NAMUR - Interessengemeinschaft
Automatisierungstechnik der Prozessindustrie e.V.

AK-PRAXIS

Angriffserkennung nach IT-Sicherheitsgesetz 2.0

Stand:
2022-09-15

AK 4.18 Automation Security

Verfasser: Klaus Hunsänger, Bundesamt für Sicherheit in der Informationstechnik
Marc Meyer, Bundesamt für Sicherheit in der Informationstechnik
Markus Linnartz, Evonik
Dr. Thomas Steffen, BASF
Henry Hoppe, BASF
Alexander Lehmann, Bayer

AK-Leiter: Erwin Kruschitz, anapur

Diese AK-PRAXIS spiegelt die Erfahrungen der Mitglieder im AK 4.18 wider und ist im Rahmen des Arbeitskreises abgestimmt. Sie hat nicht den Konsensgrad einer NAMUR-Empfehlung oder eines NAMUR-Arbeitsblatts. Mit einer AK-PRAXIS hat der Arbeitskreis die Möglichkeit, zeitnah eigene Erfahrungen für interessierte Leser zur Verfügung zu stellen.

Vorwort

Angriffserkennung im IT-SiG 2.0 bzw. BSI-G
Das „Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz - BSIG)“ fordert „Angriffserkennung“.

Im Folgenden finden sich Textauszüge, die im Zusammenhang dieser Forderung relevant sein könnten:

Auszug aus § 2 Begriffsbestimmungen
(1) Die Informationstechnik im Sinne dieses Gesetzes umfasst alle **technischen Mittel zur Verarbeitung von Informationen**.

(9b) **Systeme zur Angriffserkennung** im Sinne dieses Gesetzes sind durch technische Werkzeuge und organisatorische Einbindung unterstützte **Prozesse zur Erkennung von Angriffen** auf informationstechnische Systeme. Die Angriffserkennung erfolgt dabei durch Abgleich der in einem informationstechnischen System verarbeiteten Daten mit Informationen und technischen Mustern, die auf Angriffe hindeuten.

Auszug aus § 8a Sicherheit in der Informationstechnik Kritischer Infrastrukturen
(1) Betreiber Kritischer Infrastrukturen sind verpflichtet, spätestens bis zum ersten Werktag, der darauf folgt, dass diese erstmalig oder erneut als Betreiber einer Kritischen Infrastruktur nach der Rechtsverordnung nach § 10 Absatz 1 gelten, angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen maßgeblich sind. Dabei soll der Stand der Technik eingehalten werden. Organisatorische und technische Vorkehrungen sind angemessen, wenn der dafür erforderliche Aufwand nicht außer Verhältnis zu den Folgen eines Ausfalls oder einer Beeinträchtigung der betroffenen Kritischen Infrastruktur steht.
(1a) Die Verpflichtung nach Absatz 1 Satz 1, angemessene organisatorische und technische Vorkehrungen zu treffen, umfasst ab dem 1. Mai 2023 auch den Einsatz von Systemen zur Angriffserkennung. **Die eingesetzten Systeme zur Angriffserkennung müssen geeignete Parameter und Merkmale aus dem laufenden Betrieb kontinuierlich und automatisch erfassen und auswerten. Sie sollten dazu in der Lage sein, fortwährend Bedrohungen zu identifizieren und zu vermeiden sowie für eingetretene Störungen geeignete Beseitigungsmaßnahmen vorzusehen.** Absatz 1 Satz 2 und 3 gilt entsprechend.

Der Begriff Angriffserkennung im Energiewirtschaftsgesetz

(1a) Der Betrieb eines sicheren Energieversorgungsnetzes umfasst insbesondere auch einen angemessenen Schutz gegen Bedrohungen für Telekommunikations- und elektronische Datenverarbeitungssysteme, die für einen sicheren Netzbetrieb notwendig sind.

(1d) Betreiber von Energieversorgungsnetzen und von solchen Energieanlagen, die durch Inkrafttreten der Rechtsverordnung gemäß § 10 Absatz 1 des BSI-Gesetzes als Kritische Infrastruktur bestimmt wurden, haben spätestens ab dem 1. Mai 2023 in ihren informationstechnischen Systemen, Komponenten oder Prozessen, die für die Funktionsfähigkeit der von ihnen betriebenen Energieversorgungsnetze oder Energieanlagen maßgeblich sind, in angemessener Weise Systeme zur Angriffserkennung einzusetzen. Die eingesetzten Systeme zur Angriffserkennung müssen geeignete Parameter und Merkmale aus dem laufenden Betrieb kontinuierlich und automatisch erfassen und auswerten. Sie sollten dazu in der Lage sein, fortwährend Bedrohungen zu identifizieren und zu vermeiden sowie für eingetretene Störungen geeignete Beseitigungsmaßnahmen vorsehen.
Dabei soll der Stand der Technik eingehalten werden. Der Einsatz von Systemen zur Angriffserkennung ist angemessen, wenn der dafür erforderliche Aufwand nicht außer Verhältnis zu den möglichen Folgen eines Ausfalls oder einer Beeinträchtigung des betroffenen Energieversorgungsnetzes oder der betroffenen Energieanlage steht.

Zusammenfassung / Executive Summary

IT-SiG 2.0 fordert von Betreibern von „Kritischer Infrastruktur“:

- Prozesse zur Erkennung von Angriffen
- auf Informationstechnische Systeme, welche durch
- technische Werkzeuge und
- organisatorische Einbindung unterstützt werden.

Die Angemessenheit einzelner Maßnahmen zur Erfüllung dieser Vorgaben hängt von einer Vielzahl von Faktoren ab. Dazu gehören u.a.:

- die Kritikalität der Anlage im Sinne des IT-SIG 2.0,
- die Komplexität des Informationstechnischen Systems,
- die vorhandene Security-Kompetenz in den umsetzenden Organisationseinheiten,
- die Exposition des Informationstechnischen Systems gegenüber Cyber-Bedrohungen,
- sich auf die IT-Sicherheit nachteilig auswirkende Seiteneffekte einzelner Angriffserkennungsmaßnahmen
- weitere Gegebenheiten von Bestandanlagen.

Diese Parameter fließen in eine Risikoanalyse ein und werden bewertet. Aus der Risikoanalyse wird ein angemessenes Maßnahmenpaket erstellt und umgesetzt. Die Umsetzung soll stufenweise erfolgen, also z.B. ein erstes Maßnahmenpaket im Bestand und zu einem späteren Zeitpunkt (z.B. Systemmigration) ein weiteres.

Das Dokument konkretisiert das Thema SzA (Systeme zur Angriffserkennung) der BSI-Veröffentlichung *Orientierungshilfe zum Einsatz von Systemen zur Angriffserkennung inklusive Formulare für den Nachweis zu § 8a (1a) BSIG und § 11 (1d) ENWG* (zum Zeitpunkt dieser Veröffentlichung als Community-Draft vorliegend) um Branchenspezifika der chemischen Prozessindustrie.

Im Folgenden wird jeweils ein Steckbrief zu den einzelnen technischen Maßnahmen, die zur Angriffserkennung beitragen können, dargestellt. Welche Maßnahmen in einer konkreten Anlage zur Angriffserkennung eingesetzt werden, hängt von der Risikoanalyse ab. Details finden sich im Kapitel 5. Aufwand und Komplexität für Installation und Betrieb steigt mit jeder weiteren Maßnahme an.

Beschreibung	**Einsatzfeld**
Ingress Egress Monitoring Darunter wird die Überwachung des Netzwerkverkehrs aus und in das System verstanden. Voraussetzung für die Funktionstüchtigkeit dieser Maßnahme ist, dass neben dem überwachten Übergabepunkt keine weiteren Datenübertragungswege möglich sind.	Diese Maßnahme ist ein integraler Bestandteil der standardmäßigen Segmentierung und wird von NAMUR für alle **vernetzten Systeme stark empfohlen**.
Lean Monitoring Unter Lean Monitoring ist die konsequente Ausnutzung von systemeigenen Informationsquellen (Logs) zu verstehen. Der Anschluss an eine zentrale Meldeinstanz (z.B.) über Log Kollektoren ist für den effizienten Betrieb sinnvoll.	Diese Maßnahme erscheint für den Großteil der PLS Systeme adäquat und wird deshalb **von NAMUR als bevorzugtes technisches Werkzeug zur Angriffserkennung empfohlen**.
Network Based Monitoring Darunter wird die Auswertung des Netzwerkverkehrs an einem zentralen Punkt im Netzwerk des Systems verstanden.	Diese Maßnahme ist für **stärker vernetzte und / oder größere bzw. komplexe Systeme** unter Verfügbarkeit von kompetentem Personal geeignet.

