

Industrial- und IoT Security

Jahresrückblick 2019

14 Experten teilen ihre Meinung zu Entwicklung und Trends



sichere *industrie* 



ACHT:WERK
Jens Bußjäger
[Seite 3](#)



Archer International
Patrick Miller
[Seite 4](#)



Axians
Eric Dreier
[Seite 6](#)



CERT@VDE
Andreas Harner
[Seite 7](#)



FORTINET
Mirco Kloss
[Seite 8](#)



IBM
Lisa Unkelhäuser
[Seite 9](#)



McAfee
Raj Samanin
[Seite 10](#)



Phoenix Contact
Dr. Lutz Jänicke
[Seite 11](#)



Rhebo
Kristin Preßler
[Seite 12](#)



secunet
Torsten Redlich
[Seite 13](#)



secuvera
Tobias Glemser
[Seite 15](#)



VDMA
Steffen Zimmermann
[Seite 16](#)



Verve
Ron Brash
[Seite 17](#)



Wago
Jens Sparmann
[Seite 19](#)



Zusammenfassung
[Seite 20](#)

Betrachtet man das Jahr 2019 aus der Perspektive der Industrial Security, merkt man vor allem eins: Es tut sich was! Nicht nur ist die Anzahl an bekannt gewordenen Vorfällen gestiegen, sondern auch der Markt entwickelt sich beständig weiter: Die Nachfrage auf der Betreiberseite wächst, die Hersteller versuchen sich immer mehr an „Security by Design“, weltweit entstehen Communities und Konferenzen und auch das Bundesamt für Sicherheit in der Informationstechnik (BSI) treibt einen neuen Entwurf für das IT-Sicherheitsgesetz weiter voran.

Und doch steckt die Entwicklung noch in den Kinderschuhen. Wir fangen erst jetzt an richtig zu definieren, was „Industrial Security“ überhaupt bedeutet und wie diese perspektivisch einmal aussehen sollte.

Viele Rollen sind hierbei noch unklar und zahlreiche Konzepte, wie beispielsweise Security-By-Design, Zertifizierungen oder Komponentensicherheit fehlt es zum Großteil noch an einer praxisnahen Umsetzung.

Ebenso werden viele neuen Anbieter und auch Produkte aus dem Markt wieder verschwinden oder durch strategische Zukäufe in bestehende Unternehmen integriert.

Trotz dieser Ungewissheit und den strategischen Ausrichtungen stehen wir heute schon vor der Herausforderung, dass wir etwas „konkretes“ gegen die aktuelle Bedrohungslage unternehmen müssen, ohne dabei den Blick in die Zukunft zu vernachlässigen.

Die verschiedenen Experten/innen, die sich regelmäßig mit dem Thema auseinandersetzen, werden hierbei von zentraler Bedeutung sein. Klar ist, dass Industrial Security ganzheitlich betrachtet werden muss. Dies erfordert einen Fachaustausch aus unterschiedlichen Perspektiven. Hier sind vor allem die Hersteller, Integratoren und Dienstleister der Supply-Chain gefragt, aber auch die Security-Anbieter selbst, um gemeinsam mit den Anlagenbetreibern sinnvolle und handhabbare Inhalte zu schaffen.

Für diesen Jahresrückblick 2019 haben wir hierzu bei ganz unterschiedlichen Personen nachgefragt, wie sie persönlich die wahrgenommene Entwicklung und auch die aktuelle Bedrohungslage im Bereich der Industrial Security empfinden.

Ich wünsche Ihnen viel Spaß beim Lesen und weiterhin ein erfolgreiches Jahresende, erholsame Feiertage und einen guten Start ins neue Jahr!

Max Weidele



Jens Bußjäger

ACHT:WERK



Jens Bußjäger

Geschäftsführung, Acht-
werk GmbH & Co. KG



Wie haben Sie die Entwicklung der Industrial Security in diesem Jahr wahrgenommen?

Nachdem in 2017 der Versicherungsschutz für den Schaden an Mon-dolez durch die Erpressersoftware Notpetya die Zurich Versicherung mit einem Verweis auf „kriegsähnliche Handlungen“ abgelehnt wurde, kann man sich durchaus fragen:

„Ist denn schon Cyber-Krieg?“

Der Nato-Gipfel in Wales hatte bereits 2014 beschlossen, dass Cyberangriffe mögliche Auslöser des Bündnisfalles nach Artikel 5 sein können. Und auf dem Nato-Gipfel 2016 in Warschau wurde der Cyberraum zu einem eigenständigen Operationsgebiet erklärt.

Angriffe über Datennetze werden nun wie solche durch Land-, See- oder Luftstreitkräfte behandelt. So bedeutet dies, dass virtuelle Attacken den Bündnisfall auslösen könnten.

Im February 2018 wurden die Cyberangriff mit Notpetya sowohl von der USA als von Großbritannien der russischen Regierung zugeschrieben. So ist die Lage.

In welche Richtung werden sich Ihrer Meinung nach die Bedrohungen und Störfälle im nächsten Jahr entwickeln?

Nachdem simple Malware in 2019 bereits zu erheblichen Ausfällen und Schäden geführt hat, fragt man sich vielleicht zurecht **wieviele Regulierung die Industrie in Deutschland benötigt**, um deutsche Infrastrukturen zu schützen?

Dazu erwarte ich in 2020 einiges!

Wie sollte sich die Security anpassen, um dieser Entwicklung gerecht zu werden?

Am Ende des Tages ist es ja egal, ob Krieg oder Kriminelle die Schäden verursachen.

Wichtig ist, dass die Maßnahme eines **dedizierten Security Managements mit Angriffserkennung** für die Produktionsanlage oder kritische Infrastruktur, sowohl das eine als auch das andere behandelt.

OT-Security muss vor allem für Automatisierer sein und sich **am Kerngeschäft an der Industrie**, bzw. des produzierenden Gewerbe oder der kritischen Infrastrukturen ausrichten, und nicht an IT-Technologien. (wie IIoT oder Cloud)

„OT-Security muss vor allem für Automatisierer sein und sich am Kerngeschäft an der Industrie [...] ausrichten, und nicht an IT-Technologien.“

Patrick Miller

Archer International



Patrick Miller

Managing Partner,
Archer International



Gab es 2019 einen Security-Vorfall im Industriebereich, der Ihrer Meinung nach besonders relevant war?

