

Industrial- und IoT Security *Jahresrückblick 2020*

16 Experten teilen ihre Meinung zu Entwicklung und Trends



sichere industrie ///



Airbus CyberSecurity

Jörg Schuler

[Seite 3](#)



AK: ITSGA

Tim Bauer

[Seite 5](#)



FORTINET

M. Kloss, D. Buhmann

[Seite 7](#)



HiSolutions AG

Manuel Atug

[Seite 9](#)



IBM

Lisa Unkelhäuser

[Seite 11](#)



ICS GmbH

M. Zappe, S. Stürzl, P. Birr

[Seite 12](#)



Intelligent Buildings

Fred Gordy

[Seite 14](#)



MB connect line GmbH

Siegfried Müller

[Seite 15](#)



Phoenix Contact

Dr. Lutz Jänicke

[Seite 16](#)



secuvera GmbH

Tobias Glemser

[Seite 17](#)



TÜV Hessen

B. Eibich, M. Groß

[Seite 18](#)



Verve Industrial Protection

Ron Brash

[Seite 19](#)



Zusammenfassung

[Seite 22](#)

Das Jahr 2020 war definitiv außergewöhnlich! Zugegeben - je nach persönlichem Hintergrund lässt sich diese Einschätzung vermutlich für so manches der vergangenen Jahre treffen. Allerdings war das Jahr 2020 tatsächlich eine besondere Herausforderung, denn die Corona-Pandemie hat Auswirkungen, die global jeden einzelnen betreffen, und zwar sowohl privat als auch beruflich. Wir sind inzwischen angekommen in einer neuen Realität mit neuen Gewohnheiten und Regeln im Miteinander, mit veränderten Arbeitsweisen und Kommunikationswegen und selbst mit neuen Begrifflichkeiten. Und noch ist kein Ende in Sicht!

Die Pandemie hat Unternehmen vor die Herkulesaufgabe gestellt, viele Prozesse, die bislang lokal vor Ort stattfanden, remote zu ermöglichen. So musste eine rapide angewachsene Zahl von Homeoffice-Arbeitsplätzen und Remotezugängen in industriellen Produktions- und Automationsbereichen eingerichtet werden, weil ohne viel Vorlauf kaum mehr jemand ins Büro oder in die Leitstände der Produktionsbetriebe kommen sollte. Heute kommt es den einen schon völlig normal vor, im Homeoffice zu arbeiten und den Komfort von Remote-Lösungen zu haben. Für andere ist es noch immer schwierig und bleibt es vielleicht. Die Digitalisierung hat durch die Pandemie einen großen Schub erfahren und die Art wie wir arbeiten nachhaltig verändert. Eine Entwicklung, die ohne Corona vermutlich wesentlich länger gedauert hätte.

Wie steht es mit der Absicherung dieser neuen IT-Infrastrukturen im OT-Bereich und welche Auswirkungen hat die Entwicklung der letzten Monate auf die vielen **Industrial Security Projekte und Zielsetzungen**, die endlich auf die Tagesordnung gesetzt wurden?

Die Dringlichkeit, umfassende Sicherheitskonzepte zu errichten, bleibt durch die sich weiter verschärfende Bedrohungslage durch Cyberangriffe aktuell wie nie. Das BSI hat dazu im aktuellen BSI Lagebericht erst kürzlich beeindruckende Zahlen veröffentlicht. Verantwortliche in Unternehmen aller Branchen, vor allem aber in kritischen Infrastrukturen, müssen der Situation mit wirksamen und umfassenden Konzepten begegnen. Immerhin geht es um die Sicherheit von Mensch und Umwelt und um die Anlagenverfügbarkeit von Industrien, die für uns als Gesellschaft von wesentlicher Bedeutung sind.

