

Industrial und IoT Security Jahresrückblick 2021

*19 Experten teilen ihre Meinung zu
Entwicklung und Trends*



Vorwort

Wenn man das Jahr 2021 im Hinblick auf die Entwicklungen der Security im Industrieumfeld betrachtet, dann kamen wir an zwei Themen nicht vorbei:

Nach einigen Referentenentwürfen und kontroversen Diskussionen bei Interessengruppen und Verbänden hat es die **Neufassung des IT-Sicherheitsgesetzes** im Mai über die Ziellinie geschafft. Der Kreis der Unternehmen, die jetzt von der Regulierung betroffen sind, erweitert sich mit den Änderungen der Schwellenwerte in der neuen KRITIS-Verordnung, den Unternehmen im besonderen öffentlichen Interesse und dem neuen Sektor Siedlungsabfallensorgung.

Dabei stehen nicht nur **Betreiber** von Kritischen Infrastrukturen vor neuen Herausforderungen. In einigen Belangen sind vor allem die **Hersteller** betroffen, deren IT-Produkte für die Erbringung der Leistung in den KRITIS-Betrieben von wesentlicher Bedeutung sind. Security ist eine Gemeinschaftsaufgabe!

Unser zweites Thema (wer hätte es erwartet), das die Aufmerksamkeit für Security in den Unternehmen erhöht, liegt in der weiter zunehmenden **Professionalisierung von Cyberangriffen**. Ransomware-as-a-Service – das bedeutet eine arbeitsteilige und damit hocheffektive Vorgehensweise von Cyberkriminellen, die in vernetzten Lieferketten die Schwachstelle des einen schnell zum Problem für alle macht.

In Kritischen Infrastrukturen ist der Druck, Lösegeldforderungen für verschlüsselte Daten zu zahlen, besonders hoch. Aber auch bei anderen Unternehmen nimmt die Motivation zu, Aufwände für Industrial Security zu leisten oder aber einzufordern.

Eine Konsequenz aus der Entwicklung ist die steigende Anzahl an Anpassungen in den Beschaffungsprozessen der Unternehmen. Unter dem Thema **“Supply Chain Security”** werden Security-Mindestkriterien von Lieferanten gefordert, wie beispielsweise ein Produktentwicklungsprozess nach der IEC 62443 oder ein Incident Response Team.

Der wachsenden Bedrohungslage und den gesetzlichen Vorgaben gerecht zu werden, das ist eine Herausforderung für Betreiber, Integratoren und Hersteller gleichermaßen. Orientierung bieten dabei Organisationen und Arbeitsgruppen sowie die wachsende Community, die sich der Industrial Security in Automationsumgebungen verschrieben hat.

Wir haben Experten gebeten, ihre persönlichen Einschätzung der Entwicklungen und einen Ausblick für das neue Jahr zu teilen. Sie zeichnen ein umfassendes, aber auch persönliches Bild für eine herausfordernde Situation.

Ich wünsche Ihnen viel Spaß beim Lesen der interessanten Beiträge, außerdem einen erfolgreichen Abschluss des Jahres 2021 und einen guten Start in 2022.

Bleiben Sie gesund!



Max Weidele
Gründer
» Sichere Industrie «

Gibt es eine Entwicklung im Bereich Industrial Security, die aus Ihrer Sicht für das Jahr 2021 besonders war?

Ja, es gibt da was Besonderes, leider. Es ist besonders traurig zu sehen, wie oft inzwischen im Bereich Industrial Security Ransomware- und andere Cyberangriffe erfolgreich durchgeführt werden und wie das kontinuierlich steigt. Gegenmaßnahmen haben offenbar weder das IT-SiG 2.0 bewirkt noch die ganzen Befugnisserweiterungen oder offensiven Vorgehensweisen, welche die Regierung mit den Sicherheitsbehörden da als vermeintliche Allheilmittel sieht.

Wichtig ist daher, dass ein Umdenken stattfindet, hin zur Erhöhung der Cyberresilienz von ICS-Umgebungen, so dass die Widerstandsfähigkeit gegenüber Cybervorfällen kontinuierlich steigen kann.

Verändert die zunehmende Marktanforderung nach Security Ihrer Einschätzung nach etwas spürbar in den Unternehmen?

Bei kritischen Infrastruktur-Betreiberinnen kommt so langsam Bewegung in die Security-Fragestellungen da, wo es beispielsweise durch das BSI-Gesetz reguliert und vorgegeben ist. Aber auch hier könnte es deutlich zügiger gehen und es könnte deutlich mehr passieren, so dass seltener Ausfälle geschehen.

Es ist also weiterhin sehr viel zu tun. Insbesondere stelle ich fest, dass die Awareness inzwischen überall vorhanden ist, allerdings ist das Verständnis, was dies für die eigenen Risiken bedeutet, nicht sehr ausgeprägt. Hier muss also noch die Transformation passieren. Gegebenenfalls müssen auch die richtigen Anreize geschaffen werden, angereichert mit Incentivierungen, so dass Security in solchen Umgebungen verstanden und eingebracht wird und am Ende alle davon profitieren.

»Wichtig ist daher, dass ein Umdenken stattfindet, hin zur Erhöhung der Cyberresilienz von ICS-Umgebungen, so dass die Widerstandsfähigkeit gegenüber Cybervorfällen kontinuierlich steigen kann.«

Was ist Ihrer Meinung nach die größte Herausforderung im Kontext Security für 2022?

Die desolate Cybersicherheitspolitik in Deutschland. Es ist ein Cyberwimmelbild der Verantwortungsdiffusion an verschiedensten Akteuren mit unklaren Zuständigkeiten vorhanden und ständig kommen weitere Akteure dazu.

Gefühlt müssen Sicherheitsmaßnahmen auch und insbesondere für Industrial-Security-Umgebungen - also beispielsweise kritische Infrastrukturen - gegen die Vorstellungen der Regierung eingebracht werden.

Speziell der KRITIS-Sektor Staat und Verwaltung, zu dem durchaus auch kommunale Betreiberinnen mit ICS-Umgebungen gehören, unterliegt weiterhin keinen klaren Security-Anforderungen. Hier sind immerhin schon die KRITIS-Betreiberinnen durch BSIG § 8a deutlich weiter, aber noch lange nicht am Ziel. Ohne diese Anforderungen wird es sehr herausfordernd, Security in Zukunft zu erhöhen oder besser zu etablieren und kontinuierlich zu leben.