Der Anschluss an eine zentrale Meldeinstanz (z.B. SIEM) ist für den effizienten Betrieb notwendig.	Diese Maßnahme kommt insbesondere dann infrage, wenn die Risikoanalyse ergibt, dass die vorausgegangenen Methoden oder deren Kombination keine ausreichende Sichtbarkeit erzielen.
Host based Monitoring Darunter wird die Auswertung von Informationen der einzelnen Netzwerkknoten (PC, Server, …) verstanden. Der Anschluss an eine zentrale Meldeinstanz (z.B. SIEM) ist für den effizienten Betrieb notwendig.	Diese Maßnahme ist für **stärker vernetzte und / oder größere bzw. komplexe Systeme** unter Verfügbarkeit von kompetentem Personal geeignet. Diese Maßnahme kommt insbesondere dann infrage, wenn die Risikoanalyse ergibt, dass die vorausgegangenen Methoden keine ausreichende Sichtbarkeit erzielen.

Ergänzender Hinweis: die in Betrieb und Installation umfangreicheren Maßnahmen wie Host based, Network based und Lean Monitoring bieten abseits des Security-Gewinns auch das Potenzial die Gesamtverfügbarkeit des Systems zu erhöhen.
Die vorausgegangene Auflistung stellt nur unterschiedliche Methoden der Angriffserkennung dar. Nur eine Kombination verschiedener Maßnahmen bilden erst ein sinnvolles System zur Angriffserkennung.

Inhaltsverzeichnis

1 Zweck und Umfang dieses Dokumentes

Diese AK-Praxis beschreibt die Eignung von verschiedenen Methoden, die als „technische Werkzeuge“ im Sinne des BSI-Gesetzes zur „Angriffserkennung“ herangezogen werden können. Aus Sicht der Autoren und des NAMUR AK 4.18.

1.1 Vorteile für NAMUR Mitglieder

- Klarheit und Hilfestellung bei der Umsetzung der Maßnahme „Angriffserkennung“.
    - Überblick darüber, welche Lösungen mit Stand heute existieren (Vor- / Nachteile)
    - Überblick darüber, welche Lösungsmethode passt auf welche Anlage / welches System
    - was kann/soll/muss gemacht werden
- Einheitliche Sichtweise im Zusammenhang mit der Erfüllung IT-SiG 2.0
- Verbesserung der Planungsprozesse (technische Planung und Kostenplanung)

1.2 Welche „vertikalen“ OT-Domänen werden betrachtet?

Im Fokus dieser AK-Praxis steht die **Prozessleittechnik** in der Chemischen / Pharmazeutischen / Öl- & Gas Industrie.
Hinweis: Bei Anlagen nach BSI-KritisV sind über die Prozessleittechnik hinaus gegebenenfalls noch andere IT und OT Systeme auf Angriffe zu überwachen. Z.B. Gebäude, Labor, Logistik, Verwaltung etc., sofern sie für die Erbringung der kritischen Dienstleistung erforderlich sind. Neben der Angriffserkennung sind auch Maßnahmen zum physischen und logischen Schutz der Anlagen und Computersysteme gefordert. Diese verstehen sich jedoch nicht im Umfang dieser AK-Praxis.

1.3 Welche Lebenszyklusphasen werden betrachtet?

Im Fokus der AK-Praxis steht die Lebenszyklusphase **Betrieb & Wartung**
Folgende Lebenszyklusphasen sind zunächst nicht im Fokus dieses Dokuments:

- Planung
- Außerbetriebnahme

1.4 Welche Asset - Typen werden betrachtet?

Im Fokus der AK-Praxis stehen folgende Asset – Typen

- Hardwarekomponenten
- Softwarekomponenten
- Netzwerkkomponenten (Hardware, Software, Konfigurations-Apps)
- Services (z. B. Domain Services, Authentifizierungsdienste, etc.)

Folgende Asset – Typen sind nicht im Fokus dieser AK-Praxis:

- Daten (Data at Rest)
- Organisationen (Lieferanten, IT-Operations, SOC, Legal, Behörden)

1.5 Organisatorische Prozesse und organisatorische Maßnahmen

Implementierte organisatorische Prozesse sind essenziell, um Angriffe im Unternehmen zu erkennen und alle notwenigen Aktionen im Zusammenhang damit einzuleiten. Dies betrifft zum Beispiel die Bewertung von Ereignissen sowie die anschließende Meldekette. Organisatorische Prozesse werden in Kapitel 6 beschrieben. Organisatorische Prozesse sind nicht zu verwechseln mit organisatorischen Maßnahmen, die ergänzend zu technischen Maßnahmen zur Angriffserkennung eingesetzt werden. Diese werden in Kapitel 5.2 beschrieben.

2 Begriffe und Definitionen

2.1 Was ist ein „Angriff“

Ein Angriff ist eine vorsätzliche Form der Gefährdung, nämlich eine unerwünschte oder unberechtigte Handlung mit dem Ziel, sich Vorteile zu verschaffen bzw. einen Dritten zu schädigen. Angreifer können auch im Auftrag von Dritten handeln, die sich Vorteile verschaffen wollen. Die Wirkung eines Angriffs äußert sich aus Betreibersicht zumeist als Abweichung vom gewünschten Anlagenbetrieb oder den Verlust des Know-hows.

2.2 Ungezielte Angriffe

Ungezielte Angriffe sind Angriffe, die kein spezifisches Ziel haben, sondern möglichst viele potenzielle Opfer erreichen sollen. Dies sind z.B. breit gestreute Phishing-E-Mails mit einer Schadsoftware im Anhang oder Links auf manipulierte Webseiten. Häufig werden in einzelnen Kampagnen tausende E-Mails versendet.

Auch ein Fehlverhalten von Mitarbeitenden kann Angriffe ermöglichen oder begünstigen. Beispiele für solch ein Fehlverhalten sind unbeabsichtigte Fehlkonfiguration oder das Öffnen von E-Mails mit Schadsoftware.

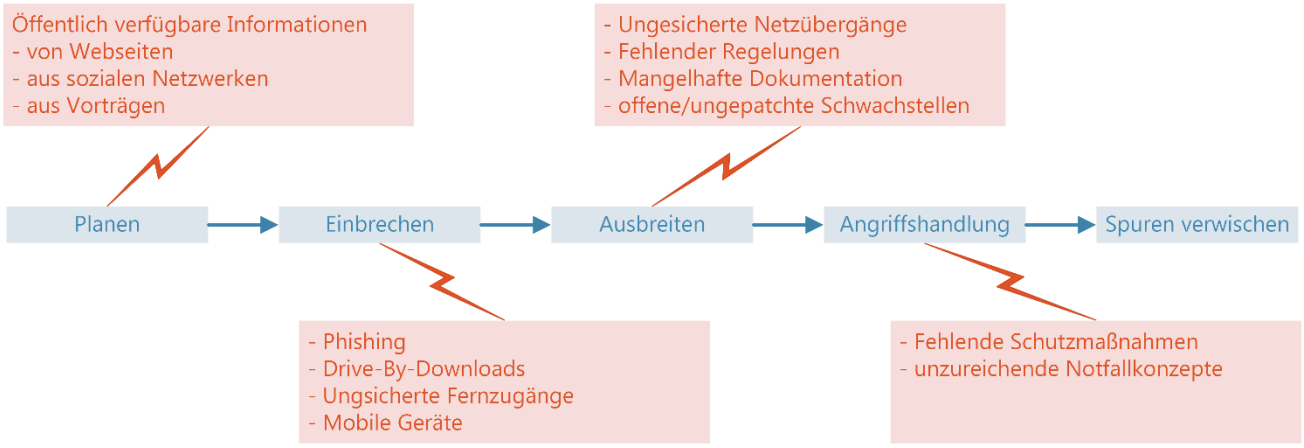
2.3 Gezielte Angriffe

Gezielte Angriffe haben spezifische Angriffsziele (bestimmte Branche, bestimmter Betreiber, bestimmte Systeme, etc.). Betreiber werden dabei häufig mit maßgeschneiderten Schadprogrammen angegriffen, die gegebenenfalls nicht zuverlässig von Virenschutzprogrammen erkannt werden. Z. B. werden Führungskräfte per Social Engineerings dazu verleitet, schädliche E-Mail-Anhänge zu öffnen. Auch die Personalabteilung einer Institution kann beispielsweise ein Angriffsziel sein, indem etwa mit Schadsoftware infizierte Bewerbungsunterlagen auf elektronischem Wege zugesendet werden. Eine ergiebige Quelle über Mitarbeiter sind soziale Netzwerke oder sonstige öffentlich verfügbare Informationen, z.B. von Lieferanten. Mit den gesammelten Informationen plant der Angreifer, wie er in das Unternehmen eindringt. Der eigentliche Angriff beginnt oft mit einer Phishing-E-Mail, die z.B. eine ausführbare Datei oder manipuliertes Office-Dokument enthält. Anschließend hat das Ausbreiten im Unternehmenssystem für den Angreifer oberste Priorität, bis er alle für ihn wichtigen Systeme infiltriert hat. Dazu wird er sicherstellen, dass die Schadsoftware auch nach einem Neustart funktioniert. Er wird zudem nach und nach seine Rechte und Zugriffsmöglichkeiten erweitern, sowie weitere Systeme kompromittieren.

