secunet

# Whitepaper

# Trusted Platform at the Edge

Wie die Absicherung am Rande des Netzwerks Industrie 4.0 ermöglicht

Juni 2020 | Version: 1.1

# Inhaltsverzeichnis

# 1. Einführung

Industrie 4.0 lässt Informationstechnologie (IT) und die Prozesstechnologie (kurz OT für „Operational Technology“) zusammenwachsen und vereint damit zwei Welten, die zuvor völlig voneinander getrennt waren. Vernetzte Sensoren, Maschinen und ganze Anlagen sorgen in den Ökosystemen der Industrie 4.0 für eine erhöhte Komplexität und bieten Cyberkriminellen unzählig neue Möglichkeiten, Angriffe zu starten.

Industrie 4.0 – die vierte industrielle Revolution – wird zur Beschreibung der Digitalisierung des Produktionsumfeldes verwendet. Unternehmen, die bereits auf den digitalen Zug aufgesprungen sind, können die Relevanz, Bedeutung und Chancen dieser Revolution klar benennen und haben spezielle funktionsübergreifende Teams zusammengestellt, um Anwendungsfälle für digitale Geschäftsmodelle sowohl in ihrer eigenen Organisation als auch darüber hinaus im ganzen Industriesektor zu identifizieren und zu erproben.

In diesem Whitepaper mit dem Titel „Wie die Absicherung am Rande des Netzwerks Industrie 4.0 ermöglicht“ wird die Konvergenz von IT- und OT-Umgebungen untersucht und anschließend näher betrachtet, wie Anforderungen zu Connectivity, Edge Computing – hier vereinfacht definiert als Möglichkeit zur Datenverarbeitung am Entstehungsort und Kopplung mit Cloud-Diensten – mit Cyber Security zusammenspielen.

Darüber hinaus wird die Digitalisierung im Kontext von Industrie-4.0-Anwendungsfällen beleuchtet. Die Industrie benötigt Systeme 1. zur sicheren Vernetzung, 2. zur Anbindung an interne sowie externe IT-Dienste und 3. eine Überwachung der Kommunikation von Maschinen und Anlagen (Cyber Physical Systems). secunet stellt einen Ansatz für eine skalierbare, modulare und sichere Edge-Computing-Lösung vor. Diese Lösung bedient nicht nur Anforderungsbereiche der Industrial Security, sondern stellt auch Basisfunktionen zur Umsetzung von Industrie-4.0-Konzepten bereit. An dieser Stelle wird deutlich, dass Cybersecurity-Technologie bei richtigem Einsatz zum Enabler werden kann.

## 2. Konvergenz von IT und OT

Das Bundesministerium für Wirtschaft und Energie beschreibt das Produktionsumfeld in der Industrie 4.0 als flexibler, individueller und effizienter.[i]

Wissenswertes: Durch die Anpassung an die Industrie 4.0 wird das Produktionsvolumen um 20 bis 25 Prozent gesteigert und die Ausfallzeit von Maschinen im Produktionsumfeld um bis zu 45 Prozent reduziert.[ii]

Die wesentliche Treibkraft für dieses Szenario sind die von Anlagen und Maschinen im Produktionsumfeld erzeugten Datenmengen. Sie werden von IT-gestützten Systemen verarbeitet, korreliert und analysiert, um zum einen ein aktuelles Lagebild und zum anderen zeitnahe und fundierte Entscheidungsfindung für Betriebsabläufe zu ermöglichen.

IT-Sicherheit ist ein entscheidender Faktor in der Digitalisierung. Grundlage der Digitalisierung und der Industrie 4.0 ist die umfassende Vernetzung und Vermengung der zuvor getrennten Sparten der Informationstechnologie und der Prozesstechnologie. Anlagen und Maschinen der OT-Umgebung werden zentral über Leitsysteme gesteuert und überwacht und arbeiten mit Informations- und Kommunikationssystemen zusammen. Immer häufiger müssen die ehemals isolierten Netzwerke mit IT-Diensten innerhalb und außerhalb der eigenen Organisation interagieren. Sei es zum Zwecke der Fernwartung, zur Ausleitung von Leistungsdaten der Maschinen oder zum Einleiten von Daten die der Optimierung der Betriebsführung dienen. Dieser Grad an Vernetzung führt zwangsläufig zu neuen Herausforderungen und Risiken.

Aus der Praxis geht hervor, dass eine akute und allgegenwärtige Bedrohung durch Cyberangriffe besteht und dementsprechend Schutzvorkehrungen getroffen werden müssen. Die Sicherheit der vernetzten Maschinen ist eine echte und ständige Herausforderung für Unternehmen.

Wissenswertes: 83 % der Unternehmen mit mehr als 1.000 Angestellten sind mehrmals im Monat von Angriffen betroffen – die Hälfte davon fast täglich.[iii]

Heutzutage sehen sich Betreiber mit IT-Sicherheitsbedrohungen konfrontiert, die in der Vergangenheit im Arbeitsumfeld von Ingenieuren und Technikern noch keine Rolle spielten. Das Bundesamt für Sicherheit in der Informationstechnik berichtete, dass Cyberangriffe auf Maschinen der OT beinahe identisch sind mit denen in einer klassischen IT-Umgebung.[iv] Dadurch werden die Anforderungen an die Maßnahmen, die erforderlich sind, um solchen Bedrohungen und Angriffen entgegenzuwirken, um einiges komplexer. Die Implementierung von Schutzmaßnahmen ist daher ein entscheidender Faktor für die Umsetzung einer erfolgreichen Digitalisierungsstrategie.