Manuel Atug
Head of Business
Development
HiSolutions AG



Tim Bauer **AK: IT-Sicherheit in der Gebäudeautomation**

Gibt es eine Entwicklung im Bereich Industrial Security, die aus Ihrer Sicht für das Jahr 2021 besonders war?

Mehr denn je waren Smart-Building-Technologien im Fokus und die Nachhaltigkeiten von Gebäuden wurden auf die Probe gestellt: Mobiles Arbeiten und die Etablierung von Home-Office-Arbeitsmodellen bringt viele Fragestellungen beispielsweise hinsichtlich der Nutzung von Gebäuden mit sich. Es ergeben sich besondere Herausforderungen, wenn gesetzliche Vorgaben etwa für die Zutrittskontrolle nach bestimmten Voraussetzungen, hinsichtlich der maximalen Raumnutzung oder für die Belüftung einzuhalten sind.

Auch das Hochfahren von Gebäuden nach langen Stillstandsphasen ist nicht immer problemlos zu bewerkstelligen. Wenn die Technologien in den Fokus geraten und teilweise schnell umgesetzt werden sollen, wird klar, dass Smart Building zu 80% vom Einsatz von IT-Infrastruktur und Technologien abhängig ist, und zwar flächendeckend und gebäudedeckend. Dabei liegt die Verantwortung beim Facility Management und Betreibern, die den professionellen IT-Betrieb eigentlich nicht zu ihren Kernkompetenzen zählen.

Industrial Security oder eben Smart Building Security hat einen ganz wichtigen Fokus erhalten, weil es um Themen wie Fernwartung, Building Management in der Cloud und Informationsbeschaffung von der Feld- bis in die Managementebene geht. Jeder Smarte Sensor, jeder Akteur, jedes Gerät erweitert die Angriffsfläche und verändert die Risikoeinschätzung.

Verändert die zunehmende Marktanforderung nach Security Ihrer Einschätzung nach etwas spürbar in den Unternehmen?

Unternehmen beschäftigen sich immer mehr mit der Frage, wie sie ihre innovative Projektinstanz „Smart Building“ in den Betrieb überführen können. Es kommen zunehmend Anfragen aus dem Facility Management und von Betreibern der Gebäudeautomation, die vor der Aufgabe stehen, die Gebäudeautomation als Teil der OT in die Sicherheitsbetrachtung einzubeziehen und dabei die Vorgaben der IT entsprechend umsetzen zu müssen.

„[...] Smart Building Security hat einen ganz wichtigen Fokus erhalten, weil es um Themen wie Fernwartung, Building Management in der Cloud und Informationsbeschaffung von der Feld- bis in die Managementebene geht.“

Was ist Ihrer Meinung nach die größte Herausforderung im Kontext Security für 2022?

Die Landkarte der Security ist so groß, die Angriffsvektoren so vielfältig, dass wir schnell aus den Augen verlieren, wo wir eigentlich ansetzen müssten: bei den Basics!

Transparenz ist notwendig, um die Mehrwerte zu erkennen, die auf lange Sicht den größten Effekt bieten. Das erfordert Basisarbeit, und zwar mehr denn je: Assetmanagement (ich kann nur schützen, was ich kenne), Risikobewertung und -einschätzung, um Maßnahmen abzuwägen. Außerdem braucht es echte, stabile Netzwerkdesigns als Unterbau. In der Industrial Security ist das Netzwerk oft unsere einzige echte Handhabe, um die Security zu erhöhen.

Das bringt auch Anforderungen an die Organisation mit sich, um notwendige Ressourcen zu erkennen und aufzubringen. Ein Smart Building erzeugt nicht weniger Aufwand in der Verwaltung, vor allem, wenn es einfach so nebenher gemanaged werden soll.



Tim Bauer
Gründer & Lead

AK:
IT-Sicherheit in der Gebäudeautomation



In your opinion, has 2021 been a special year for industrial security concerns? If so, why?

2021 has shown both society and industry that regardless of geography, domestic or abroad - supply chains can be affected by cascading changes, shortages, and failures.

Texas power outages combined by an aggregate of “conditions that were not supposed to happen”. The Oldsmar water treatment facility being accessed via unauthorized commodity third-party remote access software & credentials - thankfully being noticed by human operators. Colonial was unable to schedule, transport, and ascertain the quantity of product shipped, and a controlled shutdown led to shortages of fuel due to ransomware. Large-scale meat industries disrupted again due to ransomware. Chip shortages due to COVID19 manufacturing & shipping delays cascaded their way into many industries leading to stoppages of manufacturing lines, and increasing uncertainties for the end consumer of whether network infrastructure equipment would arrive on time.

Then there was the new Executive Order from the Biden administration that pushed forward critical infrastructure and Software Bills of Materials (SBOMs) as priorities. And nearly simultaneously, the TSA issued their own controversial regulations for cybersecurity.

All of these events, and others during 2021 demonstrate the past and current fragility of systems built upon systems, and a significant need to rethink technology & resilience paradigms if society is to be protected. One solution (or part of) may be regulation, but time will tell - especially if organizations continue to exhibit conditions ripe for ransom, backdooring, or being utilized as an attack platform (e.g., SolarWinds).

Do you recognize a changed attitude within companies due to the upcoming market requirements for security?

The majority of executives in large critical infrastructure and manufacturing sectors are beginning to take a far more serious look at securing their environments with initiatives that are more than mere lip-service to shareholders.

From a general standpoint, industries that have a higher public profile such as oil & gas or energy, are taking the lead on making an impactful difference in their risk profiles. Unfortunately, where low-margins/high-volume products generally dominate, these sectors will need a much larger commitment in terms of budget and continual investment, and will continue to lag behind for the near-term future.

Conversely though, the OT cybersecurity outlook has improved and a base-level understanding of the need for OT/ICS cybersecurity awareness, or looking towards external impacts/consequences is trending positive. This is a significant achievement, and it's even being seen with procurement questionnaires (arguably not the most effective, but still an improvement), security being transformed from an extra cost and to a mandatory requirement due to legislation, boards asking hard questions, and of course, an increase in fundamental OT cybersecurity upgrades - even if its a knee jerk reaction.

»The fragility of systems built upon systems cause a significant need to rethink technology & resilience paradigms if society is to be protected.«

According to your assessment - what will be the main challenge for 2022 regarding security subjects?

Ransomware will continue to be a challenge for organizations that are non-homogenous and burdened with several eras of systems and integrations. However, beyond this, the demand and also legislation for improved cybersecurity of software/devices through SBOMs will be a major challenge for asset owners already swimming in an ever growing swamp of vulnerabilities and broken/useless CVSS CPEs.

