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 17. Januar 2018

Niklas Breuer

Abtract

Abstract formulieren

Todo list

Inhaltsverzeichnis

Kapitel 1

Einleitung

TODO

Kapitel 2

Grundlagen

2.1 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 nicht-authorisierten 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.

2.2 Security Information and Event Management

2.2.1 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 verschiedenen 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.

2.2.2 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 Sicherheitsanalyse 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.

2.2.3 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. 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 Netz-

werkelementen 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.

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.

2.2.4 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. 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 (Quellen einfügen, siehe Latex Kommentar).

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.

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

2.2.5 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.

2.2.6 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 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 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.

2.3 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.

2.3.1 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

2.3.2 Architekturen & Anforderungen

Unternehmen können in verschiedener Art und Weise in einer Architektur strukturiert sein, die auf das entsprechende Firmenmodell angepasst sind. Ein grundlegender Aufbau kann z.B. so aussehen:

Bild für typische Enterprise Network Architecture einfügen

Zunächst besteht eine Verbindung zum Internet, 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 Sicherheitssystemen überwacht werden.

Enterprise Networks Architecture: Ausbauen - Netzwerkzonen, Beschreibung der Verschachtelung der Netzwerke, Spezifische Positionen (IDF, MDF, NOC)

2.3.3 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.

Beschreibung DNS hinzufügen

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 erfolgen. Die verschiedenen Schichten sind u.a. im OSI Layer Model festgehalten.

Enterprise Kommunikation - VPN & Remote Access beschreiben

Enterprise Kommunikation - Fehlt hier sonst noch etwas?

2.3.4 Bekannte Angriffsvektoren

Enterprise Angriffsvektoren: Allgemeine Bedrohungen formulieren

Ggf. eine Ebene tiefer gehen, Recherche falls notwendig und formulieren

Prinzipiell: - Der Mensch als Ziel - DDoS - Malware & (Spear) Phishing - Ransomware

2.4 Infrastruktur industrielle Produktionsnetzwerke

2.4.1 Geräte

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

- Speicherprogrammierbare Steuerung (SPS)
- Verteiltes Kontrollsystem
- Human-Machine Interface
- Industrial Ethernet Switch
- Computer für den verwaltenden Zugriff auf angeschlossene SPSen
- Sensor & Aktuator

Eine speicherprogrammierbare Steuerung (SPS) ist ein Kontrollelement, welches für die Kontrolle eines Prozessschrittes genutzt wird. Auf der SPS befinden sich sowohl eine Firmware als auch ein Programm. Die Firmware kontrolliert die Steuerung der SPS an sich. Das Programm wird in einen programmierbaren Speicher gelade. 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.

Ein weiteres Element eine industriellen Netzwerkes ist ein verteiltes Kontrollsystem. Ein verteiltes Kontrollsystem ist für die Koordinierung und Überwachung eines Netzwerkes aus speicherprogrammierbaren Steuerung zuständig und kann empfangene Daten u.a. an einen Leitstand weiterleiten und/oder an einem Human-Machine Interface (HMI) sichtbar machen. Das HMI dient den Mitarbeitern für die Kontrolle eines Prozesses und die Zustände der ausführenden Elemente.

Für die Kommunikation über die Industrial Ethernet Schnittstelle existieren Industrial Ethernet Switches. Diese leiten den Datenpakete wie gewöhnliche Switche an die adressierten Empfänger weiter, sind aber darüber hinaus auch besonders für die Anforderungen in Fertigungsanlagen angepasst.

Zusätzlich zu dem Leitstand und den HMIs kann auch eine Verbindung zu SPSen über eine besondere Schnittstelle hergestellt werden, die es erlaubt Daten aus einer SPS auszulesen und ein neues Programm zu laden.

Sensoren und Aktoren sind schließlich die Werkzeuge des Produktionsprozesses. Sensoren sammeln Daten über den Zustand der Produktion, etwa über die Höhe einer Flüssigkeit, die Temperatur eines Produktionselementes oder die Rotation eines Motors. Die Aktoren werden verwendet um genaue Anpassungen für den Prozess basierend auf der Daten der Sensoren und der Arithmetik der SPS-Programme vorzunehmen.

2.4.2 Architektur & Anforderungen

Die Architektur eines industriellen Netzwerkes ist darauf ausgelegt, einen Fertigungsprozess zu kontrollieren. Dementsprechend existiert eine hierarchische Struktur, wel-

che 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 Kontrollsystemen. Diese Kontrollsysteme können in verschiedenen Architekturen abgebildet werden.