The **Norsk Hydro Lockergoga ransomware** incident was the most significant of 2019 for me. Not just for the fact that it impacted ICS, but mostly for the **solid example Norsk Hydro provided** when it comes to

- 1) the ability to keep some operations alive **through manual process** ; and
- 2) the **transparency** of the incident response process. Too many organizations could easily fail at both.

A sobering reminder to test your ability to operate manually and test your incident response plans.

Wie haben Sie die Entwicklung der Industrial Security in diesem Jahr wahrgenommen?

While there were new products and services introduced, it was not a step-function shift in our security posture. I would call it positive, but incremental progress. Many new solutions are making bold promises but in reality, **we need more people cross-trained** in operations/engineering/process and IT/OT/ICS cybersecurity concepts.

Budgets are increasing for automation and technologies, but unfortunately they are still flat (or minimally improving) for personnel. The challenge here is that we still need people, even when we bring in new technologies or automate. I would argue **that the higher the degree of technology and automation, the more crucial the human actions become.**

In welche Richtung werden sich Ihrer Meinung nach die Bedrohungen und Störfälle im nächsten Jahr entwickeln?

We will likely see more “accidents” such as ransomware finding its way into ICS, but I expect **nation states** and other **non-governmental organizations** to continue practicing their abilities to impact more and more of the industrial footprint.

I expect to see just about everything in the industrial space impacted in some way – whether through an incident or through disclosure of research. **Obscurity is no longer on our side.** In fact, quite the opposite has happened. ICS is now one of the more interesting targets on the landscape.

Wie sollte sich die Security anpassen, um dieser Entwicklung gerecht zu werden?

Prepare for ransomware and wipers. **Backup** and **incident response** will determine whether you can survive or not.

Understand how to operate manually. Maybe not in full production mode, but practice how you can operate through an attack without stopping everything. This may mean islanding parts of your environ-



Patrick Miller **Archer International**

ment to protect them or possibly re-introducing some analog components in critical process steps.

Trained and experienced **people are the key component** in this plan though. The cost of hiring, education and retention is lower than a single crippling cyberattack.

„... the higher the degree of technology and automation, the more crucial the human actions become.“

Eric Dreier Axians



Eric Dreier

Business Development
Manager, **Axians**



Gab es 2019 einen Security-Vorfall im Industriebereich, der Ihrer Meinung nach besonders relevant war?

Ja, den gab es, nämlich **Norsk Hydro**. Hier konnte man sehr deutlich erkennen, welche Auswirkungen ein Cybersecurity-Vorfall haben kann. Nicht nur sind bei Norsk Hydro große Teile der Produktion für längere Zeit ausgefallen, es gab auch spürbare **Auswirkungen auf den globalen Markt** von Aluminium und Aluminiumerzeugnissen.

Wie haben Sie die Entwicklung der Industrial Security in diesem Jahr wahrgenommen?

Das vergangene Jahr hat mehrfach gezeigt, dass Schutz notwendig ist. Dies ist auch bei den meisten Betreibern von nicht KRITIS-relevanten Produktionsanlagen mittlerweile angekommen und führt dazu, dass sich immer mehr Unternehmen des Themas annehmen und es **gewollt auch zur Vorstandssache erklären**.

In welche Richtung werden sich Ihrer Meinung nach die Bedrohungen und Störfälle im nächsten Jahr entwickeln?

Meiner Meinung nach werden wir im nächsten Jahr noch nicht viel Veränderung in der Art der Vorfälle feststellen.

Bei dem Vorfall bei Norsk Hydro konnte man gut sehen, wie ein Vorfall einen Markt beeinflussen kann. Ich befürchte, dass in Zeiten von starken sozialen, politischen und ökonomischen Strömungen und Veränderungen, in denen wir uns derzeit befinden, solche **marktbeeinträchtigenden Szenarien** in den kommenden Jahren **gezielt eingesetzt** werden.

Damit ist dann nicht mehr nur im weitesten Sinne das angegriffene Unternehmen an sich, sondern (je nach Erfolg des Angriffs) auch die vom Angegriffenen abhängigen Unternehmen (Zulieferer, aber auch Mitbewerber) sowie die dort arbeitenden Menschen betroffen.

Wie sollte sich die Security anpassen, um dieser Entwicklung gerecht zu werden?

Security muss smarter werden. Es reicht heutzutage nicht mehr aus nur den „eigenen“ Cyberraum im Blick zu halten.

Bewertungen von Cyberrisiken müssen schon in der Planung auch das Marktumfeld einbeziehen, damit **mögliche Angriffsziele einer Branche oder Zulieferkette sich untereinander austauschen können** und somit auch ganze Branchen, Produktionsketten und Märkte resistenter gegen Manipulation aus dem Cyberraum werden.

„...mögliche Angriffsziele einer Branche oder Zulieferkette [sollten] sich untereinander austauschen können [damit] auch ganze [...] Märkte resistenter gegen Manipulation aus dem Cyberraum werden.“



Andreas Harner

Abteilungsleitung
CERT@VDE, VDE



Gab es 2019 einen Security-Vorfall im Industriebereich, der Ihrer Meinung nach besonders relevant war?

Ich sehe den Vorfall von **Norsk Hydro** als besonders relevant an, da er zeigt wie anfällig die ICS Welt ist und welche drastischen Konsequenzen Vorfälle in diesem Bereich nach sich ziehen.

Die vielen Angriffe auf die Intellectual Property der Firmen bleiben ja meist unerkannt und **werden leider nicht als persistente Gefahr wahrgenommen!**

Wie haben Sie die Entwicklung der Industrial Security in diesem Jahr wahrgenommen?

Es gibt mehr Firmen, bei denen die Awareness gestiegen ist und einige Firmen die proaktiv dieses Thema auch angehen, d.h. z.B. im CERT@VDE mitarbeiten. Allerdings sehen wir noch **viele Firmen im KMU Bereich**, für die das Thema **Security noch „ganz weit“ entfernt** ist...

In welche Richtung werden sich Ihrer Meinung nach die Bedrohungen und Störfälle im nächsten Jahr entwickeln?