Die Angriffshandlung eines gezielten Angriffs hängt von den Zielen des Angreifers ab. Sollte es dem Angreifer um das Ausspionieren oder Manipulieren von Informationen gehen, wird er die entsprechenden Systeme suchen und die für ihn relevanten Daten ausleiten oder verändern.

Bei einem Produktionssystem als Ziel, wird der Angreifer die Phasen vom Eindringen bis zur Schadaktion gegebenenfalls mehrfach durchlaufen müssen. Dies ist für den Angreifer notwendig, da die Produktionssysteme sich meist in separaten Netzwerkbereichen befinden. So wird der Angreifer beispielsweise zu Beginn nur auf einen Computer in der Verwaltung eindringen, um dann interne Informationen zu sammeln und den Einstieg in das Produktionsnetz zu planen. Hat er genug Informationen gesammelt, wird der nächste Angriff durchgeführt und in das Produktionsnetz eingedrungen. Dieses Vorgehen kann sich so lange wiederholen, bis er im Zielsystem seine Ziele in die Tat umsetzen kann.

Um eine Entdeckung zu vermeiden bzw. ein Identifizieren zu verhindern, wird der Angreifer versuchen seine Spuren zu verwischen. Dies erfolgt häufig bereits während des Angriffs. Es kann aber auch sein, dass der Angreifer als letzten Schritt alle Daten auf den kompromittierten Systemen löscht.



2.4 APT

APT steht für advanced persistent threat und bezeichnet einen komplexen und gezielten Angriff, der mit erheblichen finanziellen und technischen Ressourcen durchgeführt werden kann. Da die Angriffe mit erhebliche technische Fähigkeiten auf Seiten der Angreifer erfolgen, sind sie entsprechend schwer zu detektieren.

2.5 Was sind „Systeme zur Angriffserkennung“

Gemäß der BSI-Veröffentlichung *Orientierungshilfe zum Einsatz von Systemen zur Angriffserkennung inklusive Formulare für den Nachweis zu § 8a (1a) BSIG und § 11 (1d) ENWG* ergeben sich im Hinblick auf die Funktionalität von SzA die wesentlichen Aufgabenbereiche Protokollierung, Detektion und Reaktion.

- Die Systeme müssen durch fortlaufende Auswertung der gesammelten Informationen (Protokollierung) sicherheitsrelevante Ereignisse erkennen (Detektion). Diese Aufgaben können beispielsweise durch Missbrauchserkennung oder Anomalie-Erkennung erfolgen.
- Die Systeme zur Angriffserkennung sollten Maßnahmen implementieren, um Störungen infolge von Angriffen zu verhindern oder auf sie zu reagieren (Reaktion). Dies kann sowohl durch technische als auch durch organisatorische Maßnahmen umgesetzt werden.

3 Umfang der Angriffserkennung („risikobasierter Ansatz“)

Bevor eine Angriffserkennung etabliert werden kann, muss deren erforderliche Art und Umfang bestimmt werden. Als Basis-Informationsquellen für technische Werkzeuge zur Angriffserkennung dienen dabei unter anderem aktives Netzwerkmonitoring, Events und Logfiles der Systeme. Es ist risikobasiert zu prüfen, welche Assets in welchem Umfang aktiv Informationen an eine zentrale Melde- und Auswerteinstanz (engl. Security Information and Event Monitoring, SIEM) senden sollten. Bei Systemen, die bisher nicht oder wenig vernetzt sind, ist das erhöhte Risiko neuer/zusätzlicher Netzwerkverbindungen zu beurteilen und die Risiken ggf. durch passives Netzwerkmonitoring zu behandeln.
Die KRITIS-Kernkomponenten bilden bei der Risikoanalyse, aus Sicht der Verfügbarkeit, das Prozessleitsystem und das Safetysystem. Dem aus betrieblicher Sicht gleichzusetzen sind (aus Sicht der Vertraulichkeit) die (streng) vertraulichen Daten (z.B. Rezepte). Weitere kritische Systemteile können sich aus der Einzelfallbetrachtung ergeben.

Die Evaluierung für die Angriffserkennung muss

A) die relevanten Angriffsvektoren identifizieren und
B) deren Detektion im Umfang als auch in der Tiefe (Sensitivität) definieren.
C) Bei der Auswahl geeigneter Detektionsmethoden ist zu berücksichtigen, dass diese keine negativen Auswirkungen auf bestehende Systeme nehmen dürfen.

Dabei zu beachten sind folgende Parameter:

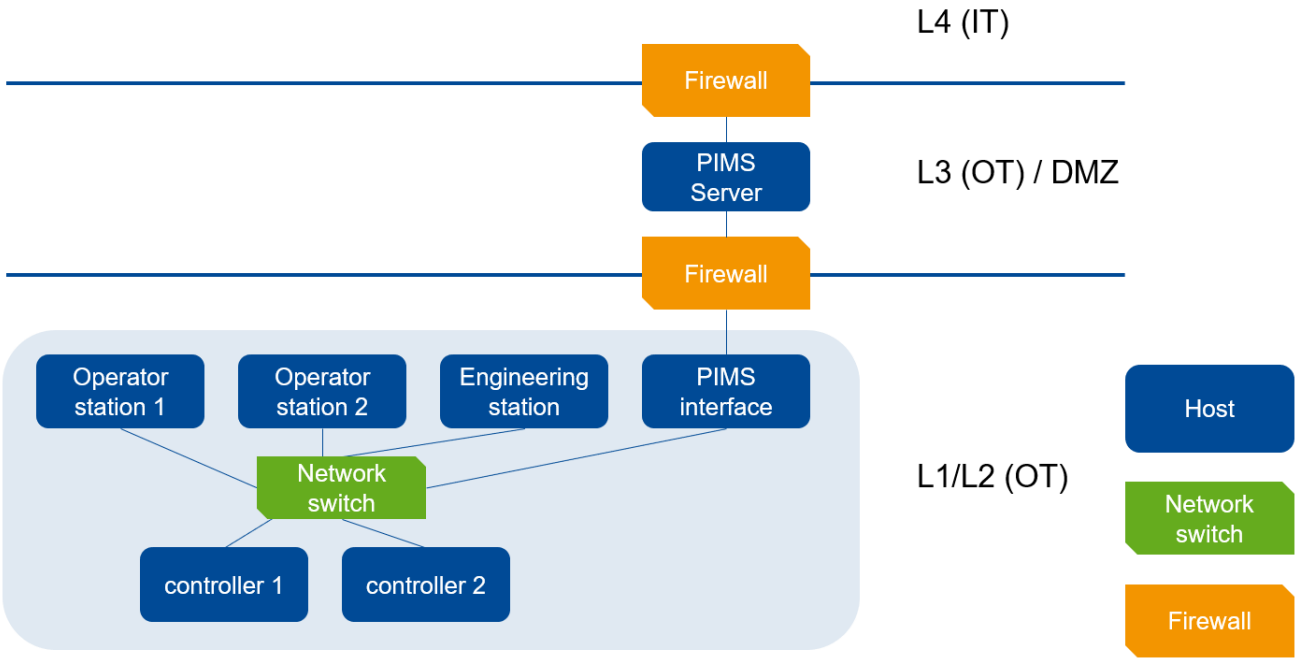
A) Wie können Angriffe erfolgen?