Vendors too will struggle in identifying software components in products that have already been deployed or end-of-lifed (EoL), and to keep up with component/vulnerability tracking & notification overall; especially where fast paced FOSS or frameworks have been integrated. One solution will include SBOMs and VEX documents combined, however, there will be a major need for accurate, and seamless vulnerability tracking in inventory management systems, vendors to produce products that feature frequent updates, and asset owners to increase their pace with electronic asset maintenance. But none of this will take place without significant investment into enriching reported risks and vulnerabilities.

Product/asset security will be messy before it gets better in 2022; especially when some pundits argue against increased transparency because it will help the “bad guys”. But, my argument is that it's often too easy for most attackers to cause an OT outage via legitimate functionality, and improved product development is not a bad thing for anyone (plus, it might even lower total cost of ownership TCO).



Ron Brash
VP of Technical
Research &
Integrations

**aDolus
Technology Inc.**



Gibt es eine Entwicklung im Bereich Industrial Security, die aus Ihrer Sicht für das Jahr 2021 besonders war?

Die Digitalisierung schreitet voran, denn ohne Daten sind Use Cases wie zum Beispiel Digital Twin und Predictive Maintenance nicht möglich. Cybercrime hat das erkannt, auch den Use Case „Wenn die Produktion steht, ist das Unternehmen at Risk“. Daher gibt es immer mehr Ransomware-Angriffe auf diese Unternehmen, um die Produktion zu stören und damit einhergehend auch eine Unterbrechung der Lieferkette zu erzwingen.

Die Anforderung nach Segmentierung bis ins untere Level des Purdue-Modells in den Anlagen ist angekommen und wird von den Kunden immer mehr angenommen. Auch verschwimmen die klassischen Grenzen des Purdue-Modells immer weiter, da immer mehr smarte Sensoren angeschlossen werden und Technologien wie 5G Einzug halten. Die Cloud ist daher so langsam in der OT angekommen, inklusive der Security Herausforderungen. Wir bekommen inzwischen zunehmend die Anfragen der Anlagenbetreiber in Richtung der Hersteller mit, Teile der Leitsysteme in die Cloud zu verlegen. Was für die Hersteller ähnlich herausfordernd ist, wie der Drang nach Virtualisierung vor wenigen Jahren.

Verändert die zunehmende Marktanforderung nach Security Ihrer Einschätzung nach etwas spürbar in den Unternehmen?

Die Veränderung hat bereits vor einigen Jahren angefangen und ist nun im C-Level angekommen. Wir sehen die Anforderungen nach Security auch immer mehr in Ausschreibungen, und Security wird auch von Lieferketten entsprechend immer mehr eingefordert.

Die Novelle des IT-Sicherheitsgesetzes, das sogenannte IT-SiG2.0, trägt ebenfalls zu erhöhter Nachfrage nach Security bei den Unternehmen bei, bringt auf der anderen Seite aber auch Verunsicherung unter den Anlagenbetreibern mit sich.

Allerdings fördert der weiter zunehmende Fokus auf die Security und eine ganzheitliche Absicherung beider Welten, IT & OT, die Zusammenarbeit. Die alten „Grabenkämpfe“ gehören daher immer mehr der Vergangenheit an. Und das ist auch gut so!

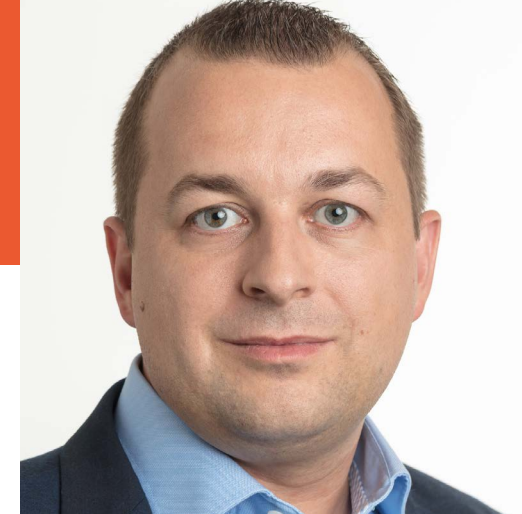
»Die Cloud ist so langsam in der OT angekommen, inklusive der Security-Herausforderungen.«

Was ist Ihrer Meinung nach die größte Herausforderung im Kontext Security für 2022?

OT- & IT-Know-how sind hier zu nennen, denn der Fachkräftemangel ist hier noch ausgeprägter. Daher wird auch immer mehr die Frage nach dem Betrieb der OT Security gestellt werden müssen und damit einhergehend wird es eine Steigerung der Anfragen nach Managed Services und Outsourcing geben.

Auch ist eine weitere Zunahme der smarten Sensoren zu erwarten und daher muss die Security auch mehr in Richtung dieser Sensoren gebracht werden. Dieses erwarten wir nicht nur in Industrieumgebungen, sondern auch im Bereich der Smart Infrastructure, wie zum Beispiel der Gebäudeleittechnik, aber auch beim Thema der zukünftigen Mobilität und anderen mehr.

Ebenfalls wird die Luft langsam dünn für die Endpoint Security im OT-Bereich. Die Unterstützung alter Betriebssysteme wird nach und nach von den klassischen (und den Automatisierungsherstellern freigegebenen) Endpoint-Lösungen abgekündigt. Neue Lösungen werden hier Einzug halten.



Daniel Buhmann
Principal Systems
Engineer OT/IoT



Mirco Kloss
Business Development
Manager Operational
Technology DACH

FORTINET, Inc.



Gibt es eine Entwicklung im Bereich Industrial Security, die aus Ihrer Sicht für das Jahr 2021 besonders war?

Im Jahr 2021 gab es eine besondere Entwicklung in der Industrial Security, welche nichts mit aktuellen Sicherheitsvorfällen zu tun hatte. In der IEC-Standardisierung hat die Arbeit an drei neuen 62443-Projekten begonnen. Alle drei Projekte werden von deutschen Expertinnen und Experten geleitet sowie von vielen weiteren auch stark inhaltlich unterstützt.

Die zum Teil sehr träge Arbeit an der 62443 in den letzten Jahren wird damit neu belebt, und die Arbeit an einzelnen Teilen wird hoffentlich auch zukünftig schneller fertiggestellt. Die drei Projekte beschäftigen sich mit der Entwicklung von Profilen für die 62443, ein wichtiges Projekt, um die Norm einheitlich auf spezielle Anforderungen zuschneiden zu können. In zwei weiteren Projekten werden Prüf-/Evaluierungsmethoden entwickelt. Diese beiden Projekte sind wichtige Beiträge, um Qualitätssicherung und Zertifizierung international einheitlich durchzuführen.