Daraus lässt sich schließen, dass in der OT-Umgebung der gleiche Bedarf an zuverlässigem Schutz besteht wie bei klassischen IT-Systemen. Jedoch können vorhandene, bereits etablierte Ansätze zur Verhinderung von Cyberangriffen nicht einfach auf die OT-Umgebung übertragen werden. Für Maschinen, die in der OT betrieben werden, sind Lebenszyklen von mehr als 15 Jahren typisch. Untypisch dagegen sind Modifikationen von Komponenten, um Maschinen und Anlagen gegen aktuelle IT-Bedrohungen zu wappnen. Für ein Sicherheitsniveau nach aktuellem Stand der Technik bedarf es regelmäßiger Updates, Anpassungen und Patches, die in der klassischen IT-Umgebung gängig und üblich sind und fast schon als obligatorisch gelten.

In der OT-Welt ist ein solcher Ansatz aus verschiedenen Gründen eindeutig nicht möglich: Fehlende Standardprozesse, z. B. im Patch-Management zur Installation regelmäßiger Updates oder fehlende Testumgebungen zur Sicherstellung der Funktionalität nach einer Änderung, verstärken oft die Angst des Betreibers vor Systemausfällen durch Änderungen. Die Devise lautet: Never change a running system. Allerdings wird dabei das Risiko, das die Vernetzung ungeschützter, veralteter Technologie mit sich bringt, unterschätzt. In Gefahr gerät nicht nur der einwandfreie Betrieb der Maschine selbst. Auch andere Teilnehmer im Netzwerk sind gefährdet, zudem können sich Einfallstore für potenzielle Cyberattacken öffnen.

Die Vernetzung unsicherer und veralteter IT-Komponenten stellt ein erhebliches Risiko für den ordnungsgemäßen Betrieb der Anlage und Maschine dar sowie für alle anderen Teilnehmer im Netzwerk und kann die Tür für Cyberangriffe öffnen. Dazu kommen, wie bereits erwähnt, der lange Lebenszyklus einer Maschine und die unzureichende Berücksichtigung der IT-Sicherheit seitens der Maschinenhersteller, wodurch Maschinen Sicherheitslücken oder nur schwache Schutzmechanismen aufweisen können.

Wenn solche Maschinen direkt mit dem Internet verbunden sind, werden sie sichtbar und können von spezialisierten Suchmaschinen wie Shodan[v] erkannt werden. Angreifer können so diese Anlagen oder Maschinen leicht finden und über inhärente Schwachstellen oder schwache Zugriffsmechanismen Zugang erhalten.

Wissenswertes: Schäden durch Cyberangriffe haben fast immer weitreichende Folgen:

- Ausfallzeiten – Betriebsstillstand
- Sach- und Personenschäden
- Kosten zur Wiederherstellung des geordneten Betriebs
- Verringerung der Fertigungsqualität
- Konsequenzen für das Unternehmen und Führungspersonal – einschließlich Bußgelder
- Marken- und Reputationsschäden

Die Dringlichkeit zur Etablierung von Sicherheitsmaßnahmen für eingesetzte Maschinensteuerungen in OT-Umgebungen, wird durch Schwachstellen deutlich, die in den großflächig genutzten Remote-Desktop-Diensten weit verbreiteter Betriebssysteme vorhanden sind.[vi] Aufgrund des hohen Risikos dieser Schwachstellen wurden vom Hersteller sogar Updates für nicht mehr unterstützte Versionen des Betriebssystems veröffentlicht.[vii]

Trotz dieser Gegenmaßnahmen stehen Betreiber und Hersteller von Maschinen aus den bereits genannten Gründen weiterhin vor großen Herausforderungen: Die Installation dieser Updates kann gar nicht oder nicht innerhalb eines angemessenen Zeitrahmens durchgeführt werden.

Es reicht jedoch nicht aus, sich nur auf die Absicherung der Anlagen und Maschinen zu konzentrieren. Die IT-Sicherheit dient als Grundlage und Wegbereiter der Digitalisierung, so dass alle Anwendungsfälle auf ihr aufbauen können und sollten. Daher ist ein ganzheitliches Konzept erforderlich, das die IT-Sicherheit auf einem möglichst hohem Niveau Einzug in die OT-Umgebung halten lässt. Die Einbindung der IT-Sicherheit sorgt zugleich für eine sichere Konnektivität und ermöglicht die sichere Anbindung von Maschinen an interne und externe Dienste wie IIoT-Plattformen.

Die folgenden Aspekte adressieren ein ganzheitliches Sicherheitskonzept für einzelne Maschinen oder für Maschinensegmente:

| Funktionsdomänen | |
|---|---|
| **Schützen** | Sichere Vernetzung und reglementiertes Kommunikationsverhalten von Maschinen bei gleichzeitigem Schutz des Netzwerks |
| **Verbinden** | Möglichkeit der flexiblen Integration der Maschinen in Anwendungsfälle des Industrial Internet of Things (IIoT) und der Industrie 4.0 – Einsatz von Software zur Vordatenverarbeitung oder Anbindung an IT-Dienste |
| **Überwachen** | Security Monitoring der Maschinenkommunikation zur Identifikation von anomalen Verhalten und damit Stärkung der Abwehrkräfte |

# 3. Schützen: Schutz der Maschinen am Rande des Netzwerks

Die ständige Bedrohung durch Cyberangriffe im OT-Umfeld unterscheidet sich kaum von der in klassischen IT-Netzwerken. Ein Höchstmaß an IT-Sicherheit aufzubauen und aufrechtzuerhalten ist demnach gleichermaßen in der OT gefordert. Allerdings muss die Implementierung von IT-Sicherheit den Anforderungen der OT-Umgebungen gerecht werden. Dabei gilt es, die Herausforderungen, Risiken und Anforderungen des OT-Umfelds sorgfältig abzuwägen.

Der Einsatz herkömmlicher Sicherheitssysteme ist aus verschiedenen Gründen nicht ausreichend: Eine klassische Firewall-Appliance erfüllt bspw. weder in ihrer Bauform die nötigen Voraussetzungen, noch kann sie extremen und rauen Umgebungseinflüssen wie Hitze, Staub und Vibrationen dauerhaft standhalten. Außerdem können die in der OT verwendeten Kommunikationsprotokolle von herkömmlichen Sicherheitssystemen nicht verarbeitet werden. Es bedarf also geeigneter Hardware-Konzepte, spezieller Laufzeiteigenschaften und Abdeckung industriespezifischer Kommunikationsarten.