B) Wie und wo können die Angriffe unter Berücksichtigung der vorhanden Geräte- und Netzwerk-Infrastruktur sinnvoll und effizient erkannt werden?
C) Wie erfolgt eine Angriffserkennung in abgeschotteten Bereichen, wo Angriffe nur von innen (physisch) heraus erfolgen können?
D) Wie können Angriffserkennungssysteme angelernt, konfiguriert und betrieben werden, um möglichst wenige Fehlalarme (False Positives) zu erzeugen. Betriebsspezifische Situationen müssen Berücksichtigung finden, damit ein Ereignis (z.B. Veränderung des Programms) bewertet werden kann (in der Situation „Änderung“ oder „Engineering“ -> kein Angriff; im laufenden Betrieb: Angriff).

Hinweis zu Fehlalarmen: Fehlerhafte Konfigurationen können dazu führen, dass eingesetzte Detektionssysteme nicht ordnungsgemäß funktionieren. Ist beispielsweise die Alarmierung falsch eingestellt (z.B. falsch gewählter Schwellenwert), können vermehrt Fehlalarme (False Positives) auftreten. Die zuständigen Mitarbeiter können dann eventuell nicht mehr zwischen einem Fehlalarm und einem Security-relevanten Ereignis unterscheiden oder nehmen relevante Meldungen nicht schnell genug wahr. Dadurch bleiben möglicherweise Angriffe unerkannt. Ebenso steigt der Aufwand an, um die Menge der Meldungen auszuwerten.

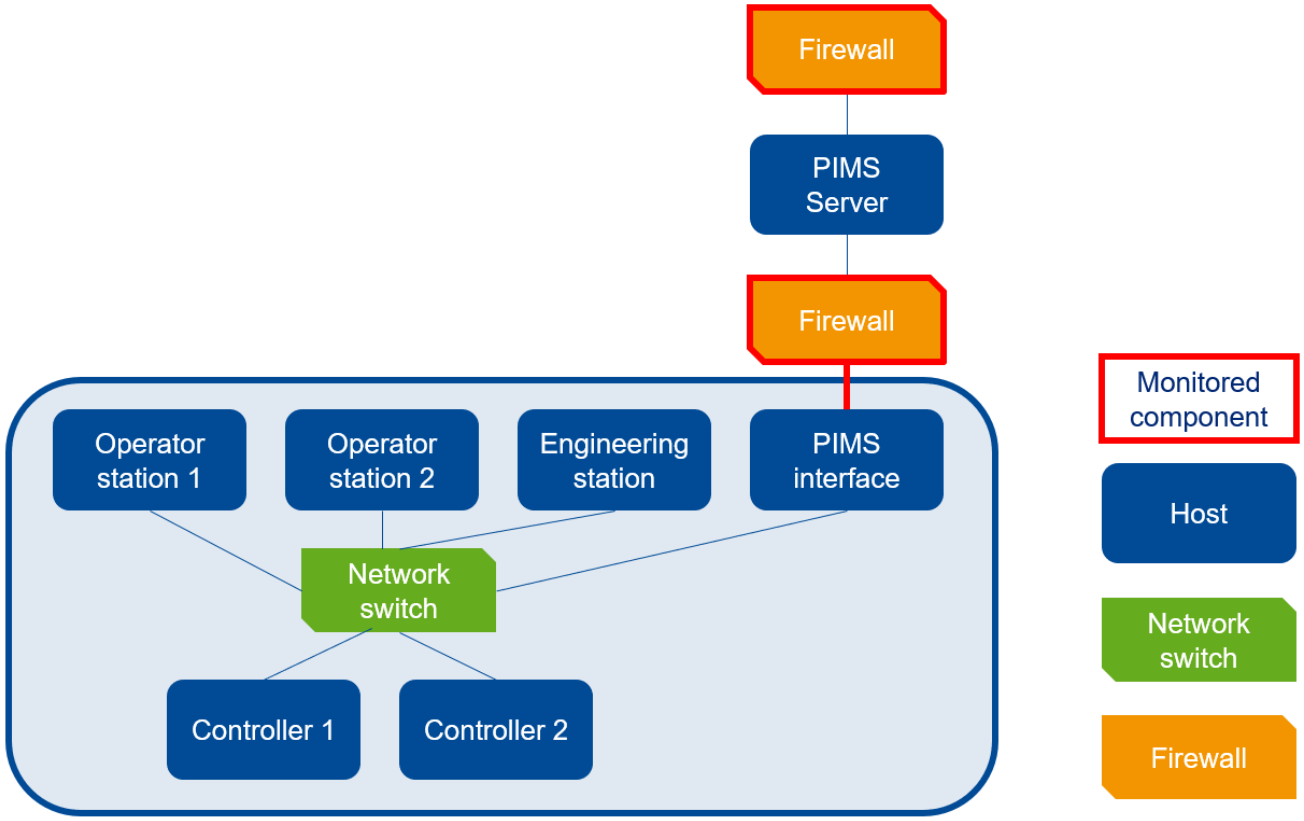
4 Methoden der Angriffserkennung

Von IT-Anbietern und Herstellern von Automatisierungstechnik werden zahlreiche Lösungen zur Angriffserkennung (oder Teillösungen dazu) angeboten. Der Einsatz von unterschiedlichen Komponenten (Teile einer Angriffserkennung) von unterschiedlichen Herstellern kann dabei in Bezug auf Schwachstellen wie auch der Erkennung sinnvoll sein. Nachfolgend wird anhand des Beispiels „Prozessleitsystem“ (PLS) eine Referenzstruktur eingeführt, um die verschiedenen Lösungsansätze dieser Angriffserkennungssysteme nach Methoden zu gruppieren. Dies bietet eine Orientierungshilfe und vereinfacht die Diskussion zum Stand der Technik. In der Praxis werden die Methoden teils kombiniert in Produkten eingesetzt.
Die beschriebenen Methoden fokussieren auf den Aspekt der Systembeobachtung (Informationsbeschaffung / Monitoring). Sie differenzieren also welche Systemkomponenten welche Daten und Informationen zur Angriffserkennung liefern. In der Beschreibung wird auch auf die Aspekte der Analyse / Verarbeitung dieser Daten und Informationen (Detection) und Alarmierung eingegangen. Außen vor bleiben organisatorische Prozesse wie Bewertung und Reaktion.



Vereinfachtes Strukturbild eines Prozessleitsystems (hellblau hinterlegt) in einer typischen Netzwerk-Levelarchitektur gemäß IEC 62443