Eine mögliche Form ist die Supervisory Control and Data Acquisition (SCADA) Architektur. In dieser Architektur existieren prinzipiell vier verschiedene Ebenen (von Level 4 (Verwaltung) zu Level 0 (Sensoren und Aktoren):

- Level 4 repräsentiert die Schnittstelle zum Unternehmensnetzwerk. Systeme auf dieser Ebene sind für die Produktionsplanung verantwortlich.
- Level 3 repräsenteirt die Produktionskontrolle über die Anlage. Systeme auf dieser Ebenen kontrollieren den Produktionsprozess indirekt durch die Überwachung von Zielen und Produkten.
- Level 2 beinhaltet weitere Systeme für die Beaufsichtigung wie z.B. den Leitstand. Die Elemente werden genutzt um Aktionen auf Level 1 und Level 0 zu kntrollieren. Human Machine Interfaces (HMI) gehören zu diesen Elementen und stellen eine grafische Benutzeroberfläche für Mitarbeiter zur Verfügung. Außerdem beinhaltet dieses Level das verteilte Kontrollsystem.
- Level 1 ist die Ebene mit direkter Kontrolle auf die Prozessschritte über die angeschlossenen SPSen.
- Level 0 beinhaltet Sensoren und Aktoren, die für die Kontrolle und Anpassung der Prozessschritte verwendet werden

2.4.3 Kommunikationstechnologien

In industriellen Netzwerken kommen verschiedene Elemente und Technologien zum Einsatz. Da Verfügbarkeit garantiert werden muss, werden Elemente wie SPSen über Jahre hinweg eingesetzt, sodass sich eine homogene Technologielandschaft ergibt, die unterschiedliche Kommunikationstechnologien unterstützt. So können bspw. ältere SPSen nur per Feldbus angesprochen werden, während neuere SPSen oder emulierte SPSen auch durch eine industrielle Version der Ethernet-Technologie angesprochen

werden können. Während die Feldbustechnologie sich in der Produktionswelt durchgesetzt hat, wurde das Ethernet in Unternehmensnetzwerken umgesetzt. Heutzutage wird jedoch versucht auch die industrielle Version der Ethernet-Technologie stärker in der Produktion zu etablieren. Die Verbindung dieser Technologien für die Umsetzung des Konzeptes der Industrie 4.0 wird auch als Virtual Automation Network (VAN) bezeichnet.

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. Die Feldbuskommunikation stellt einen gemeinsamen Datenbus für angeschlossene SPSen bereit. Dabei können verschiedene Methoden der Kommunikationskontrolle angewendet werden um die Nutzung des gemeinsamen Kommunikationsbusses nutzbar zu machen. So wird etwa das sogenannte Master-Slave Prinzip angewendet, bei dem eine Master SPS den Kommunikationsfluss der anderen SPSen kontrolliert und Informationen von einer bestimmten SPS anfragt, die damit entsprechend die Erlaubnis zum Senden von Informationen erhält. Eine andere Möglichkeit ist das Master-Master Prinzip, bei dem ein Token von SPS zu SPS übertragen wird. Die SPS im Besitz des Tokens besitzt auch die Sendeerlaubnis.

Eine andere Kommunikationstechnik wird in Form einer industriellen Version der Ethernet-Technologie verwendet, auch "Real-Time Ethernet"genannt. Dabei werden verschiedenen Ansätze verfolgt:

- Local soft real-time (TCP/IP Mechanismen mit ModbusTCP oder PROFINET CBA)
- Deterministic real-time
- Isochronous real-time

Jeder der Ansätze kann unter bestimmten Bedingungen eingesetzt werden, basierend vorallem auf der Schnelligkeit der Übetragungen.

Diese Kommunikationstechnologien müssen bestimmte Anforderungen erfüllen. So muss eine sichere und robuste Kommunikation sowie schnelle Übertragungsgeschwindigkeiten garantiert werden, da eine verspätete Reaktion oder fehlerhafte Kommunikation eine Gefahr für die physischen Geräte und auch für die Sicherheit der Mitarbeiter darstellen kann. Daher ist die Verfügbarkeit das höchste Schutzziel, dass es zu erfüllen gibt.

2.4.4 Kommunikationsprotokolle

Industrial Kommunikationsprotokolle: Formulierung nach Quellen des SPS Sec Paper

2.4.5 Bekannte Angriffsvektoren

- Nicht viel bekannt - Forscher haben verschiedene Elemente aufgedeckt - Prinzipielles Prinzip

2.5 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. Dabei sollen sogenannte SSmart 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.