Ransomware Angriffe auf die IT, die z.T. mit der Produktion verbunden ist, werden m.E. weiter ein bestimmendes Thema sein. Wann das **Einfallstor nicht mehr die IT sondern die OT Systeme** sind kann ich nicht beurteilen. Die Gefahr dafür ist allerdings real.

Wie sollte sich die Security anpassen, um dieser Entwicklung gerecht zu werden?

Security muss in der kompletten Wertschöpfungskette abgebildet werden: Zulieferer, Hersteller, Integratoren/Maschinenbauer und Betreiber müssen in diesem Netzwerk ihren Anteil dazu beitragen. Das CERT@VDE unterstützt diesen Ansatz, da es nur so gelingen wird, nachhaltig und übergreifend ein signifikant höheres Sicherheitsniveau in der Industrie zu erreichen.

„Security muss in der kompletten Wertschöpfungskette abgebildet werden.“



Mirco Kloss

Business Development
Manager IoT/OT - Enhanced
Technologies DACH,
FORTINET



Gab es 2019 einen Security-Vorfall im Industriebereich, der Ihrer Meinung nach besonders relevant war?

Die Zunahme von Ransomware und der **Fokus-Shift der CyberCrime-Community auf Industrie-Unternehmen** sind hier meiner Meinung nach zu nennen.

Anhand der 2019 Beispiele von **Norsk Hydro über Rheinmetall bis zu Pilz** sieht man, dass die Angriffe weit gefächert waren, wobei ein Angriff auf ein Safety produzierendes Gewerbe eine gewisse „Ironie“ mit sich bringt.

Wie haben Sie die Entwicklung der Industrial Security in diesem Jahr wahrgenommen?

Das Bewusstsein, etwas zu unternehmen und zumindest einmal Sichtbarkeit in OT Netzen zu schaffen, hat zugenommen.

Die Erkenntnis, dass die nach IEC 61508 beschriebene „Funktionale Sicherheit“ nicht mehr ausreichend ist, sondern auch ein **Augenmerk auf die darin verwiesene IEC 62443** bzgl. Cyber-Sicherheit gelegt werden muss, ist gewachsen.

Allerdings ist **Basis-Cyber-Sicherheit**, wie Segmentierung und sicherer Zugang zu den Systemen, in großen Unternehmen angekommen, **in der Fläche jedoch noch ausbaufähig**.

In welche Richtung werden sich Ihrer Meinung nach die Bedrohungen und Störfälle im nächsten Jahr entwickeln?

Auf der einen Seite werden Ransomware Angriffe auf die Industrie lukrativ bleiben und damit weiter wachsen und auf der anderen Seite werden auch „Attacken“, **besonders auf kritische Infrastrukturen**, weltweit zunehmen.

Wie sollte sich die Security anpassen, um dieser Entwicklung gerecht zu werden?

„Gemeinsam sind wir stark“, sprich **Lösungen sollten nach dem „Best of Integration“ Prinzip funktionieren**, sodass gewachsene Infrastrukturen nicht nur an die neuen Herausforderungen angepasst, sondern auch eingepasst werden können.

Dieses sollte aber nicht nur technologisch geschehen, sondern **auch auf der Mitarbeiterebene zwischen der OT und IT Abteilung**, sowie bestehende Prozesse aus der funktionalen Sicherheit um Cybersicherheit erweitert werden müssen.

„...gewachsene Infrastrukturen [sollten] nicht nur an die neuen Herausforderungen angepasst, sondern auch [in bestehende Prozesse] eingepasst werden können.“

Lisa Unkelhäußer

IBM



Lisa Unkelhäußer

Security Channel Leader
DACH, IBM



Gab es 2019 einen Security-Vorfall im Industriebereich, der Ihrer Meinung nach besonders relevant war?

Hier in der Region hat vor allem der **Angriff auf die Firma Pilz** für erhebliche Auswirkungen gesorgt. Nicht nur, weil die Lieferkette betroffen war, sondern auch durch die geographische Nähe und die **transparente Art und Weise wie Pilz mit dem Angriff umgegangen ist**. Das hat für sehr viel Awareness gesorgt.

Wie haben Sie die Entwicklung der Industrial Security in diesem Jahr wahrgenommen?

Das Thema hat **deutlich an Relevanz zugenommen**. Dies war sowohl auf der diesjährigen Industrie Messe in Hanover, als auch auf der it-sa deutlich zu sehen.

Abgesehen davon erhalten wir auch deutlich mehr Anfragen von Kunden. Dennoch sind **aktuell noch sehr selten wirklich Budgets eingestellt**, damit Projekte auch umgesetzt werden können.

Außerdem fehlt an vielen Stellen noch das nötige Know How, um das Thema richtig anzugehen.

Wie sollte sich die Security anpassen, um dieser Entwicklung gerecht zu werden?

Meiner Meinung nach müssen **die Bereiche Produktion und IT noch viel enger zusammen arbeiten**. Somit sehe ich die Entwicklung, dass Industrie & IT Messen das Thema aufgenommen haben, als sehr positiv.

Oftmals sollen eher **gemeinsame erste Pilotprojekte** angegangen werden als langwierig Strategien oder Konzepte zu diskutieren. Dies würde auch fehlenden großen Budgets entgegen kommen. Transparenz ist oftmals schon ein deutlicher Mehrwert, der auch Security einen großen Schritt nach vorne bringt.

„...die Bereiche Produktion und IT [müssen] noch viel enger zusammen arbeiten.“

Raj Samani McAfee



Raj Samani

Chief Scientist,
McAfee



Gab es 2019 einen Security-Vorfall im Industriebereich, der Ihrer Meinung nach besonders relevant war?

Well there have been many, but the recent work **McAfee Advanced Threat Research** published on a **vulnerability in a globally utilized building controller** was particularly notable.

Beyond discovery of the vulnerability, McAfee ATR **identified those systems that remain vulnerable**. This in many ways demonstrates the challenges for cybersecurity within this space, whereas in the IT space patching is part of parcel of regular operations. Here we have a perfect example of the challenge facing ICS systems.

Wie haben Sie die Entwicklung der Industrial Security in diesem Jahr wahrgenommen?