4.1 Ingress-Egress Monitoring



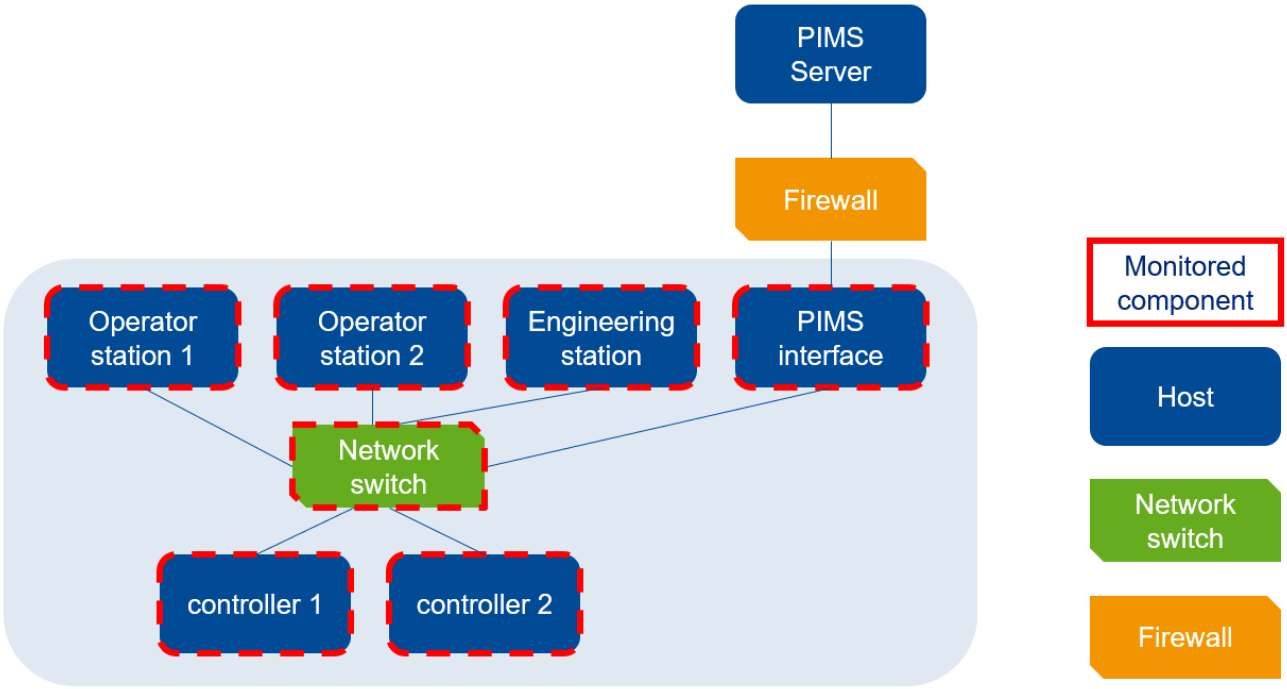
Automatisierungssysteme kommunizieren häufig nur wenig mit anderen Systemen über definierte Schnittstellen. Das Prozessleitsystem (PLS) kann folglich als „Zone“ und die Verbindung zu anderen Systemen, insbesondere die Verbindung in L3 Netze durch eine Firewall, als „Conduit“ aufgefasst werden (vgl. IEC 62443: Zones and Conduits). Viele Angriffe sind an diesem Conduit erkennbar, da Schadsoftware häufig versucht Daten nach außen zu senden (exfiltration) oder Daten von außen zu empfangen (z.B. Nachladen von Schadcode oder Befehlen vom „command & control“-Server). Eine striktes Whitelisting auf der Firewall in Verbindung mit einer DMZ-Struktur vorausgesetzt, werden diese Verbindungsversuche meist als geblockte Verbindungen erkennbar sein (da andere Protokolle und Hosts als in den freigeschalteten Regeln verwendet werden). Firewalls nach Stand der Technik sind immer in der Lage unzulässige Verbindungsversuche als Ereignis an überlagerte Systeme (Security Information and Event Monitoring, SIEM) weiterzuleiten (z.B. syslog forwarding). Moderne Firewalls (oft als „next generation firewalls“ vermarktet) haben darüberhinausgehende erweiterte Erkennungsmöglichkeiten (integrierte IDS/IPS Funktionalität).

Vorteilhaft ist bei der „Ingress-Egress“ Methode, dass die Erkennung bei Angriffen von außen nach innen während einer frühen Phase des Angriffs erfolgt und daher auch als präventive Maßnahmen genutzt werden kann. Falls mehrere PLS eine einzelne Firewall gemeinsam für die Kommunikation in die DMZ verwenden, kann die Angriffserkennung für mehrere PLS erfolgen, ohne dass Implementierungsaufwand pro PLS entsteht. Die Methode ist daher selbst in heterogenen Automatisierungslandschaften einheitlich umsetzbar. Sie ist zudem aus Sicht des PLS passiv, d.h. am PLS selbst müssen keine Änderungen vorgenommen werden (d.h. Umsetzung im Brownfield ist ohne Einschränkungen möglich, was ebenfalls ein Alleinstellungsmerkmal dieser Methode ist). Daraus ergibt sich unmittelbar der weitere Vorteil, dass keine Freigabe des PLS-Herstellers erforderlich ist, was insbesondere in heterogenen Systemlandschaften relevant ist. Die Qualität und Quantität der Information ist mittel. Nachteilig ist, dass Angriffe, die vollständig innerhalb des PLS erfolgen oder etablierte Verbindungen zur Kommunikation missbrauchen, prinzipiell nicht erkennbar sind.

Diese Methode erweitert den Schutz für alle Anlagentypen, insbesondere wenn sie mit fortschrittlicher Firewall-Technologie umgesetzt wird (Next-Gen-FW mit Application Layer Filtering, IDS/IPS-Funktionen und TI-Subskription). Insbesondere für die Erkennung von gezielten Angriffen sind darüber hinaus weitere technische

Maßnahmen zur Angriffserkennung innerhalb der Schutzzone (Kommunikation, Logfiles, Ereignisse, etc.) erforderlich.

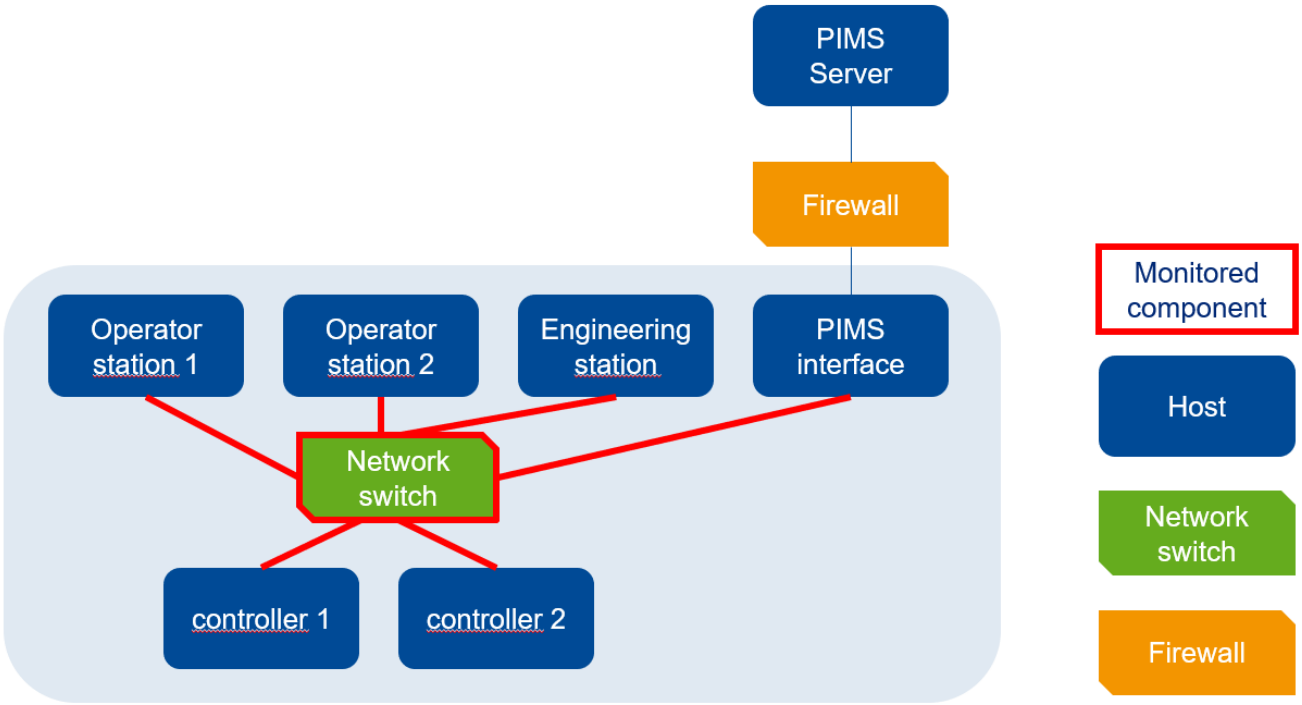
4.2 Lean Monitoring



Lean Monitoring ist eine kostengünstige Erkennungsmethode, die ohnehin im PLS vorhandene Logfiles und erhobene Ereignisse unter dem Aspekt Security zusammenführt. Dies ist deshalb möglich, weil zur Gewährleistung der Verfügbarkeit des PLS eine permanente Überwachung des Systemzustands (z.B. Netzwerklast) erfolgt. Darin sind typischerweise alle Systemkomponenten einbezogen. Darüber hinaus werden moderne PLS durch zahlreiche Securitymaßnahmen vor Angriffen geschützt. Diese primär zum Schutz eingesetzten Methoden (protective controls) lassen sich oft auch zur Erkennung (d.h. als detective controls) nutzen. Ein eingängiges Beispiel ist ein Virenscanner, der die Schadsoftware nicht nur erkennt und deren Ausführung verhindert, sondern den Fund auch an das „Lean Monitoring“ System im PLS meldet. Das Verfahren ähnelt daher dem Host-basierten Verfahren, ohne jedoch dessen Flexibilität und Erkennungstiefe zu erreichen.

Vorteilhaft an dieser Methode ist, dass der Herstellersupport gewährleistet und das Kosten-Nutzen-Verhältnis günstig ist, obwohl es dezentral umgesetzt werden muss. Die Qualität und Quantität der gewonnenen Informationen sind mittel. Die Methode ist bei Neuprojekten (Greenfield) leicht anwendbar, aber in Absprache mit dem Hersteller teils auch im Bestand (Brownfield) umsetzbar.