Ein Ansatz zum Erreichen der IT-Sicherheit für Maschinen in der OT besteht darin, sie zu isolieren und vom IT-Netz zu entkoppeln, so dass sie nicht ohne weiteres über die IT-Infrastruktur zugänglich sind. So wird eine Entkopplung des Lebenszyklus der Maschinen-IT von den klassischen IT-Anforderungen ermöglicht und schafft Sicherheit im Betrieb von älter und anfälliger werdenden Systemen. Als Koppelelement selbst kommt ein Sicherheitssystem zum Einsatz, welches zwischen der Maschine (oder dem Maschinensegment) und dem IP-basierten IT-Netzwerk geschaltet wird.

Das Sicherheitssystem isoliert die vernetzten Maschinen vollständig vom eigentlichen IT-Netzwerk und bietet zusätzliche Sicherheitsfunktionen zu ihrem Schutz. Das Sicherheitssystem ist dabei Teil des IT-Netzwerks und muss selbst Cybersecurity-Bedrohungen abwehren können. Eine entsprechende Härtung des Betriebssystems, Minimalisierung von Zugängen und Zugriffen und Systemüberwachung sollte als Basis gesetzt sein. Zudem ist lediglich das gehärtete und minimierte Betriebssystem des Sicherheitssystems von schnelllebigen Update-Zyklen betroffen. Dadurch lassen sich Updates problemlos durchführen, so dass das Gesamtsystem stets auf aktuellem Stand ist, ohne dass Nebenwirkungen oder Auswirkungen auf die Verfügbarkeit der Maschinen in Kauf genommen werden müssen.


*Abbildung 1: Integration des Sicherheitssystems als Kommunikationsschnittstelle zwischen Maschine und Netzwerk*

Wissenswertes: Das Sicherheitssystem fungiert als Gatekeeper für vernetzte Maschinen und verringert deren Sichtbarkeit im Netzwerk. Wenn es weniger wahrscheinlich ist, gesehen zu werden, ist es auch weniger wahrscheinlich, angegriffen zu werden.

Die integrierte Firewall-Funktion ermöglicht Mikrosegmente, indem sie eine dedizierte Zone schafft und so vor äußeren Einflüssen schützt. Jede ein- und ausgehende Kommunikation wird über das Sicherheitssystem geführt. Der Datenfluss und Kommunikationsverbindungen zwischen den Netzwerksegmenten Maschine <> LAN/WAN wird somit vollständig kontrollierbar.

Zum Schutz der Maschinen gehört auch der geeignete Umgang mit Protokollen die mittlerweile als unsicher eingestuft werden. Die langen Laufzeiten von Maschinen bringen es mit sich, dass deren Datenübertragung oft auf alten Protokollstandards basiert. Ein Nachrüsten geeigneter Maßnahmen ist schwierig, gerade wenn Daten noch über veraltete Schnittstellenstandards übertragen werden müssen.

Wenn Maschinen im Netzwerk über unsichere Protokolle kommunizieren, kann weder auf die Vertraulichkeit noch auf die Integrität der zu übertragenden Daten vertraut werden. Infolgedessen besteht ein hohes Risiko, dass der Netzwerkverkehr durch Dritte mitgelesen oder manipuliert wird. Eine Protokollübersetzung von einem unsicheren in ein sicheres Protokoll verhindert eine solche ungesicherte Übertragung von Daten im Netzwerk und reduziert das Risiko auf die minimale Strecke zwischen dem Sicherheitssystem und der damit verbundenen Maschine. Dazu werden die von einer vernetzten Maschine an das Sicherheitssystem gesendeten Daten „on the fly“ übersetzt und unter Verwendung eines sicheren Protokolls weitergeleitet, z. B. von File Transfer Protocol (FTP) zu Secure File Transfer Protocol (SFTP) oder File Transfer Protocol über SSL (FTPS).

**Der Aspekt „Schützen“ zusammengefasst:**

1. Maschinen sollen vom Lebenszyklus der klassischen IT entkoppelt werden
2. Zur Entkopplung benötigt es ein Sicherheitssystem, das wie eine Schutzhülle um das älter und anfälliger werdende Maschinenkonstrukt wirkt
3. Mikrosegmentierung, Netzwerke sicher koppeln, Kommunikationsflüsse regeln und steuern, unsichere Protokolle in sichere Protokolle wandeln sind wichtige Schutzfunktionen in der Isolation einer Maschine
4. Das Sicherheitssystem selbst muss hohen Sicherheitsansprüchen genügen und gängige Update-Möglichkeiten und Erweiterungsoptionen mit sich bringen