The **research being conducted within industrial security** has been particularly impressive, and it demonstrates the focus from the industry into the threats or rather potential threats. This is very encouraging since the potential impact of a system being exploited is considerably more damaging than traditional IT systems.

In welche Richtung werden sich Ihrer Meinung nach die Bedrohungen und Störfälle im nächsten Jahr entwickeln?

I wish I had a crystal ball! If we consider the overall theme for 2019 – the one thing we can be sure of is that the adversary will continue to improve and adapt.

Wie sollte sich die Security anpassen, um dieser Entwicklung gerecht zu werden?

Organizations, governments, private sector needs to **work together, faster and more effectively**. We have to do everything we can to protect the systems that safeguard our society.

„...one thing we can be sure of is that the adversary will continue to improve and adapt.“

Dr. Lutz Jänicke

Phoenix Contact



Dr. Lutz Jänicke

Product & Solution Security Officer, **Phoenix Contact Gruppe**



Wie haben Sie die Entwicklung der Industrial Security in diesem Jahr wahrgenommen?

Die öffentliche Wahrnehmung war 2019 deutlich geprägt von Ransomware-Vorfällen, die sowohl Behörden als auch Unternehmen betroffen haben, auch in der Automatisierungsbranche gab es Opfer.

Inwieweit Produktionsausfälle durch den Befall zentraler Unternehmenssysteme oder von Fertigungsanlagen verursacht wurden, ist sicher im Einzelfall zu betrachten. **Angriffe auf zentrale Systeme** und Dienste wie z.B. ein ERP-System wirken **schnell und weitreichend**, Angriffe auf verteilte, heterogene Systeme, wie häufig in der Produktion zu finden, stellen eine Herausforderung in der Wiederherstellung dar.

In welche Richtung werden sich Ihrer Meinung nach die Bedrohungen und Störfälle im nächsten Jahr entwickeln?

In Gesprächen zeichnet sich deutlich ab, dass die offensichtlich zunehmenden Risiken wahrgenommen werden. Wann und in welchem Umfang dies tatsächliche Auswirkungen auf die **Investitionsbereitschaft** in den Unternehmen haben wird, bleibt dennoch abzuwarten. Zumeist gibt es hier einen **deutlichen zeitlichen Versatz**.

Auf jeden Fall ist zu beobachten, dass auf **Lieferantenseite in der Breite deutliche Anstrengungen** in Form von sicheren Entwicklungsprozessen und weiterentwickelten Produkten unternommen werden.

Wie sollte sich die Security anpassen, um dieser Entwicklung gerecht zu werden?

Es ist zu erwarten, dass sich die Bedrohungslage weiterhin und möglicherweise schnell verschärfen wird. Angriffssoftware und professionelle, kriminelle Strukturen sind vorhanden und es gibt keinen Grund anzunehmen, dass hier von selbst eine Abrüstung stattfinden wird.

Gerade bei Ransomware sollte eine Risikoreduktion im Sinn der Schadensbegrenzung dadurch möglich sein, dass **Konzepte für die Sicherung und Wiederherstellung** von Daten und Systemen umgesetzt und die Verbreitung durch **Segmentierung** eingeschränkt wird. Auch sollte der Aspekt der **Resilienz** beleuchtet werden, nämlich wie kann auch unter eingeschränkten Bedingungen weitergearbeitet werden.

Letztlich sind **zentrale Systeme** oder eine sehr homogene Landschaft nicht nur einfacher in der Administration, sondern bieten für Angreifer auch einen „**Single Point of Attack**“. Nicht umsonst ist das ursprüngliche Internet mit verteilten, redundanten Routen und Namensdiensten gestaltet worden, die einen Teilausfall gut kompensieren können.

„Letztlich sind zentrale Systeme [...] nicht nur einfacher in der Administration, sondern bieten für Angreifer auch einen „Single Point of Attack“.

Kristin Preßler Rhebo GmbH



Kristin Preßler

COO, Rhebo GmbH



Wie haben Sie die Entwicklung der Industrial Security in diesem Jahr wahrgenommen?

Industrial Security ist 2019 **insbesondere bei kritischen Infrastrukturen angekommen.**

Die geplante Verschärfung des IT-Sicherheitsgesetzes, Störfälle wie am US Stromnetz im März oder die vielfältigen Vorfälle des Vorjahres in großen Industriekonzernen haben das **Bewusstsein der lückenhaften Absicherung klar geschärft.**

In welche Richtung werden sich Ihrer Meinung nach die Bedrohungen und Störfälle im nächsten Jahr entwickeln?

In den nächsten Jahren werden die Angriffe immer **spezifischer auf die jeweiligen Infrastrukturen zugeschnitten** und gängige signaturbasierte Angriffserkennung umlaufen.

Insbesondere IoT-getriebene Systeme werden ins Visier der Akteure geraten.

Wie sollte sich die Security anpassen, um dieser Entwicklung gerecht zu werden?

Die Industrial Security Entwicklung geht deshalb eindeutig Richtung **Defense-in-Depth**, die durch ein integriertes **Netzwerkmonitoring mit Anomalieerkennung** eine 360° Absicherung gegen externe Angriffe, Innentäter und menschliche Fehler ermöglicht.

„Insbesondere IoT-getriebene Systeme werden ins Visier der Akteure geraten.“

Torsten Redlich secunet



Torsten Redlich

Deputy Head of Division
Critical Infrastructures,
**secunet Security
Networks AG**



Gab es 2019 einen Security-Vorfall im Industriebereich, der Ihrer Meinung nach besonders relevant war?

Es gab verschiedene Medien relevante Ereignisse (**Pilz, NextPharma, Norsk Hydro**) über die ausführlicher berichtet wurde. Nicht zuletzt auch weil die Unternehmen damit Sensibilisierung schaffen wollen.

Es sind auch sehr **viele Sicherheitsfälle in kleinen und mittelständischen Industriebetrieben** bekannt - **nicht öffentlich** - wo Betriebsabläufe nachhaltig geschadet wurden und hohe Wiederherstellungskosten angefallen sind. Diese sind aus meiner Sicht besonders alarmierend, da diese Betriebe nicht allein mit der Bewältigung solcher Sicherheitsvorfälle klarkommen. Umso mehr KMU Betriebe demnach betroffen sind, desto mehr Schäden werden in der Breite zu registrieren sind.

