspiel und die Anordnung / Strukturierung der Komponenten in einem industriellen Netzwerkes zu verstehen, ist es sinnvoll die grundlegenden Konzepte hinter einer solchen Architektur zu beleuchten. Die Grundlage bildet die industrielle Automatisierung, durch die sich ein industrieller Fertigungsprozess abbilden lässt. Ein automatisierter Fertigungsprozess ist ein Prozess, der ohne das Eingreifen von Menschen ablaufen kann und bei dem ein Material oder ein Produkt mit Energie und Informationen umgewandelt wird [21]. Die industrielle Automatisierung durchzieht verschiedene Hierarchieebenen, die unterschiedliche Aufgaben erfüllen. Für die Darstellung dieser Ebenen kann auf die Automatisierungspyramide verwiesen werden.

Einfügen eines Bildes der Automatisierungspyramide

Es wird zwischen den folgenden Hierarchieebenen unterschieden:

- Unternehmensleitebene
- Betriebsleitebene
- Produktionsleitebene
- Prozessleitebene (mit weiteren Unterteilungen)
- Feldebene

In der Unternhemensleitebene werden Prozesse durchgeführt, die die Ausrichtung des Unternehmens bestimmen. Dazu werden u.a. sogenannte Enterprise Resource Planning (ERP) Systeme (z.B. von SAP) für die Verwaltung der zur Verfügung stehenden Resourcen sowie für die Verwaltung der kaufmännischen Prozesse eingesetzt. Die Betriebsleitebene hat die Aufgabe die eingehenden Aufträge zu verwalten und fristgerecht durchzuführen, inklusive der Produktionsplanung und der Verwaltung und Überwachung der täglichen Betriebsprozesse [21]. In dieser Ebene werden MES-Systeme für die Produktionssteuerung und Kontrolle der Fertigung in Echtzeit eingesetzt [30]. Die kurzfristigere Planung des Einsatzes bestimmter Maschinen oder Anlagen ist Teil der darunterliegenden Produktionsleitebene. In dieser Ebene werden sogenannte Supervisory Control and Data Acquisition (SCADA) Systeme eingesetzt.

SCADA-Systeme, siehe Handbuch Quelle

Die Prozessleitebene strukturiert die verschiedenen Fertigungszellen des Produktionsprozesses. Abhängig von der Größe der Anlage, kann sie in mehrere Unterebenen unterteilt werden, die widerum hierarchisch die Anlage, Gruppen von Fertigungszellen und einzelne Fertigungszellen (Zellebene) abbilden. Innerhalb dieser Fertigungszellen wird ein bestimmter Bearbeitungsprozess durchgeführt, der durch verschiedene Bearbeitungsmaschinen durchgeführt wird. Die Bearbeitungsmaschinen werden durch speicherprogrammierbare Steuerungen (SPS) kontrolliert, die ihrerseits Daten aus der Feldebene und übergeordneten Systemen erhalten. Zu der Feldebene werden Aktoren, Sensoren und Anzeigegeräte gezählt, d.h. diese Ebene umfasst die Erfassung und Weiterleitung von (Mess-)Daten sowie die Ausführung von veränderten Stelldaten, die als Reaktion auf die ausgewerteten Informationen der Messdaten veranlasst werden[21].

Prozessleittechnik und Architekturanforderungen

Auf der Grundlage der oben beschriebenen Ebenen, ihre Funktion und ihre Aufgaben wird im folgenden der Begriff der Prozessleittechnik und die damit in Verbindung stehenden Anforderungen an die Komponenten der Architektur beleuchtet. Die Prozessleittechnik ist eine Unterkategorie der Produktionsleittechnik. Sie betrachtet Aspekte der Mess-, Steuer- und Regelungstechnik sowie die systematische Ordnung von Produktionsprozessen, die Informations- und Kommunikationstechnik sowie die Konzeption für das Erstellung und Betreiben von Leitsystemen. Damit dient die Prozessleittechnik als Schnittstelle zwischen der technischen Umsetzung des Prozesses und der Beobachtung/Bedienung des Prozesses durch den Menschen. Sie bildet das Zusammenspiel zwischen Prozessleitebene und Feldebene ab. Die Grundfunktion der Prozessleittechnik ist die Erfassung, Übertragung, Verarbeitung und Ausgabe von Prozessdaten für die Steuerung und Überwachung des Produktionsprozesses. Dafür müssen abhängig von den Informationen, die aus den verarbeiteten Daten gewonnen werden, Entscheidungen innerhalb eines bestimmten Zeitraumes getroffen werden um Fehlfunktionen zu vermeiden. Dies wirkt sich allerdings auf die Qualität der getroffenen Entscheidung aus. Aus diesem Grund wird die Entscheidungsfindung hierarchisch auf verschiedene Teilsysteme (Unterebenen) aufgeteilt, die eine geringe Menge an Daten verarbeiten müssen. Durch diese hierarchische Struktur wird die Informationsdichte zu den oberen Ebenen hin höher, die Anforderungen bzgl. Reaktionsschnelligkeit und Zuverlässigkeit/Verfügbarkeit können jedoch im Vergleich zu den unteren Ebenen mit weniger Priorität betrachtet

werden. Neben der Verfügbarkeit und Zuverlässigkeit ist auch die Robustheit gegenüber Fehlern eine Anforderung. Auch diese Anforderung ist durch die autarken Teilsysteme in der grundlegenden Architektur eines Fertigungssystems verankert. Im Bezug auf Soft- und Hardwareanforderungen sind die Anforderungen ebenfalls abhängig von der Hierarchieebene. In der Feld- und Prozessleitebene ist die Anzahl der Teilnehmer an der Kommunikation ist geringer und die zu übertragenden Datenmengen vergleichsweise klein, dafür ist es wichtig, dass Anweisungen sehr schnell (in Echtzeit) gesendet und verarbeitet werden können. Dazu werden zusätzlich standardisierte Softwarebausteine verwendet um die Zuverlässigkeit des Programmablaufs zu maximieren. In den oberen Ebenen wie etwa der Betriebsleitebene werden andere Anforderungen wie in einem Unternehmensnetzwerk priorisiert[21].

2.6.2 Geräte

In industriellen Netzwerken werden verschiedene Komponenten und Technologien auf den verschiedenen Ebenen der Prozesskontrollstruktur eingesetzt. Zu den Hauptkomponenten zählen:

- Speicherprogrammierbare Steuerung (SPS)
- Human-Machine Interface (HMI)
- OPC Server
- Sensor & Aktuator
- Weitere Server und Arbeitsstationen der Büroebenen

Speicherprogrammierbare Steuerungen

Eine speicherprogrammierbare Steuerung (SPS) ist ein Gerät, welches Maschinen und Anlagen steuern oder regeln kann. Für die Steuerung als auch für die Regelung einer Maschine wird ein vordefiniertes Programm verwendet, welches auf der vorhanden Firmware ausgeführt wird. Die Firmware beinhaltet die verwendbaren Operanden und Programmbausteine, die für die Programmierung genutzt werden können. Für die Programmierung selbst werden von vielen SPSen standardisierte Bausteine der Norm IEC 61131-3 unterstützt [11]. Das auf die SPS geladenen Programm verarbeitet Informationen, welche von den Eingangsmodulen empfangen werden. An die Eingangsmodule sind üblicherweise ein bestimmter Sensortyp angeschlossen, welcher Informationen über einen bestimmten Aspekt des Prozessschrittes liefert. Basierend auf der Implementierung des Programms, dies kann z.B.

eine logische Sequenz, eine Zeitschaltung oder eine arithmetische Operation sein, wird durch diese Informationen ggf. über ein Ausgangsmodul ein Aktor (z.B. ein Motor) aktiviert, der ein Element des Prozessschrittes kontrolliert und Änderungen anstößt oder durchführt. Ein Programm kann mehrere Operanden kombinieren und in Zusammenhang setzen, inklusive Input, Output, Arguments, Counter, Timer und Function Blocks. Eine modulare SPS besteht aus mehreren Basiskomponenten, zu der noch weitere Module optional hinzugefügt werden können. Das Basisset umfasst mindestens einen sogenannten Baugruppenträger, d.h. einen Kasten in dem die Module platziert werden können, eine Stromversorgung, eine Baugruppe, welche die CPU und den Speicher enthält sowie digitale und analoge Ein- und Ausgänge für spezifische Elemente der Feldebene. Dazu können noch weitere Module wie etwa ein Kommunikationsprozessor (Communication Processor (CP)) für die Anbindung der SPS an ein Netzwerk, weitere Kommunikationsmodule sowie Zähler-, Positionier- oder Regelungsmodule [11].

Sensoren und Aktoren

Auf der Feldebene werden neben speicherprogrammierbaren Steuerungen Sensoren und Aktoren eingesetzt. Ein Sensor ist ein Element, welches Änderungen einer physikalischen Gegebenheit in seiner Umgebung registriert und in ein elektronisches Signal umwandelt. Sensoren sind ein wichtiges Element, da Daten aus dem Produktionsprozess mit hoher Zuverlässigkeit und zeitnah an die kontrollierende SPS bzw. die Prozesskontrolle übermittelt werden müssen [15]. Sensoren sind üblicherweise als Teil des Schaltkreises eines Sensorgerätes. Abhängig von der Art des Sensors reagiert das Sensorelement auf eine bestimmte physikalische Veränderung. Sensoren unterscheiden sich daher in der Art der wahrgenommenen Veränderung, zu denen in der Automatisierungsindustrie u.a. die folgenden zählen:

- Änderung des Widerstands
- Änderung der Kapazität
- Änderung der Induktivität
- Elektromagnetische Induktion
- Thermoelektrischer Effekt
- Sonar
- Optische Veränderung

- Hall

Durch die technologische Entwicklung stehen heutzutage auch sogenannte Mikrosensoren zur Verfügung. Mikrosensoren, oder auch „Smart Sensors“, integrieren signalverarbeitende Schaltkreise, Analog-Digital-Wandler, programmierbaren Speicher und Mikroprozessoren in ein Sensorgerät. Zudem ist es auch möglich über die Integration einer Antenne eine kabellose Verbindung zu ermöglichen und Sensoren in kabellosen Sensornetzwerken (Wireless Sensor Networks (WSN)) zu strukturieren[15].

Aktoren ermöglichen es per SPS auf die prozessnahen Maschinen des Produktionsprozesses einzuwirken und den Prozess zu kontrollieren. Aktoren verwenden u.a. Federmechanismen, hydraulische und/oder pneumatische Geräte, Magnetismus oder Termalenergie. Analog zu den Sensoren ist es möglich Aktoren mit zusätzlichen Elemente auszustatten um u.a. die Kommunikationsmöglichkeiten zu erweitern[15].

Human Machine Interface (HMI)

Ein Human Machine Interface, oder auch Mensch Maschinen Schnittstelle (MMS), ist die Bedienungsschnittstelle zwischen Mensch und Maschine. Sie dienen daher als Element für die Steuerung und Beobachtung der Prozesse durch einen Menschen. In der industriellen Fertigung werden HMIs in Form von Panelen, Stand-alone PCs oder auch Thin Clients (d.h. mit der Prozesskontrolle vernetzte Monitore) eingesetzt [12]. Die Anwendung einer bestimmten Hardwareform für die Benutzerschnittstelle wird dabei durch den speziellen Zweck als auch durch die Einsatzumgebung bestimmt. Die verschiedenen Typen unterscheiden sich dabei u.a. durch die Kommunikationsmodule, Größe und Art des Displays, Performance und angebotenen Zusatzmodulen[29]. HMIs sind oft auf einen speziellen Zweck spezialisiert, der durch den Einsatz und die konfiguration spezialisierter Softwarekomponenten umgesetzt wird[12].

Server und industrielle PCs

Die bereits im Unterkapitel „Infrastruktur Office“definierten Server-Komponenten finden auch verschiedene Einsatzmöglichkeiten in industriellen Produktionsnetzwerken. Abhängig von der betrachteten Hierarchieebene werden diese Server für verschiedene Zwecke eingesetzt. Während Server in den oberen Hierarchieebenen Aufgaben des Büroumfeldes wie etwa die Funktion als Datenbankserver übernehmen, werden Server der Produktionsleitebene und speziell der Prozessleitebene für Kontroll- und Überwachungsfunktionen des Produktionsnetzes eingesetzt.

Eine Anwendungsmöglichkeit ist es den Server als SCADA-Server oder -System zu nutzen. SCADA steht für Supervisory Control and Data Acquisition und be-

schreibt ein wahlweise zentrales oder dezentrales Softwaresystem, welches Informationen der prozessnahen Komponenten (PNK) sammelt, die Informationen zu Analyse- und Überwachungszwecken verarbeitet und steuernd in den Prozess eingreifen kann. Dabei werden die PNKs als sogenannte Datenpunkte betrachtet, die auf Basis von bestimmten E/A-Werten und mathematischer Berechnungen bestimmt werden. Zu den Betriebssystemen, die die Ausführung eines SCADA-Systems erlauben zählen u.a. DOS-basierte, Windows NT-basierte, Unix-basierte und Linux-basierte Betriebssysteme. Abhängig von der Größe des SCADA-Systems können mehrere tausende bis hunderttausende E/A-Kanäle umfassen[13]. In Richtung der oberen Hierarchieebenen kann ein SCADA-System u.a. mit ERP & MES Systemen kommunizieren[1].

Ein SCADA-Server kommuniziert auf verschiedenen Ebenen. Zu Bedien- und Beobachtungszwecken kann ein SCADA-Client mit einem SCADA-Daten-Server kommunizieren per TCP/IP-Schnittstelle. Die Daten-Server kommunizieren je nach Kommunikationspartner entweder über ein bestimmtes Feldbussystem (z.B. Profibus) mit PNKs oder untereinander über die Ethernet-Schnittstelle. Für die Kommunikation zwischen verschiedenen SCADA-Systemen kann das SCADA-Protokoll „Sinaut“verwendet werden[13].

Der Zugriff von SCADA- und Prozessleitsystemen auf Elemente der Feldebene kann sowohl direkt oder über Prozesskontrollserver erfolgen. Ein Prozesskontrollserver ist ein Server mit zusätzlichen E/A-Schnittstellen, die für die Anbindung herstellerspezifische PNKs genutzt werden können. Um die herstellerspezifischen Datensätze in einem einheitlichen Format an die höheren Hierarchieebenen weiterleiten zu können, bedient man sich der OPC-Schnittstelle. Diese Schnittstelle erlaubt es mithilfe eines spezifischen OPC-Treibers die Datensätze in OPC-Objekte umzuwandeln und OPC-Funktionen zu unterstützen. Die OPC-Schnittstelle dient also zu der Sammlung von Daten aus einem Netzwerk von Sensoren, Aktoren und SPSen unterschiedlicher Hersteller. Abhängig von der OPC-Spezifizierung basiert OPC auf der DCOM-Schnittstelle von Microsoft und erfordert somit, dass der Server ein Windows-Betriebssystem verwendet. Diese Spezifizierung, das klassische OPC, umfasst Spezifizierungen für die Übertragung von Echtzeitdaten, Alarmen und Events, Zugriff auf historische Datensätze und die direkte Kommunikation zwischen OPC-Servern. Der neuere OPC-Standard wird OPC-UA (Unified Architecture) genannt. Das Ziel dieses Standards ist es u.a. einen Standard unabhängig von DCOM und einem bestimmten Betriebssystemtyp für die zyklisch gesteuerte Kommunikation mit PNK-Netzwerken zu setzen.

In industriellen Produktionsnetzen werden auch PCs in Anlagen verwendet.

Diese unterscheiden sich im Vergleich zu herkömmlichen Büro-PCs durch erhöhte Hardware- und Softwareanforderungen. Zu den Hardwareanforderungen zählen u.a. eine gewisse Robustheit gegenüber Einflüssen der Umgebung wie extreme Temperaturen, Schmutz, Feuchtigkeit oder elektromagnetische Felder und Vibrationen, aber auch eine gute Abschirmung des Gehäuses und der Anschlüsse (in Umgebungen, die empfindlich auf Störgrößen dieser Art reagieren). Unabhängig von der Umgebung müssen diese Computer jedoch vorallem ein hohes Maß an Zuverlässigkeit bieten und eine schnelle und einfache Wartung ermöglichen (z.B. die Möglichkeiten eine Festplatte innerhalb von Sekunden auszutauschen). Dies erfordert auch, dass die gleiche Hardware über einen langen Zeitraum betrieben werden kann, da Änderungen der Hardware zu Fehlern bzw. zur Unbrauchbarkeit von gesicherten Speicherabbildern führen können.

Zu den wichtigen Softwareanforderungen gehören vorallem die zuverlässige, fehlerfreie Ausführung sowie die Verarbeitung von Daten in Echtzeit. Zu diesem Zweck wird etwa die Hauptplatine eines PCs durch ein speziell angepasste Platine mit mehr Steckplätzen für Busschnittstellen verwendet.