Wie das in Zukunft gelingen kann, das haben wir Expertinnen und Experten gefragt, die besonders nah dran sind an diesen Themen. Dabei war uns wichtig, Einschätzungen und Einblicke aus verschiedenen Lagern zu erhalten, von Herstellern, Consultants und Integratoren für unterschiedliche Branchen. **Ich freue mich sehr, diese interessanten Beiträge mit Ihnen teilen zu können!**

Max Weidele





Jörg Schuler

Head of Portfolio &
Strategy - Airbus IT/OT
CyberSecurity Services
Airbus CyberSecurity



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

Wie auch in den letzten Jahren hat sich 2020 **Ransomware erneut als zunehmende Bedrohung** für Unternehmen erwiesen. Zusätzlich machten Angriffe auf die öffentliche Infrastruktur, beispielsweise auf ein großes **Krankenhaus in Nordrhein-Westfalen**, in dramatischer Weise deutlich, dass Cyberangriffe nicht nur finanzielle Schäden, sondern sogar Personenschaden nach sich ziehen können. Wir sehen, dass dieser **Zusammenhang zwischen Safety und Security** und das damit verbundene Risiko auch im Industriebereich nun bei mehr und mehr Unternehmen wahrgenommen wird, dennoch können wir nicht bestätigen, dass dies bereits durchgängig der Fall ist.

Positiv ist zu bewerten, dass das Thema Industrial Security nun zunehmend in Unternehmen auf die Agenda der CXO Ebene rückt. **Aufgrund der COVID Pandemie konnten jedoch nicht die Fortschritte realisiert werden**, die aus den Gesprächen im letzten Jahr zu erwarten waren.

Durch knappe Ressourcen und Einschränkungen beim Zugang zu Produktionsanlagen wurden angedachte Projekte zur Verbesserung des Sicherheitsniveaus im industriellen Bereich **entweder vom Umfang reduziert oder sogar verschoben**. Ferner ist davon auszugehen, dass sich insgesamt das Cyber-Risiko nochmals erhöht hat, da u.a. zusätzliche Remote Zugriffe auf Produktionssysteme ermöglicht werden mussten, um den Betrieb aufrecht zu halten.

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

Weiterhin ist mit einer Zunahme von zielgerichteten Angriffen auf OT-Umgebungen zu rechnen. Waren bestimmte Angriffe seit Jahren aus der klassischen IT Welt bekannt, scheinen Angreifer nun **verstärkt die bewährten Angriffsmuster für OT Umgebungen** anzuwenden.

Dieser Trend wird sich aus unserer Sicht in den nächsten Jahren noch deutlich verstärken. Insbesondere auch durch die Erfahrungen in diesem Jahr wird sich die Digitalisierung im Produktionsumfeld weiter beschleunigen. **Remote Zugriffe bringen neben hohem Nutzen natürlich steigende Risiken mit sich.**

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

Um den aktuellen und zukünftigen Bedrohungen sowie regulatorischen Anforderungen, wie z.B. dem IT-Sicherheitsgesetz 2.0 gerecht zu werden, ist es wichtig, dass Unternehmen **ganzheitliche Konzepte** für ihre Security implementieren.

Diese Konzepte müssen sich organisatorisch und/oder technisch abbilden lassen und zum Beispiel über gesamte Lieferketten oder Product Lifecycle Management Prozesse anwendbar sein. Hierfür muss Industrial-, genauso wie Information-Security, **verstärkt in den Fokus und die Pflicht der Governance** rücken.

Security muss noch mehr als Enabler verstanden und Security-by-Design noch selbstverständlicher für die Digitalisierung von Produktionen werden. Ein solcher Paradigmenwechsel könnte langfristig dazu führen, dass Security nicht mehr als „Verhinderer“ sondern als Enabler wahrgenommen wird, und zukünftig auch bei der Verbindung von Safety und Security zum Beispiel bei der Kollaboration von Mensch und Roboter wichtige Beiträge liefert.

„Security muss noch mehr als Enabler verstanden und Security-by-Design noch selbstverständlicher für die Digitalisierung von Produktionen werden.“

Tim Bauer

AK: IT-Sicherheit in der Gebäude-automation



Tim Bauer

Gründer & Lead
AK: IT-Sicherheit in der Gebäudeautomation



Gab es 2020 einen Security-Vorfall im Industriebereich, der Ihrer Meinung nach besonders relevant war?

Es fällt mir schwer, den EINEN Security-Vorfall zu nennen. Beeindruckt hat mich viel mehr, wie viele Vorfälle es gab bzw. wie viele Vorfälle es schlussendlich in die Medien geschafft haben. Es verging kein Tag ohne neue Nachrichten zu lahmgelegten Produktionen, IT-Systemen und schlussendlich lahmgelegten Unternehmen.