Weiter hat der TeleTrust Use Cases veröffentlicht, um die 62443-4-2 (Security Anforderungen an Komponenten) handhabbarer zu machen und die Einstiegshürde bei Anwendung der Norm zu reduzieren.

Für einige Anwender wird die Norm damit vielleicht aber auch wieder abschreckender. Doch auch, wenn die Aufnahme neuer Teile die Einstiegshürde subjektiv erhöht, so galt schon immer, nicht alle Teile müssen angewandt werden.

Verändert die zunehmende Marktanforderung nach Security Ihrer Einschätzung nach etwas spürbar in den Unternehmen?

Die Marktanforderungen bezüglich Cybersecurity setzen viele Unternehmen aktuell noch vor viele Fragezeichen. Dies liegt insbesondere daran, dass klare Lieferantenanforderungen noch selten sind, zudem gibt es mit dem Cybersecurity-Act (CSA) eine noch sehr abstrakte Anforderung für eine zukünftige, einheitliche Produktzertifizierung. In dieser Gemengelage ist aktuell die nachhaltigste Empfehlung, sich mit der Umsetzung eines sicheren Entwicklungsprozesses zu beschäftigen, was aber auch keine kurzfristige Aufgabe ist.

Für viele Unternehmen ist die Beachtung von Security leider weiterhin ein optionales Feature und keine grundsätzliche Daseinsvorsorge.

»Für viele Unternehmen ist die Beachtung von Security leider weiterhin ein optionales Feature und keine grundsätzliche Daseinsvorsorge.«

Was ist Ihrer Meinung nach die größte Herausforderung im Kontext Security für 2022?

Die Adaption und Anwendung der 62443-4-1-Vorgehensweise (Sicherer Entwicklungsprozess) in Unternehmen, und insbesondere im Mittelstand, ist eine der wichtigsten Herausforderungen im kommenden Jahr. In den letzten Jahren haben wir schon gesehen, dass die großen Hersteller über Zertifizierungen darstellen konnten, dass die Norm für sie anwendbar ist. Der Beweis, ob dies auch effektiv und wirtschaftlich für den breiten Mittelstand möglich ist, steht allerdings noch aus.

Zu Beginn und während der Pandemie haben wir mit vielen Unternehmen gesprochen, welche den sicheren Entwicklungsprozess umsetzen wollten, leider sind viele Initiativen sehr früh wieder zurückgestellt worden. Unsere Erfahrung aus der Praxis hat gezeigt, dass entgegen der allgemeinen Annahme hierfür keine riesigen Budgets notwendig sind. Der Mittelstand hat gute Voraussetzungen, um die Umsetzung anzugehen, muss dies jetzt aber auch noch machen.



Sebastian Fritsch
Leiter Industrial
Security/Prüfstelle



Mirco Weber
Industrial Security
Experte

secuvera GmbH





Fred Gordy
Director of Cybersecurity
Intelligent Buildings, LLC



» Without a doubt ransomware will remain the number one threat to building control systems. «

Fred Gordy **Intelligent Buildings, LLC**

In your opinion, has 2021 been a special year for industrial security concerns? If so, why?

Yes. This year has seen some things that have happened that were shocking, but not surprising.

The release of the Iranian cyber papers specifically called out how to hack Smart Buildings and introduction of the new term „Killware“. Killware as e.g. used for the attack on a water treatment system in Florida brings attention to the fact that manipulating control systems in a certain way would result in death. Basically the term refers to any type of attack that is intended to result in harm or death to a human though any kind of attack can cause lethal impacts.

Do you recognize a changed attitude within companies due to the upcoming market requirements for security?

Yes. We have companies contacting us to cyber assess control systems that are looking to purchase and making “buy or not buy” based on the outcome of the assessment.

According to your assessment - what will be the main challenge for 2022 regarding security subjects?

Without a doubt ransomware will remain the number one threat to building control systems.

»Security diffundiert mehr und mehr in die Lieferketten.«

Andreas Harner **CERT@VDE**

Gibt es eine Entwicklung im Bereich Industrial Security, die aus Ihrer Sicht für das Jahr 2021 besonders war?

In unserem Kontext ist die extrem stark anwachsende Zahl an Advisories und CVEs etwas Besonderes. Es zeigt, dass sich die mit dem CERT@VDE kooperierenden Unternehmen Ihrer Verantwortung bewusst sind und handeln.

Verändert die zunehmende Marktanforderung nach Security Ihrer Einschätzung nach etwas spürbar in den Unternehmen?

Ja: Security diffundiert mehr und mehr in die Lieferketten. Unternehmen, die Bestandteil dieser Lieferketten bleiben möchten, müssen sich um Cybersecurity im eigenen Unternehmen und in den eigenen Produkten kümmern.

Was ist Ihrer Meinung nach die größte Herausforderung im Kontext Security für 2022?

Wir haben viel zu wenige Security-Experten auf dem Arbeitsmarkt. Es braucht hier eine gemeinsame Kraftanstrengung zwischen Staat und Industrie, um dieser Herausforderung in 2022 zu begegnen.



Andreas Harner
Abteilungsleiter
CERT@VDE &
Cybersecurity

DKE Deutsche
Kommission Elektro-
technik Elektronik
Informationstechnik
in DIN und VDE





Dr. Lutz Jänicke
Corporate Product &
Solution Security
Officer

PHOENIX CONTACT
GmbH & Co. KG



»Die allgemeine Entwicklung der Bedrohungslage [...] sollte jedem Unternehmen klarmachen, dass Security nicht ignoriert werden darf.«

Dr. Lutz Jänicke **PHOENIX CONTACT** **GmbH & Co. KG**

Gibt es eine Entwicklung im Bereich Industrial Security, die aus Ihrer Sicht für das Jahr 2021 besonders war?

Ich würde die Entwicklung als evolutionär einschätzen. Die allgemeine Entwicklung der Bedrohungslage (Ransomware, Exchange-Server, Zero-Day-Schwachstellen) und die Professionalisierung der Angreifer sollte jedem Unternehmen klarmachen, dass Security, egal in welchem Bereich, nicht ignoriert werden darf. Dies wird auch im Markt bestätigt, indem von Betreiberseite aus mehr und intensivere Security-Anforderungen gestellt werden.

