Industrial Security 4.0 – Zukünftige Herausforderungen und Lösungen zur Absicherung von Cyber-physischen Produktionssystemen

Henning Trsek, Daniel Mahrenholz, Stefan Schemmer, Ralf Schumann

rt-solutions.de GmbH, Oberländer Ufer 190a, 50968 Köln
{trsek, mahrenholz, schemmer, schumann}@rt-solutions.de

Abstract

Heutige Produktionssysteme nutzen in zunehmendem Maße aus Standard-IT-Komponenten. Sie sind außerdem weitreichend mit anderen Anlagenteilen und oft mit dem Internet vernetzt und werden somit immer angreifbarer von außen. Mit komplexen, nachhaltigen Angriffsformen ist es bereits mehrfach gelungen, Produktionsnetze zu manipulieren, sodass die funktionale Sicherheit der Anlage beeinträchtigt wurde. Im Office-Bereich wird diesen Angriffsformen durch den Einsatz von Security Information and Event Management (SIEM) Systemen begegnet, welche eine „Erkennen und Beheben" Strategie verfolgen, da Angriffe nicht vollständig verhindert werden können. Dieser Ansatz ist auch im industriellen Umfeld vielversprechend. Dieser Beitrag diskutiert das Konzept eines Industrial SIEM und analysiert die Besonderheiten, die bei einem Industrial SIEM gegenüber entsprechenden Systemen der Office IT beachtet werden müssen. Weiterhin wird die Integration eines Industrial SIEM in bestehende Produktionssysteme und hierfür relevante Aspekte betrachtet.

1 Einleitung

Die Individualisierung von Produkten bei gleichzeitiger kosteneffizienter Fertigung erfordert aktuelle und genaue Informationen über Fertigungsanlagen und deren Status und das nicht nur auf der Steuerungsebene, sondern auch auf der Fabrikebene bis hin zu externen Lieferanten. Dies bedeutet eine vertikale Integration der Ebenen und eine horizontale Integration entlang der Wertschöpfungskette durch eine umfassende Vernetzung der Systeme untereinander und mit dem Internet.

Infolgedessen müssen die Anlagen immer flexibler werden, bis hin zu zukünftigen Produktionssystemen, die aus intelligenten, autonom agierenden Produktionseinheiten bestehen, die umfassend miteinander kommunizieren. In aktuellen und zukünftigen Produktionsanlagen werden außerdem zunehmend Standard-IT-Komponenten verwendet.

Beides hat zur Folge, dass die Produktionssysteme nicht mehr als isolierte Systeme betrachtet werden können und angreifbarer von außen werden. Aktuelle Vorfälle haben gezeigt, dass es Angreifern unter Verwendung von komplexen, nachhaltigen

Angriffsformen, sogenannten Advanced Persistent Threats (APT), gelingt, über die Office IT bis in die Produktionsnetze vorzudringen und diese zu manipulieren. Die Absicherung der Systeme durch klassische präventive Maßnahmen ist nur eingeschränkt möglich, da die Angreifer über ein sehr umfangreiches technisches Know-how verfügen und es häufig schaffen, die etablierten Schutzmaßnahmen zu umgehen. In der Office IT begegnet man dieser Situation seit einiger Zeit mit dem Einsatz von Security Information and Event Management (SIEM) Systemen. Ein SIEM verfolgt eine „Erkennen und Beheben" Strategie, statt Angriffe vollständig zu vermeiden. Vor dem Hintergrund der aktuellen Bedrohungssituation im industriellen Umfeld ist der Einsatz von SIEM Systemen auch hier vielversprechend.

Dieser Beitrag geht zunächst anhand von realen Zwischenfällen auf die aktuelle Bedrohungslage ein. Ausgehend davon wird im Anschluss das allgemeine Konzept eines Security Information and Event Managements sowie eines SIEMs für den industriellen Einsatz (Industrial SIEM) vorgestellt. Ein Industrial SIEM überwacht Security-relevante Ereignisse in einer Produktionsanlage und kann diese in Echtzeit korrelieren, um anormales Verhalten und mögliche Angriffe zu erkennen und an die verantwortlichen Stellen zu melden. Die bestehenden grundlegenden Unterschiede zwischen den industriellen Szenarien und der Office IT werden analysiert und aufgezeigt. Beispielsweise werden sich voraussichtlich die Regeln zur Erkennung von Angriffen, aber auch die Prozesse zur Reaktion darauf von der Office IT unterscheiden. Weiterhin wird die Integration eines Industrial SIEM in bestehende Produktionssysteme und hierfür relevante Aspekte betrachtet.