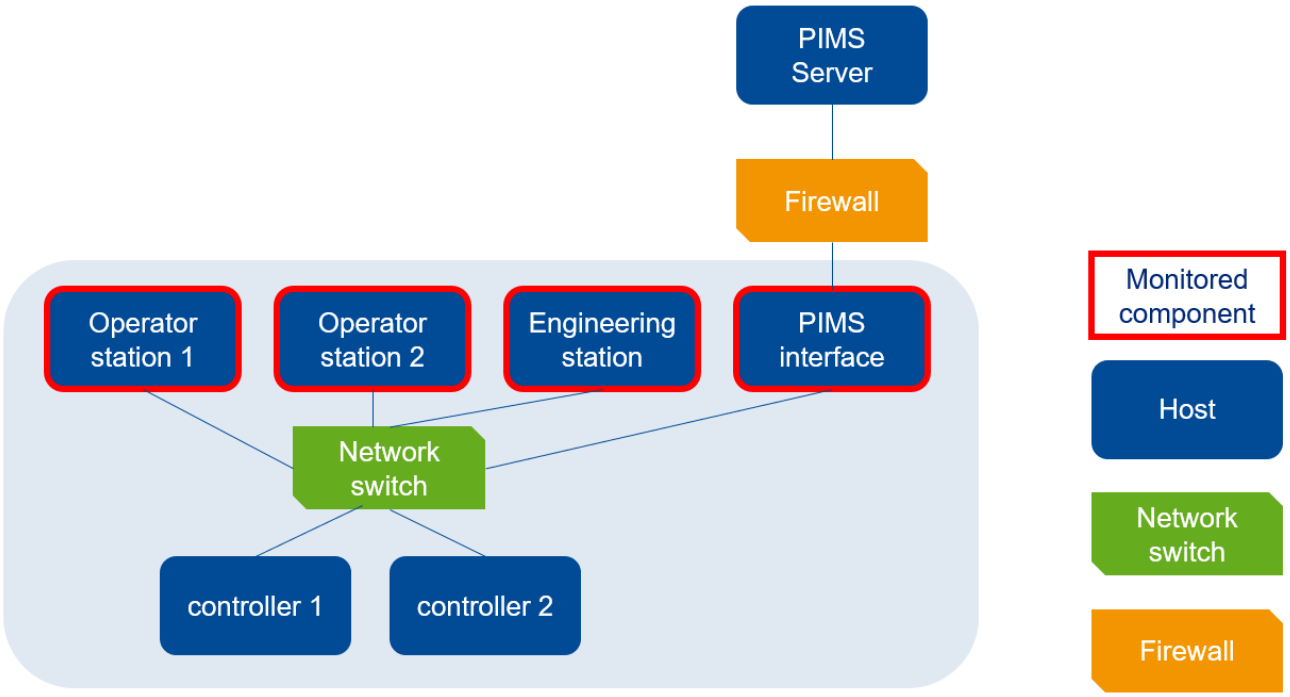
4.3 Network Based Monitoring



Die Netzwerkbasierte Erkennungsmethode beobachtet im Bereich des Angriffsziels den Netzwerkverkehr zwischen den einzelnen Komponenten des PLS. Dazu wird der Datenverkehr auf allen Ports der Netzwerkswitche an einen speziellen Port gespiegelt (mirror port /span port) und mit einem Monitoring-Gerät (teils „Sensor“ genannt) verbunden. Dieses Gerät wertet den Netzwerkverkehr aus, um Angriffe zu erkennen. Zur Angriffserkennung kommen verschiedene Strategien zum Einsatz. Die beiden häufigsten sind „musterbasiert“ und „anomaliebasiert“. Die musterbasierte Erkennung vergleicht den beobachteten Datenverkehr mit bekanntem Kommunikationsverhalten von Schadsoftware („signaturbasiert“ oder „verhaltensbasiert“ auf Basis von Indicators of Compromise (IoC)), wodurch einerseits nur bekannte Angriffe erkannt, andererseits praktisch keine Fehlalarme erzeugt werden. Die anomaliebasierte Erkennung nutzt aus, dass das Kommunikationsverhalten der PLS-Komponenten relativ statisch ist (d.h. es kommunizieren immer wieder die gleichen Komponenten mit den gleichen Protokollen). Es wird daher zunächst in einer (angriffsfreien) Lernphase der Datenverkehr beobachtet und ein akzeptiertes Kommunikationsverhalten abgeleitet (Baseline). Anschließend wird in der Erkennungsphase fortlaufend geprüft, ob der beobachtete Datenverkehr aus der Lernphase bekannt ist. Ist dies nicht der Fall, liegt eine Anomalie vor, die auf einen Angriff hindeuten kann. Voraussetzung für die Wirksamkeit dieser Methode ist, dass die Schadsoftware nicht bereits während der Lernphase aktiv ist (und als akzeptiertes Verhalten mitgelernt wird). Die Alarmierung kann lokal oder in einem SIEM erfolgen.

Vorteilhaft ist, dass diese Monitoringsysteme auch von den PLS-Herstellern selbst angeboten werden und dadurch vollen Support erhalten (was nicht der Fall ist, wenn die Systeme als Drittprodukt verwendet werden). Sie erzielen bei anomaliebasierter Erkennung eine gute Sichtbarkeit (d.h. viele Angriffe werden erkannt). Bei musterbasierter Erkennung ist die Sichtbarkeit eingeschränkt, da für die OT nur wenige Indicators of Compromise (IoC) vorliegen. Die Qualität der Informationen ist bei musterbasierter Erkennung sehr hoch. Bei anomaliebasierter Erkennung müssen die Ereignisse jedoch bewertet werden, ob tatsächlich ein Angriff vorliegt. Die anomaliebasierte Erkennung erzeugt insofern häufig Fehlalarme (false positives), die durch manuelles Anpassen der Baseline reduziert werden können. Eine Nachrüstung im Bestand (Brownfield) ist zu prüfen, weil dazu gegebenenfalls die Switche gegen leistungsfähigere Modelle getauscht werden müssen, was gegebenenfalls nur in Abstellungen möglich ist. Selbst bei geeigneten Switchen muss zumindest deren Konfiguration verändert werden, was im laufenden Betrieb ein potentielles Verfügbarkeitsrisiko darstellt. In Greefield-Anlagen ist die Methode uneingeschränkt nutzbar.

4.4 Host Based Monitoring



Die hostbasierte Erkennung nutzt vorhandene Quellen (Logfiles, Ereignisse, etc.) der Komponenten des PLS sowie teils zusätzliche Daten, die eigens zur Angriffserkennung durch Zusatzprogramme (agents) erhoben werden. Die Methode fokussiert dabei auf die PC und Server, nutzt aber meist auch Daten, die von Netzwerkinfrastrukturkomponenten zur Verfügung gestellt werden (z.B. SNMP traps). Je nach Erkennungstiefe sind für die Umsetzung dieser Methode Konfigurationsänderungen der Komponenten erforderlich, die bei Brownfield-Anlagen gegebenenfalls nur mit Rücksprache oder Einbeziehung des Herstellers möglich sind. Bei Neuprojekten (Greenfield) ist die Methode leichter umsetzbar und wird vielen PLS-Herstellern angeboten. Für die Analyse der erhobenen Daten existieren verschiedene Ansätze. Diese kann lokal im PLS oder zentral im SIEM (empfohlen) erfolgen. Als Erkennungsstrategie hat sich bewährt, vordefinierte Anwendungsfälle (use cases) zu beschreiben (z.B. fünf Ereignisse „fehlgeschlagener Login“ binnen einer Minute) und die dazu nötigen Daten zu übertragen.

Vorteilhaft ist bei dieser Methode, dass sie vom PLS-Hersteller umgesetzt wird und somit vollen Support erhält. Die Erkennung von use cases erzeugt wenige Fehlalarme und erzielt eine sehr hohe Qualität der Information. Da die Daten direkt an der Quelle (auf dem Host) erhoben werden, können prinzipiell sehr viele Daten erhoben werden und die Angriffserkennungsrate gesteigert werden. Die Methode ist in Neuprojekten leicht umzusetzen.

Nachteilig ist, dass die Auswahl der erhobenen Daten, d.h. die Definition der use cases, einen gewissen initialen Arbeitsaufwand darstellt. Host Based Monitoring erkennt einen Angriff typischerweise erst während einer späteren Angriffsphase. Host-basierte Lösungen können ggf. leichter vom Angreifer manipuliert oder angehalten werden.

