STORMSHIELD

DPI-Systeme und Netzwerk-sicherheit

Eindringungsschutz mit Stateful DPI in OT-Umgebungen

Kurzfassung

Die Segmentierung von OT-Netzwerken gilt heute als erste Verteidigungslinie im Kampf gegen Cyberangriffe. Zur wirksamen Abwehr neuer und immer ausgefeilterer Bedrohungen sind jedoch Lösungen erforderlich, die Tiefenanalysen (DPI, *Deep Packet Inspection*) ausgetauschter Nachrichten durchführen und sensible Netzwerke auf diese Weise schützen können.

Um die Herausforderungen der OT bewältigen zu können, müssen die implementierten Sicherheitslösungen in Bezug auf **Verfügbarkeit, Integrität und Vertraulichkeit** strenge Vorgaben erfüllen, die sich aus den operativen Anforderungen an OT-Netzwerke ergeben.

Bei der Implementierung eines Systems für Eindringungsschutz (IPS, *Intrusion Prevention System*), das eng mit Automatisierungssystemen zusammenarbeitet, müssen diese Aspekte berücksichtigt werden, um proaktive und nachhaltige Sicherheitsrichtlinien zu etablieren und die Zuverlässigkeit der OT-Netzwerke zu gewährleisten.

Der Schwerpunkt sollte bei diesen vier Bereichen liegen:

- Eine **integrierte Lösung**, die Industrieprotokolle genau analysieren kann
- Die **Möglichkeit, die Konformität von Betriebsmeldungen zu prüfen**, um Anomalien besser erkennen und die Komponenten im OT-Netzwerk schützen zu können
- **Proaktiver Schutz vor verschiedenen Bedrohungen**, um Cyberangriffe abzuwehren und Produktionsausfälle zu vermeiden
- **Kontextbasierter Ansatz für den Meldungsaustausch,** um die Konformität der operativen Prozesse zu gewährleisten

Dieses Whitepaper beschreibt die verschiedenen Funktionen, die IPS-Lösungen bieten müssen, um Bedrohungen zuverlässig erkennen und abwehren zu können. Außerdem werden die Elemente genannt, die IPS-Lösungen integrieren müssen, damit sie sich perfekt an Ihre Sicherheitsanforderungen anpassen lassen.

Dieses Whitepaper richtet sich an Betriebsleiter, an Wartungsleiter für Anlagen und Prozesse mit Verantwortung für kritische Infrastrukturen sowie an Sicherheitsverantwortliche für IT-Systeme.

Stormshield

Überall auf der Welt müssen Unternehmen, Regierungseinrichtungen und Verteidigungsbündnisse auf verlässliche Partner vertrauen, die ihre digitale Transformation begleiten und die Cybersicherheit ihrer Infrastrukturen, Benutzer und Daten sicherstellen. Die Technologien von Stormshield sind nach den höchsten europäischen Normen zertifiziert (EU Restricted, NATO Restricted, Common Criteria EAL3+/EAL4+, ANSSI-Qualifikationen und -Visa) und erfüllen die Anforderungen für IT und OT zum Schutz Ihrer Tätigkeiten. Dank unserer Sicherheitslösungen können Sie sich wieder voll auf Ihr Geschäft konzentrieren.

Inhalt

1. Kontext
2. Cyberrisiken in OT-Netzwerken
3. Abwehrsysteme: Netzwerksensor oder IPS?
4. Grundlegendes zu Eindringungsschutzsystemen (IPS, Intrusion Prevention System)

   Signatur oder gezielte Protokollsuche: zwei Ansätze für die Konformitätskontrolle der Protokolle

   Kontextbasierte Analyse als Herzstück des sicheren Datenaustausches

   Suche nach Bedrohungen beim Datenaustausch im Netzwerk

   Notwendigkeit selbst generierter Signaturen

5. Kriterien für die Wahl der richtigen IPS-Lösung
6. Die Stormshield-Engine *Stateful DPI*

Kontext

Cyberangriffe gegen operative Infrastrukturen werden immer ausgefeilter. Sie erfolgen in mehreren Stufen, verbreiten sich virusartig und werden von den verschiedenen Sicherheitssystemen nur schwer erkannt. Bei *Advanced Persistent Threats* (APT) handelt es sich um Cyberangriffe, die mehrere strategisch kombinierte Techniken und Methoden nutzen, um ein genau definiertes Ziel zu erreichen. Dabei geht es meist um die Exfiltration hochwertiger Daten wie Patente und Geschäftsgeheimnisse. Um keinen Verdacht zu wecken, bleiben sie dabei möglichst lange unter dem Radar.