2 Aktuelle Bedrohungen und Vorfälle

Vor einigen Jahren wurde im Umfeld der IT-Sicherheit eine neue Bedrohung mit einer bis daher unbekannten Qualität namens *Advanced Persistent Threat* (APT) identifiziert. Ein APT ist ein zielgerichteter Angriff auf ein ausgewähltes Unternehmen, bei dem sich der Angreifer einen nachhaltigen Zugriff auf die Systeme des angegriffenen Unternehmens verschafft und diesen sukzessive ausweitet. Die Angriffe werden häufig unter Einsatz von großen personellen sowie finanziellen Ressourcen und so lange durchgeführt, bis die Angreifer ihr Ziel erreicht haben. Die Angreifer verfügen über sehr hohe technische Fähigkeiten, sodass die Angriffe sehr schwer erkennbar sind und die klassischen Schutzmaßnahmen der IT-Sicherheit fast immer von den Angreifern umgangen werden können. Die entscheidenden Phasen eines Angriffs sind in Abbildung 1 dargestellt. Während der Phasen Eindringen und Festsetzen sind die Angreifer nur mit geringem Erfolg zu erkennen. In der Phase der Ausbreitung besteht hingegen die höchste Wahrscheinlichkeit der Erkennung. Überdies stellt das Pflegen der Präsenz in der letzten Phase den wesentlichen Kern eines nachhaltigen Angriffs dar.

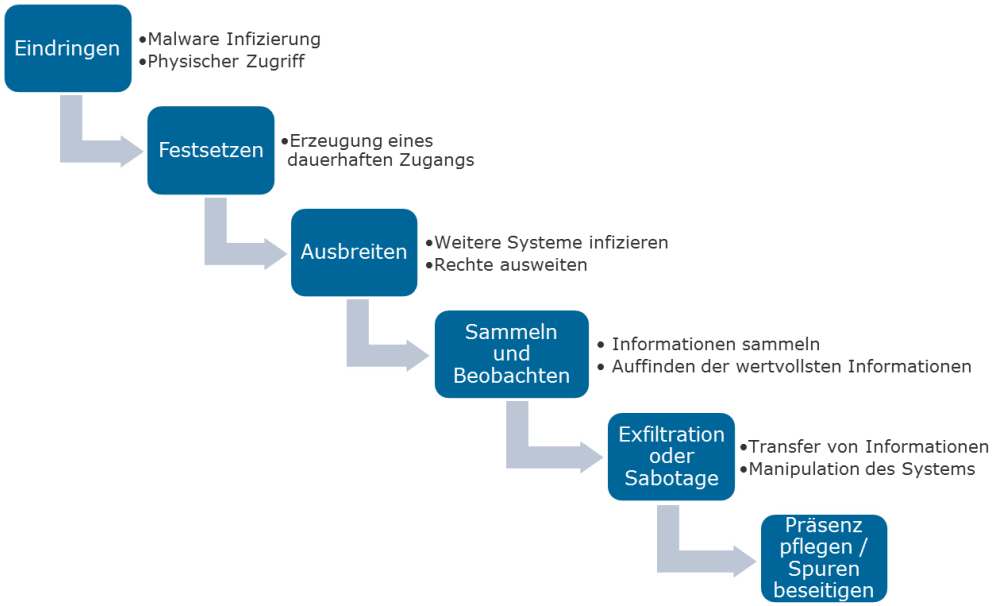

Abbildung 1: Verschiedene Phasen eines APTs

Im Kontext von industriellen Systemen bedeutet dies, dass die Angreifer sich zunächst einen Zugang zum Netzwerk der Office IT verschaffen und diesen im Anschluss bis hin zu den Produktionssystemen ausweiten. Die Kenntnisse der Angreifer sind meistens sowohl im Bereich der klassischen IT-Sicherheit als auch im Bereich von Steuerungsanlagen und Produktionsprozessen sehr ausgeprägt.