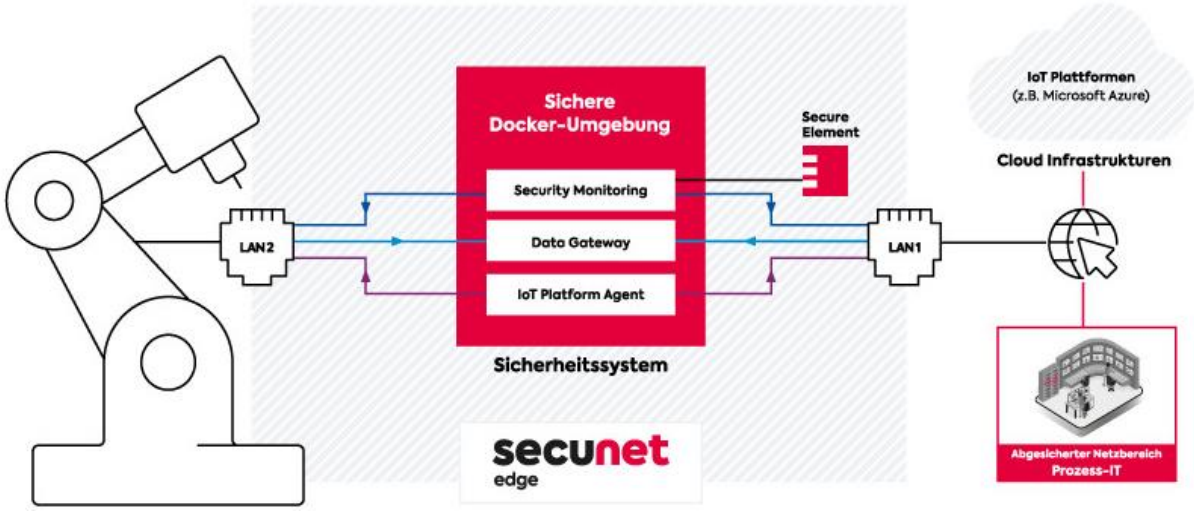



*Abbildung 2: Beispiel einer mittels IIoT-Anwendung geschützten sicheren Ausführungsumgebung*

Die Gründe zur Verarbeitung von maschinenerzeugten Daten sind vielschichtig. Möglicherweise sollen zur Optimierung eigener Prozesse sowie zur Minimierung von Ausfallzeiten maschinenerzeugte Daten an IIoT-Plattformen übertragen und analysiert werden. Oder Techniker sollen aus Kostengründen die Maschinen aus der Ferne über das Internet warten. Bei solchen Anforderungen ist eine sichere und kontrollierte Anbindung der Maschinen an interne und externe Dienste erforderlich.

Die Anwendungsfälle besitzen je nach Betreiber individuelle Anforderungen, wodurch die Gesamtkomplexität schnell steigt. Häufig leidet das Umsetzungstempo in der Realisierung gleich mehrerer Anwendungsfälle dabei sehr.

Ein Sicherheitssystem mit modularem Plattform-Konzept in Form einer Ausführungsumgebung für Anwendungen kann Abhilfe schaffen. Anwendungen, die darin ausgeführt werden, beispielsweise Agenten von IIoT-Plattformen, Anwendungen zur Datenvorverarbeitung oder zur Kommunikation mit internen Diensten, erhalten einen kontrollierten Zugriff auf Informationen verbundener Maschinen und können diese sicher und gerichtet an den jeweiligen Dienst übermitteln bzw. entgegennehmen.

Vom Sicherheitssystem aus werden die Daten beispielsweise durch eine Transportverschlüsselung gesichert an die jeweiligen Dienste übertragen. Die Bündelung verschiedener Anwendungen auf dem Sicherheitssystem als sichere Edge-Computing-Plattform reduziert die Komplexität und der Bedarf von Individuallösungen je Anwendungsfall wird deutlich minimiert oder gar aufgelöst.

Auch Entwickler sowie Anbieter von Datendiensten, beispielsweise im Bereich der künstlichen Intelligenz oder Big Data, profitieren von einem solchen Konzept. Sie können ohne tiefgreifendes Security-Know-how und ohne Einschränkungen in Hardware-Fragen ihre plattformunabhängigen Anwendungen über die Plattform sicher anbinden und damit überhaupt erst anbieten.

### Verarbeitung von Daten am Rande des Netzwerks

Neben der Verarbeitung von Informationen durch zentralisierte Dienste, welche sich beispielsweise in der Cloud befinden, wird das Paradigma des Edge-Computings immer relevanter. Über diverse Sektoren hinweg unterstreichen bereits über 100 Anwendungsfälle [viii] die Relevanz des Paradigmas. Dabei kann Edge-Computing in IIoT- und Industrie 4.0-Anwendungsfällen ergänzend zu den bekannten zentralisierten Cloud-Diensten wirken. Reaktionszeiten lassen sich durch eine Datenverarbeitung auf der Edge-Computing-Plattform reduzieren und Ergebnisse direkt an die Maschinen zurückspielen. Maschinenerzeugte Daten können vorverarbeitet werden, damit dann nur die Ergebnisse Bandbreiten schonend in die Cloud-Dienste übertragen werden.

# 4. Überwachung: Erhöhung der Widerstandsfähigkeit gegenüber Cyberangriffen

**Ziel: Permanente Maschinenkontrolle zur Aufrechterhaltung der Sicherheit**

Um den Sicherheitsstatus eines Netzwerks zuverlässig zu ermitteln, sind die Identifizierung aller Systeme im Netzwerk und die Aussage über ihr IT-Sicherheitsniveau sowie die kontinuierliche Kontrolle ihres Kommunikationsverhaltens unerlässlich. Die zunehmende Verbreitung von Systemen innerhalb einer Netzwerkinfrastruktur führt zu einem unweigerlichen Heranwachsen der übertragenen Datenmengen bei gleichzeitiger Reduzierung der Transparenz der in den Netzwerken stattfindenden Kommunikationsflüsse. Um ein höchstmögliches IT-Sicherheitsniveau in IIoT- und Industrie 4.0-Szenarien zu erreichen, ist neben der grundlegenden Absicherung die stete Überwachung der Kommunikation von und zu den Maschinen entscheidend.

Derzeit werden Firewalls, Monitoring-Systeme und andere präventive Sicherheitsmaßnahmen zur Überwachung des Datenflusses eingesetzt. Firewalls verwenden ein definiertes Regelwerk gemäß den Ansätzen des White- oder Blacklistings, nach denen Pakete entweder durchgelassen oder verworfen werden. Monitoring-Systeme sammeln hingegen in erster Linie Daten über die im Netzwerk befindlichen Systeme, analysieren die erfassten Informationen und stellen diese in Form von Zustandsberichten dar. Anhand von vordefinierten Schwellwerten und Regeln können solche Systeme auf mögliche Probleme oder Bedrohungen hinweisen. Die festgestellten Probleme werden dann in Form von Warnungen angezeigt und erfordern eine manuelle Überprüfung und gegebenenfalls das Einleiten weiterer Maßnahmen.