Die meisten Unternehmen und Organisationen sind der Meinung, hinreichend für Cyberrisiken und deren Folgen (Datenverlust oder -diebstahl, Produktionsunterbrechungen usw.) sensibilisiert zu sein. In Wirklichkeit ist die Gefahr jedoch größer als sie denken. Seit dem Aufkommen des industriellen Internet der Dinge (IIoT, Industrial Internet of Things) in den letzten Jahren richten sich Cyberangriffe gezielt gegen Unternehmen in Branchen wie Luftfahrt, Kernenergie, Elektrizität, Gesundheit usw. Mit anderen Worten: Bei den bevorzugten Zielen handelt es sich um die Betreiber kritischer Infrastrukturen.

In einigen Fällen kennen diese Betreiber die Schwachstellen in ihren Systemen, verfügen aber nicht über die Möglichkeiten, um die betroffenen Anwendungen bzw. Anlagen auszutauschen. Besonders häufig betrifft das operative und kritische Netzwerke (z. B. im Gesundheitswesen), in denen häufig Anwendungen laufen, die nur von veralteten Betriebssystemen unterstützt werden. In der Industrie werden oft veraltete Netzwerkkomponenten weiter genutzt, was die Gefahr von Angriffen vergrößert, die bereits vor längerer Zeit unbemerkt eingeschleust wurden. Eine Untersuchung vom November 2019[1] zeigt, dass bestimmte Schwachstellen und Bedrohungen bereits seit mehr als zehn Jahren von Hackern genutzt werden und bis heute aktuell sind.

> Die Herausforderung besteht in der Entwicklung einer Architektur, die die Übertragung, Verarbeitung und **Gewährleistung der Datenintegrität** zwischen Systemen ermöglicht.
>
> Cigref

Cybersicherheit für die Industrie ist jedoch eine relativ neue Disziplin. Erfahrungen aus der Welt der IT[2], zum Beispiel in Form von Risikoanalysen, sind mit einigen Anpassungen hilfreich, um angemessen und wirksam reagieren zu können.

Dieses Whitepaper beschreibt und analysiert Netzwerkschutzmethoden wie IPS sowie die Herausforderungen beim Schutz von OT-Netzwerken.

[1] Stormshield, www.stormshield.com/de/news/welche-tendenzen-zeichnen-sich-fuer-die-cybersicherheit-2020-ab

[2] Stormshield, www.stormshield.com/de/news/it-ot-netzwerke-grunde-fur-eine-schwierige-konvergenz

Cyberrisiken in OT-Netzwerken

In den letzten Jahren hat die digitale Transformation, die durch die Konvergenz der IT/OT-Netzwerke – sowie den Einsatz von Edge/Cloud Computing[3] – geprägt wurde, in Industrieunternehmen aller Größen die Konnektivität der Unternehmensnetzwerke verstärkt. Projekte für **Operational Excellence** in Verbindung mit Industrie 4.0 (wie die fortschreitende Optimierung zwischen Produktionskette und ERP) machen die OT-Netzwerke immer durchlässiger für Cyberangriffe.

Erst kürzlich machte der EKANS-Angriff (oder Snake) **(erneut) die Gefahren deutlich**, die erfolgreiche Eindringungen in industrielle Netzwerke mit sich bringen. Verschiedene Faktoren können das Risiko solcher Angriffe noch erhöhen. Dazu gehören die fehlende Vereinheitlichung zwischen Geräten und Steuerungen sowie industrielle Komponenten, für die unterschiedliche Normen bzw. Anforderungen gelten. Wenn sich diese Elemente in der gleichen Umgebung befinden, kann dies zu Störungen bis hin zum Absturz des gesamten Systems führen.[4]

Fest steht, dass die Hacking-Möglichkeiten zunehmen, sobald zuvor getrennte Systeme und Geräte an das OT-Netzwerk angeschlossen werden. Das kann zu schwerwiegenden Problemen wie physischen Schäden, Produktionsunterbrechungen oder sogar Diebstahl industrieller Fertigungsprozesse führen.