Im Folgenden werden einige beispielhafte Vorfälle in industriellen Anlagen in chronologischer Reihenfolge aufgezeigt, beginnend mit dem aktuellsten. Die dargestellten Angriffe wurden mit teilweise sehr großem Aufwand durchgeführt. Betroffen waren hierbei sowohl gewöhnliche Fertigungsanlagen, als auch Anlagen die zu den kritischen Infrastrukturen gezählt werden.

Im Jahr 2014 fand ein gezielter Angriff auf ein Stahlwerk in Deutschland statt [1], bei dem die Angreifer sich zunächst mittels Social Engineering und Spear-Phishing Zugang zum Büronetz des Unternehmens verschafften und im Anschluss bis in die Produktionsnetze vordrangen. Während des Angriffs häuften sich die Ausfälle einzelner Steuerungssysteme bis hin zu dem Ausfall eines Hochofens, der eine massive Beschädigung der gesamten Anlage zur Folge hatte.

Mit dem ebenfalls im Jahr 2014 bekannt gewordenen Schadprogramm Havex [2] wurden mehrere deutsche Unternehmen angegriffen. Im ersten Schritt verlief der Angriff über die Hersteller von industriellen Steuerungssystemen. Die Webseiten der Hersteller wurden manipuliert. Auf diese Weise konnten die Angreifer eine angepasste Firmware für die Geräte zur Verfügung stellen, die bereits mit Havex infiziert war. Sobald ein Betreiber seine Geräte aktualisierte, wurde die Schadsoftware ebenfalls installiert. Havex sammelt gezielt Informationen über das Produktionsnetz und leitet

diese an die Angreifer weiter. Momentan wird davon ausgegangen, dass die Angreifer die gesammelten Informationen im nächsten Schritt für weitere Angriffe nutzen werden. In diesem Zusammenhang sind allerdings bislang keine Beeinträchtigungen von Anlagenfunktionen bekannt.

Der wohl bekannteste Vorfall ist der Stuxnet Angriff [3]. Im September 2010 wurde die Steuerung der Zentrifugen zum Anreichern von Uran in einer iranischen Atomanlage so manipuliert, dass minimale Abweichungen auftraten, die von den Bedienern nicht erkannt werden konnten, die aber den Verschleiß drastisch erhöhten und zu umfangreichen Beschädigungen bzw. Zerstörungen der Zentrifugen führten.

Die diskutierten Beispiele zeigen eindrucksvoll, dass Schwachstellen in Geräten und Kommunikationssystemen der industriellen Automatisierungstechnik nicht nur ein hohes Risiko für den Anlagenbetreiber hinsichtlich eines wirtschaftlichen Schadens bedeuten, sondern teilweise sogar sicherheitsgerichtete Funktionen und somit die funktionale Sicherheit der Anlage beeinträchtigen. Der Schutz des Menschen und der Umwelt vor dem technischen System kann somit nicht mehr gewährleistet werden.

Einerseits teilen industrielle Kommunikationssysteme einige relevante Security-Charakteristiken mit Standard-IT-Systemen aus dem Enterprise-Umfeld. Andererseits bestehen einige Unterschiede, beispielsweise die hohe Verfügbarkeit von Anlagen, die es nur schwer ermöglichen, die industriellen Systeme identisch abzusichern und daher Anpassungen erfordern.

Vor dem Hintergrund der geschilderten Bedrohungslage wird es in zukünftigen Anlagen für den zuverlässigen Betrieb eines Systems erforderlich bzw. sehr hilfreich sein, wenn Angriffe frühzeitig erkannt und entsprechend reagiert werden kann. Das gilt insbesondere für APTs, die mit klassischen, präventiven Maßnahmen nicht oder nur sehr schwer zu verhindern sind.

3 Security Information and Event Management (SIEM)

Der geschilderten Bedrohungslage begegnet man im Bereich der Enterprise IT seit einiger Zeit mit dem Einsatz von *Security Information and Event Management* (SIEM) Systemen. Ein SIEM verfolgt eine „Erkennen und Beheben“ Strategie unter dem Bewusstsein, dass Angriffe nicht vollständig vermieden werden können, da sie zielgerichtet von professionellen Angreifern durchgeführt werden.