Ein Fertigungssystem umfasst noch weitere Elemente wie etwa Systeme, die die Produktion von der Produktionsleitebene steuern (Manufacturing Execution System (MES)) oder die Überwachung und Verwaltung auf dieser Ebene ermöglichen über einen Leitstand, der alle Informationen des Fertigungsprozess zentral sammelt und darstellt. Auf der Feldebene existieren zudem noch speziellere Maschinen, etwa für die Qualitätssicherung des Produktes, den Transport des zu verarbeitenden Materials oder für das Austauschen verwendeter Werkzeuge. Da jedoch eine tiefere Beschreibung dieser Elemente für die Kategorisierung der verfügbaren Informationsmenge nicht erforderlich sind, sei an dieser Stelle jediglich darauf verwiesen, dass diese Elemente in diesen Netzwerken existieren [11].

2.6.3 Kommunikationstechnologien

In industriellen Netzwerken herrschen abhängig von der Hierarchieebene unterschiedliche Anforderungen an die Kommunikationswege zwischen den Komponenten. Während in den oberen Hierarchieebenen die Anforderungen der Unternehmensnetzwerke gelten, sind für die Kommunikation in den Bereichen der Prozessleitebene und Feldebene die Anforderungen der Echtzeitfähigkeit und der deterministischen Eigenschaft des Kommunikationssystems oder -protokolls zu erfüllen. Unter der Echtzeitfähigkeit versteht man die Fähigkeit eines Kommunikationssystems Daten innerhalb weniger Millisekunden oder sogar unterhalb einer Millisekunde zu übertragen. Dies ermöglicht eine schnelle Erkennung von Veränderungen innerhalb des physika-

lischen Prozesses und schnelle Reaktionen auf diese Veränderungen. Die notwendige Übertragungsgeschwindigkeit ist abhängig von der notwendigen Reaktionszeit. Die Anforderung des Determinismus beschreibt die *Garantie* das Daten innerhalb eines bestimmten Zeitraumes übertragen werden. Diese Anforderung ergibt sich daraus, dass die Steuerungen garantiert mit den aktuellen Daten versorgt werden müssen um Reaktionszeiten einzuhalten und die Sicherheit der Anlage und der Mitarbeiter zu gewährleisten. Durch die technologischen Eigenschaften des Ethernetstandards ist dieser Determinismus nicht gegeben.

Die verwendeten Kommunikationssysteme in diesen Ebenen verwenden entweder Kommunikationsprotokolle, die den vorhandenen Ethernetstandard um diese Fähigkeiten oder verwenden andere Datenbustechnologien. Für die Kommunikation innerhalb der Prozessleitebene zwischen den OPC-Servern und hierarchisch höher liegenden Systemen wie etwa dem SCADA-System oder dem Leitstand wird der Ethernetstandard durch Kommunikationsprotokolle erweitert. Diese werden unter dem Begriff „Industrial Ethernet“Protokolle zusammengefasst. Für die Kommunikation mit den Steuerungen innerhalb der Feldebene werden historisch bedingt Feldbusse eingesetzt. Allerdings finden auch hier vermehrt Industrial Ethernet Protokolle Einzug. Die Basis für die Verwendung der Feldbusse ist die taktbezogene Arbeitsweise der speicherprogrammierbaren Steuerungen. Für die Steuerung der Sensoren und Aktoren werden widerum andere Busse wie etwa der AS-I-Bus oder der HART-Bus verwendet. Netzwerke, die aus Sensoren und Aktoren bestehen für die bessere und redundante Überwachung des Prozesses werden als Aktor-Sensor-Netzwerk bezeichnet.

Feldbus

„Unter Feldbus versteht man ein Bussystem, dass in rauer Umgebung (Feld) eingesetzt wird. Neben besonderen Anforderungen an die mechanische Ausführung sind insbesondere auch Anforderungen an die Robustheit (Störempfindlichkeit) des Datenprotokolls. “[10] Ein Bussystem ist ein Kommunikationssystem, bei dem mehrere Kommunikationsteilnehmer die gleiche Datenleitung (Datenbus) verwenden. Um die Kommunikation möglich zu machen, darf nur ein Teilnehmer pro Zeiteinheit als Sender agieren, während die anderen Teilnehmer den Datenbus abhören. Man spricht in diesem Zusammenhang auch von einer Punkt-zu-Gruppe Kommunikation[10]. Für die Freigabe bzw. das Recht eines Teilnehmers Daten zu senden existieren verschiedene Modelle, deren Ausprägung abhängig sind von der verwendeten Topologie und der benötigten Funktionalität. Eine Form ist das sogenannte Master-Slave-Prinzip. Bei diesem Prinzip fragt ein autorisierter Teilnehmer (Master) Informationen der

anderen Teilnehmer (Slaves) an und erteilt für den Empfang der Daten die temporäre Sendeerlaubnis. Dieses Prinzip wird in vielen Feldbussystemenen verwendet wie etwa PROFIBUS[10]. Für die Feldebene gilt, dass die Zuverlässigkeit der Kommunikation und die Verfügbarkeit der Daten garantiert werden muss. Ein entscheidender Faktor ist dabei die Behandlung von Kollisionen, welche auftreten wenn mehrere Teilnehmer gleichzeitig auf dem Datenbus senden. Zu diesem Zweck wird entweder CSMA/CD (Kollisionseerkennung) und CSMA/CA (Kollisionsvermeidung) verwendet. Bei der Kollisionserkennung stoppen alle Teilnehmer das Senden von Daten und der Teilnehmer mit der Sendeerlaubnis wiederholt das Senden der Nachricht. Durch diese Wiederholung kann es zu unterschiedlich großen Zeitfenstern kommen in denen eine Nachricht gesendet wird. Dieser Zustand kann zu Problemen in einer taktgesteuerten Umgebung wie der Feldebene führen wenn eine Nachricht innerhalb eines bestimmten Zeitfensters gesendet werden muss, d.h. die Kommunikation muss „deterministisch“sein. Zu diesem Zweck wird die Methode der Kollisionsvermeidung verwendet, bei der Datentelegramme höherer Priorität Datentelegramme niedrigerer Priorität bei den Empfängern überschreiben sodass die Daten nicht erneut gesendet werden müssen. In Kombination mit dem Master-Slave-Prinzip, durch das quasi eine temporäre Punkt-zu-Punkt Verbindung zwischen Master und Slave hergestellt wird, kann eine deterministische Kommunikation implementiert werden[10]. Feldbusnetzwerke sind standardisierte, aber auch proprietäre Netzwerke. In den Standards IEC 61158 und IEC 61784 existieren zehn verschiedene Konzepte. Sieben dieser Konzepte stellen eine eigene Protokoll Suite zur Verfügung, die anderen drei Konzepte basieren auf Ethernet Funktionalität. Beispiele für Protokolle sind etwa PROFIBUS oder DeviceNet.

Industrial Ethernet

Zusätzlich zu der Feldbustechnologie existieren in industriellen Netzwerken auch abgewandelte Formen des Ethernet Standards. Im Folgenden wird diese Abwandlungskategorie als „Echtzeit-Ethernet“bezeichnet. Der intendierte Einsatz dieser Technologie hat mehrere Vorteile. Das Echtzeit-Ethernet ermöglicht diese die Verbindung zwischen Büro- und Produktionsnetzwerken. So können etwa Echtzeitdaten aus dem Produktionszyklus sowie IT-relevante Daten nahezu zeitgleich und über dasselbe Medium übertragen werden, die Anzahl der Teilnehmer in einem Netzwerk kann erhöht und der gleichzeitige Zugriff auf den Datenbus möglich gemacht werden [6]. Neben der Echtzeitfähigkeit spielt auch die funktionelle Sicherheit, d.h. Schutz gegen Unfälle durch Fehler im Kommunikationsprotokoll, eine wichtige Rolle[25]. Der Ethernet-Standard für sich erfüllt allerdings auf Grund der Verwendung des Prin-

zips der Kollisionsvermeidung (s. Feldbus) und der damit nicht vorhandenen Deterministik nicht die Echtzeit-Anforderungen der Feld- und Steuerebene. Aus diesem Grund wurden von verschiedenen Herstellern verschiedene Echtzeit-Ethernet Protokolle entwickelt um die Echtzeit-Anforderungen in den verschiedenen Ebenen zu ermöglichen. Die Klassifizierung der Protokolle kann anhand der vorgegebenen Reaktionszeit und Deterministik nachvollzogen werden.

- „Weiche“Echtzeit (TCP/IP Mechanismen mit ModbusTCP oder PROFINET CBA), keine harten Zeitgrenzen
- Deterministisch (Harte Echtzeit), 1 bis 10ms
- Isochron, 250 μs bis 1ms

[25]

Wie für Feldbusse existiert bisher auch kein fester Standard für Industrial Ethernet-Protokolle, wodurch die Kommunikation zwischen Feldbus und Industrial Ethernet mit komplementären Protokollen durchgeführt werden müssen. In der in dieser Arbeit folgenden Analyse der industriellen Netzwerke wird die Umsetzung dieser Klassifizierungen am Beispiel von Profinet näher beleuchtet [7].

Industrial Ethernet: Einsatz Feldbus vs. IE sinnvoll?

2.6.4 Kommunikationsprotokolle

Industrial Kommunikationsprotokolle: Wird dieser Unterteil benötigt? (Abhängig von der Analyse und notwendigen Definitionen)

2.6.5 Bekannte Angriffsvektoren

Wie die Systeme in Unternehmensnetzwerken sind auch Systeme der industriellen Netzwerke Angriffen ausgesetzt. Dabei müssen diese Netzwerke nicht zwangsläufig an das globale Netz (Internet) angeschlossen sein wie etwa das Beispiel Stuxnet belegt, bei dem eine Infektion der Anlage und mehrerer Komponenten über die angeschlossene USB-Speichereinheit eines Mitarbeiters.

Eine Liste des Bundesinstitut für Sicherheit in der Informationstechnik (BSI) [8] umfasst in einer Übersicht eine Reihe von Angriffsszenarien:

- Social Engineering & Phishing Angriffe
- Einschleusen von Schadsoftware über Wechseldatenträger und andere externe Hardware

- Infektion mit Schadsoftware über einen Zugriff aus dem Internet oder Intranet
- Einbruch über Schnittstellen, die eine Fernwartung von Systemen ermöglichen
- Menschliches Fehlverhalten und Sabotage
- Internet-verbundene Steuerungskomponenten
- Technisches Fehlverhalten und höhere Gewalt
- Kompromittierung von Extranet und Cloud-Komponenten
- (D)DoS Angriffe
- Kompromittierung von Smartphones im Produktionsumfeld

Diese Szenarien lassen sich in die bereits beschriebenen Kategorien der Angriffsvektoren von Unternehmensnetzwerken beschrieben und sind teilweise bedingt durch das Vorhandensein von Komponenten der Unternehmensnetzwerke (wie etwa Webserver oder Benutzer-PCs). Das Ziel des Angreifers ist es direkt oder indirekt Zugriff auf den Netzwerkverkehr und/oder Netzwerkteilnehmer innerhalb des Fertigungssystems zuzugreifen um Informationen zu sammeln und Daten zu stehlen, zu manipulieren oder Schäden an der Infrastruktur und damit verbundene Ausfälle des Fertigungssystems zu verursachen. Eine weitere Methode um das Ziel eines temporären Ausfalls zu erzielen, ist die Auslösung eines Notfallprozederes, dass die temporäre Abschaltung des gesamten Systems oder eines Teilsystems zur Folge hat.

Kapitel 3

Analyse der Informationsquellen in einer typischen Unternehmensstruktur

SIEM Systeme sind, vorallem in großen Unternehmensnetzwerken (siehe SANS Paper Proactive), zu einem Standard geworden um Informationen aus Logs verschiedener Systeme und anderen Kontextdaten zu gewinnen und diese in Szenarios einzuordnen. Um das Zwischenziel einer Bewertung der aktuellen Informationsmenge eines industriellen Netzwerkes zu erhalten bietet es sich durch diesen Zustand an, einen Abgleiches zwischen dem, im Bezug auf SIEM Technologie, etablierten Informationstand in Unternehmensnetzwerken und industriellen Netzwerken auszuführen. In diesem Kapitel soll es deshalb um eine akkurate Beschreibung der Informationsmenge eines typischen Unternehmensnetzwerkes gehen, die aus einer Analyse der gängigen Informationstypen und -kategorien erfolgt. Dazu wird im folgenden zunächst der Analyseansatz geschildert, der das Vorgehen schildert und die Analyse nachvollziehbar gestalten soll.

3.1 Verwendete Analysemethode

Die erste Frage für die Wahl des Analyseansatzes stellt sich sowohl in der gewählten Tiefe als auch in einer zielgerichteten Methodik. Das Ziel der Analyse ist es die sicherheitsrelevanten Infortmationsmenge zu erfassen. Informationen werden als sicherheitsrelevant betrachtet, wenn diese Informationen genutzt werden können um die Nutzung eines bestimmten Angriffsvektors erkennen zu können. Da Angriffsvektoren sehr zahlreich und spezifisch für ein bestimmtes System oder eine Applikation sein können, ist eine allumfassende Analyse aller Angriffsvektoren nicht möglich.

Deshalb werden in dieser Analyse vereinfachte, repräsentative Beispiele verwendet um eine Einschätzung der möglichen Informationsmenge zu ermöglichen.

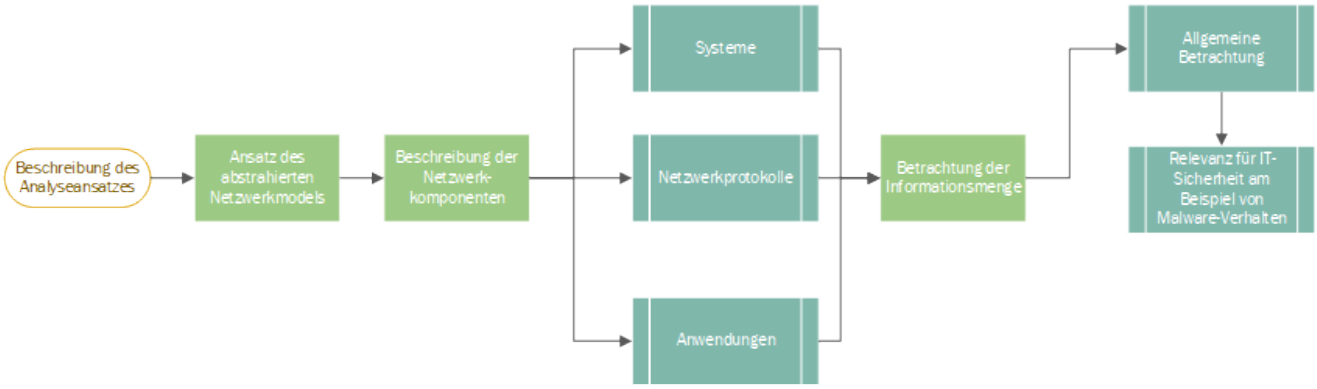

Abbildung 3.1: Analysestruktur (Placeholder)

Bei der Erkennung von Angriffsszenarien spielen erste Anzeichen, die potentiell auf einen Angriff hindeuten eine tragende Rolle. Informationen, die zu solchen Anzeichen ausgewertet werden, werden als „Indicator of Compromise“(IoC) bezeichnet. Ein IoC ist eine Information, die auf ein anomales Verhalten oder einen anomalen Zustand eines Netzwerkelementes schließen lässt. Um dieses Verhalten zu erkennen ergeben sich prinzipiell zwei Bereiche der Analyse: 1) Das Verhalten des Netzwerkelementes in sich, also der Zustand des Elements und Änderungen dieses Zustandes sowie 2) die Interaktion mit anderen Netzwerkelementen in Form des Austauschen von Nachrichten über die Netzwerkverbindung (vgl. Kaspersky Paper). Diese Beobachtung wird durch das Vorgehen in Unternehmen durch den „Incident Response Process“ gestützt. Dieser Prozess dient als Durchführungsplan eines Teams, das für die Aufklärung und Behebung von Indikatoren und Brüchen des Sicherheitszustandes eines Netzwerkes zuständig ist.