Mit der zunehmenden IT/OT-Konvergenz beginnen viele Unternehmen, globale Governance ihrer Anlagen einzuführen, um einen besseren Einblick in ihre OT-Netzwerke zu erhalten. Ein ausreichendes Verständnis der Probleme der industriellen Cybersicherheit zu erhalten, **müssen die IT- und die OT-Welten daher kommunizieren, sodass Risiken analysiert sowie bewertet und effektive Verwaltungs- und Managementprozesse für die Netzwerksicherheit implementiert werden können.**

[3] Forbes, www.forbes.com/sites/ronshevlin/2020/08/17/cloud-computing-raises-new-cybersecurity-concerns-for-banking/#5f46307f24ae

[4] Stormshield, www.stormshield.com/de/news/das-verarbeitende-gewerbe-wird-von-cyberbedrohungen-auf-die-probe-gestellt

Vincent Riondet, Leiter des Teams für Cybersicherheits-projekte und -Services bei Schneider Electric France wies in einem früheren Bericht darauf hin, dass in den meisten Industrieunternehmen „*mehr oder weniger alte Infrastrukturen neben mehr oder weniger neuen Netzwerkarchitekturen und Betriebssystemen vorhanden eingesetzt werden, wobei das Ergebnis nicht zwangsläufig die neuesten Sicherheitsstandards erfüllt, da Änderungen viel Geld kosten*“.

Der Einsatz mehrerer Schutzmaßnahmen wie Segmentierung, Flusskontrolle, Eindringungserkennung oder -schutz kann sich als überaus hilfreich erweisen, um Bedrohungen aus dem Netzwerkverkehr abzuwehren. Auch Zugangskontrollen, bei denen einfach nur bestimmte Kommunikationsprotokolle (an einem Port) zugelassen oder blockiert werden, reichen nicht mehr aus. Vielmehr müssen auch Befehle untersucht werden, die über zulässige Branchenprotokolle gesendet werden.

Für die Sicherheit der Netzwerkarchitektur sind daher Schutzmaßnahmen erforderlich, die zudem kontinuierlich auf dem aktuellen Stand gehalten werden müssen, um Datenverluste und Störungen der operativen Prozesse zu verhindern. Das Ziel muss darin bestehen, Cyberangriffe, die jederzeit vorkommen können, besser abzuwehren. **Daher müssen proaktive Schutzsysteme so nah wie möglich an den kritischen Infrastrukturen implementiert werden.**

Abwehrsysteme: Netzwerksensor oder IPS?

Die Überwachung der industriellen Infrastruktur ist ohne Frage unverzichtbar. Es gibt es jedoch keine einheitliche technische Bewertungsmatrix, die sich für alle OT-Architekturen anwenden lässt. Eine der Fragen lautet: **Wer verarbeitet generierte Alarme und wie?** Über die rein technischen Aspekte hinaus erfordert die Implementierung eines Netzwerksensors **ein geschultes Betriebsteam**, das in der Lage ist, **große Datenmengen** zu verwalten und zu analysieren, um kritische Ereignisse zu erkennen und mögliche Sicherheitsprobleme bei Bedarf an die zuständigen Stellen zu melden.

Diese Lösungen können sich zwar ergänzen, doch die Entscheidung zwischen einem Netzwerksensor und einer IPS-Lösung muss stets auf mehreren Parametern basieren, die mit Ihren individuellen Anforderungen abgestimmt sind. Dies erfordert eine detaillierte Untersuchung Ihrer gesamten OT-Netzwerkarchitektur. **Bestimmen Sie den erforderlichen Schutz für jedes Element, indem Sie seine jeweilige Bedeutung einschätzen.** Behalten Sie dabei Ihre Anforderungen im Blick.

Ebenso wichtig sind Überlegungen dazu, wie Ihre neue Lösung in Ihre globale Cybersicherheitspolitik, in Ihre aktuellen und künftigen Prozesse sowie Abläufe integriert werden soll.

WUSSTEN SIE SCHON?

IPS-Lösungen bieten oft die gleichen IDS-Funktionen (*Intrusion Detection System*, Eindringungserkennung) wie Netzwerksensoren. Ihre Identifizierungsmöglichkeiten nicht so effektiv wie bei Sensoren, dennoch gewährleisten IDS-Lösungen die zuverlässige Erkennung der Datenflüsse innerhalb der Anlagen.

Es wird empfohlen, das **IPS schrittweise, nach einer vorausgegangenen Analyse des Netzwerkverkehrs mit IDS, einzuführen**. In dieser Vorbereitungsphase werden die Datenströme zugeordnet und mögliche Falsch-Positive erkannt, bevor der aktive Eindringungsschutz zur Abwehr böswilliger Datenflüsse gestartet wird.