Die Erkennung der Angriffe innerhalb der ersten Angriffsphasen ermöglicht dem Unternehmen, das Schadensausmaß zu reduzieren und größeren Schaden abzuwenden. Hierzu müssen der Netzwerkverkehr und sicherheitsrelevante Ereignis-Logs miteinander korreliert werden. Die aus der Korrelation gewonnenen Erkenntnisse erlauben eine Reaktion auf Angriffe und Bedrohungen in Echtzeit [4].

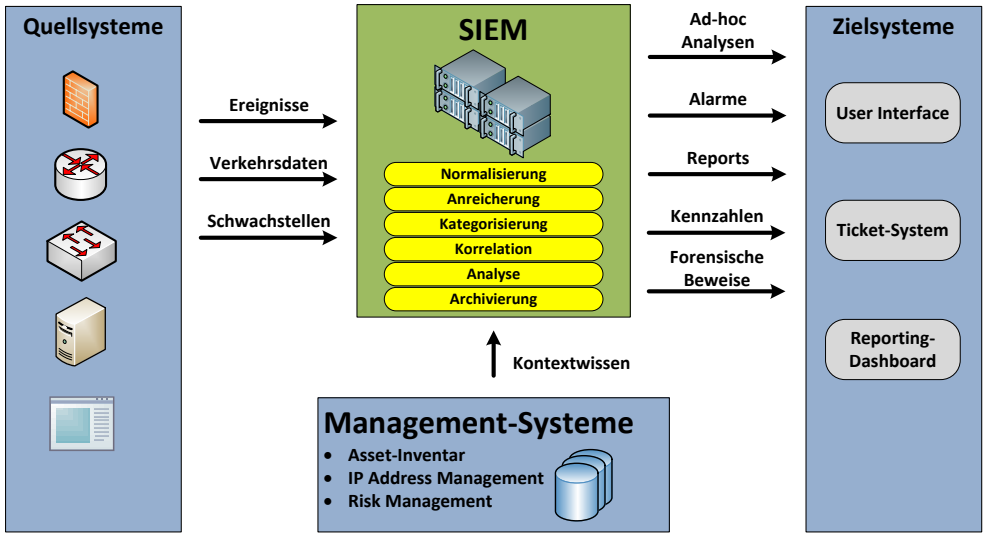

Abbildung 2: Grundsätzlicher Aufbau eines SIEM-Systems

Ein SIEM-System besteht aus einer verteilten Plattform, die Daten von verschiedensten Quellsystemen sammelt, in einem zentralen Datenspeicher sammelt und über archiviert. Die meist unstrukturierten Daten werden dabei durch Textanalyse in strukturierte Felder zerlegt (Normalisierung), mit Kontextwissen (z.B. Namen von Netzwerkzonen) angereichert und mit einer abstrakten Bedeutung versehen (Kategorisierung), um sie für einen Security-Spezialisten verständlich zu machen. Mit verschiedenen Methoden werden die Daten inhaltlich und zeitlich über die verschiedenen Quellen hinweg korreliert und mit Hilfe eines Regelwerkes bzw. Expertensystems komplexe sicherheitsrelevante Vorgänge wie beispielsweise Angriffe oder Fehlverhalten von Mitarbeitern erkannt. Außerdem existieren verschiedene Analyse- und Berichtsfunktionen um die erlangten Erkenntnisse zielgruppenspezifisch kommunizieren zu können.

Für den erfolgreichen Einsatz benötigt jedes Unternehmen jedoch ein Gesamtkonzept, in dem die spezifischen Anforderungen und Randbedingungen des Unternehmens berücksichtigt werden und das System in Abhängigkeit der bestehenden Prozesse, Personen und SIEM-Funktionalitäten integriert wird. Nur unter diesen Voraussetzungen kann ein SIEM System als ganzheitliche Lösung eingesetzt und optimal und kosteneffizient betrieben werden.

4 SIEM für den industriellen Einsatz

In diesem Kapitel wird anhand der Besonderheiten im industriellen Umfeld ein Lösungskonzept vorgestellt, welches außer der technischen Umsetzung die wichtige Fragestellung nach der Vorfallsbehandlung adressiert.

4.1 Industrielle Randbedingungen und wesentliche Unterschiede

Beim Einsatz eines SIEM Systems im industriellen Umfeld müssen zunächst die besonderen Rahmenbedingungen im Vergleich zur Enterprise-IT analysiert werden, um daraus die wesentlichen Unterschiede ableiten zu können. Die folgenden Charakteristiken sind in diesem Kontext relevant.