Der initiale Zustand dieses Plans ist die Überwachung der Netzwerkelemente und ihrer Kommunikation mit Hilfe von Detektions- und Analysesoftware (z.B. SIEM Systeme) und -hardware (z.B. „Intrusion Detection Systems“). Durch die Überwachung werden eine Vielzahl an Alarmen oder Sicherheitsereignissen produziert, die auf Fehler oder Anomalien im Netzwerk hinweisen. Werden diese Informationen aus diesen Ereignissen als potentiell kritisch eingestuft, wird ein IoC an das Team ausgegeben, dass basierend auf Risiko und potentieller Schadensgröße weitere Untersuchungen einleitet. Bei diesen Untersuchungen wird der oder die IoC(s) als Ansatz genutzt. Ein IoC kann dabei auf Informationen im Payload oder Headern von Netzwerkpaketen als auch aus Logging Informationen eines Betriebssystems oder einer Überwachungssoftware auf einem Netzwerkelement beruhen. Basierend auf dem

Ansatzpunkt können Informationen sowohl aus der Kommunikation als auch der Netzwerkelemente weitere Hinweise liefern um den potentiellen Sicherheitseinbruch einzugrenzen und schließlich zu identifizieren. Aus diesem Grund ist es wichtig, beide Domänen zu untersuchen. Der Analyseansatz lehnt sich dabei an den Incident Response Prozess an. Zunächst wird der Zustand des Netzwerkes beschrieben und alle Netzwerkelemente sowie die potentiellen Kommunikationsschnittstellen erfasst. Darauf folgt die Untersuchung der Netzwerkelemente und ihrer Kommunikation in einer iterativen Vorgehensweise. Diese Vorgehensweise ermöglicht die schrittweise Vertiefung der Analyse und soll als Ergebnis eine Übersicht pro Iterationsebene für beide Domänen erzielen. Die Analyse der Netzwerkelemente beginnt daher zunächst mit der Einteilung der Elemente in verschiedene Typen. Dabei wird unterschieden zwischen Servern mit verschiedenen Betriebssystemtypen sowie Netzwerkgeräte (Switches, Router) und Sicherheitselemente (Firewalls, Intrusion Detection Systeme). Um die Informationsmenge zu kategorisieren wird jeder Elementtyp auf die Existenz von Logdateien untersucht und die Struktur der Ereignisse in den Logdateien beschrieben. Eine Sammlung der typischen Quellen wird hinzugefügt um einen Überblick über den Ursprung typischer Ereignisse zu erreichen. Für die Betrachtung der Kommunikation werden die verschiedenen Schnittstellen basierend auf den verwendeten Netzwerkprotokollen untersucht. Für die Klassifizierung wird basierend auf der Anwendung des OSI-Modells durchgeführt, welches als repräsentatives Kategorisierungsmodell verwendet wird. Diese Klassifizierung zeigt den allgemeinen Rahmen der erwarteten Informationsmenge pro Layer auf (vgl. TCP/IP Stack) und stellt eine Basis für die Analyse der verwendeten Felder der Protokollheader dar.

Basierend auf diesen Praktiken ergibt sich die Durchführung der Analyse: Zunächst wird das benutzte Model und dessen Komponenten beschrieben. Das Ziel der Beschreibung der Komponenten ist eine grobe Klassifizierung der verfügbaren Informationsquellen der Komponente. Darauf folgend werden die betrachteten Angriffsszenarien beschrieben und die Informationsquellen der Komponenten für das jeweilige Angriffsszenario bewertet. Zu diesem Zweck wird beschrieben, welche Informationen pro Schritt des Angriffsszenarios als potentielle Indikatoren dienen könnten und ein Abgleich mit der kategorischen Verfügbarkeit der Daten, aus denen diese Informationen gewonnen werden können.

3.2 Beschreibung der Unternehmensarchitektur (Model)

Das Ziel des Modelles ist es eine repräsentative, vereinfachte Darstellung eines Unternehmensnetzwerkes mit typischen Komponenten für den Betrieb darzustellen. Der Aufbau des Netzwerkes orientiert sich an typischen Elementen, die in einem Unternehmensnetzwerk zu finden sind. Dabei besteht die Notwendigkeit das Model in seiner Größe und Komplexität einzugrenzen um eine Analyse in sinnvollem Maße zu ermöglichen, gleichzeitig aber ein möglichst vollständiges Bild erhalten zu können.

Die Architektur und Einteilung in verschiedene Netzwerkzonen ist dabei von üblichen Sicherheitszonen abgeleitet. Während die Positionierung der Elemente keine besondere Rolle spielt im Bezug auf die ermittelbaren Informationen pro Element ist jedoch anzumerken, dass auch diese Informationen, z.B. in Form der Auswertung von Netzwerkadressen, einem SIEM-System nützliche Informationen zur Verfügung stellen können. Die Architektur des Models beginnt an seinem „Rand“, dem Zugang zum WAN (Internet) über einen Gateway-Router. Dieser Router ermöglicht die Weiterleitung von Netzwerkpaketen in und aus der angrenzenden Netzwerkzone, der de-militarisierten Zone (DMZ). In der DMZ sind für diese Model ein Apache Webserver auf der Basis des Betriebssystems „CentOS“und ein E-Mail Server, bestehend aus dem Windows Webserver „Internet Information Service“(IIS) und dem darüber liegenden E-Mail Server „Microsoft Exchange“. Diese Netzwerkelemente bieten die Möglichkeit Datenverkehr über die Protokolle HTTP und die Microsoft Schnittstelle MAPI (bestehend aus RPC & HTTP Datenverkehr) zu untersuchen, sowie Informationen aus Log-Dateien sowohl von einem Linux-basierten Server als auch von einem Windows-basierten Server zu analysieren. Alle Elemente werden durch „Managed Switches“miteinander verbunden.

Die DMZ wird von der nächsten Zone, dem Extranet, durch eine Firewall überwacht, die eingehenden initiale Kommunikation blockiert. Firewalls gehören zu den Grundlagen der Sicherheit von Unternehmen und werden häufig platziert um Datenverkehr in und aus bestimmten Netzwerkzonen zu überwachen. Innerhalb der Netzwerkzone werden zwei Benutzer-PCs eingesetzt. Diese werden platziert um Abweichungen und andere Benutzerinteraktionen in die erhaltbare Informationsmenge zu integrieren. Die beiden Computer unterscheiden sich wie auch die Server der DMZ im Betriebssystem, sodass ein PC auf Basis von Windows und damit verbundener Benutzerverwaltung durch Active Directory enthalten ist, sowie ein PC mit einem Linux-basierten Betriebssystem. Zudem wird ein Netzwerkdrucker integriert.

Als dritte Netzwerkzone wird als „Restricted Area“bezeichnet. Innerhalb die-

ser Netzwerkzone werden verschiedene Windows-basierte Server eingesetzt um die Funktionalitäten eines Unternehmensnetzwerk zu simulieren. Die verschiedenen Servertypen wurden ausgewählt um erhaltbare Informationen aus unterschiedlichen, typisch genutzten Netzwerkprotokollen aufzuzeigen. Dazu gehören:

- ein Microsoft SQL Datenbankserver
- ein Active Directory Domain Controller
- ein FTP-Server

Zusätzlich ist in dieser Zone als Ergänzung auch der SIEM-Server gesetzt.

Zwischen den verschiedenen Elementen des Netzwerkes werden Informationen ausgetauscht z.B. für die Abfrage einer Ressource, Herstellung einer Kommunikation oder Übermittlung von Authentifizierungsinformationen. Dieser Austausch wird durch verschiedene Protokolle gesteuert. Der Inhalt der gesendeten Datenpakete (Payload) wird mit verschiedenen Header-Informationen gekapselt. Neben den grundlegenden Header-Daten der Protokolle auf niedrigeren Ebenen (Ethernet, IP, TCP/UDP) sollen in diesem auch verschiedene Protokolle der Ebene 7 betrachtet werden. Die zugehörigen Header-Information sind spezifisch für das entsprechende Protokoll und können z.B. Informationen über den Status der Kommunikation beinhalten. Diese Informationen sind bei der Analyse von Netzwerkdaten nützlich um den Kontext der ausgetauschten Daten zu verstehen und einen Ablauf der Kommunikation nachzuvollziehen. In dem verwendeten Model werden verschiedene Protokolle bei der Kommunikation zwischen den verschiedenen Komponenten betrachtet. Die Wahl des Protokolls hängt von der spezifischen Schnittstelle ab. Eine Auflistung der Schnittstellen für das Ansprechen der entsprechenden Komponente werden in der folgenden Tabelle aufgelistet:

Tabelle der Kommunikationsschnittstellen einfügen, Name, Protokoll, Kurzbeschreibung

Kommunikationsschnittstellen:

- Windowsserver: RDP
- Linuxserver: SSH
- Microsoft SQL Datenbank: SQL
- Active Directory: LDAP
- FTP-Server: FTP

- Firewall: SSH / HTTP
- WebServer: HTTP
- Exchange: MAPI (RPC + HTTP)

Die Betrachtung der Informationen von den Netzwerkelementen und der Kommunikation zwischen den Elementen ergibt das Gesamtbild der ermittelbaren Informationsmenge in diesem Model. Die folgenden Schritte betrachten beide Teile für die jeweils zu untersuchenden Elemente.

3.3 Beschreibung der Systeme

3.3.1 Windows

Das Windows Betriebssystem von Microsoft ist das am Weitesten verbreitete Betriebssystem in der Industrie. Wollen wir die Informationsmenge eines Windowssystems beschreiben können wir auf verschiedene Punkte zurückgreifen. Im Bezug auf Angriffsanalysen und forensischen Analyseverfahren (Quelle?) werden zu diesem Zweck drei grundlegende Teile betrachtet: Logdateien des Betriebssystems sowie installierter Software, die Windows Registry und ausgeführte Prozesse. Die Überwachung und Dokumentation dieser Bereiche ermöglicht es ein Bild über den aktuellen Zustand des Systems zu erhalten. Für die Ausführung von Prozessen und Änderungen der Registry kann eine installierte Überwachungssoftware in Form einer lokalen, systemfokussierten Lösung genutzt werden. Mit Hilfe einer solchen Lösung ist es möglich die Ausführung von ausführbaren Dateien oder das Laden dynamischer Bibliotheken zu überwachen und Sicherheitsereignisse zu generieren im Falle der Ausführung/des Ladens aus ungewöhnlichen oder für diesen Zweck gesperrten Verzeichnissen des Dateisystems. Selbiges gilt für Änderungen von Schlüsseln innerhalb der Registry.

Der dritte Teil besteht aus den Logdateien des Betriebssystems. Die Logdateien sind in einem spezifischen Format geschrieben, sodass eine Anzahl an Feldern vorgegeben ist, die durch den bereitstellenden Service bzw. den bereitstellenden Prozess gefüllt werden können (Quelle?).

Gibt es Vorgaben welche Felder gefüllt werden müssen? Microsoft Dokumentation nochmal checken!

. Die Logdateien werden im EVT (alt) bzw. EVTX (neu) Format dargestellt. In der, vom Betriebssystem bereitgestellten, Ereignisanzeige können die Daten so-

wohl in benutzerfreundlicher Formatierung als auch in einer XML-basierten Form dargestellt werden. Die folgenden Felder werden für diese Logs bereitgestellt:

- Quelle
- Ereignis-ID
- Ebene
- Benutzer
- Vorgangscode
- Protokoll
- Aufgabenkategorie
- Schlüsselwörter
- Computer
- Datum und Uhrzeit
- Zusätzliche Felder: Prozess-ID, Thread-ID, Prozessor-ID, Sitzungs-ID, Kernelzeit, Benutzerzeit, Prozessorzeit, Korrelations-ID und relative Korrelations-ID

Bild für Windowslog Eventfelder einfügen zur Verdeutlichung

Diese Felder können durch die jeweilige Quelle und das Betriebssystem mit verfügbaren Daten versehen werden. Die Quelle gibt die Software(-komponente) oder die Komponente des Betriebssystem an, die das Ereignis protokolliert hat. Die zugehörige Ereignis-ID gibt den Ereignistypen an, der z.B. das erfolgreiche Starten eines spezifischen Dienstes darstellt. Weitere Identifikatoren geben spezifischere Informationen über den auslösenden Prozess und zugehörige Elemente an. Jedes Ereignis wird zu einer bestimmten Kategorie zugeordnet, der Ebene. Die Ebene eines Ereignisses gibt den zugeordneten Schweregrad des Ereignisses an. Für alle Protokolldateien werden dafür die folgenden Ebenen zur Verfügung gestellt: Informationen, Warnung, Fehler und Kritisch. Ereignisse der Ebene „Informationen“enthalten Daten über Änderungen an Anwendungen oder Komponenten. Der erfolgreiche Start bzw. die erfolgreiche Beendigung eines Dienstes, sofern dieser nicht die Systemfunktionalität o.ä. gefährdet, seien hier als Beispiel genannt. Die Ebenen „Warnung“und „Fehler“enthalten Ereignisse, die das Auftreten eines Problems signalisieren. Der Ebene Warnung werden Ereignisse zugeordnet, die das Auftreten eines Problems anzeigen durch das ggf. ein Fehler ausgelöst oder ein Dienst beeinträchtigt werden

könnte. Ein Beispiel ist die Verzögerung der Ausführung des Herunterfahrens des Betriebssystems durch einen Prozess, dessen Beendigung verzögert oder nicht durchgeführt werden kann. Der Ebene Fehler werden Ereignisse zugeordnet, die potentiell die Funktionalität außerhalb der protokollierenden Quelle beeinträchtigen können. Damit werden Ereignisse dieser Ebene als schwerer eingeordnet als Ereignisse der Ebene Warnung. Die letzte Ebene „Kritisch“umfasst Ereignisse, die Fehler signalisieren, jedoch nicht automatisch von dem Betriebssystem behoben werden können. In Protokolldatei „Sicherheit“treten dazu noch zwei weitere Ebenen auf: „Erfolgsüberwachung“und „Fehlerüberwachung“. Diese Ebenen umfassen Ereignisse, die mit der Anwendung der Rechte des ausführenden Benutzers zusammenhängen. Ereignisse der Ebene Erfolgsüberwachung beinhalten die Dokumentation der erfolgreichen Anwendung der Rechte, Ereignisse der Ebene Fehlerüberwachung beinhalten Fehlermeldungen, die bei der Anwendung aufgetreten sind.

Ereignisse der gleichen Quelle und der gleichen Event-ID können abhängig vom Schweregrad in den verschiedenen Ebenen eingeordnet werden.

Das Windowsbetriebssystem beinhaltet zwei Kategorien für Protokolldateien: Windows Protokolle und Dienst- und Anwendungsprotokolle. Die Windowsprotokolle beinhalten Ereignisse, die durch das Betriebssystem protokolliert werden. Diese werden einer von fünf Logdateien zugeordnet: Anwendung, Sicherheit, Installation, System und Weitergeleitete Ereignisse. Das Anwendungsprotokoll beinhaltet Ereignisse, die von installierten Anwendungen protokolliert werden und etwa Fehler mit Bezug auf das Dateisystem signalisieren. Welche Ereignisse konkret protokolliert werden wird von den Entwicklern der Anwendung bestimmt. Das Sicherheitsprotokoll beinhaltet Ereignisse bzgl. sicherheitsrelevanter Elemente wie z.B. Fehlern bei der Anmeldung eines Benutzers oder bzgl. der Ressourcenverwendung bei der Erstellung, Öffnung und Löschung von Objekten. Die Administratoren des Betriebssystems entscheiden, welche Ereignisse dieser Kategorie protokolliert werden. Das Systemprotokoll enthält Ereignisse, die von Systemkomponenten des Betriebssystems protokolliert werden und das Setupprotokoll sichert Ereignisse, die bei der Installation von Anwendungen auftreten können.

Die zweite Kategorie, Anwendungs- und Dienstprotokolle, beinhaltet Protokolle, deren Ereignisse im Kontext von einzelnen Programmen auftreten und keine systemweiten Auswirkungen haben. Diese Kategorie wird in vier Unterkategorien unterteilt: Verwaltung, Betrieb, Analyse und Debug. Verwaltungsprotokolle enthalten Ereignisse mit Problemen und vordefinierten Lösungspfaden für Administratoren. Betriebsprotokolle enthalten Ereignisse, deren Daten für die Analyse und Diagnose von auftretenden Problemen sowie für das Auslösen von installierten Werkzeugen

oder Programmen genutzt werden können. Die Analyse- und Debugprotokolle sind standardmäßig deaktiviert und müssen zunächst aktiviert werden für die Verwendung. Dabei enthält das Analyseprotokoll Ereignisse zu Programmoperationen und Problemen, die nicht vom Benutzer behoben werden können, während das Debugprotokoll weitere Daten für Entwickler beinhaltet.

In der Logdatei SSicherheit"konnten bei einer Untersuchung eines in der Produktion eingesetzten Windowsserver die mit Abstand größte Zahl an Ereignissen festgestellt werden. Im Sicherheitsprotokoll werden Ereignisse festgehalten, die verschiedene Komponenten bzgl. der Sicherung des lokalen Servers oder Computers als auch Zugriffe auf geteilte Resourcen innerhalb einer Windowsdomäne oder mehrere Domänen betreffen. Im Detail können diese Kategorien einen guten Einblick über die Merkmale der überwachten Elemente durch das Betriebssystems geben:

- Account Logon
- Account Management
- Detailed Tracking
- DS (Directory Service) Access
- Logon/Logoff
- Object Access
- Policy Change
- Privilege Use
- System

Grundsätzlich lassen sich die Unterkategorien bzw. Ereignisse in zwei Bereiche unterteilen: Domänen- bzw. Directory Service basierte Ereignisse und lokale Ereignisse. Erstere Ereignistypen beziehen sich auf den Zugang zu Domänen und allgemeine Zugriffs- und Rechteverwaltung sowie auf die technisch darunterliegenden Protokolle und Services. Lokale Ereignistypen beziehen sich auf lokale Ereignisse bzgl. des Zugangs zu dem Betriebsystem und die Benutzung von Privilegien und die damit verbundenen Sicherheitsrichtlinien.