A.1.1.1 Informationsquelle DNS-Resolver

Schadsoftware versucht in vielen Fällen zu einem „Command & Control-Server (C&C-Server)“ Kontakt aufzunehmen, um dorthin Daten über das infizierte Netzwerk zu übertragen oder von dort aktuelle Daten und Steuerbefehle zu erhalten. Beim Verbindungsaufbau versucht die Schadsoftware in der Regel den CNAME des Servers aufzulösen. Unter bestimmten Voraussetzungen kann dieses Verhalten einfach für die Angriffserkennung genutzt werden. Dazu muss auf dem DNS-Resolver ein DNS Query Logging und anschließend ein Log File Parsing (ggf. auf einem dedizierten Analysesystem) aktiviert werden. In diesem Prozess werden die DNS-Anfragen auf definierbare Muster von potenziell schädlichen bzw. unpassenden Domains durchsucht und bei einem Pattern-Matching alarmiert.

Um die Zahl der Fehlalarme gering zu halten, ist es hilfreich, dedizierte DNS-Resolver für OT-Systeme zu nutzen, deren Mustererkennung dann sehr restriktiv eingestellt werden kann. Diese Methode funktioniert auch dann, wenn durch Firewalls unterbunden wird, dass der C&C-Server tatsächlich erreicht wird.

A.1.1.2 Informationsquelle “Virenscanner” Denylisting

Unter Denylisting sind die traditionellen „Virenscanner“ zu verstehen. Virenscanner schützen vor bekannter Malware. Die verbreitete Einsatzerfahrung und Verfügbarkeit für Standard-Betriebssysteme, spricht für diese Maßnahme. Allerdings muss beim Einsatz beachtet werden, dass Virenscanner tief ins Betriebssystem eingreifen und für manche Systeme ein Performance- und Integritätsrisiko darstellen. Darüber hinaus benötigen Virenscanner Verbindungen, um aktuelle Virenpattern nachzuladen und ggf. Meldungen abzusetzen. Der dafür neu zu schaffende Informationsaustausch kann insbesondre bei vorher nicht vernetzten Geräten zu einer Verschlechterung der Gesamtsituation führen.

A.1.2 Informationsquelle Allowlisting / Whitelisting

Beim Allowlisting kann der Zugriff auf Dateien und Ausführung von Programen auf explizit erlaubtes Maß (die Allowlist) beschränkt werden. Diese Maßnahme wird einerseits durch Betriebssysteme selbst bereitgestellt und kann andererseits durch zusätzliche Applikationen realisiert werden. Die Maßnahme ist zunächst eigentlich eine Schutzmaßnahme kann jedoch in Verbindung mit Protokollaufzeichnung und optionalen Meldungsweiterleitung im Falle von nicht erlaubten Zugriffen zu einer effizienten Erkennungsmaßnahme erweitert werden.

HINWEIS:

Neben den klassischen Anforderungen (Social Engineering, Schwachstellen, Konfigurationsfehler etc.)

wollten wir nur einige typische Anforderungen auch etwas genauer darstellen.

5 Meldungsweiterleitung

Das Vorgängerkapitel geht primär auf die Erkennung von Angriffen ein. Die Meldung über erkannte Angriffe kann über eine zentrale Meldeinstanz (SIEM) oder beispielsweise, bei entsprechend geringerer Kritikalität, durch eine E-Mail-Benachrichtigung gewährleistet werden.

Zu beachten ist bei der Meldungsweiterleitung, dass durch das Herstellen einer neuen Verbindung nicht zusätzliche Angriffsfläche geschaffen wird, Dies könnte im Falle von alten, verwundbaren, nicht vernetzten Systemen zu einer Verschlechterung der Gesamtsicherheitslage führen.

5.1.1 E-Mail-Benachrichtigungen

Auch Unternehmen ohne eigenes zentrales Ereignismanagementsystem können auf detektierte Angriffe reagieren. Es ist möglich, dass die Detektionstools eine Alarmierung per E-Mail-Verteiler senden. Diese Verfahrensweise sollte folgende Merkmale aufweisen:

- Eine aktive Verwaltung der Zieladressen muss sicherstellen, dass alle Empfänger benannt und dokumentiert sind, und dass die Mailadressen existent sind.
- Keine vertraulichen Inhalte im Mail-Content oder starke Verschlüsselung
- Der Mailversand muss im Detektionstool protokolliert werden
- Es ist sinnvoll, die korrekte Funktion regelmäßig zu testen

A.1.2.1 Potenzialfreier Meldekontakt

Bei streng gekapselten Anlagen ist eine Meldungsweiterleitung über potenzialfreie Meldekontakte in Betracht zu ziehen. Nachteilig ist der geringe Informationsgehalt des Meldeweges.

5.2 Organisatorische Maßnahmen

Abhängig von der Risikobewertung kann die Meldungsweiterleitung gegebenenfalls durch organisatorische Maßnahmen ergänzt werden. Beispiele hierfür sind:

- manuelle Durchsicht von Logfiles, um Auffälligkeiten zu identifizieren
- manuelle Registrierung von lokal erkannten Angriffen in den zentralen Meldesystemen des Unternehmens.

6 Die Rolle des Herstellers

Hersteller von Komponenten und Systemen sowie Integratoren spielen eine wesentliche Rolle im Zusammenhang mit OT-Security und auch im Zusammenhang mit Angriffserkennung.

Hersteller und Integratoren sollten hinsichtlich der OT-Security Ihrer Produkte und Dienstleistungen den Stand der Technik einhalten und auch in der Lage sein dies nachzuweisen. Entsprechende Prozesse müssen dort implementiert und überwacht werden. Diese Prozesse sollen sicherstellen, dass der Hersteller:

a) Security by Design“ und “Security by Default” liefert. Das bedeutet im Zusammenhang mit diesem Papier beispielsweise, dass Erkennungswerkzeuge (z.B. Logfiles) im Auslieferungszustand „aktiviert“ sind
b) Angriffserkennung als inhärenten Systembestandteil (als Systemalarm) versteht und entsprechend die Informationen in einem Log-Collector sammelt und die Fähigkeit zur Weiterleitung über herstellerneutrale Schnittstellen an ein SIEM bereitstellt.
c) eine vollständige Kommunikationsmatrix bereitstellt, in der er erklärt und dokumentiert was als normaler Datenverkehr einer Komponente / eines Systems zu bewerten ist
d) die Benachrichtigung über Schwachstellen und deren Behebung (Advisories) zeitnah und mit Bezug auf CVE zur Verfügung stellt. Maschinenlesbarkeit nach –aktuell- CSAF 2.0 ist von Vorteil.
e) „Indicators of Compromise“ (IoC) zeitnah zu deren Bekanntwerden zur Verfügung stellt
f) Ein qualifiziertes Product Security Incident Response Team (PSIRT) unterhält und ein Kontakt dorthin zur Verfügung steht.
g) Die Fähigkeiten bereithält, erkannte Abweichungen vom Normalzustand (Anomalie) analysieren, bewerten, beurteilen und an Anwender kommunizieren zu können.

7 Organisatorische Prozess

7.1 Sicherheitsrichtlinie für die Detektion von Security-relevanten Ereignis

Ausgehend von der allgemeinen Sicherheitsrichtlinie der Institution sollte eine spezifische Sicherheitsrichtlinie für die Detektion von Security-relevanten Ereignissen erstellt werden. In der spezifischen Sicherheitsrichtlinie sollten nachvollziehbare Anforderungen und Vorgaben beschrieben werden, wie die Detektion von sicherheitsrelevanten Ereignissen geplant, aufgebaut und sicher betrieben werden kann. Die spezifische Sicherheitsrichtlinie sollte allen im Bereich Detektion zuständigen Mitarbeitern bekannt und grundlegend für ihre Arbeit sein. Falls die spezifische Sicherheitsrichtlinie verändert wird oder von den Anforderungen abgewichen wird, dann muss dies mit dem verantwortlichen ISB abgestimmt und dokumentiert werden. Es sollte regelmäßig überprüft werden, ob die spezifische Sicherheitsrichtlinie noch korrekt umgesetzt ist. Die Ergebnisse der Überprüfung sollten sinnvoll dokumentiert werden.