Diese genannten Ansätze zur Kontrolle und Überwachung des Datenflusses basieren auf starren, vordefinierten Regeln, die regelmäßig überprüft und angepasst werden müssen. Diese Mechanismen sind in Industrieumgebungen, in der selten IT-Betriebspersonal ausreichend und schon gar keine Sicherheitsexperten vorhanden sind, schwer umzusetzen. Sie sind in der Pflege der Regelwerke und Interpretation einzelner Alarme sehr zeitaufwendig und fehleranfällig.

**Hier kommt die automatisierte Erkennung von Anomalien[ix] zum Tragen**.

Anomalien sind unerwartete Abweichungen von der Verhaltensnorm. Im Umfeld einer Produktion und im Maschinenbetrieb sind sie als Abweichungen von „normalen Betriebszuständen“ zu verstehen. Um Anomalien zu erkennen, muss der „Normalzustand“ eines Systems – in diesem Fall eines Produktionsnetzwerks oder einer einzelnen Maschine – bekannt sein. Mit Hilfe einer Lernphase kann der Normalzustand automatisiert erhoben werden. Auf dieser Basis kann in der Folge anormales Verhalten – also das erstmalige Vorkommen von abweichenden Ereignissen – automatisch „erkannt“ werden. Hier einige einfache Beispiele:

- Erkennung neuer Maschinen im Netzwerk
- Erkennung der Kommunikation zwischen Maschinen
- Erkennung neuer Protokolle im Netzwerk
- Erkennung von Verbindungen zu unsicheren Netzwerken, z. B. dem Internet
- Erkennung von Angriffen mit unbekannten Signaturen
- Erkennung von fortgeschrittenen, andauernden Bedrohungen (APT)

Eine kombinierte Verwendung der drei Funktionen - Firewall, Monitoring und Anomalieerkennung - zur Datenflusskontrolle und Kommunikationsüberwachung schafft die nötige präventive und detektive Sicherheit in IIoT- und Industrie 4.0-Netzwerken.

Aus architektonischer Sicht lassen sich diese drei Funktionen gut auf einem Sicherheitssystem am Rande des Netzwerks realisieren. Aufgrund der Positionierung eines solchen Sicherheitssystems als Koppelelement zwischen unterschiedlichen Netzwerken kann dieses den ein- und ausgehenden Datenfluss zur bzw. von der Maschine kontinuierlich erfassen. Die nachfolgende Abbildung verdeutlicht die Positionierung des Sicherheitssystems mit integrierter Firewall-Funktion und Sensor zum Monitoring und zur Anomalieerkennung.

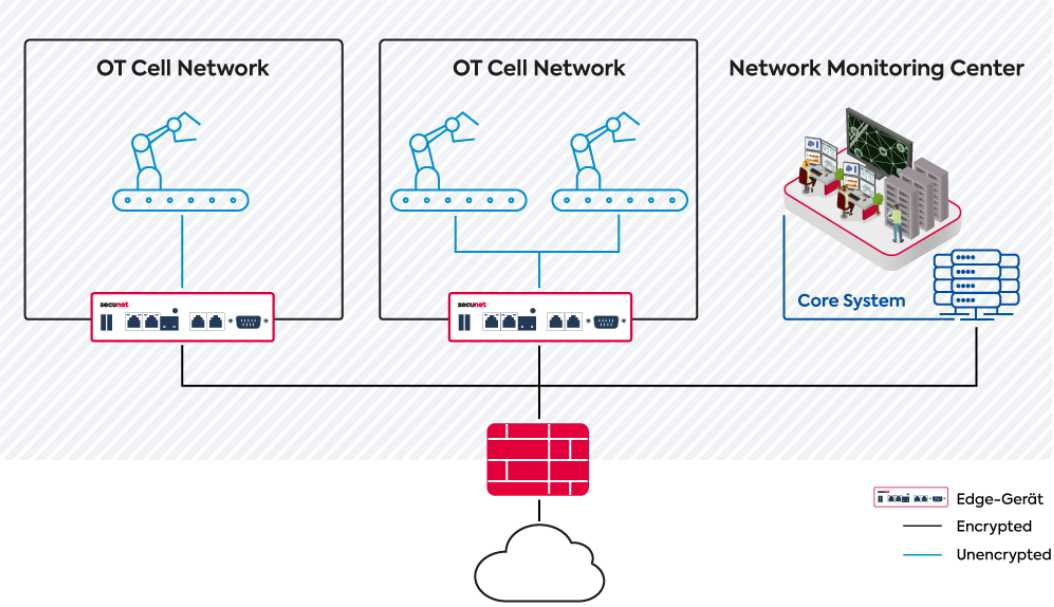



*Abbildung 3: Platzierung der Edge-Geräte (Sensoren) in der Infrastruktur.*

Ein Core-System stellt an zentraler Stelle vorkonfigurierte Regelsätze gemäß den Ansätzen des White- und Blacklisting bereit und analysiert die von der Sensorik gesendeten Informationen. Hierdurch wird der Datenfluss transparent und lässt sich überwachen.

Zusätzlich lernt das Core-System durch maschinelles Lernen das Normalverhalten der Kommunikation der in den Mikrosegmenten befindlichen Maschinen.

Entsprechend kann das Auftreten eines abnormalen Kommunikationsverhaltens erkannt werden, welches u.a. durch die Infektion eines Gerätes mit Malware oder durch einen nicht gewollten Verbindungsaufbaus eines Angreifers hin zum Gerät auftritt. Die intelligente Kombination aus vordefinierten Regeln, Anomalieerkennung und Firewall-Funktionen auf dem Sicherheitssystem ermöglicht das automatisierte Treffen von Entscheidungen und dadurch die Blockierung potenziell gefährlicher Datenflüsse, wodurch ein Höchstmaß an Sicherheit für Maschinen oder Maschinensegmente gewährleistet wird.