Ein Netzwerksensor ist ein **passives** Tool, das potenziell schädliche Datenflüsse im Netzwerk **erkennt**		**Ein Eindringungsschutzsystem (IPS)** ist ein **aktiver** Schutzmechanismus, der potenziell schädliche Datenflüsse im Netzwerk **erkennt** und **blockiert**
• Blockiert keine Datenpakete im Netzwerk	VS	• Blockiert verdächtige Datenpakete im Netzwerk
• Benötigt menschliche Unterstützung bei der Verarbeitung von Vorfällen	VS	• Kann ausgelöste Alarme eigenständig verarbeiten
• Sieht eine komplette Kopie des Netzwerks	VS	• Befindet sich in-line im Netzwerk
• Liefert große Datenmengen	VS	• Löst nur bei Problemen einen Alarm aus
• Erkennt Flooding-Angriffe	VS	• Wehrt Flooding-Angriffe ab
• Ist bei einem Angriff „transparent“ im Netzwerk	VS	• Ist leichter aufzuspüren

WUSSTEN SIE SCHON?

Einige IPS-Lösungen verfügen über einen integrierten **Sicherheitsmodus (*Bypass*-Funktion), damit der Geschäftsbetrieb auch im Störfall sichergestellt wird.**

Grundlegendes zu Eindringungs-schutzsystemen (IPS, Intrusion Prevention System)

Kurzbeschreibung

Die Hauptaufgabe eines IPS besteht in der **Echtzeitüberwachung der Netzwerkpakete und ihrer Inhalte, um vorab definierte Regeln je nach erkanntem Angriff und Ziel anzuwenden**.

BITTE NICHT VERWECHSELN:

Es gibt zwei verschiedene Arten von IPS:

- **HIPS (Host-Based Intrusion Prevention System):** IPS zur Überwachung von Arbeitsplatz-Systemen.
- **NIPS (Network Intrusion Prevention System):** IPS zur Überwachung von Netzwerken.

Funktionsweise

Eindringungsschutzsysteme werden in-line in dem Netzwerk installiert, das sie schützen sollen. Sie analysieren im Netzwerk übertragene Datenpakete, um zunächst die Konformität des Protokolls sowie eventuelle Befehle zu prüfen.

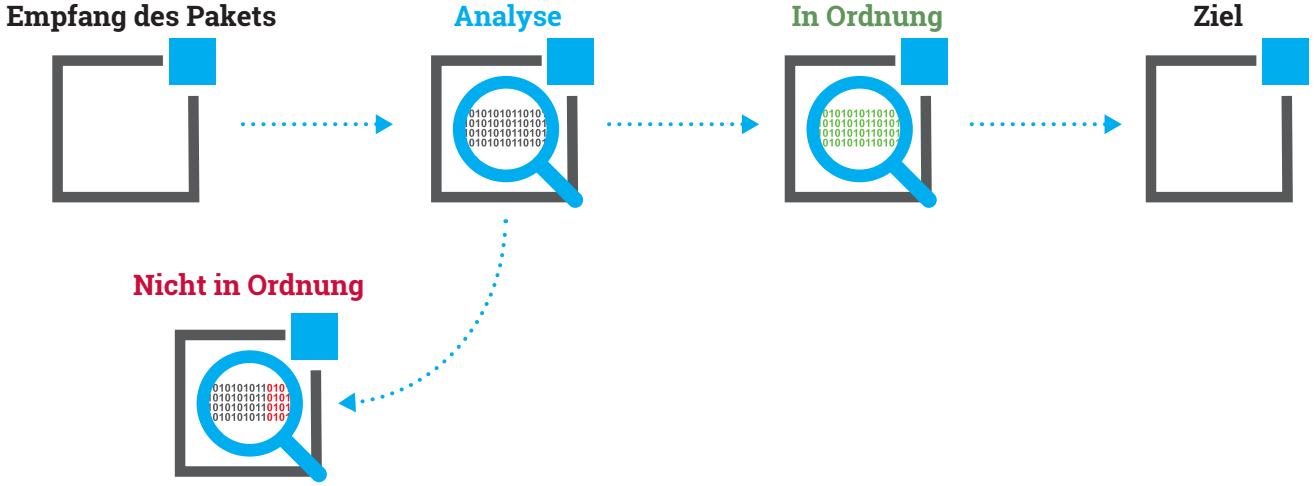
Einige IPS-Lösungen sind sogar in der Lage, anormales Verhalten zu erkennen.

Um Angriffsversuche zu blockieren, sucht die IPS-Lösung anschließend in den Datenpaketen nach Daten, die mit bekannten Malware-Signaturen übereinstimmen.

Vorteile von IPS

Mit dieser Technologie können Netzwerke in IT- bzw. OT-Infrastrukturen geschützt werden.