Die Taktzeiten einer Fertigungsanlage, die Produktionsmenge sowie deren Qualität haben die höchste Priorität [5]. Security-Maßnahmen müssen daher vorab sorgfältig geplant werden, da eine Beeinträchtigung dieser Eigenschaften z.B. im Zuge einer automatisierten Reaktion auf einen Vorfall nicht tolerierbar ist.

Eine Produktionsanlage muss typischerweise als Gesamtgewerk betrachtet werden, sodass Security-bedingte Anpassungen und Änderungen ebenfalls im Gesamtkontext geplant und durchgeführt werden müssen. Die Verfolgung einer passiven „Erkennen und Beheben"-Strategie ist daher für den industriellen Einsatz angeraten.

Im Gegensatz zur Enterprise-IT sind Produktionsnetzwerke in Bezug auf die Informationsflüsse und das Datenaufkommen relativ statisch [6]. Kommunikation zwischen unbekannten oder nicht berechtigten Partnern ist in heutigen Systemen gewöhnlich nicht zugelassen und deutet auf eine Sicherheitsanomalie hin.

Darüber hinaus muss das Industrial-SIEM-System in eine Landschaft mit einer größeren Anzahl von Kommunikationsprotokollen, die teilweise sogar proprietär sind, integriert werden. Die Funktionalitäten hinsichtlich des Loggings sind ebenfalls bei vielen Feldgeräten eingeschränkt oder gar nicht vorhanden. Im Gegensatz zum Enterprise-Umfeld sind aber grundsätzlich wesentlich weniger Knoten, und damit Datenquellen, innerhalb einer Anlage vorhanden. Die wesentlichen Unterschiede des SIEM Einsatzes im industriellen Umfeld sind in Tabelle 1 zusammengefasst.

Tabelle 1: Gegenüberstellung der SIEM Anforderungen

Enterprise IT	Industrial IT
Schutz wichtiger Informationswerte hat höchste Priorität (Vertraulichkeit)	Taktzeiten, Produktionsmenge und Qualität haben höchste Priorität (Verfügbarkeit)
Latenzzeiten sind in den meisten Anwendungen weniger relevant und unkritisch	Deterministische Kommunikation mit sehr geringen Latenzzeiten erforderlich
Kommunikationsbeziehungen und –verhalten sehr dynamisch	Kommunikationsbeziehungen und –verhalten sehr statisch bzw. deterministisch
Geringe Abhängigkeiten zwischen verschiedenen Applikationen	Konzept muss im Gesamtkontext der Anlage betrachtet werden
Standard-Kommunikationsprotokolle, umfangreiche Logging-Funktionen	Teilweise proprietäre Protokolle und eingeschränkte Logging-Funktionen

4.2 Lösungskonzept

Das erarbeitete Lösungskonzept besteht aus einem zentralen SIEM-System, welches sowohl für die Enterprise-IT als auch für die Industrial-IT eingesetzt wird. Dieser hybride Ansatz wird verfolgt, weil sich die Angreifer den Zugang häufig zunächst über das Office-Netzwerk verschaffen. Die nachfolgenden Punkte beziehen sich aber nur auf die relevanten Aspekte für das industrielle Umfeld. Ein mögliches Konzept wird in Abbildung 3 veranschaulicht und zeigt u.a. die verschiedenen Datenquellen und deren Ebene im Gesamtsystem.