# 5. Digitale Transformation: Industrie 4.0-Anwendungsfälle

Zum Thema Industrie 4.0 wurden mehrere Forschungsarbeiten von Institutionen aus Deutschland und der ganzen Welt[x] sowie von Regierungen veröffentlicht, die mit Deutschland zusammenarbeiten[xi], um aufkommende Möglichkeiten und Anwendungsfälle aktiv zu fördern, wie auf der Website[xii] der *Plattform Industrie 4.0* dargestellt wird. Dazu zählen:

- Mehr als 300 praktische Beispiele für Industrie 4.0 aus Deutschland
- Mehr als 150 bewährte Verfahren für Industrie aus Frankreich
- Mehr als 150 Anwendungsfälle für die Roboter-Revolution-Initiative aus Japan

Den zentralen Fokus und die Basis für diese Anwendungsfälle bilden Daten. Die Bedeutung von Daten wird in einem Artikel hervorgehoben, in dem argumentiert wird, dass Öl in seiner Rolle als wertvollste Ressource der Welt von Daten abgelöst wurde.[xiii] Daten, aus denen Erkenntnisse durch Analyse und maschinelles Lernen gewonnen werden können, anhand derer wiederum Maßnahmen ergriffen und Entscheidungen in Echtzeit getroffen werden können.

Von Anlagen, Maschinen oder Sensoren generierte Daten liefern wichtige Informationen über Zustand (Lebensdauer), Auslastung (Kapazität) und Ertrag (Qualität). Wenn diese vernetzt sind, können die generierten Daten verwendet werden, um die Effizienz zu steigern, die Qualität zu erhöhen und die bedarfsgerechte Zuweisung von Ressourcen zu vereinfachen.

*In der folgenden Tabelle 3 sind die Informationen aufgeführt, die aus den Daten abgeleitet werden können:*

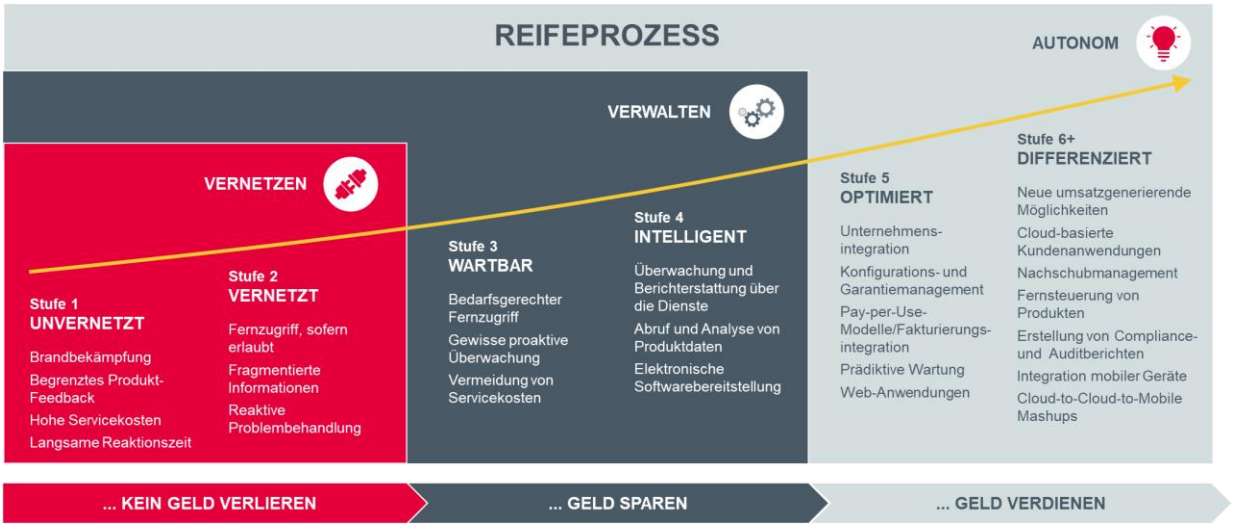
| Kategorie | Erzeugte Informationen |
|---|---|
| **Zustand (Lebensdauer)** | Parameter wie unter anderem Druck, Temperatur, Vibration, Durchfluss und Undichtigkeit geben wertvolle Informationen über den allgemeinen |
| **Auslastung (Kapazität)** | Nutzungskennzahlen wie OEE (Gesamtanlageneffektivität) und TEEP (totale effektive Anlagenproduktivität) liefern Einblicke in die Produktionskapazität. |
| **Ertrag (Qualität)** | Der Ertrag einer Maschine spiegelt die Prozessqualität wider. |

In einem Artikel von McKinsey (November 2018) ermittelten und erklärten die Autoren nach einer umfassenden Marktanalyse die Hintergründe für 107 Anwendungsfälle im Bereich Edge Computing. Die folgende Abbildung zeigt einige der Sektoren mit zugehörigen Anwendungsfällen, um das Spektrum an möglichen Einsatzszenarien für Edge Computing in der Industrie zu verdeutlichen.[xiv]

*Die nachstehende Abbildung 4 zeigt eine Auswahl von Sektoren und Anwendungsfällen, entnommen aus einem Artikel von McKinsey (November 2018)*


## Jede digitale Transformation ist eine Reise

Die Optimierung der vorhandenen Wertschöpfung oder die Entwicklung neuer digitaler Geschäftsmodelle ist abhängig von vielen Faktoren. Entlang eines Reifeprozess müssen sich Kon-zepte, Betriebsabläufe und Verhalten der Organisation neu finden. Es beginnt mit dabei klassisch mit der Phase der Vernetzung in der überhaupt Grundlagen für weitergehende digitale Prozesse gelegt werden. Im besten Fall wird in dieser Phase ein Sicherheitsfundament gesetzt, auf dem die Ausweitung in Verwaltungsaspekte der Maschinen einfach möglich ist. In dieser Phase der Betriebsoptimierung geht es häufig um Effizienzgewinne und Kostenreduktion in Produktionsab-läufen. Einen Schritt weiter lassen sich mit automatisierten Abläufen und neuer Datenverfügbar-keit neue Services für Kunden und damit Neugeschäft entwickeln.