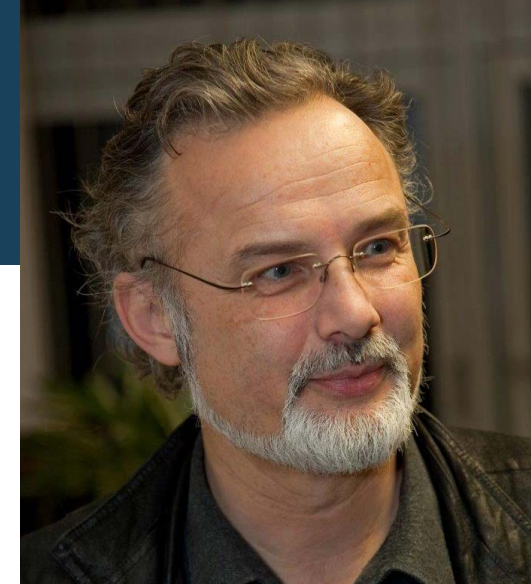
Verändert die zunehmende Marktanforderung nach Security Ihrer Einschätzung nach etwas spürbar in den Unternehmen?

Ja. Immer mehr Kunden formulieren ihre Anforderungen und insbesondere große Kunden setzen mit ihrer Einkaufsmacht die Lieferanten unter Druck. Dies gelingt, wenn auf dem Markt genügend Angebote in der notwendigen Security-Qualität vorhanden sind oder neu entstehen. Dann bleibt den Anbietern nur die Wahl, die geforderte Security zu liefern oder entsprechende Kunden aufzugeben.

Was ist Ihrer Meinung nach die größte Herausforderung im Kontext Security für 2022?

Es gilt, die richtige Balance zu finden zwischen den Möglichkeiten der Digitalisierung und Automatisierung und den größer werdenden Security-Risiken. Auf der einen Seite werden immer mehr Funktionen bereitgestellt und die Effizienz gesteigert, indem immer mehr integriert, teils zentralisiert wird, dabei zudem die Komplexität gesteigert. Auf der anderen Seite muss die (Cyber-)Resilienz gesteigert werden, was typischerweise durch Redundanz, Dezentralisierung, Entkopplung, Vereinfachung und Reserven geprägt ist.

Ein klassischer Zielkonflikt, für den es keine einfachen Antworten gibt.



Dr. Michael Missbach
SAP & IoT Architect

KAESER
KOMPRESSOREN



»Die größte Herausforderung ist es, Prinzipien und Methoden zu implementieren, die wirklich sicher sind, statt solche, die nur so ausschauen.«

Dr. Michael Missbach **KAESER KOMPRESSOREN**

Gibt es eine Entwicklung im Bereich Industrial Security, die aus Ihrer Sicht für das Jahr 2021 besonders war?

Die zunehmende Anzahl von Meldungen über Ransomware-Angriffe in den Medien, die es auch in 2021 wieder gab, führt zu einer veränderten Haltung bei Kunden. Auch solche, die nicht tief in der IT-Materie stecken, hinterfragen bei der IoT-Thematik, wo große Datenmengen über das Internet in die Cloud geschickt werden, neuerdings den Sicherheitsaspekt.

Verändert die zunehmende Marktanforderung nach Security Ihrer Einschätzung nach etwas spürbar in den Unternehmen?

Die einfachen Zeiten sind vorbei, denn für Kunden geht es längst nicht mehr nur um die Funktionalität der eingesetzten Produkte. Mit jeder neuen Ransomware-Attacke erreichen uns mehr Anfragen von Kunden, die verifizieren möchten, wie sicher die Produkte sind.

Wir müssen viel mehr Zeit investieren, um Fragestellungen mit unterschiedlicher Komplexität und Expertise zu behandeln und entsprechend zu belegen, was wir für die IT-Security tun.

Was ist Ihrer Meinung nach die größte Herausforderung im Kontext Security für 2022?

Die größte Herausforderung ist es, Prinzipien und Methoden zu implementieren, die wirklich sicher sind, statt solche, die nur so ausschauen, weil es manche Softwareunternehmen nicht besser wissen.

In your opinion, has 2021 been a special year for industrial security concerns? If so, why?

This has been a special year for industrial security because many of the threats and attacks predicted to affect the industrial side have actually happened. For example, ransomware has both directly and indirectly impacted industrial operations. Supply chain attacks have also made their way into the industrial environment. Remote access has been a persistent issue but several new attacks were recorded in 2021. An unfortunate convergence of several of the most dire risks were realized. As such, executives of industrial organizations found themselves on the front page of newspapers, in government hearings and in very difficult conversations with shareholders and boards.

A natural result of this is regulation and legislation to hopefully force industrial organizations - especially those in critical infrastructure - to at least maintain a minimum set of security controls. An interesting shift in this area is that regulators are beginning to consider both IT and OT because of the interdependencies highlighted by some of the attacks in 2021. Of course, regulation moves much slower than the threat so the approach, while necessary in some cases, will always be reactive and minimally sufficient. Given the variety in different types of companies, infrastructures and technologies, a common set of security controls that can be enforced across all sectors is challenging to establish but models such as IEC 62443 and NIST 800-82 are being examined for this purpose. Though some progress is being made on regulation, the common mantra that compliance does not equal security must be continually reinforced.

Do you recognize a changed attitude within companies due to the upcoming market requirement for security?

The global industrial solutions marketplace and industrial hardware, software and services supply chain have been severely disrupted due to balkanization and geopolitical disputes over potential theft, espionage or even possibly acts of sabotage/war. The supply chain challenges will continue to grow as political tensions and ideologies influence the development, delivery and maintenance of industrial solutions around the world. Some global organizations are attempting to balance the opposing market and political forces with varying degrees of success.

The market is responding to the security issues in productive ways. Solutions such as transparency centers, independent review boards, certification houses, software/firmware/hardware bill of materials (SBOM/FBOM/HBOM/XBOM) and similar "vetting" methods are all being explored to potentially stabilize the market and provide greater certainty in industrial purchasing options. Further, many "consumers" of industrial products are asking - and more importantly, willing to pay - for more security features in their products. Security and supply chain authenticity have become market differentiators for solutions, in addition to being required in many cases through regulation.

»Though some progress is being made on regulation, the common mantra that compliance does not equal security must be continually reinforced.«

According to your assessment - what will the main challenge for 2022 be regarding security subjects?