Die Kategorie „Account Logon“bezieht sich nicht auf die Authentisierung eines Benutzers an einem Windowsbetriebssystem, sondern auf die Funktionalität des Kerberosservices. Kerberos ist ein verteilter Authentifizierungsdienst, der für die Anmeldung an einer Windowsdomäne verwendet wird. Daher beziehen sich Ereignisse aus

dieser Kategorie auf Operationen bzw. Eigenschaften des Kerberosprotokolls. Die verwandte Kategorie „Account Management“bezieht sich auf die Verwaltung von Distribution Groups (Verteilungsgruppen für E-Mail Services) und Security Groups (Zuordnung von Benutzerrechten und Zugriffsrechten auf geteilte Resourcen). Desweiteren enthält diese Kategorie auch Informationen zu der Erstellung von Accounts sowie Zugriffsversuchen auf Passworthashs und Anfragen an die Passwortrichtlinienschnittstelle. Eine technische Kategorie des Verzeichnisdienstes wird durch „DS Access“gebildet. Diese Kategorie enthält Ereignisse bzgl. Änderungen, Zugriffen und Replikationen des Verzeichnisdienstes bzw. der im Verzeichnisdienst enthaltenen Daten.

„Detailed Tracking“weißt auf Ereignisse bzgl. der Erstellung und Vernichtung von Prozessen hin sowie Aktiviten bzgl. der Data Protection Schnittstelle „DPAPI“und Anfragen auf die RPC (Remote Procedure Call)-Schnittstelle. Die Kategorie „Logon/Logoff“kann als äquivalente lokale Kategorie gesehen werden, da diese Ereignisse bzgl. der Anmeldung/Abmeldung als lokaler Benutzer an einem Betriebssystem gesehen werden kann. Allerdings enthält diese Kategorie auch Ereignisse bzgl. der Nutzung des IPSec Protokolls und die Interaktion eines Benutzers mit einem Network Policy Server. Die Kategorie „Object Access“beinhaltet Ereignisse bzgl. des Zugriffes und der Änderung auf systemrelevante Objekte dar. So sind Ereignisse bzgl. der Verbindung zur Windows Filtering Plattform, darunter Ereignisse der Windows Firewall. Die Windows Filtering Platform ist eine Sammlung aus Schnittstellen und Systemdiensten, die für die Erstellung von Programmen zur FIlterung und Modifikation von Netzwerkdatenverkehr genutzt werden kann. Die Windows Firewall basiert auf dieser Sammlung. Desweiteren werden dieser Kategorie Ereignisse zugeordnet bzgl. Änderungen der Windows Registry Keys, des Component Object Models (COM+), Zugriffe auf das Dateisystem und geteilte Verzeichnisse sowie die Manipulation von Zugriffsoptionen auf Systemressourcen und Änderungen am Certification Service. Die Kategorie „Policy Change“beinhaltet Ereignisse, die mit der Änderungen von Richtlinien zusammenhängen. Die entsprechenden Richtlinien gehören zu den Bereichen Authentisierung, Authorisierung, Überwachung, Windows Filtering Platform sowie des MPSSVC (Teil der Windows Firewall, welcher vor nichtautorisiertem Zugriff von Benutzern aus dem Internet oder einem Netzwerk schützt) und anderer Richtlinien (z.B. im Bezug auf kryptografische Operationen). Die Kategorie „Privilege Use“beinhaltet Ereignisse zu der (nicht-)sensiblen Benutzung von Privilegien im Kontext des Betriebssystems. Schlussendlich zeigen Ereignisse aus der Kategorie „System“Änderungen am (Sicherheits-)Zustand des Systems sowie der Sicherheitssubsysteme (Local Security Authority und Security Account Manager).

Ereignisse der genannten Quellen können auch, abhängig von der ID, also dem Ereignistypen, in anderen Protokollen wie etwa dem Anwendungsprotokoll oder dem Systemprotokoll aufgeführt werden.

Windows Logs: Ggf. weitere Beispiele nennen, kurz beschreiben

Neben den fundamentalen Logdateien können weitere Logdateien von Applikation erstellt werden. Neben Microsoft-Produkten wie dem Webserver IIS, Microsoft Office oder der Benutzerverwaltung Active Directory können auch Logs von Microsoft-fernen Produkten wie z.B. einer Anti-Virensoftware oder proprietäre Netzwerkdienste durch die Applikationen zur Verfügung gestellt werden.

Loggt das Betriebssystem Elemente aus diesem Bereich? Wie funktioniert die Anbindung der Logdateien an das Betriebssystem?

3.3.2 Linux

Für die Extraktion der Informationsmenge aus einem Linuxsystem wird die gleiche analytische Basis wie für das Windowsbetriebssystem vorausgesetzt. Die Betriebssysteme unterscheiden sich von ihrem Aufbau und ihren Mechanismen teilweise deutlich, jedoch lässt sich der Grundsatz ähnlich ableiten. Das Ziel ist es alle verfügbaren Informationen zu erhalten, die bei der Ausführung des Systems entstehen. Dies schließt die Analyse von Protokollen ein, sowie die Überwachung der Ausführung von Diensten (Services) und die Ausführung von (System-)Prozessen. Im Bezug auf Linux sollen daher die vorhanden Protokollen untersucht werden sowie die grundlegenden Elemente wie zugehörige Informationen zu Services und Informationen über die Ausführung von Befehlen, speziell mit erweiterten Rechten (sudo), untersucht werden.

Bei Linux Betriebssystemen wird zwischen verschiedenen Distributionen unterschieden. Im Bezug auf Log-Dateien wird in der Literatur bzgl. der Namensgebung zwischen Debian-basierten Distributionen wie etwa Ubuntu und CentOS/RedHat unterschieden. In Linux existieren vier typische Kategorien für Log-Dateien:

- Application Logs
- Event Logs
- Service Logs
- System Logs

Unter Linux existiert wird das Protokollieren von Systemmeldungen durch „syslogd“übernommen, den system' logging daemon (mittlerweile auf manchen Distri-

butionden durch „rsyslogd“ersetzt), sowie durch „klogd“für Kernelmeldungen. Diese beiden Dienste schreiben Meldungen in Log-Dateien, die sich in dem Unterverzeichnis „syslog“(Debian-basiert / Ubuntu) bzw. „messages“(CentOS / RedHat) des Standardverzeichnis für Log-Dateien befinden (/var/log/). Dabei werden die Meldungen als Ereignisse durch Regeln den verschiedenen Log-Dateien zugeordnet, abhängig von ihrer „Facility“sowie ihrer Priorität.

Für rsyslogd bestehen die folgenden Facilities:

- auth/authpriv: Security/authorization messages (private)
- cron: Clock daemon (crond & atd)
- Daemon Messages from system daemons
- kern: Kernel messages
- local0-local7: Reserved for local use
- lpr: line printer subsystem
- mail: Messages from mail daemons
- news: USENET news subsystem
- syslog: Messages generated internally by system log daemon
- User: Generic user-level messages
- UUCP: UUCP subsystem

Für jedes Ereignis werden, ähnlich der Ebene für Windowslogs, Prioritäten vergeben:

- emerg: System is unusable
- Alert: Action must be taken immediately
- crit: critical conditions
- err: error conditions
- warning: Warning conditions
- notice: normal but significant importance
- info: informational messages

- debug: debugging messages

Basierend auf diesen Parametern werden die Ereignisse in die Log-Dateien geschrieben, deren Namen auf diesen Parametern basieren (z.B. „mail.info“).

Neben den Log-Dateien des syslog Verzeichnisses gibt es noch weitere wichtige Log-Dateien im Verzeichnis „/var/log/ “die für die Erhebung weiterer Informationen nützlich sein können. Zu den wichtigstens Log-Dateien bzw. -verzeichnissen zählen:

- auth.log (Debian) / secure (CentOS): Ereignisse bzgl. der Authentifizierung von Benutzern
- boot.log: Ereignisse während des Boot-Vorgangs
- dmesg: Nachrichten bzgl. Hardware und Hardwaretreibern
- kern.log: Ereignisnachrichten des Betriebssystemkerns
- faillog: Dokumentation von gescheiterten Login-Versuchen
- cron: Dokumentation der Ausführung und ggf. Fehlermeldungen von Cronjobs

Abhängig von der Verwendung des Servers stehen auch standardmäßig Log-Dateien zu den jeweiligen Servertypen (etwa E-Mailserver, Webserver (typischerweise Apache) oder Datenbankserver (etwa MySQL) zur Verfügung.

Beschreibe das Linux Auditing Framework um einen Überblick zu geben, wie Linux Auditing funktioniert und was überwacht wird

3.3.3 Applikationen

Apache Webserver

Der Apache Webserver ist eine freie Software als Teil der Apache Lizenz. Es werden viele Betriebssysteme unterstützt und mithilfe der APR (Apache Portable Runtime) Bibliothek wird eine Verallgemeinerungsschicht zwischen den Webserver und die Systemaufrufe gesetzt um die individuellen Stärken des Betriebssystems besser nutzen zu können. Der Webserver ist modular aufgebaut und kann um viele Funktionalitäten erweitert werden, u.a. zusätzlich zu der Unterstützung der serverseitigen Skriptsprachen PHP, Perl und Ruby kann ein Modul für Python, Lua, Tcl und .NET geladen werden. Weitere Modulfunktionalitäten sind etwa Verschlüsselungen, Authentifzierung, Proxyfunktionalitäten, WebDAV-Unterstützung oder HTTP-Rewrite. Diese Module können jederzeit aktiviert und deaktiviert werden. Als Ansprechschnittstelle dient die CGI Schnittstelle.

Ein Fehler in der Webserverkonfiguration oder auf dem Webserver aufbauenden Webanwendungen kann potentiell von einem Angreifer provoziert und ausgenutzt werden. Aus diesen Gründen wird von Apache eine Liste an Sicherheitselementen bereit gestellt, die als Anhaltspunkte für die Härtung und Sicherung der Webserver-Installation dienen sollen. Neben Sicherungshinweisen bzgl. der Aktualisierung des Servers und Abwehrmaßnahmen gegen DDoS Angriffe werden auch u.a. die folgenden Elemente genannt:

- Rechte bzgl. des ServerRoot Directories (Wurzelverzeichnis)
- Server Side Includes
- Hinweise zum Umgang mit der CGI Schnittstelle (Generell, Non-Script Aliases, Script Aliases)
- Umgang mit anderen Quellen für dynamische Webinhalte
- Schutz der Systemeinstellungen
- Standardschutz der Serverdateien
- Überwachung der Protokolldateien (Logs)

Im Zuge dieser Sicherheitsbedenken stellt der Webserver verschiedene Protokolldateien -und Funktionalitäten zur Verfügung. Da verschiedene Module unterschiedlich kritische Auswirkungen auf den Webserver haben können, existieren Protokolldateien pro Modul, die individuell anpassbar sind. Neben dem Error-Log und den Modul-Logs ist das Access-Log als eine der wichtigste Protokolldateien ausgewiesen, welche Zugriffe auf den Webserver bzw. das Webserververzeichnis protokolliert. Das Verzeichnis und der Zugriff auf das Access-Log werden von der „Custom Log Directive“verwaltet. Das übliche Logformat ist dabei wie folgt strukturiert: „IP-Adresse, Request Teil (falls vorhanden), Zeitstempel, HTTP Kommando, HTTPStatusCode, Größe der Antwort“

Es ist zudem möglich mehrere Access-Logs zu führen sowie „Conditional Logs“(Protokolldateien in denen vorkonfiguriert bestimmte Event-Typen nicht protokolliert werden). Innerhalb des Apache Webserver existieren verschiedene Log-Level, die die Ausführlichkeit der Eventdokumentation in einer Protokolldatei wiederspiegeln. Die Log-Level unterscheiden sich in: "

- emerg: Notfall - das System ist unbenutzbar
- alert: Maßnahmen müssen unverzüglich ergriffen werden

- crit: Kritischer Zustand
- error: Fehlerbedingung
- warn: Warnung
- notice: Normaler, aber signifikanter Zustand
- info: Information
- debug: Debug-Level-Nachrichten

... Es wird empfohlen, mindestens den Level crit zu verwenden. "(Zitat, Quelle angeben!)

Neben den genannten Protokolldateien gibt es noch ein paar weitere, potentiell signifikante Elemente:

- „mod_ log_ forensic“: ein Modul das forensischen Protokollierungsfunktionalität von Client-Anfragen bietet, mit zwei Einträgen pro Anfrage (davor und danach)
- „PID file“: Speichert die ParentID des Webserverdaemons / -services
- „Script Log“: Protokolliert Ein- und Ausgabe von CGI Skripten

Microsoft SQL Server

Der Kern eines Unternehmens sind Daten über das Unternehmensgeschäft. Die Aufbewahrung, Sicherung und der Zugriff zu diesen Daten ist daher von essentieller Bedeutung. Daher werden diese Daten in Datenbanken abgelegt, die die strukturierte Darstellung und Sicherung von Daten ermöglichen. Der Microsoft SQL Server ist ein relationales Datenbankverwaltungssystem (Relational Database Management System (RDBMS)). Es ermöglicht die Verwaltung mehrerer Datenbanken und steuert den parallelen Zugriff auf eine Datenbank, d.h. das parallele Abrufen und Editiern von Daten durch mehrere Personen. Zu der Verwaltung der Datenbanken werden weitere Funktionalitäten hinzugefügt, die die Analyse der Daten, Integration anderer Dienste und Anwendungen, Reporting und Sicherheit der Datenbanken und des Servers. Zudem existiert eine Client-Anwendung, das Microsoft SQL Management Studio, für den verwaltenden Zugriff auf den SQL Server.

Die Komponenten des Servers werden in zwei Kategorien eingeteilt. Die erste Kategorie umfasst Komponenten für „Business Intelligence“Zwecke, also Komponenten, die bei der Entscheidungsfindung für das Unternehmensgeschäft helfen können. Die

zweite Kategorie, „Database Engine“, umfasst Dienste, die für die Operation des Servers notwendig sind, etwa für die Verbindung und den Austausch von Daten über Transact-SQL (T-SQL) Statements.

In der Kategorie Database Engine gehören neben der primären Komponente, der Storage Engine, die folgenden Komponenten:

- T-SQL programming interface
- Replication Services
- SQL Server Agent
- High Availability and disaster recovery tools
- SQL Server Integration Services
- SQL Server Management Tools
- Security Subsystem

Das Security Subsystem wird verwendet um den kontrollierten Zugriff zum SQL Server, den verwaltenden Datenbanken, anderen Serverobjekten und Datenbanktabelleneinträgen. Zudem ermöglicht es die Verschlüsselung von Datenbankobjekten und fügt Werkzeuge für das Server Auditing.

Die Server Audit Komponente erlaubt das Verfolgen und Protokollieren von Ereignissen innerhalb der Database Engine. Für den Zweck der Protokollierung werden Objekte (Audit Objects) angelegt. Dies kann sowohl auf der Serverebene als auch auf der Datenbankebene durchgeführt werden. Die protokollierten Ereignisse können entweder in eigens dafür angelegte Dateien, in ei Windows Application Event Log oder das Windows Security Event Log geschrieben werden. Für die Protokollierung wird unter anderem „Extended Events“verwendet, ein Überwachungswerkzeug für die Serverperformanz, welches Konzepte des Windows Event Tracing nutzt. Dies erlaubt u.a. die Korrelation von Ereignisdaten innerhalb des SQL Servers. Unter bestimmten Bedingungen ist es zudem möglich Ereignisdaten des Servers mit weiteren Daten von Anwendungen und dem Betriebssystem zu korrelieren.

Die Server Audit Komponente unterteilt die zu protokollierenden Ereignisse in „SQL Server Audit Action Groups and Action“.

Diese enthalten, zusammengefasst, die folgenden Elemente:

- Änderungen (Erstellung, Löschung, Veränderung) von
  - Objekten des Servers (z.B. Schemata) oder der Datenbank

  - Zugriffsrechten und Inhaberrechten
  - Zugriffsoperationen
  - Ausführung von T-SQL Statements
- SQL-Aktionen (SELECT, UPDATE, INSERT, DELETE, EXECUTE, RECEIVE, REFERENCE)
- Audit-Aktionen CREATE, ALTER und DROP von Audit Objekten (Server Audit, Server Audit Specification, Database Audit Specification)

3.3.4 Interaktionen der Systeme (und Anwender)

Dieser Abschnitt soll die Interaktion der Netzwerkteilnehmer beschreiben, gehört ggf. in den Architekturteil mit Bild

3.3.5 Netzwerkprotokolle

HTTP (Hypertext Transfer Protocol)

Das Hypertext Transfer Protocol (HTTP) ist ein zustandsloses Protokoll, dass zur Übertragung von Daten, meist für das Laden von Webinhalten aus dem Internet genutzt wird. Der Begriff ßustandlos"bezeichnet die Eigenschaft, dass durch das Protokoll keine Informationen vorheriger Nachrichten gespeichert werden. Daher ist HTTP u.a. auf ein Transportprotokoll wie TCP auf der Transportebene angewiesen, HTTP selbst wird zur Anwendungsebene zugeordnet. Die Kommunikation zwischen Client und Server wird in Form eines Nachrichtenaustausches vollzogen, der aus zwei Elementen besteht: Anfrage (Request) und Antwort (Response).