# 6. Das Konzept der Trusted Edge Platform

Wir haben uns mit der Herausforderung auseinandergesetzt, Maschinen vor IT-Einflüssen abzusichern, diese jedoch gleichzeitig sicher mit Diensten aus der IT zu vernetzen. Ein von uns speziell für das industrielle Umfeld konzipierte Sicherheitssystem, platziert an der kritischen Schnittstelle zwischen Maschine und Netzwerk, erfüllt diesen paradox erscheinenden Anspruch durch die Bündelung folgender Ansätze:

1. **Schützen**: Sichere Vernetzung und reglementiertes Kommunikationsverhalten von Maschinen bei gleichzeitigem Schutz des Netzwerks
2. **Verbinden**: Möglichkeit der flexiblen Integration der Maschinen in Anwendungsfälle des Industrial Internet of Things (IIoT) und der Industrie 4.0 – Einsatz von Software zur Vordatenverarbeitung oder Anbindung an IT-Dienste
3. **Überwachen**: Security Monitoring der Maschinenkommunikation zur Identifikation von anomalen Verhalten und damit Stärkung der Abwehrkräfte

Hersteller und Betreiber stehen häufig vor der Herausforderung, die Vielfalt ihrer eigenen OT-Umgebung bei der Entwicklung eines Gesamtkonzepts zur Umsetzung der oben genannten Modelle zu berücksichtigen. Das Prinzip der Trusted Edge Platform schafft es, die unterschiedlichen Anforderungen an die IT-Sicherheit in einer OT-Umgebung effektiv zu erfüllen, gleichzeitig ein sicheres Trägersystem für die vielfältigen benötigen Anwendungen darzustellen.

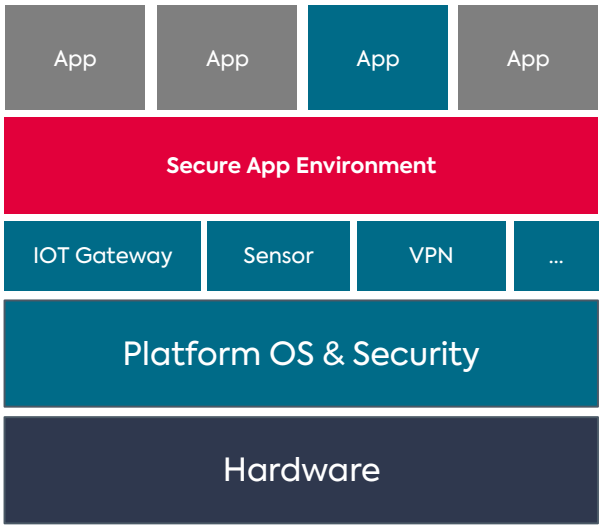



*Abbildung 4: Hardware-/Software-Stack Trusted edge Platform*

Die patentierte Hardware-Software-Appliance orientiert sich an den Empfehlungen des führenden Standards für Security in der industriellen Automatisierung ISA99 / IEC 62443. Neben Mikrosegmentierung und Isolation von Maschinen steht die sichere Konnektivität im Vordergrund. Mit dem integrierten Protokollübersetzer kann von unsicheren Kommunikationsprotokollen auf Protokolle zur sicheren Datenübertragung

in IT-Netzwerken umgesetzt werden. Zusätzlich bietet das Plattform-Konzept eine sichere Ausführungsumgebung für Applikationen. Typische Anwendungsszenarien dafür sind Fernwartung, Datenvorverarbeitung (edge computing) oder die flexible Anbindung von betreibereigenen Diensten. Externe Dienste wie IIoT-Plattformen werden ebenfalls umfassend unterstützt.

Das dazu fest verbaute, zertifizierte Secure Element (SE) – eine mit einer Smartcard vergleichbare Technologie – dient als Vertrauensanker und ermöglicht es beispielsweise, Verschlüsselungsmechanismen auszuführen oder kryptographische Schlüssel innerhalb eines manipulationssicheren Chips zu verwahren. Diese Sicherheitsfunktionen sind auch für externe Anwendungen nutzbar, die auf der Plattform ausgeführt werden. Dadurch ist Datenverschlüsselung und der Integritätsschutz von beispielsweise Sensordaten ebenso auf hohem Sicherheitsniveau umsetzbar wie auch die Identifikation der Maschinenkommunikation oder die Authentifikation von Fernzugriffen. Ebenfalls denkbar ist es, die mit der Sicherheitsplattform verbundene Maschine mit einer digitalen Identität zu versehen und in eine Public-Key-Infrastruktur (PKI) zu integrieren, was eine Vielzahl weiterer Anwendungsmöglichkeiten schafft.