Wie haben Sie die Entwicklung der Industrial Security in diesem Jahr wahrgenommen?

In den letzten Jahren **steigt die Awareness** - langsam aber kontinuierlich - und damit auch die Stärkung der Betriebsstätten.

Die Sicherheitsindustrie ist schon voll im Thema und investiert viel in neue Produkte und deren Produktplatzierung. Auch **Forschungsprogramme sind aktiv**, um passende Lösungen und Methoden mit zu entwickeln.

An was es aber definitiv fehlt, sind Personenkraft und Know How zur Umsetzung wichtiger Sicherheitsmaßnahmen auf Betreiberseiten. Die Umsetzung geht häufig einher mit **grundsätzlichen Fragen zur Modernisierung von Systemen und Prozessen**. Einfach neue Sicherheitsprodukte nehmen und einsetzen funktioniert nicht. Die über Jahrzehnte geprägte Anlagenlandschaft benötigt neben sehr gutem Risikomanagement (Ressourcen) auch gute **Sicherheitsarchitekturkonzepte und wandlungsfähige Produkte**.

In welche Richtung werden sich Ihrer Meinung nach die Bedrohungen und Störfälle im nächsten Jahr entwickeln?

Je nach Interesse der Angreifergruppen (staatlich, terroristisch, wirtschaftlich) wird man sich verschiedener Bedrohungen in Deutschland stellen müssen. Aktuell nimmt man eher Erpressungen und damit wirtschaftliche Interessen als direkt spürbare Gefahr war.

Aber auch **Spionage ist ein akutes Problem**, welches teilweise schwerer wahrnehmbar ist. Schon gar nicht in Netzwerken, in denen es keine Ressourcen für umfassendes Security Monitoring gibt. Ich persönlich aber auch immer auf **steigende IT-Komplexität und fehlende IT-Ressourcen** als wachsende Bedrohung hin. Sicherheitsvorfälle („IT-Pannen“) gibt es dazu mittlerweile einige.



Torsten Redlich secunet

Wie sollte sich die Security anpassen, um dieser Entwicklung gerecht zu werden?

Das lässt sich sicher nicht in einzelnen Aspekten bewerten und beantworten. Von Politik (die Rahmenbedingungen schaffen müssen) bis Herstellerfirmen (die Sicherheitsfunktionen im Planen und Bauen von Maschinen und Systemen) gibt es eine große Spannbreite an zu bedienenden Aufgabenfeldern.

Als einen interessanten Punkt möchte ich ein Dilemma herausgreifen, was zu lösen ist. Häufig spricht und **bewertet man den Reifegrad der IT-Sicherheit im „Maschinenraum“ sehr unterschiedlich**, also im Zusammenspiel der Netzwerke, Systeme und Anwendungen. Entscheidungsträger (Manager), Leiter der Anlagen, IT-Fachkräfte und Sicherheitsexperten haben unterschiedliche Sichten und Aussagen zum Thema. **Ohne die Möglichkeit gemeinsam – von Technik bis Management – die Risikolage und konkrete Auswirkungen zu bewerten**, werden Awareness und nötige Budgeteinstellungen ausbleiben.

Risikosimulationen und eine **allgemein gültige Methode für eine Sicherheitsbilanz**, die Auskunft über den Sicherheitszustand der betrieblichen IKT Infrastruktur gibt (analog eines KonTraG und Handelsgesetzbuches), könnten hier wertvolle Konzepte sein, die über Regulierung mit forciert werden.

„Ohne die Möglichkeit gemeinsam – von Technik bis Management – die Risikolage und konkreten Auswirkungen zu bewerten, werden Awareness und nötige Budgeteinstellungen ausbleiben.“

Tobias Glemser

secuvera GmbH



Tobias Glemser

Geschäftsführung,
secuvera GmbH



Gab es 2019 einen Security-Vorfall im Industriebereich, der Ihrer Meinung nach besonders relevant war?

Wie vermutlich alle anderen: **Pilz**. Große Auswirkung, noch unklare Ursache, aber transparente Kommunikation.

Wie haben Sie die Entwicklung der Industrial Security in diesem Jahr wahrgenommen?

Insgesamt beschäftigen sich mehr und mehr Firmen mit den Herausforderungen von Industrial Security. Immer mehr Firmen nehmen darüber hinaus wahr, dass den **Industriestandard IEC 62443** gibt.

Gleichzeitig scheint sich in manchem Bereichen eine **Industrial Security Community zu bilden**, die sich sehr gut in diesem Bereich auskennt. In der IT-Sicherheit gibt es ebenfalls eine Security Community. So wie die IT-Security-Community eine von der normalen IT getrennte Community darstellt, kann es leider auch bei Industrial Security laufen: Es werden Spezialrollen geschaffen, die disjunkt von den Geschäftsmodellen sind. **Die Integration von Industrial Security in die Geschäftsmodelle ist leider nur bei wenigen Firmen erkennbar.**

In welche Richtung werden sich Ihrer Meinung nach die Bedrohungen und Störfälle im nächsten Jahr entwickeln?

Die Angriffe werden gezielter werden. Ist ein Angreifer im Unternehmensnetz, wird die Infiltrierung exakter und für den Angreifer nachhaltiger erfolgen. So kann der monetäre Erfolg maximiert werden.

Umgekehrt werden staatliche Angreifer mehr und mehr **Störfälle mit Auswirkungen auf die nationale Wirtschaft** haben. Ein Beispiel gab im September diesen Jahres der Einsatz des Virus Shamoon auf gegen die Öl- bzw. Gasförderfirmen Aramco in Saudi Arabien und and RasGas in Qatar.

Wenngleich die Angriffe vor allem die Office-IT betrafen, war das Ziel der Angriffe offensichtlich: Den großen Ölhahn zumindest zeitweise virtuell zuzudrehen.

Wie sollte sich die Security anpassen, um dieser Entwicklung gerecht zu werden?

Für bestehende Umgebungen ist oft die Angriffsoberfläche nicht ausreichend aufgeklärt. Segmentierung flacher Netze ist eine vielleicht plump wirkende, aber sehr relevante Aufgabe. Für beides gibt es gute Ansätze. Bei Neuentwicklungen - egal ob auf Komponenten- oder Anlagenebene - sind **Standards vorhanden**, die nur darauf warten genutzt zu werden.