Daher muss bei der Wahl der IPS-Lösung darauf geachtet werden, dass die im Unternehmen eingesetzten Betriebsprotokolle unterstützt werden, da die Steuerungsbefehle nur so umfassend geschützt werden können.



Signatur oder gezielte Protokollsuche: zwei Ansätze für die Konformitätskontrolle der Protokolle

Die besten IPS-Engines ermöglichen die Decodierung der verwendeten Protokolle und prüfen die Konformität (Länge des Datenpakets, Protokolltyp usw.) jeder Meldung basierend auf dem erwarteten Format, das in genormten Protokollstandards festgelegt ist. Sie sind in der Lage, Daten sehr detailliert zu analysieren – daher auch die gebräuchliche Bezeichnung ***Deep Packet Inspection* (DPI)**.

DPI (Deep Packet Inspection) prüft den Header des übertragenen Pakets sowie die zugehörigen Daten und beseitigt jegliche Konformitätsabweichung des Protokolls.

Nehmen wir beispielsweise ein Datenpaket, das einen Befehl im Netzwerk transportiert:

Header		Befehl	Parameter		
1100	0011	1101	1110	1110	1000

Bei der Konformitätsprüfung der Protokolle sucht ein IPS vor allem aus zwei Gründen nach bestimmten Bytefolgen:

1. **Protokollerkennung:** Zunächst wird durch die Suche nach charakteristischen Markern das verwendete Protokoll erkannt.
2. **Konformitätsprüfung des Protokolls:** Anschließend wird überprüft, ob sich die Bytefolgen des verwendeten Protokolls tatsächlich im Datenpaket befinden.

WUSSTEN SIE SCHON?

Bei der Implementierung von Protokollen in industriellen Umgebungen werden größtenteils benutzerdefinierte Befehlswerte (*custom command*) benutzt. **Die signaturbasierte Protokollanalyse erkennt diese Werte nicht und generiert dadurch Prüffehler.**

In diesem Beispiel wird mit einer **Signaturanalyse** an jeder Stelle des Pakets nach der Zeichenfolge ***111101*** gesucht.

Header		Befehl	Parameter		
1100	0010	1101	1110	1110	1000

Hier sind die mit diesem Ansatz erkannten Bytes zwar vorhanden, aber nicht an der richtigen Stelle im Paket. Die signaturbasierte Technik lässt das Paket jedoch trotzdem durch (wodurch ein falsch-negatives Ergebnis entsteht).

Mit dem gezielten Ansatz werden die gewünschten Informationen an der richtigen Stelle gesucht, also genau dort, wo sie sein sollen. So wird verhindert, dass falsch formatierte (und möglicherweise bösartige) Pakete passieren können.

Bei diesem Ansatz werden falsch formatierte Pakete blockiert.

Header		Befehl	Parameter		
1100	0010	1101	1110	1110	1000

Die **gezielte Protokollanalyse** bietet somit zwei wesentliche Vorteile:

1. **Zuverlässige Protokollkonformität**
2. **Weniger Prüffehler**

Kontextbasierte Analyse als Herzstück des sicheren Datenaustausches

Dieser Ansatz verhindert Cyberangriffe, indem Meldungen, die zwischen zwei Netzwerkelementen ausgetauscht werden, kontextbasiert geprüft werden. Die **kontextbasierten Analyse** verifiziert, ob die Abfolge der Meldungen der in der Protokollnorm festgelegten Logik entspricht und kein anormales Verhalten zu erkennen ist.

Die kontextbasierte Analyse untersucht und verifiziert die zwischen zwei Geräten ausgetauschte Meldung, berücksichtigt jedoch auch die vorangegangenen Meldungen. **Diese fortschrittliche Technologie schützt und gewährleistet die Integrität Ihrer OT-Anlagen und -Umgebungen.**