**Die Vorteile einer Trusted Edge Platform im Überblick:**

| Funktionen | Vorteile |
|---|---|
| **Korrektive Maßnahmen** | Altgeräte werden durch Isolation oder Segmentierung vor unbefugtem Zugriff geschützt. Eine sichere Kommunikation von und zu den Geräten ist gegeben. Durch die Überwachung des Informationsflusses wird die IT-Sicherheit auf höchstem Niveau gehalten.<br><br>**Ergebnis:** Verhinderung von Sicherheitsvorfällen, Maschinenstillständen und damit verbundenen Kosten |
| **Präventive Maßnahmen** | Der Zustand von Maschinen kann überwacht werden. Darauf aufbauend können geplante und kontrollierte Wartungsprozesse eingeleitet werden. Der Fernwartungszugriff und die Fernwartungsleistung werden nahtlos, sicher und kostengünstig.<br><br>**Ergebnis:** Reduzierung der Betriebskosten |
| **Smarte Konzepte** | Die sichere Anbindung von IIoT- und Industrie 4.0-Systemen in der Infrastruktur kann gewährleistet werden. Erweiterte Anwendungsfälle wie Edge Computing und M2M-Vernetzung können implementiert werden.<br><br>**Ergebnis:** Effizienzsteigerung durch Automatisierung |
| **Mehrwertdienste** | Lieferanten und Drittanbieter können sicher in die OT-Umgebung integriert werden. Daten können flexibel, zeitnah und kostengünstig an interne und externe Dienstleister und Anbieter weitergegeben werden.<br><br>**Ergebnis:** neue Geschäftsmodelle und Umsatzmöglichkeiten |

# 7. Fazit

Mit dem Trusted Edge Platform Ansatz werden nicht nur verschiedene Anforderungsbereiche der Industrial Security und Maschine Security bedient, sondern auch Basisfunktionen zur Umsetzung von Industrie-4.0-Konzepten bereitgestellt. Hier wird offenbar, was IT-Sicherheitsanbieter schon seit Längerem postulieren: Cybersicherheitstechnologie kann, richtig eingesetzt, zum Enabler werden.

Eine Schutzhülle, die sich gleichsam um die Maschine legt, ist variabel und kann dadurch einfach an zukünftige Erfordernisse angepasst werden. Deshalb profitieren nicht nur Betreiber, die ihren Maschinenpark nachrüsten und den Digitalisierungsprozess mit einem soliden Fundament der IT-Sicherheit untermauern wollen, von solch einem Konzept. Auch Maschinenhersteller, die neue Maschinen-Designs mit einer zukunftssicheren Schutzhülle versehen möchten – und gleichzeitig den Anforderungen ihrer Kunden zur Absicherung von Bestandsmaschinen nachkommen wollen –, gehören zum Interessenkreis. Nicht zuletzt können Systemintegratoren sich der trusted edge Platform zunutze machen und ihre IT-Dienste an die Maschine des Betreibers bringen.

Maschinen stehen zwar strukturell gesehen am Rande eines Industrie-4.0-Netzwerks – „at the edge“ –, doch nichtsdestotrotz kommt ihnen eine zentrale Rolle zu. Deshalb ist es so wichtig, sie angemessen zu schützen und ihr Potenzial durch neue Technologien auszuschöpfen. Der Drang zur Verarbeitung von am Rande des Netzwerks erzeugten Daten entwickelt sich im Rahmen der digitalen Transformation rasant!

**Sie haben konkrete Rückfragen oder einen Bedarf an weiterführenden Informationen?**

Besuchen Sie die Website secunet.com/edge

oder schreiben Sie eine E-Mail an kritis@secunet.com

Für Rückfragen persönlich zur Verfügung steht Ihnen:

**secunet Security Networks AG**

Torsten Redlich

Stellvertretender Leiter
Division Kritische Infrastrukturen

Tel.: +49 201 5454-3068

# 8. Informationen zu secunet

secunet ist einer der führenden deutschen Anbieter für anspruchsvolle IT-Sicherheit. Mehr als 600 Experten konzentrieren sich auf Themen wie Kryptographie, E-Government, Business Security und Automotive Security und entwickeln dafür innovative Produkte sowie hochsichere und vertrauenswürdige Lösungen.

Zu den mehr als 500 nationalen und internationalen Kunden gehören viele DAX-Unternehmen sowie zahlreiche Behörden und Organisationen. secunet ist IT-Sicherheitspartner der Bundesrepublik Deutschland und Partner der Allianz für Cyber-Sicherheit.

secunet wurde 1997 gegründet und erzielte 2019 einen Umsatz von 226,9 Millionen Euro. Die secunet Security Networks AG ist im Prime Standard der Deutschen Börse gelistet. Weitere Informationen zu secunet finden Sie unter www.secunet.com.

---

[i] Bundesministerium für Wirtschaft und Energie, Industrie 4.0,
https://www.bmwi.de/Redaktion/DE/Dossier/industrie-40.html, zuletzt besucht im Juli 2019

[ii] McKinsey Digital, Industry 4.0 - How to navigate digitization of the manufacturing sector, 2015
[iii] Deloitte, Cyber-Security Report 2017 – Teil 2, 2017
[iv] Bundesamt für Sicherheit in der Informationstechnik, Industrielle Steuerungs- und Automatisierungssysteme, 2019

[v] https://www.shodan.io/

[vi] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-0708, zuletzt besucht im Juli 2019

[vii] https://support.microsoft.com/de-de/help/4500705/customer-guidance-for-cve-2019-0708, zuletzt besucht im Juli 2019
[viii] https://www.mckinsey.com/industries/high-tech/our-insights/new-demand-new-markets-what-edge-computing-means-for-hardware-companies
[ix] Bundesamt für Sicherheit in der Informationstechnik, Monitoring und Anomalieerkennung in Produktionsnetzwerken, 2019
[x] https://www.researchgate.net/publication/315670892_Past_present_and_future_of_Industry_40_-_, zuletzt besucht im August 2019
[xi] https://www.plattform-i40.de/PI40/Navigation/DE/Plattform/InternationaleKooperationen/internationale-kooperationen.html, zuletzt besucht im August 2019
[xii] https://www.plattform-i40.de/PI40/Navigation/DE/In-der-Praxis/Anwendungsbeispiele/anwendungsbeispiele.html, zuletzt besucht im August 2019
[xiii] https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data, zuletzt besucht im August 2019
[xiv] https://www.mckinsey.com/industries/high-tech/our-insights/new-demand-new-markets-what-edge-computing-means-for-hardware-companies?cid=soc-app