Die Nachrichtenpakete werden in Kopf (Header) und Rumpf (Body) unterteilt. Der Header enthält Informationen über das gesendete Nachrichtenpaket. Eine typische Anfrage ist wie folgt strukturiert:

<Methode> <URL> <Protokollversion>
<Host>
<Payload>

Dummypräsentation, Bilder von HTTP Request und Response müssen später eingefügt werden

Die Methode stellt die Art der Anfrage dar. Üblicherweise werden entweder die Methoden „GET“(Anforderung einer Resource per URI (Uniform Resource Identifier)) oder „POST“(Senden von Daten an den Server zur Verarbeitung). Weitere Methoden sind HEAD, PUT, PATCH, DELETE, TRACE, OPTIONS und CONNECT.

Die URL gibt den Server an, an den die Anfrage gesendet wird. Das Host-Feld wird genutzt um mehrere DNS-Namen, die unter der gleichen IP-Adresse erreichbar sind, zu unterscheiden. Der Payload enthält Informationen zu der angeforderten Resource.

Die Antwortnachricht wird in folgendem Format gesendet:
<Protokollversion> <HTTPStatusCode> <Beschreibung>
Server: <Webserverversion> <PHP Version>
Content-Length: <Größe der Resource in Byte>
Content-Language: <Sprachkürzel> (z.B. „de“)
Connection: <Verbindungsstatus>
Content-Type: <Resourcentyp> (z.B. HTML)
<Payload>

Die Antwortnachricht enthält Informationen bzgl. der angefragten Resource sowie Informationen über den liefernden Webserver. Der HTTPStatusCode repräsentiert einen dreistelligen Code, der die erfolgreiche Bearbeitung der Anfrage repräsentiert oder einen Fehlercode anzeigt. Die Codes werden wie folgt kategorisiert:

- 1xx: Informationen
- 2xx: Erfolgreiche Bearbeitung
- 3xx: Umleitung der Anfrage (wenn bspw. eine Resource verschoben wurde)
- 4xx: Clientseitiger Fehler
- 5xx: Serverseitiger Fehler

Secure Shell (SSH)

Secure Shell (SSH) ist ein Netzwerkprotokoll bzw. ein System, welches für die sichere Kommunikation zwischen zwei Computern verwendet wird. Ein SSH-Server erlaubt SSH-Clients Anfragen zu senden um sich etwa über das Netzwerk auf dem Server zu anzumelden, Daten zu senden oder Kommandos auszuführen. Dabei sollen grundsätzliche die Ziele der Vertraulichkeit der Kommunikation, der Integrität der Nachrichten und sicheren Authentisierung der Kommunikationsteilnehmer sowie der authorisierte Zugriff sicher durchgeführt werden. SSH kann zudem genutzt werden um weiteren Datenverkehr auf der Basis von TCP/IP zu „tunneln“, d.h. die Nachrichten zu verschlüsseln und verschlüsselt über die vorhandene Sitzung weiterzuleiten. Es existieren verschiedene Versionen dieses Protokolls. Die folgende Beschreibung beschränkt sich auf die Version SSH-2, die als sicherere Variante im Vergleich zu SSH-1, gilt.

Für die Kommunikation zwischen dem Client und dem Server verschiedene Verschlüsselungsschlüssel benutzt, sowohl für die Herstellung der Kommunikation als auch für die Dauer der Verbindung (Sitzung (Session)). Die Herstellung der Kommunikation erfolgt über das Public-Key-Verschlüsselungsverfahren, welches die privaten und öffentlichen Schlüssel des Clients und des Servers nutzt um eine Verschlüsselungsmethode sowie einen Sitzungsschlüssel für die Verschlüsselung auszuhandeln. Durch diese Methode wird gleichzeitig die Authentisierung des Benutzers sowie des Servers gegenseitig gesichert.

Grundsätzlich gehören zu den Paketfeldern die Gesamtlänge des Paketes, ein gewisser Padding-Bereich, der Payload, ein weiterer zufälliger Paddingbereich und der Message Authentication Code (MAC).

Das SSH-2-Protokoll wird in verschiedene Layer unterteilt:

- SSH Transport Layer Protocol
- SSH Authentication Layer Protocol
- SSH Connection Layer Protocol

Das SSH Transport Layer Protocol dient als Basis. Mithilfe dieses Layers wird die intiale Verbindung aufgebaut (Prüfung der Server Authentizität, Aushandlung der zu verwendenden Verschlüsselungsmethode, Intialisierung der Sitzung) und somit grundlegende Funktionalität für die Verschlüsselung der Pakete und die Sicherung der Nachrichtenintegrität mithilfe von kryptografischen Hash-Funktionen.

Im Speziellen wird die Kommunikation mit der Nachricht „SSH_ MSG_ KEXINIT“ausgelöst. Die Felder der Nachricht enthalten neben einem Byte-Array (Cookie) eine Reihe von weiteren Arrays, in denen Listen der unterstützten Algorithmen für Server Host Key, Verschlüsselung, MACs und Komprimierung gesendet werden. Durch einen Abgleich und weitere Protokollregeln ergeben sich die verwendeten Methoden für die Kommunikation. Sollte bei diesem Ablauf ein Fehler oder sonstige Störungen auftreten, wird eine „SSH_ MSG_ DISCONNECT“Nachricht gesendet. Diese enthält u.a. einen sogenannten „reason code“, der einem Grund für den Verbindungsabbruch zugeordnet werden kann.

Darauf folgend kann mithilfe des SSH Authentication Layer Protocol die Authentisierung des Benutzers vorgenommen werden. Für die Authentisierung stehen drei Methoden zur Verfügung („Public Key“, „hostbased“und „password“). Nach der erfolgreichen Authentisierung besteht im Folgenden die Möglichkeit über das SSH Connection Layer Protocol die weiterreichenden Funktionalitäten von SSH zu nutzen (inklusive Port Forwarding, Remote Access und Remote Program Execution).

Für den Zweck der Authentifzierung des Servers existieren sogenannte „Host Keys“. Diese werden genutzt um die Authentizität der Serveridentität zu bescheinigen. Mit SSH-2 wird auf einem Server pro Netzwerksockel ein individueller Host Key verwendet. Die Benutzerauthentisierung findet u.a. per Passwort statt. Um die Rechtezuordnung pro Account bzw. pro Server zu konfigurieren, werden Konfigurationsdateien verwendet (etwa /.ssh2/authorization).

Remote Desktop Protocol (RDP)

Das Remote Desktop Protocol ist ein Protokoll, dass die Darstellung und Kontrolle des Bildschirminhaltes eines anderen Computers mit dem Windows Betriebssystem ermöglicht. Es basiert auf dem T-120 Standard der ITU (International Telecommunication Union), der eine Sammlung an Kommunikations- und Anwendungsprotokollen enthält.

Das Protokoll regelt u.a. wie die Dienste und Anwendungen auf der entfernten Windows-Maschine (Terminalserver) angesprochen und verwendet werden können. Dabei ist es möglich mehrere virtuelle Kanäle zu unterschiedlichen Maschinen zu öffnen und Kommunikations- sowie Präsentationsdaten zu übertragen. Für die Kommunikation notwendige Umgebungsvariablen werden aus den RPC-TCP Einstellungen ermittelt.

Die grafischen Daten werden auf dem Server von einem RDP-zugehörigen grafischen Treiber in Netzwerkpakete verpackt und über das Netzwerk gesendet. Der Client empfängt diese Daten und wandelt sie über Aufruf der Graphic Device Interface (GDI) Programmierschnittstelle in eine Darstellung um. Eingabedaten von Tastatur- und Maus werden über das RDP vom Client auf den Server umgeleitet.

Der Ablauf einer RDP-Verbindung kann in verschiedene Teile unterteilt werden. Für den Aufbau der Verbindung werden u.a. die folgenden Schritte durchgeführt. Für die Kommunikation werden in TCP/IP verpackte X.224 Paketeinheiten (Protocol Data Unit, PDU) verwendet:

- Initierung der Verbindung
- Austausch der grundlegenden Basiseinstellungen
- Erstellung eines dedizierten Kommunikationskanals
- Austausch von Sicherheitseinstellungen
- Versendung der Verbindungslizenz des Servers zum Client zu Validierungszwecken während der Verbindung

- Finalisierung der Verbindungsdetails

Für den Abbruch der Verbindung existieren verschiedene Szenarien, die unterschiedlich behandelt werden. Zu diesen zählen die vom Benutzer-initierte Beendigung der Verbindung auf der Clientseite (durch Beenden der RDP-Anwendung) sowie auf der Serverseite (durch Beenden der Sitzung). Als weiterer Fall wird das erzwungene Beenden der Verbindung durch einen Administrator genannt.

Microsoft SQL Server Protocol Suite

Für die Kommunikation mit dem Microsoft SQL Server werden verschiedene Protokolle verwendet, die für bestimmte Anwendungszwecke und Funktionen verwendet werden. Zu den Anwendungsbereichen zählen:

- Netzwerkverbindungen und Anwendungsentwicklung
- Verwaltung
- SQL Server Services
  - Master Data Service
  - Reporting Services
  - Analysis Services
- Database Engine
- Complex Event Processing (CEP) Engine

Im Folgenden wird eine Untergruppe dieser Protokolle beschrieben, die für die Netzwerkverbindungen verwendet werden.

Der Verbindungsverlauf mit einer Client-Anwendung erfolgt in den folgenden Schritten:

1. Authentifizierungs Handshake zwischen Client und Server mit einem ausgewählten Schema (SQL Server Authentifzierung oder Windows Authentifzierung)
2. Der SQL Server verifiziert die übermittelten Anmeldedaten.
   - Sind die Anmeldedaten korrekt, erfolgt die Bestätigung der Verbindung durch den Server
   - Sind die Anmeldedaten nicht korrekt, wird die Verbindung durch den Server abgebrpchen und eine entsprechende Rückmeldung gesendet

3. Nach erfolgreicher Anmeldung werden Befehle gesendet

4. Der Server beantwortet diese Anfrage mit einem Ausführungsstatus und einer Antwort

5. Die Verbindung wird durch die Client-Anwendung beendet

Dieser Ablauf gilt für die Verwendung des Native Web Services (SSNWS) Protokolls und des Tabular Data Stream (TDS bzw. SSTDS (TDS v4.2) Protokolls. Das Native Web Services Protokoll ist ein Netzwerkprotokoll, welches für die Verbindung der Database Engine mit WebService-basierten Anwendungen genutzt wird. Auf der Basis von SOAP 1.1 und 1.2 definiert es Kommunikationslogik und Nachrichtenformate für den Austausch von T-SQL Abfragen. Das TDS Protokoll ist ein Protokoll der Anwendungsebene regelt die Übertragung von T-SQL Anfragen und Antworten zwischen Client-Anwendungen und Datenbanken auf dem SQL Server. Die Version 4.2 (SSTDS) fügt dem Protokoll weitere Eigenschaften hinzu (u.a. Authentifizierung, Kannalverschlüsselungsverhandlung, Spezifikationen für SQL-Anfragen und RPC-Integration).

Neben diesen Protokollen werden desweiteren die folgenden Protokolle für die Netzwerkverbindungen verwendet:

- Session Multiplex Protocol (SMP): Dieses Protokoll wird für die Kommunikation zwischen Datenbankanwendungen und der SQL Server Database Engine verwendet. Es ermöglicht darüber hinaus Multiplex-Datenbankkommunikation über eine einzelne, stabile Transportverbindung.

- SQL Server Resolution Protocol (SSRP): Dieses Protokoll dient der Namensauflösung von SQL-Serverinstanzen im Netzwerk, sowie für die Auflistung der erreichbaren Serverinstanzen.

3.4 Analyse des Informationspools im Bezug auf Angriffsszenarien

In Folge der Beschreibung der Elemente des zu analysierenden Modells stellt sich die Frage der Relevanz im Bezug auf die Nutzbarkeit für die Erkennung von Sicherheitsvorfällen, u.a. mit Hilfe eines SIEM-Systems. Zu diesem Zweck wird im Folgenden zunächst der Informationspool als Gesamtmenge betrachtet und daraufhin unter dem Aspekt der Analyse von Angriffsszenarien.

3.4.1 Betrachtung der Datenmenge

Die Untersuchung der Netzwerkteilnehmer ergibt, dass auf jedem System eine Art Protokolldatei zur Verfügung steht, die Informationen über Veränderungen des Systems enthält. Diese Informationen umfassen u.a. Daten zu den Zeitpunkten der Veränderung, dem Objekt der Veränderung sowie abhängig von der Protokolldatei und der protokollierenden Software weitere Details wie etwa Verzeichnisdaten. Zudem erlaubt die Integration der Elemente im Netzwerk basierend auf dem einheitlich verwendeten Ethernet-Standard eine Betrachtung der Kommunikationsflüsse innerhalb des Netzwerkes durch die Analyse der Protokolldatein der Firewalls, Switche und Router sowie der zugehörigen Protokolldateien der Server.

Die grundlegenden Protokollierungsmechanismen der Betriebssysteme erlauben eine Übersicht über alle laufenden Prozesse und deren Abhängigkeiten, sowie der ausgeführten grundlegenden Operationen (z.B. die Erstellung eines Prozesses). Mit dieser Funktionalität werden zudem Events über Veränderungen von Dateien und Änderungen von Betriebssystemkomponenten (wie etwa Änderungen an der Registry-Komponente des Windows Betriebssystems) dokumentiert. Desweiteren ist mit der vorhanden Grundlage die Erstellung anwendungsspezifischer Protokolle von auf dem Betriebssystem aufsetzender Appplikationen möglich. Die Protokollierung der Betriebssystem umfasst zudem Daten über die Zugriffszeitpunkte, Dauer des Zugriffes und Rechtevergabe für Benutzer der Systeme. Die Limitierung der Dokumentation der Systemveränderungen ergibt sich aus der Verwendung der Protokollierungsplattform durch Entwickler der installierten Anwendungen, etwa in Form der Nutzung der vorhanden Datenfelder und dem Definitionsgrad der Fehlermeldung und anderer Events im Bezug auf die Funktionalität der jeweiligen Anwendung.

Neben der Protokollierungfunktionalität der Betriebssysteme können zusätzlich weitere Überwachungs- und Analysewerkzeuge, wie etwa Endpoint Security Lösungen, verwendet werden um zusätzliche Informationen durch Auswertung der unterliegenden Datenlage sowie der Überwachung definierter Elemente des Systems im Rahmen der vorhanden Resourcen bzgl. Rechenleistung und Zeitkosten.

Zusätzlich zu der systembezogenen Überwachung und Analyse können die Protokolldatein von Netzwerkkomponenten (Firewalls, Switche, Router) genutzt werden um Informationen über die Kommunikation innerhalb des Netzwerkes, sowie der Kommunikation mit Kommunikationsteilnehmern außerhalb des Netzwerkes nachzuvollziehen und auf Unregelmäßigkeiten zu prüfen. Zu den verfügbaren Daten gehören Daten über den Ablauf der Kommunikation, das Ziel der Kommunikation (etwa die Anfrage und Übermittlung von Datenbankdaten), die Dauer der Kommunikation und auch die Anzahl an Kommunikationsfehlern, Verbindungsabbrüche und andere

Störungen.

3.4.2 Relevanz für die Sicherheitsbetrachung mit Hilfe von SIEM-Systeme

Um die Relevanz der dargestellten Informationen für ein SIEM-System darzustellen wird im Folgenden anhand von Beispielen, die Analyse von Angriffsszenarien bzgl. der Infektion von Systemen durch Malware beschrieben. Die Aufgabe eines SIEM-Systems ist es, wie bereits im Grundlagenkapitel beschrieben, Daten über den Status der Systeme im Unternehmensnetzwerk zu sammeln, zu speichern, auszuwerten und zu verknüpfen. Die zu diesem Zweck erstellten und fortlaufend aktualisierten Regeln basieren u.a. auf der Kenntnis des Verhaltens von Malware.

Bei der Infektion, Ausführung und Verbreitung von Malware auf einem System werden Teile des Systems verändert um eine möglichst lange Ausführung der Malware zu ermöglichen. Diese Veränderungen werden durch das System an verschiedenen Stellen dokumentiert. Diese Daten werden im Rahmen einer Untersuchung und Überwachung eines Systems als Indikatoren für die Kompromittierung eines Systems (IoC, „Indicator of Compromise“) bezeichnet. Für die Erkennung dieser Indikatoren wird bspw. für die Überwachung der normale Betriebszustand möglichst präzise definiert, sowie eine Analyse des infizierten Systems und der darauf befindlichen Malware durchgeführt, durch die potentielle Erkennungsmerkmale festgestellt und zu Indikatoren zusammengestellt werden. Diese werden von einem Sicherheitssystem wie etwa einem Softwareagenten eines SIEM-Systems oder einer Anti-Malware Software für die Erkennung und/oder Schutzmaßnahmen verwendet.