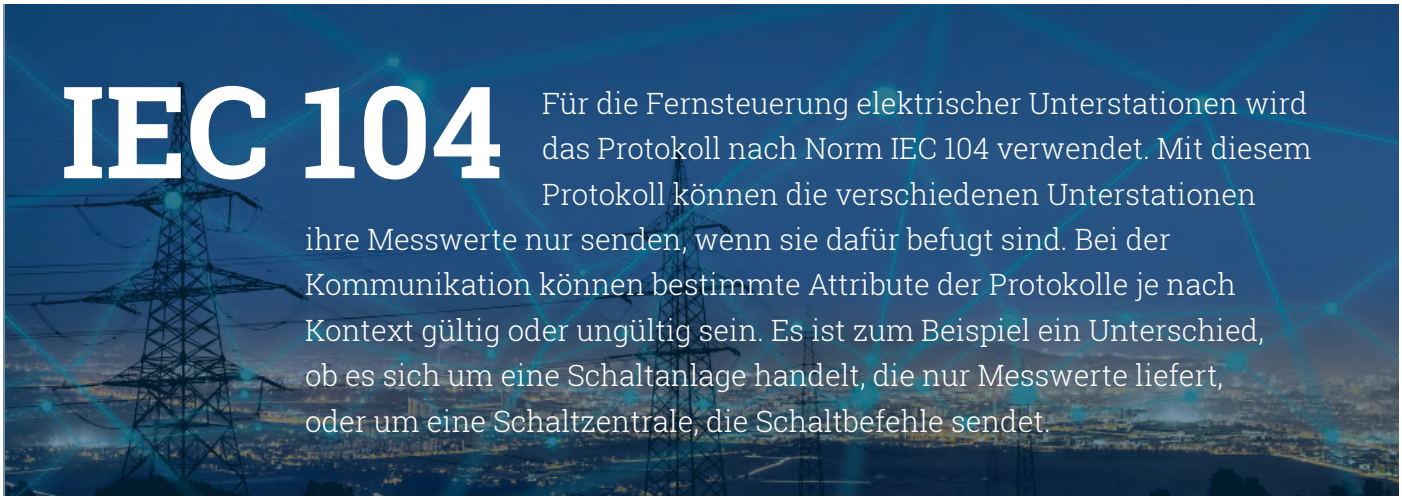
Nehmen wir beispielsweise ein Automatisierungssystem „A“, das von mehreren Controllern gesteuert werden kann. Ein Controller „A“ sendet eine Anforderung, um die Steuerung zu übernehmen. Das Automatisierungssystem „A“ geht dieser Anforderung nach und sendet eine Bestätigung über den Empfang des Befehls, sofern die Steuerung nicht bereits von einem anderen Controller übernommen wurde.

VORTEILE

Diese Art von IPS-Lösung, die als ***Stateful DPI*** bezeichnet wird, **verbessert die Sicherheit in der OT-Infrastruktur und verringert so die Gefährdung von Netzwerkressourcen.**

Nehmen wir nun an, dass ein Angreifer versucht, die Steuerung über das Automatisierungssystem „A“ zu übernehmen. Das IPS sieht ein spontan vom Automatisierungssystem „A“ gesendetes Paket, mit dem der Empfang einer Anforderung bestätigt wird, die es jedoch nicht erfasst hat. Mit Hilfe der Kontextinformationen kann das IPS dieses Verhalten als anormal erkennen und blockieren.

Da die IPS-Lösung die im OT-Netzwerk übertragenen Pakete einer **kontextbasierten Analyse** unterzieht, werden Informationen zum Meldungsaustausch zwischen zwei Geräten berücksichtigt. **Die Lösung berücksichtigt mehrere Parameter der aktuellen Meldung und vergleicht diese mit den zuvor ausgetauschten Informationen.** Solche Parameter sind beispielsweise die Kommunikationsrichtung zwischen beiden Geräten, die Art des auszuführenden Befehls sowie die Befehlswerte, die übernommen werden sollen.



IEC 104

Für die Fernsteuerung elektrischer Unterstationen wird das Protokoll nach Norm IEC 104 verwendet. Mit diesem Protokoll können die verschiedenen Unterstationen ihre Messwerte nur senden, wenn sie dafür befugt sind. Bei der Kommunikation können bestimmte Attribute der Protokolle je nach Kontext gültig oder ungültig sein. Es ist zum Beispiel ein Unterschied, ob es sich um eine Schaltanlage handelt, die nur Messwerte liefert, oder um eine Schaltzentrale, die Schaltbefehle sendet.

Suche nach Bedrohungen beim Datenaustausch im Netzwerk

Die Triton-Malware macht die Schwachstellen in OT-Netzwerken und die Bedeutung von IPS für die Erkennung von Netzwerkbedrohungen deutlich. Das gilt besonders für Angriffe, die Vorgaben für Protokollkonformität erfüllen und der Protokollnorm-Logik folgen. Die IPS-Technologie überprüft hierzu, ob die Paketdaten eine Bytefolge enthalten, die einer bekannten Angriffssignatur entspricht.