„So wie die [klassische] IT-Security-Community eine von der normalen IT getrennte Community darstellt, kann es leider auch bei Industrial Security laufen.“

Steffen Zimmermann

VDMA



Steffen Zimmermann

Head of Competence
Center Industrial Security,
VDMA



Gab es 2019 einen Security-Vorfall im Industriebereich, der Ihrer Meinung nach besonders relevant war?

Der Vorfall ist noch gar nicht so lange her und jedem in der Industrie präsent. Die **Ransomware-Attacke auf PILZ** hat gezeigt, dass das Thema der OT-Security (Eigensicherheit) selbst bei solchen Unternehmen, die sich mit Industrial Security beschäftigen, nicht zu 100% wirksam umgesetzt werden kann. **100% Security gibt es nicht.**

Wie haben Sie die Entwicklung der Industrial Security in diesem Jahr wahrgenommen?

Dieses Jahr gab es zwei Hauptrichtungen. Auf der Produkt-Seite zum einen die Diskussion um **Vertrauenswürdigkeit in der Lieferkette** und zum anderen um die **Kennzeichnung der Cybersicherheit vernetzter Geräte**. Wir erleben die Renaissance der Regulierung. Selbst die Sektorverbände rufen nach einem horizontalen, harmonisierten Rechtsakt.

Auf der anderen Seite die Einschläge in der produzierenden Industrie rund um Ransomware – mit massiven Auswirkungen bis in die Fertigung. Die Einschläge kommen nicht nur näher – sie **werden auch deutlich aggressiver geführt**. Es ist ein Geschäftsmodell geworden.

In welche Richtung werden sich Ihrer Meinung nach die Bedrohungen und Störfälle im nächsten Jahr entwickeln?

Professionelle Ransomwareangriffe auf Industrieunternehmen werden weiter zunehmen. Durch die Konvergenz von IT und OT steigt die Abhängigkeit der verteilten Produktionssysteme weiter an, Stichwort OPC UA und Azure-Cloud-Anbindung. Hier wird sich zeigen, dass die **„8 Fallacies of Distributed Computing“ immer noch aktuell** sind und die Systemdesigner, Administratoren und Geschäftsführer die gleichen Fehler machen wie schon vor 30 Jahren.

Darüber hinaus ist die Zeit mal wieder reif für eine **Open Source Lücke** apokalyptischen Ausmaßes. Und nicht zuletzt befürchte ich einen Cyberangriff, der sich **in einer kritischen Infrastruktur ausbreitet** und damit den Weg für eine Verschärfung der Gesetzeslage bereitet. Gut möglich, dass wir auch den ersten **KI-gestützten Cyberangriff** sehen.

Wie sollte sich die Security anpassen, um dieser Entwicklung gerecht zu werden?

Die Industrial Security sollte zukünftig die Möglichkeiten der **KI für devensive Security** nutzen. **Security by Design** sollte verpflichtend werden für den Einsatz von vernetzten Produktionssystemen in der Industrie. Weg vom Gedanken, dass diese mit einem „Security-Label“ verkauft werden; hin zur Formulierung von Anforderungen für den sicheren Betrieb (Safety+Security). Das gibt weder das IT-Sicherheitsgesetz her (nur IT-Security!), noch die Arbeitsstättenverordnung (nur Safety).

„[Cyberangriffe sind] ein Geschäftsmodell geworden.“

Ron Brash

Verve Industrial Protection



Ron Brash

Director of Cyber Security
Insights, **Verve Industrial
Protection**



Gab es 2019 einen Security-Vorfall im Industriebereich, der Ihrer Meinung nach besonders relevant war?

In my opinion, **Norsk Hydro** was among one of the most relevant OT cyber security attacks for a number of reasons.

The actual complexity of the attack was not particularly advanced, but rather it was indicative of a few new paradigm shifts: one, they were **specifically targeted**, two, **it came through IT infrastructure** that affected OT systems (think IT commodity systems being used for OT tasks), three, there were obvious and **very costly OT impacts** in regards to output, four, traditional mechanisms such as printed „paper“ orders and **manual processes help achieve a minimal level of continued productivity**, partial success with cyber insurance claims to recover damages, and finally, also demonstrates how **transparency and out of band technologies** aided the success of the organisation's recovery (internally and globally).

Norsk is a hallmark of how many organisations should behave during and after an incident.

Wie haben Sie die Entwicklung der Industrial Security in diesem Jahr wahrgenommen?

The development of the OT cyber security market has been relatively stagnant in terms of products despite global awareness. Few truly novel solutions were added to the market and although others had more celebrity like media coverage, **asset owners want** OT systems management (OTSM) technologies that **enable activity, recovery, prevention, inventorying and daily duties**. Passive anomaly detection tools will be purchased by various vendors and become a standard feature, but also their usability is beginning to diminish with the advent of **secure industrial network protocols**.

Additionally despite the flare for threat intelligence/hunting technologies, **secure supplychain technologies will leap frogg ahead** and are evolving such that they can be utilized not only for software installers or drivers, but also for documents and software libraries contained/ utilized by various OEM tooling. This has another great effect to support asset owners in validating solution components installed by third parties and integrators. And there is great value for these types of solutions, particularly in determining origins of a software component, and will overlap detection of fraudulent hardware/software (which had been reported several times in 2019).

In welche Richtung werden sich Ihrer Meinung nach die Bedrohungen und Störfälle im nächsten Jahr entwickeln?

In 2020, I suspect there will be an increase of events **affecting OT systems through IT/OT convergent infrastructure**, but potentially more toward OT-targeted devices such as PLCs, relays and sensors.

Some of these will be more advanced than others, but **many will be executed through Windows-based applications**, and these will creep



Ron Brash Verve Industrial Protection

into non-traditional, but critical organizations such as airports, and navigation systems.

Secondly, I predict **a rise in false, grey-market, and re-manufactured OT components**; this has several risks, and pose differing threats than a direct attack, but may well affect the safety, reliability and productivity of any number of industrial facilities.