Der Ablauf eines Angriffsszenarios, bei dem eine Malware für einen oder mehrere Zwecke auf einem System installiert wird, lässt sich grob in die folgenden Schritte einteilen:

1. Erlangen des Zugriffs auf das System über einen Angriffsvektor (z.B. Phishing, infizierte externe Speicher, infizierte Webinhalte)

2. Erstellung eines Zugriffspunktes, Sicherstellung der Persistenz und Verschleierung der Aktivitäten

3. Hinzufügen weiterer Werkzeuge von einem internen oder externen Speicherpunkt

4. Ausführung der Malware auf dem System

5. Ggf. Informationssammlung über weitere Systeme im Netzwerk und Verbreitung der Malware

Quelle (Quelle hier einfügen!) beschreibt anhand eines Beispieles die Erstellung von IoCs. In diesem Beispiel wird zunächst der Angriffsvektor in Form einer Phishing-E-Mail analysiert. Durch das Herunterladen und den Versuch der Öffnung einer PDF-Datei im Anhang der E-Mail wurde die erste Komponente der Malware platziert, durch die eine Hintertür geöffnet und dem Angreifer Zugriff auf das System verschafft wurde. Bei der Betrachung des Vorfalles durch den zuständigen Analysten konnte dieser Prozess durch dokumentierte Operationen des Betriebssystems nachvollzogen werden. Im Speziellen wurde Operationen im Dateisystem protokolliert, die die Erstellung der PDF-Datei durch Herunterladen des Anhangs zeigen (inklusive des dazugehörigen Zeitstempels, Verzeichnispfades und der Betriebssystemoperation) sowie die Erstellung einer Anwendungsdatei (.exe) zum vermuteten Zeitpunkt des Öffnungsversuches durch den Benutzer. Im nächsten Schritt konnten protokollierte Änderungen von Einträgen innerhalb der Windows Registry entdeckt werden, sowie weitere Spuren in Form von Dateien und Dateisystemoperationen, die dem Hinzufügen weiterer Funktionalität in dem Verzeichnispfad „C:
$RECYCLE.BIN“(verstecktes Verzeichnis des Papierkorbes), etwa eines Werkzeuges für die Durchsuchung des Dateisystems, sowie der Verschleierung der Aktivitäten dienten. Ein typischer Fund konnte etwa das Hinzufügen der Malware in den Autostart-Schlüsseln der Windows Registry verzeichnet werden, durch das die Ausführung der Malware beim Start des Systems sichergestellt werden soll. Zudem wurde der Aufruf des Verzeichnises per Internet Browser dokumentiert sowie weitere Aktivitäten mit dem Ziel Informationen über Systeme im lokalen Netzwerk zu sammeln.

Andere Quellen und Beispiele der Untersuchung von Malware-Typen, u.a. Keylogger-Werkzeugen, Ransomware und trojanischen Pferden ergeben ähnliche Funde (Quellen einfügen!). Darüber hinaus werden diese Indikatoren auch für die Herstellung von Malware-Signaturen verwendet, die von Anti-Malware-Programmen genutzt werden um Malware-Infektionen zu erkennen und zu verhindern oder einzudämmen.

Diese Beispiele zeigen, dass die Dokumentation jeglicher Systemprozesse sowie die kontinuirliche Auswertung dieser Dokumentationen essentiell sind um Angriffe durch Malware-Infektionen zu verhindern. Daraus ergibt sich die Relevanz der Informationsmenge für den Einsatz eines SIEM-Systems.

Kapitel 4

Analyse der Informationsquellen in einem industriellen Produktionsnetzwerk

In diesem Kapitel soll in Folge der Analyse der relevanten Informationsmenge in Unternehmensnetzwerken eine Betrachtung des Zustandes in industriellen Produktionsnetzwerken erfolgen. Als industrielles Produktionsnetzwerk werden dafür in diesem Kapitel die Netzwerkstrukturen in der Produktionsleit- und Feldebene betrachtet.

Wie bereits im vorherigen Kapitel ist das Ziel der Analyse ist es die sicherheitsrelevanten Infortmationsmenge zu erfassen. Informationen werden als sicherheitsrelevant betrachtet, wenn diese Informationen genutzt werden können um die Nutzung eines bestimmten Angriffsvektors erkennen zu können. Da automatisierte Anlagen abhängig vom Industriezweig und selbst von Unternehmen zu Unternehmen und zweckgebunden unterschiedlich sind, wird ein stark vereinfachtes Model verwendet, welches die Elemente eines Automatisierungsnetzwerkes zeigt. Da das grundlegende Ziel die Ermittlung der Informationsmenge ist, werden Elemente wie etwa die weite Verteilung / Verbreitung von Fertigungssystemen in diesem Kapitel nur am Rande berücksichtigt.

Äquivalent zu der Betrachtung der Unternehmensnetzwerke wird das benutzte Model und dessen Komponenten beschrieben. Das Ziel der Beschreibung der Komponenten ist eine grobe Klassifizierung der verfügbaren Informationsquellen der Komponenten. Da in industriellen Netzwerken konkurrierende Standards verwendet und viele proprietäre Protokolle und Geräte verwendete werden, muss eine Einschränkung stattfinden. Aus diesem Grund werden für das Model populäre Elemente im europäischen Raum verwendet. Desweiteren wird basierend auf der individuellen Natur der Programmierungen und Parameteranpassungen auf den zu steuernden

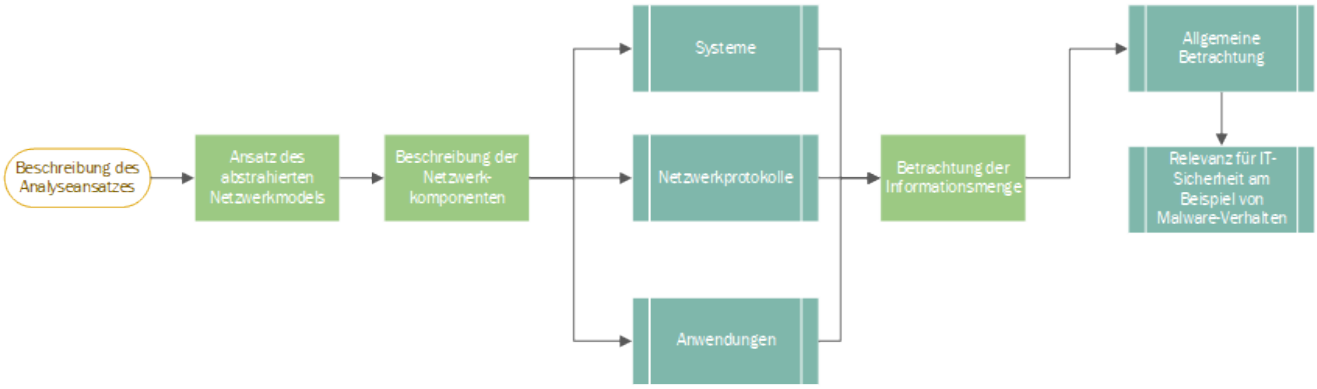

Abbildung 4.1: Analysestruktur (Placeholder)

Prozess der Fokus der Beschreibungen basierend auf der betrachteten Komponente angepasst.

Darauf folgend werden die betrachteten Angriffsszenarien beschrieben und die Informationsquellen der Komponenten für das jeweilige Angriffsszenario bewertet. Zu diesem Zweck wird beschrieben, welche Informationen pro Schritt des Angriffsszenarios als potentielle Indikatoren dienen könnten und ein Abgleich mit der kategorischen Verfügbarkeit der Daten, aus denen diese Informationen gewonnen werden können.

4.1 Beschreibung der Unternehmensarchitektur (Beispiel)

Das verwendete Modell dient dem Zweck der Darstellung des Pfades vom Leitsystem (inklusive eines SCADA Systems) zu den Elemente der Feldebene (SPS und Aktoren/Sensoren). Das Leitsystem wird mit einem Industriellen PCs in der Funktion eines Servers für die Datenabfrage aus der Feldebene verbunden. Das verwendete SCADA System wird das Siemens WinCC System verwendet. Für die Kommunikation zwischen Server und der Kontrolleinheit des Prozesschrittes (SPS) wird das Industrial Ethernet Protokoll PROFINET eingesetzt. Für die Kommunikation mit einem Sensor und zugehörigen Aktor wird das Feldbussystem PROFIBUS verwendet. Als SPS wird eine Siemens S7 eingesetzt.

4.1.1 Systeme

SIMATIC S7-1200 (SPS)

Die SIMATIC S7-1200 wird als Beispiel für eine gebräuchliche SPS herangezogen. Wie im Grundlagenkapitel bereits erläutert, wird die Funktionsweise der SPS durch die Firmware für die unterliegenden Funktionen des Ansprechens der Baugruppen und der Zentralen Einheit (CPU) und das Anwenderprogramm bestimmt. Basierend auf diesem Zustand ist es nicht möglich eine allgemeine Aussage darüber zu treffen, welche Daten grundsätzlich protokolliert und verfügbar gemacht werden können. Aus diesem Grund widment sich diese Beschreibung genauer den verfügbaren Befehlen und Optionen der SPS und der SPS-Programmierung um eine Abschätzung der verfügbaren Datenmenge und Art der Daten vorzunehmen.

Grundlegend besteht die S7-1200 aus den folgenden Baugruppen:

- Zentralbaugruppe (CPU): Ausführung des Anwenderprogrammes
- Signalbaugruppen: Schnittstellen zu den Aktoren und Sensoren
- Kommunikationsbaugruppen: Erweiterung der SPS um weitere Kommunikationsschnittstellen
- Technologiebaugruppen: Erweiterung der SPS um spezielle Funktionen (z.B. das Messen von Energiedaten)

Basierend auf dieser Auflistung wird für eine gemeinsame Grundmenge im Folgenden auf die Zentralbaugruppe eingegangen. //

Grundlegend werden für die Programmierung einer SPS Programmbausteine verwendet. Diese dienen dem Zweck der Steuerung und Ausführung des Anwenderprogrammes. Grundsätzlich wird zwischen den folgenden Bausteinen unterschieden:

- Organisationsbausteine (OBs): Diese Bausteine legen die Struktur des Programmes fest und fungieren für den Aufruf und die Ausführung bestimmter Unterprogramme und Alarme
- Funktionsbausteine (FBs) und Funktionen (FCs): Funktionen werden etwa durch die CPU bereitgestellt. Sowohl FBs als auch FCs enthalten ausführbaren Programmcode, der für die Ausführung einer bestimmten Aktion und die Definition von E/A-Parametern im Umgang mit bestimmten Modulen genutzt wird.

- Datenbausteine (DBs): Datenbausteine werden für die temporäre Speicherung von Daten (z.B. Rechnungsergebnissen) verwendet. DBs können auf verschiedenen Ebenen eingesetzt werden, wodurch der Zugriff auf die Daten durch andere Funktionsbausteine oder Programme möglich wird.

Diese Bausteine werden relevant u.a. im Bezug auf die Interaktion mit den Betriebszuständen der CPU. Die Steuerung der Programmausführung durch die OBs umfasst u.a. die folgenden Bereiche: Strukturierung des Programmzykluses, Strukturierung des Anlaufes, Strukturierung des Aufrufes von Alarmen (Weckalarm, Prozessalarm, Zeitfehler und Diagnosefehler). Dies ist u.a. deshalb relevant, weil Fehlerereignisse in den Diagnosepuffer eingetragen und über eine Schnittstelle abgerufen werden können. //

Für die CPU sind die folgenden Betriebszustände definiert:

- STOP: Programm wird nicht ausgeführt, Laden eines neuen Programmes ist hier möglich
- STARTUP: Einmalige Ausführung von OBs, die für den Anlauf des Programmes notwendig sind
- RUN: Ausführung des Programmes in einem sich wiederholenden Zyklus

Basierend auf diesen Zuständen kann die Ausführung eines Anwenderprogrammes gesteuert werden. Treten Fehler auf, können diese Ereignisse u.a. in den Diagnosepuffer geschrieben werden. Ein Diagnoseereignis werd durch Datum, Uhrzeit, Kategorie und Beschreibung des Ereignis beschrieben. Ereigniskategorien sind etwa Systemereignisse, die durch Diagnosefunktionen ermittelt werden, CPU-Fehler und Modulfehler. Zudem wird jede Änderung des Betriebszustandes protokolliert. Der Diagnosepuffer speichert die neuesten fünfzig Ereignisse. //

Für die Parametrisierung und den Zugriff auf Daten ist es essentiell den Datenspeicher und seine Bereiche zu betrachten. Für den Zugriff auf bestimmte Daten ermöglicht die Programmierumgebung für die Steuerungslogik, „STEP7“, das Binden von Datenadressen an symbolische Namen, äquivalent zu Variablen in höheren Programmiersprachen. Der Speicher wird unterteilt in die folgenden Bereiche:

- E: und A: - Prozessabbild der Eingänge und Ausgänge
- M: Merker (Elemente, die für das temporäre Speichern von Zwischenergebnissen genutzt werden)
- DB: Zugriff auf einen Datenbaustein

Bzgl. des Zugriffes auf die Ein- und Ausgänge ist es zudem möglich direkt auf die physischen Eingänge und Ausgänge zuzugreifen. Das Schreiben von Daten ist jedoch nur für die Ausgänge möglich, da die Eingänge direkt mit den Sensoren und Aktoren verbunden sind und die enthaltenen Zustände dementsprechend nicht überschrieben werden dürfen. //

Informationen und Ereignisse Im Folgenden wird basierend auf den verfügbaren Anweisungsmöglichkeiten und Funktionen eine Auflistung der potentiellen Daten vorgenommen. Für diese Arbeit wurden die folgenden Kategorien definiert:

- Potentielle Systemereignisse basierend auf Änderungen der Systemkonfiguration
- Fehlerereignisse basierend auf Funktionalitäten
- Fehlerereignisse basierend auf Kommunikationsaktivitäten

Eine Auswahl an potentiell wichtigen Informationen wird in der folgenden Tabelle dargestellt. Die Limitierung durch die maximale Größe des Anwendungsprogrammes und des Speichers wird in diesem Abschnitt noch nicht berücksichtigt.
Tabelle erstellen und Listen ersetzen

- Kommunikation:
  - PROFINET / PROFIBUS Analysefunktionen
    - Verbindungsinformationen (MAC-Adresse, IP-Adresse oder Busadresse, Spezifikationen des Gerätes)
    - Auslesen der Diagnoseinformationen mit GET_ DIAG
    - Abrufen der Betriebszustände von Peripheriegeräten oder Modulen
    - Abrufen von LED-Zuständen
  - Fehler bei Zugriffen auf die Peripherie
- System:
  - Änderung der System- oder Lokalzeiten
  - Weck- und Verzögerungsalarme (Auslöser für die Ausführung eines Programmteils)
  - (De-)Aktivierung von Unterprogrammen (durch Fehlerereignisse von Alarm-OBs)
  - Ziehen / Stecken-Ereignisse beim Entfernen / Hinzufügen von Baugruppen

  - Fehler bei Baugruppenträgern
  - Gemeinsame Fehlercodes für erweiterte Anwendungen bzgl. E/A-Ereignissen und Zugriffe auf DBs
- Funktionalitäten:
  - Diagnosefehler
  - Ereignisse bzgl. des Zugriffsschutz der CPU und bestimmter Bausteine

Basierend auf diesem Ausschnitt wird das Potential der Verfolgung von funktionalen Fehlern im Prozess sowie bei der Prozessausführung dargestellt. Ein besonderes Augenmerk soll desweiteren auf die Möglichkeit der Datenprotokollierung gelegt werden.

Die S7-1200 und andere Siemens SPSen unterstützen die Erstellung von Protokolldateien im CSV-Datenformat. Für die Einträge von Daten in diese Protokolldateien werden verschiedene Funktionen für die Erstellung, Schreiben und Schließung dieser Dateien bereitgestellt. Jede Protokolldatei kann maximal 256 Einträge speichern. Über interne Ereignisse lässt sich der Zustand und die Erstellung und Schließung der Dateien kontrollieren. Dabei können mehrere Protokolldateien, maximal jedoch acht verschiedenen Dateien, gleichzeitig geöffnet sein. Die Gesamtmenge an Protokolldateien wird durch die Größe des Ladespeichers bzw. einer hinzugefügten Speicherkarte definiert. Die Gesamtmenge darf maximal 25% des Speichers einnehmen (basierend auf der Größe des Ladespeichers 250-500 KByte / Speicherkarte bis zu 6 MByte). Der Zugriff auf die Log-Dateien kann entweder über die Aktivierung des Webservers oder den direkten Zugriff auf Log-Dateien über einen Webbrowser („http://<IP-Adresse>/DataLog.html?FileName=<Name der Protokolldatei>“) erfolgen, sofern eine geeignete Verbindung (z.B. über PROFINET) vorhanden ist. Protokolldateien werden im Ladespeicher oder auf einer Speicherkarte abgelegt, dürfen jedoch maximal 25% der Speicherka

4.1.2 Kommunikationsmedien

PROFIBUS

PROFIBUS ist ein serielles Feldbussystem, welches u.a. in der Fertigungs-, Prozess- und Gebäudeautomatisierung verwendet wird. Es ermöglicht die zeitkritische, deterministische Kommunikation von Steuer- und Peripheriegeräten (Aktoren und Sensoren) sowie HMIs und anderen Elementen. Das Kommunikationsprinzip basiert auf dem Multi-Master-Prinzip. Dies soll den gemeinsamen Betrieb mehrerer Systeme für

den Zweck der Automatisierung, des Engineerings oder der Visualisierung der Anlage, mit den verteilten Pheripheriegeräten der Anlage ermöglichen. Zu diesem Zweck werden die Kommunikationsteilnehmer in zwei Gerätearten unterteilt: Master- und Slave-Geräte. Master-Geräte bestimmten die Kommunikation und senden auf dem Feldbus, wenn sie im Besitz des Tokens sind, welches das Zugriffsrechte auf den Datenbus darstellt. Slave-Geräte hingegen können lediglich empfangene Nachrichten bestätigen oder auf Anfrage des Master-Gerätes Daten senden.