Dabei ist zu bedenken, dass Malware weiterentwickelt wird und neue Varianten auch neue Signaturen erfordern: Wenn die Signaturen nicht im IPS hinterlegt sind, ist eine signaturbasierte Bedrohungserkennung nicht möglich. **Daher sollten Sie eine IPS-Lösung einsetzen, die proaktive Signaturen für verschiedene Varianten eines Angriffs auswerten und diese erkennen kann.**

VORTEILE

Der proaktive Schutz ist ein weiterer wesentlicher Vorteil: Da weniger Signaturen als Basis benötigt werden, **wird die Suche nach bekannten Angriffsmustern im Netzwerk beschleunigt und die analysebedingte Netzwerklatenz verringert.**

Hinzu kommt: Wenn die IPS-Engine die Tiefenanalyse aus der Konformitätsprüfung der Protokolle nutzen kann, um in allen Meldungsteilen nur nach relevanten Angriffs-signaturen zu suchen, **verbessert sich die Performance weiter und die Falsch-Positiv-Rate wird deutlich gesenkt.**

Triton: ein Cyber-angriff auf ICS

Die Triton-Malware wurde als gezielter Angriff auf die ICS-Systeme eines saudi-arabischen Petrochemie-Unternehmens entwickelt, um eine Explosion herbeizuführen. Glücklicherweise begingen die Angreifer einen Fehler und lösten damit eine Notabschaltung der kritischen Systeme aus, durch die der Angriff auf das Netzwerk erkannt wurde.

Stuxnet: anschauliches Beispiel für Varianten eines Wurms

Stuxnet wurde für einen Angriff auf die iranischen Zentrifugen zur Urananreicherung entwickelt. Die Komplexität dieser Malware beruht auf umfassenden Kenntnissen industrieller Prozesse und auf Schwachstellen des Windows-Betriebssystems. Die Angreifer nutzten ausgefeilte und bis dahin wenig bekannte Zero-Day-Exploits.

Varianten von Stuxnet wurden auch später noch gegen andere industrielle Infrastrukturanlagen eingesetzt.

Einige Industrie- und Expertenorganisationen veröffentlichten daraufhin Anleitungen mit Best Practices für den richtigen Umgang mit Steuerungssystemen. Diese umfassen unter anderem Netzwerksegmentierung, Zugangskontrollen, gehärtete Systeme, die Installation von Virenschutz sowie von IPS-Engines.

Angesichts solcher Bedrohungen ist eine proaktive IPS-Lösung, die auch mögliche Varianten einer Malware erkennt, eine große – oder sogar unerlässliche – Hilfe für die Betriebsfähigkeit von Industriesystemen.

Notwendigkeit selbst generierter Signaturen

Ein IPS muss den Meldungsaustausch über industrielle Protokolle genau kennen und verwalten, um das OT-System zuverlässig schützen zu können. Jeder in den Befehlsmeldungen gesendete Wert muss korrekt analysiert und verifiziert werden, da sich jede Kommunikation im Netzwerk direkt auf einen bestimmten operativen Prozess auswirkt.

Eine IPS-Lösung muss mit Hilfe selbst generierter Signaturen kontrollieren können, ob Befehlsmeldungen mit operativen Prozessen und Vorgaben konform sind.

IPS-Lösungen können diese Verifizierung mit Hilfe selbst generierter Signaturen sicherstellen und so die Befehlsmeldungen kontrollieren und die Konformität mit den operativen Prozessen und Vorgaben gewährleisten. Dies ist überhaupt der kritischste Punkt in einer OT-Umgebung, denn auf diese Weise wird sichergestellt, dass die Werte nicht die festgesetzten Grenzwerte übersteigen und Prozesse beeinträchtigen könnten.

Betrachten wir als Beispiel einen Staudamm, bei dem gewährleistet sein muss, dass die Steuerungsbefehle den zulässigen Durchfluss eines Schiebers berücksichtigen (hier: Gesamtkapazität 50 bis 5 000 m^3/s). Auch wenn die neuen ICS/SCADA-Systeme weniger empfindlich sind, ist es bei alten Infrastrukturanlagen wichtig, dass die an den Controller gesendeten Werte diese Grenzen beachten. Dadurch werden überhöhte Durchflussmengen verhindert, die schwere Folgen wie Überschwemmungen verursachen können.

Umso wichtiger ist es, diese Werte in Echtzeit überprüfen zu können.

700+
proprietäre Protokolle

UMAS, S7, TSAA, SAAT, HNZ usw.

20+
standardisierte Protokolle

Modbus, UMAS, OPC Classic, S7, EtherNet/IP, CIP, BACnet/IP, IEC 60780-5-104, DNP3, PROFINET, IEC 61850 (MMS/GOOSE/SV), OPC UA usw.