The main challenge for 2022 will be navigating the complex and challenging mix of regulation and supply chain requirements/expectations. Some common threads have emerged, given the industrial security events of 2021. Focusing on areas such as:

- XBOM (particularly when coupled with additions like VEX - vulnerability exploitability exchange)
- Network and endpoint monitoring/visibility solutions
- Zero trust
- Intelligent isolation/islanding, shear-away networks - continued operations through the attack
- Incident response and recovery



Patrick Miller
Chief Executive Officer

Ampere Industrial Security



Gibt es eine Entwicklung im Bereich Industrial Security, die aus Ihrer Sicht für das Jahr 2021 besonders war?

Sehr positiv empfinde ich die Security-Aktivitäten vieler Organisationen und Arbeitsgruppen aus der industriellen Automatisierung. Zum Beispiel die Arbeitsgruppe Industrial Security des TeleTrust stellt sich der Aufgabe, wie man die IEC 62443 auf Komponentenebene verständlich anwendbar macht. Man verfolgt hier ein sehr pragmatisches Konzept, und zwar anhand von konkreten Anwendungsfällen wie zum Beispiel Firewall und Router im OT-Umfeld. Gleichwohl beschäftigen sich natürlich auch VDMA, ZVEI und VDE ausgiebig und immer intensiver mit Aufklärung und klaren Empfehlungen für Automatisierer.

Das Bild der letzten Jahre in Bezug auf Ransomware hat sich leider auch nicht signifikant verändert. Jedoch als besonders stellte sich schon die Situation dar, dass bei betroffenen Produktionsunternehmen quasi die IT und OT stillstand und das für Wochen oder Monate. Das zeigt deutlich, wie abhängig beide Bereiche voneinander sind.

Eine weitere positive Entwicklung ist die Etablierung des deutschen CERT (Computer Emergency Response Team). Angesiedelt beim VDE ist der CERT@VDE die optimale Plattform, wo Schwachstellen in industriellen Geräten gemeldet und verarbeitet werden. Anwender aus der Industrie haben dadurch einen schnellen und zentralen Überblick.

Verändert die zunehmende Marktanforderung nach Security Ihrer Einschätzung nach etwas spürbar in den Unternehmen?

Ja, wir spüren eine Vielzahl an Nachfragen zu IT-Sicherheitseigenschaften unserer Produkte. Bei den Gesprächen gibt es viel mehr „Tiefe“ zum Thema und die Gesprächspartner bringen schon viel Fachwissen mit. In den früheren Jahren waren es mehr Checklisten zum Ausfüllen, jetzt verstehen die Unternehmen verstärkt die Themen in der Security und fragen gezielter nach. Das fordert uns als Hersteller, aber gleichzeitig freut es mich, dass unsere langjährige Bewusstseinsbildung für die Security ihre Früchte trägt.

Unternehmen fördern verstärkt die Weiterbildung Ihrer Mitarbeiter und schaffen gezielt neue Stellen in der IT-Sicherheit. Das spürt man!

»Security und Retrofit von Maschinen und Anlagen zu vereinen, das sehe ich als die größte Herausforderung im OT-Umfeld.«

Was ist Ihrer Meinung nach die größte Herausforderung im Kontext Security für 2022?

Ich würde dazu gleich ein neues Schlagwort definieren wollen: Security@Retrofit.

Security und Retrofit von Maschinen und Anlagen zu vereinen, das sehe ich als die größte Herausforderung im OT-Umfeld. Denn der bestehende Maschinenpark wird zunehmend „IIoT“-befähigt und das bedeutet, dass Maschinensteuerungen unweigerlich aus ihrer vergangenen Isolierung geholt werden und per Netzwerk untereinander verbunden werden. Sei es zur Cloud, zur Büro-IT oder direkt an das Internet. Diese verbundenen Steuerungen haben aber wenig bis gar keine Security-Eigenschaften, beziehungsweise will man auch daran am wenigsten verändern.

Hier sollten und dürfen die Integratoren nicht nur die Funktion in den Vordergrund stellen, sondern müssen auch das Thema Security kritisch betrachten. Einfache Maßnahmen wie starke Passwörter und Schwachstellenbetrachtung können hier schon viel Wert sein. Ebenso ist ein Backup des SPS-Programms genauso wichtig, wie ein Backup der IT.



Siegfried Müller
Geschäftsführer

MB connect line
GmbH



Simeon Mussler - Jannis Stemmann - Philipp Pelkmann **Bosch CyberCompare**

Gibt es eine Entwicklung im Bereich Industrial Security, die aus Ihrer Sicht für das Jahr 2021 besonders war?

In 2021 haben wir eine Evolution statt einer Revolution gesehen: OT Security ist vor allem für KRITIS-Unternehmen im Fokus, die den Vorgaben des IT-Sicherheitsgesetzes unterliegen. Diese müssen nun auch ein aktives Monitoring durchführen, eine Maßnahme, die neu ins IT-SiG 2.0 aufgenommen wurde.

Bei vielen mittelständischen Unternehmen ist dagegen noch die klassische IT Security im Vordergrund. Die OT ist weiterhin nicht Ziel einer aktiven Attacke, vielmehr geht der Angriffsvektor über die IT und breitet sich dann auf die OT aus.

Wir sehen, dass Product Security auch im Maschinenbau zunehmend wichtig wird, der entsprechende Kompetenzaufbau in den Organisationen ist daher ein Thema.

Verändert die zunehmende Marktanforderung nach Security Ihrer Einschätzung nach etwas spürbar in den Unternehmen?

Ja, wir beobachten, dass es dabei um zwei Richtungen geht, nämlich die Absicherung über eine Cyberversicherung vs. Invest in Securitymaßnahmen.

Dazu kommt es zu einer spürbaren Aufwertung der CISO- / IT-Security-Rollen in den Unternehmen. Auch gehen immer mehr Unternehmen schrittweise den Rückstand in der OT Security an, der gegenüber der IT Security besteht.

»Es kommt darauf an, die Kritikalität der Anwendungen und Systeme zu bewerten und die individuelle Security-Strategie darauf auszurichten.«

Was ist Ihrer Meinung nach die größte Herausforderung im Kontext Security für 2022?

Es bleibt eine große Herausforderung, nicht der Versuchung zu erliegen, Marketingthemen hinterherzulaufen, wie XDR, Monitoring, ZTA in OT und anderen, sondern geeignete Sicherheitsmaßnahmen risikobasiert zu treffen.

Es kommt darauf an, die Kritikalität der Anwendungen und Systeme zu bewerten und die individuelle Security-Strategie darauf auszurichten.