Für die Zuweisung der Buszugriffsrechte wird das Fieldbus Data Link (FDL) Protokoll verwendet. Dieses verbindungslose, Layer-2-Protokoll bestimmt zu welchem Zeitpunkt ein bestimmter, aktiver Kommunikationsteilnehmer (Master) das Recht erhält Daten zu senden. Die dadurch etablierte Buszugriffskontrolle (MAC, Medium Access Control) führt die folgenden Aufgaben aus:

- Etablierung des Token-Rings während des Hochfahrens des Systems
- Hinzufügen/Entfernen von Teilnehmern
- Kontrolle der Weitergabe des Tokens

Der Token-Ring wird durch aufsteigende Busadressen der Master-Geräte realisiert. Die Tokeninformationen werden durch ein spezielles Telegram weitergegeben. Abhängig von der Definition und Größe des Systems muss das Token in einer maximalen Token-Umlaufzeit einmal an jeden aktiven Kommunikationsteilnehmer weitergesendet werden. Dieses Verfahren ermöglicht die Erstellung von Master-Slave-, Master-Master- und Misch-Kommunikationsformen. Die Adressierung wird durch einen Byte-Wert zwischen 0 und 127 kodiert. Dabei werden bestimmte Bereiche für etwa Programmiergeräte, Slaves und Master bestimmt.

Desweiteren wird durch eine Unterscheidung der verschickten Telegramme (Nachrichten) eine logische Datensicherung etabliert. Diese wird durch bestimmte Start- und Endzeichen sowie Paritätsbits und Kontrollbytes hergestellt.

Für die PROFIBUS-Protokolle der Anwendungsebene (DP-Varianten) werden Telegramtypen bereitgestellt:

- Keine Daten (SD1)
- Daten variabler Länge (SD2)
- Daten fester Länge (SD3)
- Token (SD4)
- Kurzquittung (SC)

Zusätzlich zu der FDL-Funktionalität existieren die Fieldbus Management (FMA) Dienste für die Verwaltung der Schichten 1 (Übertragungstechnik) und 2 (FDL). Diese Dienste können unterteilt werden in lokale Dienste (bzgl. der Station) und stationsübergreifende Dienste. Zu den lokalen Diensten zählen „Reset“, „Set Value“, „Read Value“, „(R)SEP (De-)Activate“und „Event“. Event ist ein Dienst, der Anwender über Ereignisse oder Fehler in den Schichten 1 und 2 informieren kann. Zu diesen Events zählen:

- Duplicate adress (Master)
- Faulty transceiver (Master)
- Time_ put (Master / Slave)
- Not_ syn (Master / Slave)
- Out_ of_ ring (Master
- GAP_ event (Master)

Zu den stationsübergreifenden Diensten zählen „Ident (Versionsdaten von Hardware und Software)“, „LSAP Status (Informationen zu einem SAP)“und „Live-List (Liste aller erreichbaren Teilnehmer)“

PROFIBUS DP dient als Protokoll für den zyklischen Datenaustausch zwischen einer Kontrolleinheit (SPS) und Peripheriegeräten. Bei der Verwendung von DP wird zwischen drei Gerätetypen unterschieden:

- DP-Master 1 (DPM1): Dieser Kommunikationsteilnehmer regelt den zyklischen Datenaustausch (typischerweise SPS oder PC)
- DP-Master 2 (DPM2): Ein zusätzliches Gerät, etwa für Bedienungs- oder Engineering-Zwecke, die Kommunikation erfolgt azyklisch
- Slave: Pheripheriegeräte (Aktoren/Sensoren)

PROFIBUS DP unterstützt Mono- und Multi-Mastersysteme. Ein Multi-Mastersystem besteht aus verschiedenen Subsystemen (Mono-Master, d.h. DPM1 mit mehreren Slaves) und weiteren DPM2-Geräten. Die Kommunikation wird mit Hilfe des FDL Protokolls geregelt.

Das Verhalten eines (Sub-)Systems hängt von dem Betriebszustand des DPM1 ab. Es wird zwischen den folgenden Betriebszuständen unterschieden:

- Stop: Kein Datenverkehr zwischen DPM1 und Slaves

- Clear: DPM1 liest Eingangsinformationen der Slaves und schaltet die Ausgänge in einen sicheren Zustand
- Operate: Zyklische Kommunikation zwischen DPM1 und Slaves (Datentransferphase)

Bei der zyklischen Kommunikation im „Operate“-Zustand sendet (schreibt) der Master per Aufruf-Telegramm Ausgangsdaten an den jeweiligen Slave und empfängt (liest) die Eingangsdaten des Slaves. Dieser Vorgang wiederholt sich in dieser Reihenfolge konsequent. Wird ein neuer Slave in das System eingefügt werden drei Phasen durchlaufen: Parametriesierungs-, Konfigurations- und Datentransferphase. Die ersteren Phasen dienen einem Ist-Soll-Abgleich zwischen DPM1 und Slave bei dem der DPM1 Gerätetyp, Format- und Längeninformationen sowie die Anzahl der Ein- und Ausgänge prüft. Nach erfolgreicher Prüfung geht die Kommunikation in die Datentransferphase über.

Neben dem Datenaustauschen zwischen einem DPM1 und einem einzelnen Slave besteht auch die Möglichkeit eines Multicasts bei dem Steuerungsbefehle an einen, eine Gruppe oder alle Slaves des von dem DPM1 verwalteten System gesendet werden können. Diese Funktionalität ermöglicht die Betriebsarten Sync und Freeze. Bei der Sync-Betriebsart werden zunächst die Ausgangszustände der Slaves eingefroren, d.h. sie können nicht mehr verändert werden. Darauf werden Ausgangsdaten vom DPM1 auf dem Slave gespeichert, die Zustände jedoch nicht verändert. Durch einen erneuten Sync-Befehl werden die Zustände überschrieben. Ein Unsync-Befehl beendet den Sync-Betrieb. Bei der Freeze-Betriebsart werden die Eingangszustände der Slaves eingefroren. Die Eingangszustände werden aktualisiert, sobald ein weiterer Freeze-Befehl gesendet wurde. Analog zu Sync wird der Freeze-Betrieb durch den Unfreeze-Befehl beendet.

Für den Schutz gegen Fehlparametrisierung, d.h. falscher Setzung der Operationsparameter, und Ausfall des Übertragungsmedium werden für DP-Master als auch DP-Slaves „Data_ Control_ Timer“ausgelöst sobald innerhalb eines festgelegten Zeitintervalls keine ordnungsgemäße Kommunikation stattgefunden hat. Im Fall des DP-Masters kann zu diesem Zweck der Parameter „Auto-Clear“aktiviert (True) sein. In diesem Falle werden die Ausgänge aller Slaves in einen sicheren Zustand geschaltet und daraufhin der Clear-Betriebszustand eingenommen.

PROFIBUS DP kann durch PROFIBUS DPV1 erweitert werden. DPV1 dient der azyklischen Kommunikation und ermöglicht die Kommunikation von DPM2-Geräten und Slaves. Die azyklische Kommunikation dient der Übertragung von Bedarfsdaten. Bedarfsdaten sind Parameter (z.B. Grenzwerte) oder Optionen (z.B.

Fehlerlisten), die von den Slaves abgerufen werden können. Zu diesem Zweck erweitert DPV1 DP um die folgenden Dienste: „Read“und „Write“.

PROFIBUS Frage: Unterschiede zwischen Informationsmengen DP vs DPV1 bzgl. Status und Alarmmeldungen?

Die azyklische Kommunikation wird parallel zur zyklischen Kommunikation durchgeführt. Der Ablauf kann am Beispiel Read demonstriert werden:

- (Für DPM2: Aufbau einer C2-Verbindung)
- DP-Master sendet den Aufruf an den DP-Slave
- Der DP-Slave bestätigt den Erhalt der Anfrage und beginnt die interne Bereitstellung der Daten (Quittierung)
- DP-Master führt zyklische Prozesskommunikation durch
- Wiederholend:
  - DP-Master sendet Poll-Request
    - Daten stehen noch nicht bereit? DP-Slave quittiert Poll-Request
    - Daten stehen bereit: DP-Slave sendet Daten an Stelle der Quittierung

Die aufgerufenen Betriebsdaten werden über den das Modul (SSlot") und den jeweiligen Parameter (Ïndex") definiert. Soll nur ein Teilwert des Parameters gelesen werden kann über die Länge ("Length") dies definiert werden. Die Indexnummern und Datentypen werden in PROFIBUS Profilen festgelegt.

Da die Leistungsmerkmale der Geräte, d.h. Busparameter und Funktionalitäten (z.B. Anzahl der E/A-Signale und Diagnosemeldungen), abhängig von Gerätetyp und Hersteller unterschiedlich sind, werden GSD-Dateien für die Definition dieser Elemente verwendet. Eine GSD-Datei stellt dabei eine Art elektronische Gerätedatenblatt da und kann während der Konfiguration, z.B. durch ein Projektierungswerkzeug, eingelesen werden. Die GSD-Dateien sind in drei Abschnitte eingeteilt:

1. Allgemeine Festlegungen
2. Master-bezogene Festlegungen
3. Slave-bezogene Festlegungen

Zudem muss in der GSD-Datei eine Identnummer vermerkt sein. Diese Identnummer muss bei der PROFIBUS-Nutzerorganisation beantragt werden und dient der schnellen Identifzierung eines angeschlossenen Gerätetyps durch einen DP-Master.

In der Erweiterung PROFIBUS DPV2 wird die Uhrensynchronisierung durch den DPM1 und isochrone Kommunikation hinzugefügt. Zum Zweck der Uhrensychronisation wurde der Gerätetyp DP-Master 3 (Uhrenmaster) eingefügt.

PROFINET

Profinet ist ein offener Industrial-Ethernet-Standard für die Integration von IT-Systemen in den Automatisierungsprozess auf Basis von TCP/IP.

Wie bei PROFIBUS werden Kommunikationsteilnehmer in einem Profinet-IO-System in verschiedene Gerätekategorien eingeteilt: IO-Controller (typischerweise eine SPS), IO-Device (Gerät der Feldebene) und IO-Supervisor (Programmiergerät, PC, HMI oder anderes zusätzliches Werkzeug (etwa für Engineering-Zwecke)). Der IO-Supervisor entspricht dem PROFIBUS DP-Master 2.

Zusätzlich werden wie bei PROFIBUS Geräte- bzw. Anwendungsprofile in Form von GSDML-Dateien verwendet. Diese werden durch den Hersteller erstellt und beschreiben Eigenschaften, Leistungsmerkmale und Verhaltensweise der Geräte. Dabei wird zwischen allgemeinen Anwendungsprofilen mit verschiedenen Einsatzmöglichkeiten und spezifischen Anwendungsprofilen unterschieden.

Geräte der Feldebene werden durch ihr Gerätemodell beschrieben, welches die technischen und funktionellen Möglichkeiten beschreibt. Das Gerätemodell wird definiert durch den Zugriffspunkt (Device Access Point (DAP)) und die für eine bestimmte Gerätefamilie definierten Module (Baugruppen über die die Kommunikation der Prozessdaten abläuft). Der DAP dient als Schnittstelle für die Ethernet-Kommunikation und Verarbeitungsprogramme. Die Module erlauben die Adressierung der E/A-Daten über die Parameter Slot (Steckplatz/Baugruppe), Subslot (Prozess-Schnittstelle, definiert durch den Hersteller), den Index (gibt den Parameter an) sowie den Application Profile Identifier (API). Diese Daten werden azyklisch per Read/Write ausgelesen. Der Ausbaugrad eines Anwendungsprofils wird kategorisiert als "kompakt"(nicht-veränderbar) oder "modular". Die GSDML-Datei wird auf einer XML-Basis erstellt.

Die Kommunikationswege innerhalb eines PROFINET-Systems werde auf Basis dieser GSDML-Dateien erstellt während der Projektierung. Der Datenaustausch zwischen Kommunikationsteilnehmern wird innerhalb einer Application Relation (AR) durchgeführt, die verschiedene Communication Relations (CRs) spezifiziert:

- Recorded Data CR: Standardkanal für Konfigurationsdaten
- IO Data CR: Kanal für die zyklische Übertragung von Echtzeitdaten
- Alarm CR: Kanal für Alarme und Fehlermeldungen

Sollen mehrere IO-Controller auf die gleichen Daten eines IO-Device zugreifen, muss dieses während der Projektierung angegeben werden. Jeder IO-Controller kann genau eine AR zu einem bestimmten IO-Device aufbauen. Jedes Feldgerät erhält zudem einen symbolischen Namen als Identifier, welcher als Schlüssel für die Zuordnung von MAC- und IP-Adresse verwendet wird. Die Zuordnung dieses Namens kann über das „Discovery and basic Configuration (DCP)“Protokoll, alternativ aber auch über die Topologie und Nachbarschaft zu einem bestimmten IO-Controller, durchgeführt werden. Die Zuweisung der IP-Adresse wird per DHCP oder einen hersteller-spezfischen Mechanismus durchgeführt. Die verwendbaren Möglichkeiten sind innerhalb der GSDML-Datei definiert.

Für die Adressierung innerhalb des PROFINET-Systems werden eindeutige 48-Bit-MAC-Adressen verwendet. Die MAC-Adresse wird zusammengesetzt aus der FIrmenkennung und einer Organization Unit ID (OUI), welche gegen eine Gebühr von IEEE-Departments vergeben werden.

Der Funktionsumfang von Profinet ist flexibel anpassbar abhängig von der notwendigen Funktionalität. Für eine Differenzierung der Funktionalitäten teilt man Profinet in die folgenden Konformitätsklassen ein:

- CC-A: Grundfunktionen
- CC-B: CC-A wird um Netzwerkdiagnose und Topologieinformationen erweitert
- CC-B(PA (Process Automization)): CC-B wird um Systemredundanzen erweitert
- CC-C: Basisfunktionen für Geräte und hardwareunterstützte Bandbreitenreserver für isochrone Echtzeitkommunikation (Basis für taktsynchrone Anwendungen)

Grundfunktionen

Die Grundfunktionen umfassen den zyklischen Austausch von E/A-Daten mit Echtzeiteigenschaften sowie azyklische Kommunikation (Read/Write) von bedarfsorientierten Daten (Parameter, Diagnose) sowie Identifizierungs- und Verwaltungsfunktionen (Identification and Maintenance (I& M)) und eine Alarmfunktionalität für die Signalisierung von Geräte- und Kommunikationsfehlern.

Der zyklische Datenaustausch wird über eine IO Daten CR auf Layer 2 des OSI-Modells in einem Zeitfenster zwischen 250 μs und 512ms durchgeführt. Die gesendeten Daten werden durch den Empfänger nicht bestätigt. Die Telegramme enthalten neben den Prozessdaten weitere Informationenen für die Bestätigung der Gültigkeit

der Daten, Redundanz- und diagnosedaten sowie Informationen über den Taktzyklus des Providers. Wie auch bei PROFIBUS werden die Zeitintervalle zwischen den Kommunikation überwacht und Mechanismen ausgelöst, falls der Zeitabstand überschritten werden sollte.

Der azyklische Datenaustausch wird über die Record Data CR auf Basis von TCP/IP durchgeführt. Die Read/Write-Frames werden verwendet um Diagnose- und Identifzierungsinformationen über das Netzwerk und die Kommunikationsteilnehmer abzurufen. Die Diagnosedaten enthalten u.a. mehrstufige Alarmereignisse. Das Zustandsmodell unterscheidet zwischen den Kategorien „gut“, „Wartungsbedarf (etwa bei einem Ausfall der Medienredundanz-Funktionalität)“, „Wartungsanforderung“und „fehlerhaft“. Zudem wird zwischen Diagnosealarmen und Prozessalarmen unterschiedene. Diagnosealarme umfassen Fehler oder Ereignisse, wie etwa das Abziehen oder Aufstecken einer Baugruppe, innerhalb des IO-Devices und im Bezug auf zusammenhängende Komponenten. Prozesslarame werden durch den Anwender definiert und signalisieren etwa die Überschreitung eines Grenzwertes.