Thirdly, there may also be **a rise of non-human based attacks** with the advent and commoditization of relatively „simple“ logic that mimics a smarter application that automates probing and attacking systems. This may increase the number of low-impact, but high-frequency events that put the financial feasibility of various industries into question; similar to ransomware attacks.

Finally, there will be an **increase of wireless/RF-enabled attacks** in the industrial sectors. Equipment is getting cheap enough for ubiquitous deployment, but also, by third-parties to add remote connectivity solutions to „ease“ their jobs despite bypassing security controls of an organisation. Technologies do not exist today that are easily available nor focused on non-wired networks.

Wie sollte sich die Security anpassen, um dieser Entwicklung gerecht zu werden?

Security will never be guaranteed nor will it be absolute, but there will be a focus on **getting the basics right**, upgrading to managed technologies, improved asset management (logical and physical), better system configuration & patching, and logging/alerting, but more importantly, **ensuring effective action in response and prevention vs. mere alerting**.

Better technologies will be adopted to improve human efficiencies along the lines of orchestration and algorithms, but the overall expectation is that **humans still need to be in the Observe, Orient, Decide and Act circular process** in regards to changing threats and management.

As for supply chain, signed firmware validation and infrastructure will also evolve, but with requirements for vendor interoperability.

And finally, **new wireless anomaly detection** techniques and appliances will also emerge as well to counter RF threats (malicious, insider and other). These will be more widely sought after in a number of industries as electronic warfare continues to grow at the nation state levels, but also by domestic and localised hacking organizations/persons.

„Norsk [Hydro] is a hallmark of how many organisations should behave during and after an incident.“

Jens Sparmann

WAGO Kontakttechnik GmbH & Co. KG



Jens Sparmann

Systemspezialist Security,
**WAGO Kontakttechnik
GmbH & Co. KG**



Gab es 2019 einen Security-Vorfall im Industriebereich, der Ihrer Meinung nach besonders relevant war?

Norsk Hydro und Pilz waren aus meiner Sicht sehr interessant zu beobachten. Nicht ganz der Industriebereich, aber der Angriff auf den **Heise Zeitschriften Verlag** mit anschließender Aufarbeitung ist ebenfalls nennenswert.

Wie haben Sie die Entwicklung der Industrial Security in diesem Jahr wahrgenommen?

Die **Vernetzung der Unternehmen ist gestiegen**. Viele, meist lokale Treffen, bieten eine gute Plattform des Austausches. Auch die Hersteller machen Ihre Hausaufgaben in Bezug auf die IEC 62443. **Aus Hersteller Sicht ist die Zusammenarbeit mit verschiedenen Gremien und dem BSI gut.**

In welche Richtung werden sich Ihrer Meinung nach die Bedrohungen und Störfälle im nächsten Jahr entwickeln?

Ich denke, dass die **Gebäude-Automatisierung stärker in den Fokus der Angreifer** rücken wird. Die Frequenz der Angriffe wird zunehmen und von komplexerer Qualität sein.

Wie sollte sich die Security anpassen, um dieser Entwicklung gerecht zu werden?

Die **Awareness der Betreiber muss steigen**, das gelingt am besten in dem wir darüber sprechen. Nur durch einen gemeinsamen Austausch werden wir in der nötigen Geschwindigkeit besser und können uns gut aufstellen.

„Nur durch einen gemeinsamen Austausch werden wir in der nötigen Geschwindigkeit besser und können uns gut aufstellen.“

Aus dem Jahresrückblick haben sich viele verschiedene Perspektiven, u.a. mit bereits konkreten prozessualen und technischen Ansätzen, ergeben. Diese Zusammenfassung bietet Ihnen einen Überblick zu den wichtigsten Entwicklungen, Trends und Konzepten.

Der grundlegende Fortschritt in der Industrial Security wird als positiv wahrgenommen, auch wenn allen klar ist, dass noch sehr viel Arbeit geleistet werden muss. Dies trifft sowohl auf die Kommunikations- und Communityarbeit, als auch auf die Produktentwicklung auf Herstellerseite, sowie die Umsetzung auf Betreiberseite zu.

Damit diese Vorhaben aber auch gelingen, muss zwingend die weitere Entwicklung der aktuellen Bedrohungslage betrachtet werden.

Learnings aus den Angriffen auf Pilz und Norsk Hydro



**Weitere Angriffsszenarien
finden Sie auf**

[www.sichere-industrie.de/
angriffsszenarien](http://www.sichere-industrie.de/angriffsszenarien)

In einem Punkt sind sich alle einig: Die Vorfälle bei Pilz und Norsk Hydro können beide als Musterbeispiele in diesem Jahr betrachtet werden. Dies trifft sowohl auf die Auswirkungen der Vorfälle als auch auf die Art, wie beide Unternehmen mit der Situation umgegangen sind, zu.

Neben der Tatsache, dass es kostspielige Schäden in der Produktion bzw. den Steuerungssystemen gab, fällt vor allem der Umstand ins Gewicht, dass die Angriffe über die IT-Infrastruktur (bzw. den IT/OT Schnittstellen) initiiert wurden. In beiden Fällen wurden Auswirkungen auf die gesamte Wertschöpfungskette deutlich.

Zwei Dinge haben sich hier für die Beteiligten als besonders hilfreich herauskristallisiert:

- 1) Die Fähigkeit Prozesse manuell aufrechtzuerhalten und
- 2) die transparente Art und Weise wie in der Außenkommunikation berichtet wurde.

Bei beiden Angriffen handelt es sich hierbei um eine mahnende Erinnerung, dass trotz aller Prävention- und Schutzmaßnahmen auch eine getestete Incident Response Planung dazugehören muss.

Die besonderen Herausforderungen der Industrie

Darüber hinaus existieren zahlreiche Vorfälle im KMU-Umfeld, welche in der Öffentlichkeit nicht wahrgenommen werden und so das wahre Bild der Bedrohungslage verzerren.

Dem Industrie-Mittelstand fehlt es dabei häufig an notwendigen Ressourcen, um erfolgte Angriffe erfolgreich bewältigen zu können.

Bedenklich ist vor allem der Zustand, dass entdeckte Schwachstellen im OT-Umfeld oftmals weitestgehend unbehandelt bleiben. Hier Be-



Mehr zum Thema Awareness gibt es auf

www.sichere-industrie.de/awareness

darf es vor allem einer Professionalisierung des IT-Betriebs von OT-relevanten IT-Systemen.