Simeon Mussler
Chief Operating Officer



Jannis Stemmann
Chief Executive Officer



Philipp Pelkmann
Chief Technology Officer

Bosch CyberCompare





Mirko Ross
CEO
asvin GmbH



»Unternehmen müssen sich auf zahlreiche neue regulatorische Anforderungen einstellen, die sowohl Auswirkungen auf Prozesse als auch auf Produkte haben werden.«

Mirko Ross **asvin GmbH**

Gibt es eine Entwicklung im Bereich Industrial Security, die aus Ihrer Sicht für das Jahr 2021 besonders war?

Angriffe auf die Software-Supply-Chain haben um ca. 650% im Vergleich zum Vorjahr zugenommen. Im Fokus sind Anbieter und Applikationen im Bereich Cybersecurity, Cloud und das Einschleusen von Schadsoftware in Open Source Libraries. Das Thema wird uns in den kommenden Jahren also verstärkt beschäftigen.

Verändert die zunehmende Marktanforderung nach Security Ihrer Einschätzung nach etwas spürbar in den Unternehmen?

Unternehmen reagieren immer noch zu spät, statt zu agieren. Würden alle Unternehmen Ihre IT-Infrastruktur sauber aufstellen und up to date halten, wäre Ransomware kein Thema. Die Anzahl der Ransomware-Vorfälle in 2021 zeigen hier deutlich das Defizit.

Was ist Ihrer Meinung nach die größte Herausforderung im Kontext Security für 2022?

Wir werden mehr Anstrengungen der Gesetzgeber weltweit sehen, die Cybersicherheitsrisiken zu minimieren. Das heißt, dass sich Unternehmen auf zahlreiche neue regulatorische Anforderungen einstellen müssen, die sowohl Auswirkungen auf Prozesse als auch auf Produkte haben werden.

Außerdem werden neue Normen, Standards und Gesetze zur Produkthaftung und dem technischen Aufbau für Sicherheit erwartet.

Es wird also spannend, dies mit den vorhandenen Ressourcen und Werkzeugen umsetzen zu können und dabei auch noch wirtschaftliche Geschäftsmodelle betreiben zu können.

»IT meets OT, nicht nur im Guten. Nie war es nötiger ein PSIRT zu gründen als jetzt.«

Jens Sparmann **WAGO Kontakttechnik GmbH & Co. KG**

Gibt es eine Entwicklung im Bereich Industrial Security, die aus Ihrer Sicht für das Jahr 2021 besonders war?

IT meets OT, nicht nur im Guten. Nie war es nötiger ein PSIRT zu gründen als jetzt. Als Hersteller von Automatisierungshardware können wir den Trend hinsichtlich der Bedrohungslage, der sich aus dem BSI-Lagebericht ableiten lässt, bestätigen.

Der Fokus der Personen, die Sicherheitslücken in Produkten finden, hat sich klar in Richtung Industrial Security verschoben. Wir müssen uns viel intensiver mit Security-Schwachstellen auseinandersetzen, als es uns lieb ist.

Verändert die zunehmende Marktanforderung nach Security Ihrer Einschätzung nach etwas spürbar in den Unternehmen?

Ja, das Bewusstsein für Security ist deutlich gestiegen und das nicht nur in großen Unternehmen. Zunehmend sitzen Mitarbeiter der IT mit am Tisch, wenn es um die Planung der Automatisierung geht. Das Tooling aus der klassischen IT wird vermehrt in der OT-Welt eingesetzt. Es wird deutlich mehr miteinander gesprochen.

Was ist Ihrer Meinung nach die größte Herausforderung im Kontext Security für 2022?

Die Balance zwischen IIoT Device und Industriesteuerung zu finden und richtig umzusetzen, das ist eine echte Herausforderung! Das eine steht für Schnelllebigkeit und Aktualität, das andere für garantierte Funktion über Jahre hinweg. Allein das Patchmanagement für ein 10 Jahre altes Gerät wird für Hersteller ein spannendes Thema werden.

Ebenso wird uns die Umsetzung der IEC 62443 auf Hersteller- und Integratorenmehrung die nächsten Jahre beschäftigen.



Jens Sparmann
Systemspezialist
Security

**WAGO Kontakttechnik
GmbH & Co. KG**



Gibt es eine Entwicklung im Bereich Industrial Security, die aus Ihrer Sicht für das Jahr 2021 besonders war?

Die Vielzahl von Produkten, die von Schwachstellen betroffen waren (und teilweise noch sind). Wie wenig deutsche Hersteller oftmals auf eine Kontaktaufnahme durch das BSI wegen dieser Schwachstellen vorbereitet waren, hat uns die Notwendigkeit gezeigt, die Entwicklung des Common Security Advisory Frameworks (CSAF) fortzusetzen.

Dazu hat das BSI einen Editor (secvisogram) veröffentlicht, der im nächsten Jahr verbessert und die Veröffentlichung von Informationen über Patches und Updates (sog. Security Advisories) vereinheitlichen und vereinfachen wird. Das BSI hat viel in den Bereich automatisierte Advisories durch CSAF investiert und erwartet eine erhebliche Beschleunigung beim Einspielen von - oder überhaupt das Wissen über existierende Security Advisories.

Verändert die zunehmende Marktanforderung nach Security Ihrer Einschätzung nach etwas spürbar in den Unternehmen?

Verbindliche starke Marktanforderungen an Produkte im Bereich Industrial Security sind seitens des Gesetzgebers bisher nur selten vorhanden. Mit Europäischen Vorschriften, die aktuell diskutiert werden (u. a. Radio Equipment Directive, Cyber Security Act und hier insbesondere NIS2 und der neuen Maschinenprodukteverordnung), kommen mit großer Wahrscheinlichkeit viel stärkere Anforderungen, als den meisten Herstellern bewusst ist und auf die sie oft nicht angemessen vorbereitet sind.

Cybersicherheit muss - wie beispielsweise in IEC 62443-4-1 gefordert - integraler Bestandteil des Produktentwicklungszyklus und von Anfang an berücksichtigt werden. Ohne Cybersicherheit drohen viele Hersteller in der Digitalisierung zu scheitern.

»Cybersicherheit muss [...] integraler Bestandteil des Produktentwicklungszyklus und von Anfang an berücksichtigt werden.«

Was ist Ihrer Meinung nach die größte Herausforderung im Kontext Security für 2022?