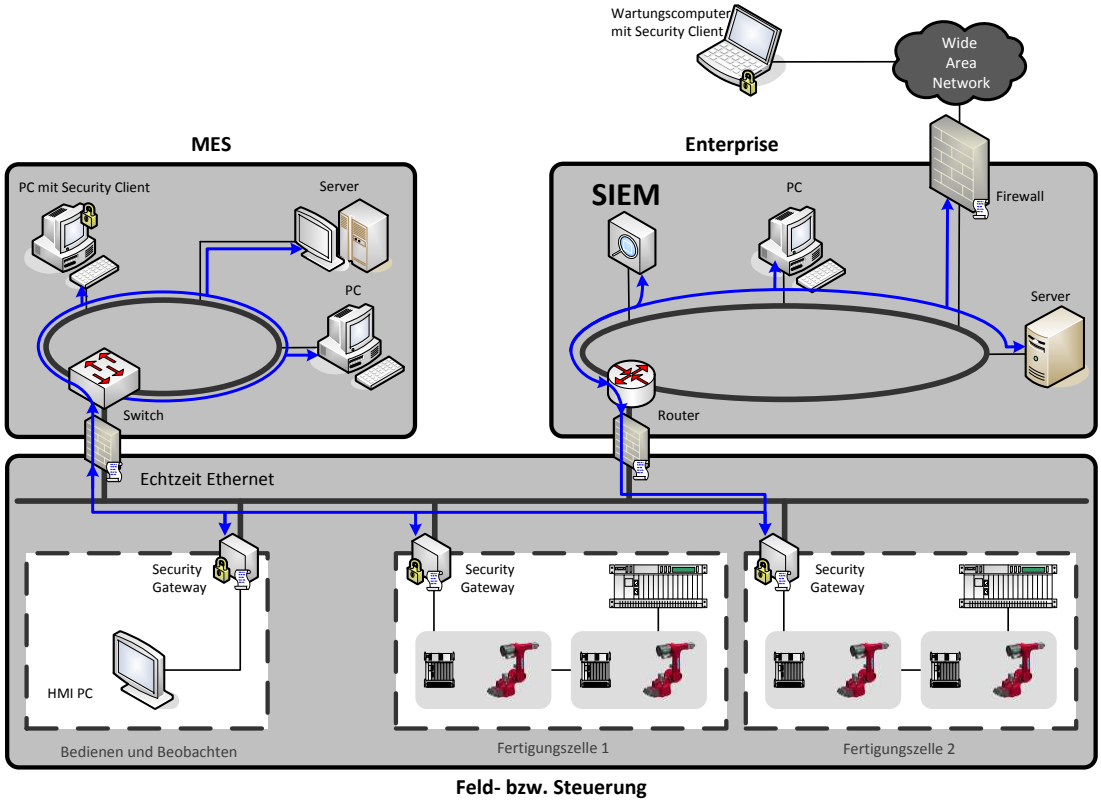

Abbildung 3: SIEM Integration in ein bestehendes Produktionssystem

Ein wichtiger Bestandteil des SIEM-Konzepts sind die zur Verfügung stehenden Datenquellen, die die erforderlichen Einzelinformationen bereitstellen. Im Wesentlichen handelt es sich dabei um den Netzwerkverkehr und die Erfassung von Log-Dateien.

Die Aufzeichnung des Netzwerkverkehrs an ausgewählten Punkten, beispielsweise an dem Netzwerkzugang zu Fertigungszellen, erlaubt die Erfassung und Auswertung der Informationsflüsse innerhalb der Anlage. Voraussetzung hierfür sind entsprechende Protokollanalysatoren, die eine Analyse der eingesetzten Protokolle ermöglichen. Da die in Produktionsanlagen eingesetzten Kommunikationsprotokolle mitunter sehr heterogen sind, muss das Konzept individuell darauf angepasst werden

und das SIEM System eventuell um die erforderlichen Schnittstellen erweitert werden.

Weiterhin ist die Erfassung von Ereignissen erforderlich, die durch die relevanten Logs von Infrastrukturkomponenten, wie z.B. Switches und Firewalls, zur Verfügung gestellt werden können. Die eingesetzten Systeme auf der Feldebene (SPS, IO-Geräte, etc.) stellen meistens keine Logging-Funktionalität bereit. Wichtige Informationen können aber beispielsweise aus einer zentralen Prozessdatenerfassung hinzukommen. Viele industrielle *Security Appliances* erlauben darüber hinaus die Überwachung auf Anwendungsebene der eingesetzten Protokolle. Diese Datenquellen liefern sogar weitaus detailliertere Informationen, als allgemein erfasste Ereignisse.

4.3 Vorfallsbehandlung

Bei einem erkannten Vorfall hängt der Erfolg von Gegenmaßnahmen und der damit verbundenen Begrenzung des Schadensausmaßes wesentlich davon ab, das gesamte Ausmaß zu verstehen und die Gegenmaßnahmen zeitnah und vollständig umzusetzen [7].