Weitere Angriffsvektoren, die möglicherweise unter dem Radar fallen, sind gefälschte bzw. wiederaufbereitete ICS-Komponenten aus dem Graumarkt und der Anstieg der Industriespionage. Erwähnenswert ist auch die Anhäufung von Vorfällen in der Gebäudeautomatisierung.

Die Awareness steigt, aber es ist noch deutlich Luft nach oben

Insgesamt lässt sich festhalten, dass die Awareness für Bedrohungen aus dem Cyberraum insbesondere bei kritischen Infrastrukturen und Industriekonzernen angestiegen ist und auch die wahrgenommene Handlungsnotwendigkeit stetig wächst. Die wohl größte Aufklärungsarbeit wird hier im KMU Bereich notwendig sein.

Bei vielen Betreibern wird die Thematik immer häufiger in die Vorstandsebene getragen, obwohl in 2019 noch selten wirkliche Investitionsbereitschaft gezeigt wurde.

Auch die Vernetzung unter den einzelnen Beteiligten ist gestiegen, national und international bilden sich Communities welche die Thematik auf Konferenzen und Messen tragen. Erfreulich ist hier auch die stark zunehmende Arbeit in Gremien und Forschung.

Trotz der positiven Entwicklung sollte jedoch nicht vergessen werden, dass viele Firmen noch sehr weit vom Thema Security bzw. dessen Umsetzung entfernt sind und darum die Aufklärungs- und Diskussionsarbeit im Moment umso wichtiger wird.

Supply-Chain-Security weiter auf dem Vormarsch

Aber auch auf der Lieferantenseite wird deutlich erkennbar, dass Anstrengungen unternommen werden. Insbesondere die Mitarbeit in Gremien wird hier hervorgehoben.

Ein möglicher Treiber für diese Entwicklung steckt sicherlich hinter der ansteigenden Diskussion um die Vertrauenswürdigkeit in der Lieferkette und der Kennzeichnung von IT-Sicherheit bei Netzwerk-Komponenten, häufig basierend auf den Anforderungskriterien der IEC 62443-4-1 und 4-2.

Es entstehen sichere SCM-Lösungen, die den Betreibern die Validierung von Drittkomponenten erleichtern und dabei unterstützen, betrügerische Hard- und Software zu ermitteln.

Spezialisierte Angriffe auf die Industrie

In einem weiteren Punkt sind sich die Experten/innen ebenfalls einig: Es ist anzunehmen, dass zukünftige Angriffe noch aggressiver, profes-

sioneller und dynamischer geführt werden.

Es wird immer mehr deutlich, dass sich Cyber-Angriffe als lohnenswertes Geschäft etablieren und sich dabei insbesondere kritische Infrastrukturen als ein lukratives Ziel anbieten.

Hier geraten zunehmend vernetzte industrielle Systeme ins Visier der Angreifer. Ransomware-Kampagnen, welche früher IT/OT-Systeme eher als Beifang kompromittiert haben, werden vermutlich in 2020 zunehmend mehr auf OT-gerichtete Geräte wie SPS, Relais oder Sensoren ausgerichtet sein.

Der Mensch im Mittelpunkt der Industrial Security

Das fehlende Know-How und die nicht vorhandenen Ressourcen sind in den Augen vieler Experten der größte Flaschenhals.

Im Beitrag wurden einige - teils bekannte - Ansätze wie Defense-In-Depth, Netzwerkmonitoring und die Heterogenisierung von Systemlandschaften aufgegriffen. Der eigentliche gemeinsame Nenner hierbei ist jedoch gut ausgebildetes Personal, welches fachübergreifendes Wissen aus der Automatisierung und der IT- und OT Security vereinen kann. Dies würde auch der noch sehr volatilen Produktlandschaft entgegenkommen.

Die Hauptaussage hierbei ist: Je mehr die Digitalisierung in industriellen Prozessen voranschreitet, desto mehr werden wir auf menschliche Interaktion angewiesen sein, um automatisierte Prozesse zu überblicken, Fehlverhalten zu überwachen und im Störfall eingreifen zu können.

Wir müssen mehr zusammenarbeiten

Und zwar nicht nur abteilungsübergreifend (beispielsweise IT und OT) sondern auch über Prozessketten und Branchen hinweg. Die Cyber-crime Community hat den Mehrwert von Kooperation längst für sich erkannt und organisiert sich immer professioneller.

Hierzu muss die IT-Sicherheit ein kleiner fester Bestandteil des täglichen Handelns werden und auch mögliche Synergieeffekte (z.B. durch Zusammenführen von IT-Sicherheit und Functional Safety) weiter verfolgt werden.

Generell gilt es den Spagat zu finden, der neben der konzeptuellen und strategischen Gedankenarbeit (aus Gremien u. Forschung) konkrete Pilotprojekte fördert. Denn klar ist, dass wir schnell viel mehr praxisnahe Erfahrungen sammeln müssen, um hieraus unsere langfristige Strategie und funktionierende Maßnahmen abzuleiten.



Vernetzen Sie sich in unserem Industrial Security Stammtisch

[www.sichere-industrie.de/
industrial-und-iiot-security-
stammtisch](http://www.sichere-industrie.de/industrial-und-iiot-security-stammtisch)

sichere-industrie.de ist ein freier Wissenspool zu den relevanten Themen der industriellen IT-Sicherheit. Der Fokus liegt auf praxisnahen Hilfestellungen und der Förderung des Austausches aller Beteiligten.

Die Plattform ist zum Mitmachen gedacht und ist damit offen für jegliche Art einer praxisnahen Beteiligung (z.B. in Form von Fachartikeln oder Veranstaltungen).

Möchten Sie Ihr Wissen teilen und damit aktiv den Fachaustausch vorantreiben? Dann freuen wir uns sehr auf Ihre Nachricht und berücksichtigen Sie auf Wunsch auch gerne für unseren kommenden Jahresrückblick im nächsten Jahr.

Email:

info@sichere-industrie.de

Online:

<https://sichere-industrie.de>



***sichere*industrie** 

simplified industrial security