Die Sicherheit der Supply Chain, dass Hersteller schnell auf bekannt gewordene Schwachstellen ihrer Zulieferer reagieren können und natürlich die Bedrohung jedes Teils der Lieferkette durch Ransomware.

Ransomware betrifft die Informationen über Kunden und Businesspläne der Firma selbst. Cyberangriffe können aber auch Quellcode und mögliche Manipulation der Produkte, die die Firma herstellt, umfassen.

Wenn Cyberkriminelle für den Bereich OT profitable Geschäftsmodelle entwickeln, stehen noch viel mehr Produktionsstillstände zu befürchten.



Jens Wiesner
Referatsleiter TK15
Industrielle
Steuerungs- und Auto-
matisierungssysteme

**Bundesamt für
Sicherheit in der
Informationstechnik**



Manuel Atug HiSolutions AG
Tim Bauer AK: IT-Sicherheit in der Gebäudeautomation
Ron Brash aDolus Technology Inc.
Daniel Buhmann, Mirco Kloss, FORTINET, Inc.
Sebastian Fritsch, Mirco Weber, secuvera GmbH
Fred Gordy Intelligent Buildings, LLC
Andreas Harner DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE
Dr. Lutz Jänicke PHOENIX CONTACT GmbH & Co. KG
Dr. Michael Missbach KAESER KOMPRESSOREN
Patrick Miller Ampere Industrial Security
Siegfried Müller MB connect line GmbH
Simeon Mussler, Jannis Stemmann, Philipp Pelkmann Bosch CyberCompare
Mirco Ross asvin GmbH
Jens Sparmann WAGO Kontakttechnik GmbH & Co. KG
Dipl. Phys. Jens Wiesner Bundesamt für Sicherheit in der Informationstechnik

Zusammenfassung

Was von einem bemerkenswerten Jahr 2021 im Gedächtnis geblieben ist

Auch für unsere Experten war 2021 ein herausforderndes Jahr mit vielen bemerkenswerten Ereignissen und Entwicklungen. In den hier geteilten Erfahrungen und persönlichen Einschätzungen bestätigt sich die sich verschärfende Cybersicherheitslage, wie es auch der aktuelle BSI-Lagebericht aufzeigt.

Ransomware-Angriffe, die auch Industriesektoren der Kritischen Infrastrukturen betroffen haben und groß angelegte Supply-Chain-Attacken haben auch in 2021 weitreichende Schäden für eine Vielzahl von Unternehmen verursacht. Dabei zeigt sich aktuell, wie anfällig komplex vernetzte Lieferketten sind und wie weitreichend die Auswirkungen auf dem weltweiten Markt werden können, wenn es zu Engpässen an einer Stelle kommt.

Was hat sich also in 2021 hinsichtlich Security getan?

Dass sich durch die zahlreichen Cybersecurity-Vorfälle die Awareness in den Unternehmen deutlich erhöht hat, das bestätigen die Experten, die sich an diesem Jahresbericht beteiligt haben, durchweg. Als Folge daraus wird Produktsicherheit mehr und mehr zum Entscheidungskriterium in Beschaffungsprozessen, was Hersteller vor die Herausforderung stellt, Securitykompetenz nachweislich aufzubauen.

In vielen Unternehmen unterstützt diese Anforderung eine engere Zusammenarbeit von OT und IT und bringt Ansprechpartner aus beiden Welten mit an den Tisch, wenn OT-Security-Themen auf die Tagesordnung kommen.

Die staatliche Regulierung mit dem Ziel, Industrieumgebungen und insbesondere Kritische Infrastrukturen abzusichern, hat nicht nur in Deutschland mit dem neuen IT-Sicherheitsgesetz auf die sich verändernde Bedrohungslage reagiert. Auch auf Europäischer Ebene und in den USA sind die Gesetzgeber mit notwendigen Anpassungen beschäftigt, die für die Unternehmen neue Anforderungen bringen werden.

Auf die neuen Herausforderungen für Security im Industriefeld reagieren Organisationen und Arbeitsgruppen mit neuen Empfehlungen und Leitlinien, wie beispielsweise neue Projekte, die im laufenden Jahr für die IEC 62443 in Gang gekommen sind. Außerdem arbeitet das BSI (Bundesamt für Sicherheit in der Informationstechnik) beispielsweise an Methoden, um Unternehmen Security Advisories schneller und handhabbarer zur Verfügung stellen zu können.

Die Herausforderungen, die vor uns liegen

Es ist davon auszugehen, dass das lukrative Geschäftsmodell Cyberkriminalität und insbesondere Ransomware-Angriffe zunehmend auf vulnerable Ziele ausgerichtet werden und die sich bietenden Einfallstore durch immer professionellere Methoden genutzt werden. Sicherheitslücken bestehen vor allem bei heterogenen Industrieumgebungen mit unzureichend geschützten Bestandsanlagen sowie bei externen Zugängen in die Netzwerke der Industrieumgebungen. Vor allem für die Absicherung der zunehmend digitalen Supply Chain ergeben sich daraus große Herausforderungen.

Aber auch IIoT muss vermehrt in den Fokus der Sicherheitsbetrachtung rücken, wenn mit einer wachsenden Zahl von Sensoren die Kommunikation in den vernetzten Anlagen immer weiter zunimmt. Security wird sich in diesem Kontext wesentlich über Produktsicherheit definieren, die die Hersteller liefern müssen.

Um den Herausforderungen mit der nötigen Expertise begegnen zu können, die ganzheitliche Security-Konzepte erfordern, brauchen wir fähiges Personal. Damit die immer dringender werdenden Security-Projekte deswegen nicht weiter ausgebremst werden, braucht es schnelle Lösungen, um dem Fachkräftemangel entgegenzuwirken.

Security bleibt deshalb vor allem eine Gemeinschaftsaufgabe!

Wir sitzen hier alle im selben Boot und das erfolgreiche Weiterkommen hängt von unserer Zusammenarbeit ab. Es bedarf des Einsatzes jedes einzelnen. Wir brauchen eine Kultur des Miteinanders und müssen Themen angehen, wichtige Punkte ansprechen und weiterhin die Extra-meile gehen, um das Security-Niveau unserer Industrien wirksam und nachhaltig zu erhöhen.

Kostenlos anmelden:

KURZ & GUT

Best-Practices für
ein erfolgreiches
Industrial Security
Projekt

Sichere
Industrie

<https://www.sichere-industrie.de/kurz-und-gut/>



Max Weidele
Gründer
» Sichere Industrie «



<https://sichere-industrie.de>

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 Interviews, 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: jahresrückblick@sichere-industrie.de