7.2 Detektion / Konfiguration

Bei der Auswahl und dem Einsatz von Detektionsmaßnahmen sollte eine größtmögliche Abdeckung der Bedrohungslandschaft erzielt werden. Dazu müssen die Ergebnisse der Risikoanalyse sowie die Größe und Struktur des Unternehmens in der Planung einbezogen werden. Zur Bestimmung der Abdeckung kann eine standardisierte Methode angewendet werden (z.B. MITRE ATT&CK). In Abhängigkeit der Unternehmensgröße und der Bedrohungslandschaft kann eine separate Betrachtung von Detektionsmaßnahmen für die IT- und OT-Umgebung erforderlich sein.

Damit die Daten korreliert und abgeglichen werden können, müssen alle Systeme zur Angriffskennung (Minimum) zeitlich synchronisiert werden. Die gesammelten Ereignismeldungen sollten regelmäßig auf Auffälligkeiten kontrolliert werden. Damit sicherheitsrelevante Ereignisse auch nachträglich erkannt werden können, müssen die Signaturen der Detektionssysteme immer aktuell und auf dem gleichen Stand sein.

Bei der Umsetzung von Detektionsmechanismen sollte initial eine Konfiguration durchgeführt werden, um festzustellen, welche Security-relevanten Ereignisse im Normalzustand auftreten (Baselining). Dies kann in Greenfieldanlagen oder in Testanlagen am einfachsten umgesetzt werden. Dazu sollte bewertet werden, ob dieser Normalzustand hingenommen werden kann oder ob Änderungen vorzunehmen sind. Die Konfiguration sollte bei Änderungen innerhalb des Geltungsbereichs oder der Bedrohungslage erneut durchgeführt werden.

Die Planung und Umsetzung der Detektion müssen in geeigneter Form dokumentiert werden. Der Abstraktions- und Detailgrad ist dabei so zu wählen, dass der effektive Einsatz der Detektionssysteme bewertet werden kann. Die Dokumentation dient im Reaktionsprozess gleichzeitig zum schnellen Einarbeiten externer Dienstleister.

Die Security-relevanten Ereignisse müssen überprüft und dahingehend bewertet werden, ob sie auf einen Sicherheitsvorfall (qualifizierter Security-relevanten Ereignis) hindeuten. Die zur Angriffserkennung eingesetzten Systeme sollten, in eindeutig zuordenbaren Fällen, eine automatisierte Qualifizierung der Security-relevanten Ereignis ermöglichen.

7.3 Organisatorische Aspekte

Um eine erfolgreiche Angriffserkennung in einem Unternehmen zu etablieren muss, wenn diese innerhalb des Unternehmens erbracht werden soll, zunächst eine effektive Security Managementstruktur (ISMS) geschaffen werden. Dabei müssen die Verantwortlichkeiten innerhalb der Struktur und auch die Meldewege zu Behörden und internen Parteien (z.B. Konzernkrisenstab) klar geregelt werden. Gleichzeitig muss ein Regelwerk geschaffen werden, das diese Rollen und die Meldewege im Ereignisfall beschreibt.

Der Aufbau der Organisation kann den Empfehlungen der ISO27001 Reihe, der IEC 62443 2-1 oder dem IT-Grundschutz folgen oder an diese angelehnt sein. Nachfolgend sind wichtige Rollen kurz beschrieben. Details finden sich in den genannten Referenzen.

Firmenleitung

Die Firmenleitung trägt die strategische Verantwortung für die Sicherheit und die Risikoentscheidungen und ist für die Einführung und kontinuierliche Verbesserung des ISMS verantwortlich. Oft werden strategischen Verantwortlichkeiten an die nächste Organisationsebene delegiert.

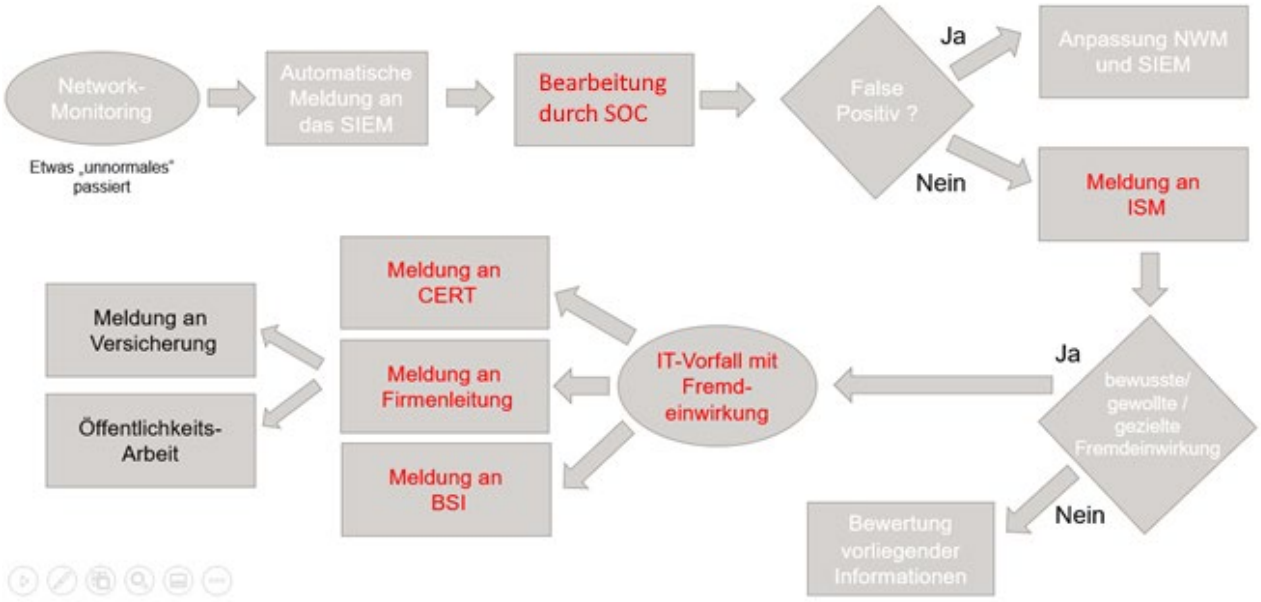
Informationssicherheits-Manager (CISO, CISM)
Der Informationssicherheits-Manager ist für die Prozesse und die Organisation des ISMS verantwortlich. Er steuert und überwacht die Maßnahmen und ist für das Risikomanagement (z.B. Bereitstellung eines Bedrohungskatalogs) und verbundene Compliance-Themen zuständig. Meldungen an Behörden und das CERT werden normalerweise von ihm initiiert.

Informationssicherheits-Beauftragter (ISB, IT-SiBe)
Der Informationssicherheits-Beauftragte setzt die Vorgaben operativ um. Er übernimmt dabei die zentrale Rolle, um die ISMS Vorgaben in den einzelnen Bereichen bekannt zu machen und meldet mögliche Ereignisse an den Informationssicherheits-Manager.

In kleineren Unternehmen können die Rollen des Informationssicherheits-Managers und -Beauftragen von der gleichen Person übernommen werden. In großen Konzernen können weitere Rollen oder mehrere Manager und Beauftragte eingesetzt werden.

Cyber Defense Team / CERT
Zusätzlich zu diesen Rollen wird ein Cyber Defense Team (für einen CERT Service) benötigt. Dieses Team dient als Ansprechpartner im Ereignisfall und muss über entsprechendes OT Kenntnisse verfügen, um Angriffen (z.B. auf Leitsysteme oder Safety-Systeme) fachgerecht begegnen zu können und die notwendigen Gegenmaßnahmen zu ergreifen.
Dabei ist zu beachten, dass die Etablierung eines eigenen CDT insbesondere in großen Konzernen sinnvoll ist. Mittlere und kleine Unternehmen können diesen Service extern erbringen lassen.

Mit den beschriebenen Rollen kann ein organisatorischer Prozess für den Ereignisfall wie folgt aussehen:



Lebenszyklus
Bei der Auswahl und Betrieb der Methoden zur Angriffserkennung ist der Lebenszyklus der überwachten Systeme zu berücksichtigen. Damit die Angriffserkennung dauerhaft wirksam bleibt, müssen Methoden und/oder Prozesse ggf. an neue Erfordernisse oder Bedrohungen anpasst werden.

Die Phasen „Planung" und „Außerbetriebnahme", welche in diesem Dokument nicht beschrieben sind, müssen dennoch berücksichtigt werden. Insbesondere in der Planungsphase sollten die Ergebnisse der Risikoanalyse sowie die Größe und Struktur des Unternehmens einbezogen werden, um Zeitpunkte und Reihenfolge der Umsetzung der Maßnahmen angemessen zu gestalten.