Da die Ressourcen zur Erkennung und Behandlung von Vorfällen häufig nicht in dem erforderlichen Umfang zur Verfügung stehen, sollten die erforderlichen manuellen Tätigkeiten zur Behandlung eines Vorfalls durch den Einsatz von automatisierten Gegenmaßnahmen unterstützt werden. Die folgenden automatisierten Gegenmaßnahmen sind denkbar:

- Direkte Kontrolle von Switch- oder Router-Schnittstellen, z.B. mittels SNMP, um diese zu deaktivieren
- Anpassung der Konfiguration von Netzwerkinfrastruktur-Komponenten mit Hilfe von Skripten, um beispielsweise Routing anzupassen oder Benutzer/Geräte zu isolieren
- Anpassung der Konfiguration von Security-relevanten Geräten (z.B. Firewalls) mit Hilfe von Skripten, um bestimmte Verkehrsflüsse zu blockieren
- Deaktivierung oder Anpassung von Benutzer-Konten und deren Rechten mit Hilfe von Skripten, falls eine maliziöse Verwendung erkannt wurde

Obwohl automatisierte Gegenmaßnahmen die SIEM-Effizienz steigern können, sollten sie eingeschränkt auf die unkritischen Sicherheitszonen des Gesamtsystems angewendet werden. Außerdem müssen die Abhängigkeiten innerhalb der gesamten Anlage berücksichtigt werden. Diese Gegenmaßnahmen sollten daher sorgfältig vorab analysiert und geplant werden.

5 Fazit

Das vorgestellte Konzept eines SIEM für den industriellen Bereich zeigt eine potenzielle und vielversprechende Lösung, um zukünftige Produktionsanlagen gegen APTs abzusichern bzw. diese Angriffe frühzeitig zu erkennen und passende Abwehrmaßnahmen einzuleiten. Die Wahrscheinlichkeit einer Beeinträchtigung der Funktionalität der Anlage und ein damit verbundener Schaden kann somit erheblich reduziert werden. Beim Einsatz und der Konzeptionierung des Systems müssen jedoch die unterschiedlichen Randbedingungen und Unterschiede berücksichtigt werden. Die zur Erkennung und Behandlung von Vorfällen erforderlichen Ressourcen sind häufig ein großes Problem. Durch den Einsatz von automatisierten Gegenmaßnahmen wird eine wesentlich effizientere Vorfallsbehandlung ermöglicht. Sie sollten aber nur in unkritischen Zonen eingesetzt werden.

Im weiteren Verlauf der geplanten Forschungsarbeiten sollen die für industrielle Anwendungen erforderlichen Korrelationsregeln entwickelt und prototypisch implementiert werden und diese insbesondere hinsichtlich der auftretenden *False-Positives* evaluiert und optimiert werden. Darüber hinaus soll in einer Fallstudie das Gesamtsystem in einer realen Anwendung betrieben werden und die daraus gewonnen Erkenntnisse zur weiteren Optimierung genutzt werden.

Referenzen

[1] Bundesamt für Sicherheit in der Informationstechnik (BSI). „Die Lage der IT-Sicherheit in Deutschland 2014“, Bonn, 2014.

[2] Langill, J.T. ”Defending Against the Dragonfly Cyber Security Attacks“, Belden Whitepaper, http://www.belden.com/docs/upload/Belden-White-Paper-Dragonfly-Cyber-Security-Attacks.pdf, Dezember 2014.

[3] R. Langner. "To kill a centrifuge: A technical analysis of what stuxnet’s creators tried to achieve." Online: http://www.langner.com/en/wp-content/uploads/2013/11/To-kill-a-centrifuge.pdf, 2013.

[4] D. Mahrenholz, R. Schumann, A. Brügmann. „SIEM – Technik allein ist keine Lösung“, In: *P. Schartner, P. Lipp. „DACH Security 2014“*, syssec (2014).

[5] National Institute for Standards and Technology (NIST). “Guide to Industrial Control Systems (ICS) Security”, SP 800-82 Rev 2, Mai 2015.

[6] E.D. Knapp, J.T. Langill. *Industrial Network Security: Securing critical infrastructure networks for smart grid, SCADA, and other Industrial Control Systems*. Syngress, 2014.

[7] D. Mahrenholz, R. Schumann. „Incident Response im SIEM-Kontext – Ein Erfahrungsbericht“, In: *P. Schartner, P. Lipp. „DACH Security 2015“*, syssec (2015).