Netzwerkdiagnose und -verwaltung (CC-B)

Die Konformitätsklasse (CC) B erweitert PROFINET um weitere Diagnoseinformationen und Topologieinformationen. Diese Informationen werden durch die Erweiterung des Link Layer Discovery Protocols (LLDP-MIB EXT) und innerhalb einer Management Information Base (MIB) gesichert. Die Informationen sind abrufbar über die Verwendung des Netzwerkprotokolls SNMP oder die Verwendung azyklischer Profinet-Dienste.

Die Erweiterung um Informationen um die Topologie des Netzwerkes wird durch die Nachbarschaftserkennung ermöglicht. Durch diese Erweiterung tauschen Profinet-Feldgeräte über LLDP vorhandene Adressierungs-Informationen aus, wodurch der phyikalische Aufbau auf Basis der Port-Nachbarn erschlossen wird. Diese Funktionalität ermöglicht einen Soll-Ist-Vergleich der Topologie sowie die Prüfung des korrekten Anschlusses für den Falls des Austausches eines Gerätes mithilfe eines Software-Werkzeuges.

Für die Verwendung dieser Erweiterung müssen die Switche als IO-Device eingesetzt werden können um die Übertragung der Alarme über die Alarm CR zu ermöglichen.

Synchrone Echtzeit (CC-C)

Um Profinet für zeitkritische, deterministische Kommunikation nutzen zu können müssen weitere Funktionalitäten hinzugefügt werden. Dies umfasst eine netzwerk-

weite Synchronisierungsfunktion und zeitliche Übertragungsschwankungen („Jitter“) von weniger als 1 ms. Zu diesem Zweck wird eine definierte Bandbreite für das Übertragen dieser Daten reserviert, während die restliche Bandbreite für den restlichen Datenverkehr genutzt wird. Die synchrone Kommunikation erfordert, dass alle Kommunikationsteilnehmer den gleichen Takt verwenden. Dies wird über einen Clock-Master für alle lokalen Taktgeneratoren innerhalb des Taktystems (IRT Domäne) umgesetzt. Zwischen den beteiligten Geräten dürfen keine nicht-synchronen Geräte verwendet werden. Um die Schnelligkeit der Übertragung zu verbessern können verschiedene, zusätzliche Mechanismen verwendet werden (Fragmentierung in kleinere TCP/IP-Pakete sowie Dynamic Frame Packing (DFP)).

4.2 Applikationen

4.2.1 WinCC (SCADA / HMI)

Als Beispiel für das SCADA-System wird in diesem Modell das System "WinCC"von Siemens verwendet. WinCC ist ein pc-basiertes System, das sowohl als eigenständiges SCADA-System als auch als HMI für Prozessleitsysteme eingesetzt werden kann. WinCC wird auf einer modernen Version des Betriebssystem Windows (z.B. Windows 7, 8.1 oder 10 sowie Windows Server 2008 oder 2016). Mit Hilfe dieses Systems ist es möglich die Durchführung und Überwachung eines Fertigungsprozesses durchzuführen. Dies beinhaltet im Kern die folgenden Funktionalitäten:

- Meldung und Bestätigung von Ereignissen innerhalb des Fertigungsprozesses
- Archivierung von Meldungen und Messwerten
- Protokollierung von Prozessdaten und Daten, die für die Konfiguration von Geräten im Fertigungsprozess, gesendet und empfangen werden
- Grafische Darstellung des überwachten Netzwerkes

Hinzu kommen Elemente wie etwa eine Benutzerverwaltung für den geregelten Zugriff auf das System.

Im Bezug auf die für diese Arbeit relevante Informationsmenge ist die Protokollierung und Überwachung des Systems und des Netzwerkes interessant. Da das Betriebssystem bereits im vorherigen Kapitel ausführlich beschrieben wurde, wird im Folgenden das System „WinCC“selbst betrachtet und die potentiellen Quellen für Informationen bzgl. des Systems selbst. Da das SCADA-System Prozessdaten und definierte Bedarfsdaten, also Parameterdaten auf den Elementen, und damit

der Elemente des Netzwerkes empfängt und Daten sendet, werden außerdem die Schnittstellen für das Senden und Empfangen der Daten betrachtet.

Für WinCC lassen sich diese Elemente im Groben in die folgenden Elemente des Systems einteilen: Tags, Nachrichten und Alarm Logging

In WinCC werden „Tags“als Elemente benutzt um Daten eines Projektes zu lesen, zu schreiben oder weiterzuleiten. Jeder Tag wird mit einer Datenadresse, einem symbolischen Namen und einem Datentyp sowie weiteren Eigenschaften definiert.

Es wird zwischen Prozesstag und internen Tags unterschieden. Ein Prozesstag ist mit bestimmten Parameter eines Automatisierungssystem (z.B. einer SPS) verknüpft und definiert u.a. den Kommunikationstreiber, der die Details der Kommunikation definiert. Diese Verbindung wird genutzt um Daten auszulesen und zu schreiben. Ein interner Tag wird genutzt um innerhalb des Projektes Daten zu verwalten und dient zudem als Schnittstelle zur Archivierungsfunktion. Interne Tags, die für die Verwaltung des Projektes notwendig sind, werden Systemtags genannt.

Für die Feststellung, Darstellung und Archivierung von Fehlern wird das Nachrichtensystem (Message System) verwendet um erkannte Fehler visuell darzustellen und an das Archivierungssystem weiterzuleiten. Die Nachrichten werden in drei Teile unterteilt: Systemblocks (Datum, Zeit, Dauer,...), User Text Blocks (vor-definierte Beschreibungen) und Process Value Blocks (Tag-Werte). Zudem wird jede Nachricht einem Typ zugeteilt: Operationsnachrichten (Status eines Prozesses), Fehlernachrichten (Fehler in einem Prozess) und Systemnachrichten (Fehler von anderen Anwendungen). Dokumentierte Ereignisse schließen binäre Ereignisse (Statusänderungen von Tags) sowie „Monitoring Events“(Archivfehler, Serverfehler, Fehler in der Prozesskommunikation) ein. Für die Archivierung werden Prozessdaten und Nachrichten für den Status der Operation und von Fehlern in einem Microsoft SQL Server gesichert.

4.3 Analyse im Bezug auf typische Angriffsvektoren

In Folge der Beschreibung der Elemente des zu analysierenden Modells stellt sich die Frage der Relevanz im Bezug auf die Nutzbarkeit für die Erkennung von Sicherheitsvorfällen, u.a. mit Hilfe eines SIEM-Systems. Zu diesem Zweck wird im Folgenden zunächst der Informationspool als Gesamtmenge betrachtet und daraufhin unter dem Aspekt der Analyse von Angriffsszenarien.

4.3.1 Betrachtung der Datenmenge

Die Betrachtung der ausgewählten Elemente zeigt eine Datenmenge, die sich hauptsächlich auf die Dokumentierung und Analyse des Fertigungsprozesses bezieht. Die verfügbaren Diagnosefunktionalitäten durch die genutzten Kommunikationssysteme PROFINET und PROFIBUS sowie die Diagnose und Alarmierungsfunktionalitäten der SPS und die Abfrage entsprechender Parameter-Tags, sowie die Möglichkeit der Speicherung und statistischen Analyse der Prozessdaten ermöglichen eine präzise Kontrolle des Prozesses. Basierend auf den verfügbaren Bausteinen und Parametern der SPS und der Protokollierung von Parametern besteht die Möglichkeit genau festzulegen, welche Daten wichtig für die Überwachung eines Prozessschrittes sind. IT-Sicherheitsfunktionen werden in Form von Zugriffskontrollen der Benutzerverwaltung und Passwortschutz auf wichtige Komponenten umgesetzt. Desweiteren bieten sich die bereits diskutieren Möglichkeiten für die Systemüberwachung des SCADA-Servers durch das Windows-Betriebssystem an. Die Protokollierung von SCADA-Ereignissen ist eingeschränkt möglich, eine genauere Betrachtung ist u.U. im späteren Verlauf zu untersuchen.

4.3.2 Relevanz für die Sicherheitsbetrachung mit Hilfe von SIEM-Systeme

Im Bezug auf die Verfügbarkeit sicherheitsrelevanter Informationen soll in diesem Fall wie im vorherigen Kapitel der Fokus auf der Möglichkeit einer Infektion der Systeme durch Malware liegen. Allgemein ermöglicht die Überwachung der Prozessdaten eine Informationsgrundlage, die grobe Manipulationen des Prozesses durch eine Malware erkennen lassen. Für eine Betrachtung anderer Szenarien, etwa der geringfügigen Manipulation im Rahmen von Prozessschwellwerten und Spionageszenarien, kann auf ein gut dokumentiertes Beispiel in Form des Stuxnet-Falles zurückgegriffen werden. Während der Umfang und Komplexität des Stuxnet-Angriffes die Möglichkeiten bestimmter Akteure ggf. übersteigt, kann dieses Beispiel jedoch einen guten Einblick in potentielle Angriffswege und -szenarien geben, wodurch eine Betrachtung sinnvoll wird. Aus diesem Grund erfolgt im Folgenden eine grobe Beschreibung des Vorgehens der Stuxnet Software und eine Betrachtung, welche Informationen für die Identifzierung genutzt wurden.

Stuxnet-Betrachtung und Informationen

Kapitel 5

Vergleich der Analysen

5.1 Vergleichsmetrik

5.2 Vergleich

Kapitel 6

Bewertung der Informationslücken

6.1 Bewertungsschema

6.2 Bewertung

6.3 Beschreibung existierender wissenschaftlichen Lösungsansätze

Kapitel 7

Lösungsansatz zur Schließung der fokussierten Informationslücke

7.1 Tiefergehende Beschreibung der Informationslücke und bestehende Abhängigkeiten

7.2 Beschreibung des Lösungsansatz

7.3 Beschreibung des Versuchsaufbaus des Beweises

7.4 Beschreibung der Ergebnisse

Kapitel 8

Fazit

Literaturverzeichnis

[1] admin. Was ist der unterschied zwischen scada und hmi? "http://www.indusoft.com/blog/2013/04/19/unterschied-zwischen-scada-und-hmi", 2013. Last visited on 20. May. 2018.

[2] S. Bhatt, P. K. Manadhata, and L. Zomlot. The operational role of security information and event management systems. *IEEE Security Privacy*, 12(5): 35–41, Sept 2014. ISSN 1540-7993.

[3] Tony Campbell. *Protection of Systems*, pages 155–177. Apress, Berkeley, CA, 2016. URL https://doi.org/10.1007/978-1-4842-1685-9_10.

[4] Conrad Constantine. What kind of logs do you need for an effective siem implementation? "https://www.alienvault.com/blogs/security-essentials/what-kind-of-logs-for-effective-siem-implementation", 2014. last visited on 20. Mai. 2018.

[5] Jeff Edwards. 7 siem and security analytics vendors to watch in 2017. "https://solutionsreview.com/security-information-event-management/7-siem-and-security-analytics-vendors-to-watch-in-2017", 2016. Last visited on 20. May. 2018.

[6] Feldbusse.de. Industrial ethernet - status und ausblick. "http://www.feldbusse.de/trends/status-ethernet.shtml", N/A. Last visited on 20. May. 2018.

[7] Feldbusse.de. Vergleich der industrial-ethernet-systeme. "http://www.feldbusse.de/Vergleich/vergleich_ethernet.shtml", N/A. Last visited on 20. May. 2018.

[8] Bundesamt für Sicherheit in der Informationstechnik. Industrial control system security - top 10 bedrohungen und gegenmaßnahmen 2016. "https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_005.pdf?__blob=publicationFile", 2016. Last visited on 20. May. 2018.

[9] Bundesministerium für Wirtschaft und Energie. Was ist industrie 4.0? "https://www.plattform-i40.de/I40/Navigation/DE/Industrie40/WasIndustrie40/was-ist-industrie-40.html", 2018. Last visited on 20. May. 2018.

[10] Jürgen Gutekunst. *Schnittstellen, Bussysteme und Netze*, pages 687–744. Springer Berlin Heidelberg, Berlin, Heidelberg, 2017. URL https://doi.org/10.1007/978-3-662-54214-9_15.

[11] Rainer Hönle. *Speicherprogrammierbare Steuerungen*, pages 745–792. Springer Berlin Heidelberg, Berlin, Heidelberg, 2017. ISBN 978-3-662-54214-9. URL https://doi.org/10.1007/978-3-662-54214-9_16.

[12] IPC2U. Hmi. "https://ipc2u.de/catalog/automatisierungstechnik/hmi/", N/A. Last visited on 20. May. 2018.

[13] ITWissen.info. Scada (supervisory control and data acquisition). "https://www.itwissen.info/SCADA-supervisory-control-and-data-acquisition-SCADA-Protokoll.html", N/A. Last visited on 20. May. 2018.

[14] D. Jayathilake. Towards structured log analysis. In *2012 Ninth International Conference on Computer Science and Software Engineering (JCSSE)*, pages 259–264, May 2012.

[15] Wootae Jeong. *Sensors and Sensor Networks*, pages 333–348. Springer Berlin Heidelberg, Berlin, Heidelberg, 2009. ISBN 978-3-540-78831-7. URL https://doi.org/10.1007/978-3-540-78831-7_20.

[16] Heinrich Kersten, Gerhard Klett, Jürgen Reuter, and Klaus-Werner Schröder. *Risikomanagement*, pages 39–62. 09 2016. ISBN 978-3-658-14693-1.

[17] Elektronik Kompendium. Iso/osi-7-schichtenmodell. "https://www.elektronik-kompendium.de/sites/kom/0301201.htm", N/A. Last visited on 20. May. 2018.

[18] M. Krotofil and D. Gollmann. Industrial control systems security: What is happening? In *2013 11th IEEE International Conference on Industrial Informatics (INDIN)*, pages 670–675, July 2013.

[19] Marc M. Lankhorst. *Introduction to Enterprise Architecture*, pages 1–10. Springer Berlin Heidelberg, Berlin, Heidelberg, 2017. ISBN 978-3-662-53933-0. doi:

10.1007/978-3-662-53933-0_1. URL https://doi.org/10.1007/978-3-662-53933-0_1.

[20] Stephen Lawton. A guide to security information and event management. "http://www.tomsitpro.com/articles/siem-solutions-guide,2-864-2.html", 2015. Last visited on 20. May. 2018.

[21] Petra Linke. *Grundlagen zur Automatisierung*, pages 1–28. Springer Fachmedien Wiesbaden, Wiesbaden, 2017. ISBN 978-3-658-17582-5. URL https://doi.org/10.1007/978-3-658-17582-5_1.

[22] Raffael Marty. Event processing – normalization. "http://raffy.ch/blog/2007/08/25/event-processing-normalization", 2007. Last visited on 20. May. 2018.

[23] McAffee. Mcafee siem event aggregation. "https://community.mcafee.com/nysyc36988/attachments/nysyc36988/business-documents/457/1/SIEM-Aggregation-AW.pdf", 2016. Last visited on 20. May. 2018.

[24] Alberto Partida and Diego Andina. *Vulnerabilities, Threats and Risks in IT*, pages 1–21. Springer Netherlands, Dordrecht, 2010. ISBN 978-90-481-8882-6. URL https://doi.org/10.1007/978-90-481-8882-6_1.

[25] Carlos E. Pereira and Peter Neumann. *Industrial Communication Protocols*, pages 981–999. Springer Berlin Heidelberg, Berlin, Heidelberg, 2009. ISBN 978-3-540-78831-7. URL https://doi.org/10.1007/978-3-540-78831-7_56.

[26] Karen Scarfone. Comparing the best siem systems on the market. "http://searchsecurity.techtarget.com/feature/Comparing-the-best-SIEM-systems-on-the-market", 2015. Last visited on 20. May. 2018.

[27] Karen Scarfone. Comparung the best siem systems on the market. "http://searchsecurity.techtarget.com/feature/Comparing-the-best-SIEM-systems-on-the-market", 2015. Last visited on 20. May. 2018.

[28] The Barking Seal. Understanding dns: Essential knowledge for all it professionals. "https://www.appliedtrust.com/resources/infrastructure/understanding-dns-essential-knowledge-for-all-it-professionals", 2009. Last visited on 20. May. 2018.

[29] Siemens. Basic hmi. "http://w3.siemens.com/mcms/human-machine-interface/de/bediengeraete/basic-hmi/Seiten/Default.aspx", N/A. Last visited on 20. May. 2018.

[30] SoftSelect. Definition mes - manufacturing execution system. "http://www.softselect.de/business-software-glossar/mes-manufacturing-execution-system", N/A. Last visited on 20. May. 2018.

[31] Mark Stingley. Infrastructure security architecture for effective security monitoring. "https://www.sans.org/reading-room/whitepapers/bestprac/infrastructure-security-architecture-effective-security-monitoring-36512", 2015. Last visited on 20. May. 2018.

[32] techopedia. Attack vector. "https://www.techopedia.com/definition/15793/attack-vector", N/A. Last visited on 20. May. 2018.

[33] Alex Teixeira. Get over siem event normalization. "https://medium.com/ateixei/get-over-siem-event-normalization-595fc36559b4", 2017. Last visited on 20. May. 2018.

Abbildungsverzeichnis

2.1 Aufbau des Grundlagenkapitels 3

3.1 Analysestruktur (Placeholder) 40

4.1 Analysestruktur (Placeholder) 65