2.5.1 Aktueller Sicherheitsstand von industriellen Produktionsnetzwerken (Schutzziele)

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. Das höchste Schutzziel in diesen Umgebungen ist die Sicherstellung der dauerhaften Verfügbarkeit der Komponenten, d.h. das Garantieren der Robustheit und

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. 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 noch sehr anfällig 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. 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.

2.5.2 Aktuelle Forschungsgebiete

Existierende Citavi Liste auswerten

Forschungsgebiete nochmal abdecken mit Suchlauf durch IEEEXplore, Elsevier, Springer und GooglePapers, Zeitrahmen: 2 Stunden

Ergebnisse der Recherche Formulieren

- Anomalieerkennung
- Konzeptionen für sicherere Industrie 4.0 Komponenten
- Untersuchung aktuell eingesetzter Komponenten und Kommunikationsprotokolle auf potentielle Sicherheitslücken

2.6 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. Die ISO27001 definiert ein Sicherheitsereignis 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.

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. 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.

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 betroffenen Vertragspartnern kommuniziert.

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. Der Begriff „Sicherheitsrelevanz“wird dazu für diese Thesis wie folgt definiert: Sicherheitsrelevante Informationen sind Informationen, die als „Indicator of Compromise“(IoC) dienen können. 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 die 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.

Daraus folgt die weitere Struktur des Kapitels: Zunächst wird das definierte Model beschrieben, woraufhin zunächst die Netzwerkelemente und daraufhin die Netzwerkprotokolle betrachtet werden.

Sollen Angriffsvektoren /-szenarien hier mit eingepflegt werden oder im Vergleich integriert werden?

3.2 Beschreibung der Unternehmensarchitektur (Model)

Das Ziel noch mehr herausstellen,Grundlegende Gedanke hinter der Erstellung des Models

Einbinden, dass das Model auf der Basis von Netzwerkarchitekturen erstellt wurde

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. 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.

Remote Access Server in Form von VPN, Protokolle? Traffic? Sinnvoll?

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.

Gehören Printserver hier rein? Welche Zusatzinformationen bringt ein Printserver?

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

3.2.1 Systeme

3.2.2 Applikationen

3.2.3 Interaktionen der Systeme (und Anwender)

3.3 Resultierende Informationstypen -kategorien

3.3.1 Extraktion und Verarbeitung

3.3.2 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.

Vertiefung möglich, kann ich die Kategorien weiter auftrennen ohne spezifischen Anwendungsfall?

EventIDs von Cylance/Sophos/Avira finden? Welche unterschiedlichen Endpoint Protection Solutions gibt es?

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 sowohl 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?

3.3.3 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“).

Beschreibe die unterschiedlichen Logformate

Neben den Log-Dateien des syslog Verzeichnisses gibt es noch weitere wichtige Log-Dateien. So beinhaltet die Log-Datei „auth.log“(Debian) bzw. „secure“(CentOS / RedHat) Ereignisse über erfolgreiche oder fehlerhafte Logins und die verwendeten Authentifizierungsmethoden. Die Log-Datei „kern“enthält Meldungen über Fehler sowie Warnungen, die vom Kernel gemeldet wurden. In der Datei „cron“werden Ereignisse gespeichert, die durch die Cron-Komponente des Linuxbetriebssystem protokolliert werden.

Abhängig von der Distribution existieren noch weitere Log-Dateien.

Fasse die Liste zusammen bzgl. der Log-Files die man auf jeden Fall überwachen sollte (minimum)

Beschreibe Ubuntu und CentOS

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

3.3.4 Beispielapplikation

3.3.5 Netzwerk

3.4 Analyse im Bezug auf Angriffsvektoren

Kapitel 4

Analyse der Informationsquellen in einem industriellen Produktionsnetzwerk

4.1 Beschreibung der Unternehmensarchitektur (Beispiel)

4.1.1 Systeme

4.1.2 Applikationen

4.1.3 Interaktionen der Systeme (und Anwender)

4.2 Verwendete Analysemethode

4.2.1 (Beschreibung der Kategorisierung und/oder wissenschaftliche Grundlage)

4.3 Resultierende Informationstypen / -kategorien

4.3.1 Extraktion und Verarbeitung

4.3.2 Feldbus im Beispiel

4.3.3 Industrial Ethernet im Beispiel

4.4 Analyse im Bezug auf typische Angriffsvektoren (s. Grundlagen)

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

Abbildungsverzeichnis