VORTEILE

Selbst generierte Signaturen bieten folgende Möglichkeiten:

- **Anpassung** an den betrieblichen Kontext
- **Implementierung** von Protokollanalysen für proprietäre Protokolle
- **Kontrolle** sensibler Werte, um die Sicherheit des OT-Systems zu gewährleisten
- **Gewährleistung** der einwandfreien Funktion der operativen Prozesse

Kriterien für die Wahl der richtigen IPS-Lösung

In Anbetracht dessen, was auf dem Spiel steht, kann die Wahl der richtigen IPS-Lösung schwierig und komplex sein.

Die folgende schematische Darstellung ermöglicht einen schnellen Überblick über die wichtigsten Funktionen.



WUSSTEN SIE SCHON?

Bei Schutzsystemen mit mehreren Komponenten ist die Integration aufwändiger. Diese Lösungen benötigen nicht nur mehrere verschiedene Managementtools, Lizenzen und Schulungen, sondern erhöhen grundsätzlich auch die Latenz im Netzwerk.

Steigern Sie die Produktivität Ihrer Teams mit einer „All-in-one"-IPS-Lösung, die sich einfach installieren und bedienen lässt. Eine übersichtliche grafische Benutzeroberfläche verbessert zudem die Integration und Verwaltung der IPS-Lösung sowie den Überblick über die zu schützenden Systeme.

Die Stormshield-Engine *Stateful DPI*

Implementieren Sie ein fortschrittliches Eindringungsschutzsystem und segmentieren Sie Ihre OT-Netzwerke, um die Verfügbarkeit und Integrität Ihrer Systeme zu gewährleisten.

Leistungsstarke Datenflussanalysen

KONFORMITÄTSKONTROLLE DER PROTOKOLLE
mit Paketprüfung und Konformitätskontrolle der Anwendungsprotokolle

DPI für mehr als 10 unterstützte Protokolle
Modbus, OPC Classic, S7, EtherNet/IP, CIP, BACnet/IP, IEC 60780-5-104, DNP3, PROFINET, IEC 61850 (MMS/GOOSE/SV), OPC UA usw.



Ein industrielles IPS

beruht auf mehrfachen Analysen und kann so proaktiv reagieren und sogar Zero-Day-Angriffe verhindern

Kontextbezogene Analyse

Kontextbezogene Verhaltensprüfung



Optimierte IPS-Integration in das vorhandene Betriebssystem



Kontextbezogene Signatursuche in einer granularen, gezielten Datenbank



Gezielte kontextbezogene Protokollanalyse, um die Latenzzeiten und Falsch-Positiv-Ergebnisse zu verringern

Hervorragende Performance

SELBST GENERIERTE SIGNATUREN

WARUM WERDEN SIE BENÖTIGT?

1. Konformitätskontrolle für operative Prozesse
2. Anpassung an eigene Protokollanalysen
3. Vermeidung von Schäden an Produktionstools und Umgebung



Intuitive Einrichtung



All-in-one-Lösung



Übersichtliche, intuitive Benutzeroberfläche

EXPERTISE BEIM SCHUTZ VON OT-NETZWERKEN: CO-DESIGN MIT GERÄTEHERSTELLERN, INDUSTRIELLEN INTEGRATOREN UND KUNDEN

www.stormshield.com

STORMSHIELD

Die europäische Lösung für Cybersicherheit



Überall auf der Welt müssen Unternehmen, Regierungseinrichtungen und Verteidigungsbündnisse auf verlässliche Partner vertrauen, die ihre digitale Transformation begleiten und die Cybersicherheit ihrer Infrastrukturen, Benutzer und Daten sicherstellen. Die Technologien von Stormshield sind nach den höchsten europäischen Normen zertifiziert (EU Restricted, NATO Restricted, Common Criteria EAL3+/EAL4+, ANSSI-Qualifikationen und -Visa) und erfüllen die Anforderungen für IT und OT zum Schutz Ihrer Tätigkeiten. **Dank unserer Sicherheitslösungen können Sie sich wieder voll auf Ihr Geschäft konzentrieren.**
www.stormshield.com/de

Die, auch teilweise, Weitergabe, Vervielfältigung oder Darstellung dieses Whitepapers zu anderen Zwecken als für den privaten Gebrauch auf jedwedem Datenträger ist untersagt und kann zu zivil- und strafrechtlichen Maßnahmen gegenüber dem Zuwiderhandelnden führen.