Dies zeigt einerseits, dass die Einschlüsse näherkommen. **Andererseits belegt es, dass es eine offenere Kultur im Umgang mit den Vorfällen gibt**, die ich sehr begrüße. Es darf und muss klar sein, dass es nur eine Frage der Zeit ist, bis es einen trifft und dass Offenheit über einen derartigen Vorfall am Ende allen hilft.

Außerdem zeigte mir die häufige Berichterstattung, wie viel Arbeit zu tun ist und dass man sich immer wieder vor Augen führen muss, dass die **Security weder ein Produkt noch ein Projekt sein darf**. Vielmehr muss Security die Basis sein für alles, was wir digitalisieren wollen. Angesichts der Tatsache, dass viele Technologien, best practices und sauber definierte Prozesse zur Prävention von Sicherheitsvorfällen längst bekannt sind, war es für mich beeindruckend zu sehen, wie viele Vorfälle es trotzdem gegeben hat.

Besonders interessant war bei vielen Sicherheitsvorfällen folgender Aspekt: **Sprungbrett für eine Kompromittierung der IT-Systeme sind zunehmend Nebenanlagen und Geräte im Schatten**, die nicht typischerweise der IT-Abteilung oder der Produktion und deren Verantwortung zugewiesen sind. Zugangskontrollsysteme, Energiemanagementsysteme, Brandmeldeanlagen und typische Systeme der Gebäudeautomation sind bereits standortübergreifend vernetzt und bilden einen optimalen Zugangspunkt, um in vermeintlich sichere Netzwerke einzudringen. Diese Systeme stehen fatalerweise oft fernab von Überwachungs- und Schutzmechanismen.

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

Die Sicherheitsdebatte rund um das Thema IoT wurde mehr angeheizt - die Branche überschlägt sich förmlich. Zu den **unübersichtlichen Netzwerkstrukturen im OT-Umfeld**, die einen Überblick über alle vernetzten Assets nur sehr schwer möglich machen, gesellen sich nun auch noch **allerlei Geräte aus Heimnetzwerke dazu**, die ein Risiko darstellen können. Security muss auch für Homeoffice Situationen machbar sein, da ist auch die Industrial Security betroffen: **Heimarbeit, Fernwartung und Fernwirktechnik sind definitiv nicht nur ein IT-Thema, sondern ebenso ein OT-Thema**.

Es fällt zunehmend auf, dass es an **Manpower und Know-How bei den jeweiligen Betreibern fehlt**. Das Ergebnis sind oft keine oder sehr halbherzig umgesetzte Sicherheitsmaßnahmen. Industrial Security geht einher mit der Modernisierung und der Digitalisierung von Anlagen und Automationsprozessen. Die Workload ist enorm, und genau das muss akzeptiert werden! Fachbereiche wie die Instandhaltung,

Tim Bauer

AK: IT-Sicherheit in der Gebäude-automation

das Facility Management oder auch Operations kommen nicht darum herum, **Know-how aufzubauen**, damit sie als Betreiber zumindest verstehen, welche Maßnahmen welche Wirkung zeigen beziehungsweise notwendig sind.

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

Wir haben gesehen, dass Ausfälle von Steuerungssystemen fast immer eine Folge von Angriffen auf typische IT-Systeme waren. Die Abhängigkeiten durch Vernetzung und Datenaustausch führen dann dazu, dass ohne IT eben auch die Produktionen und Anlagen stillstehen.

Ich gehe davon aus, dass wir vermehrt Schadcode und Angriffsmuster sehen werden, die sich **explizit mit Herstellern von Steuerungen**, deren Komponenten und den zugrundeliegenden Prozessen und Protokollen befassen. **Warum IT-Komponenten im Rechenzentrum angreifen, wenn ich das gesamte Gebäude in Beschlag nehmen kann?** Warum die Produktionslinien angreifen, wenn ich die Zugangssysteme manipulieren kann und eine Rohstoffzufuhr nicht mehr möglich ist? Verschlüsselte Steuerungssysteme, die bisher autonom weiter betrieben werden konnten, sind eine gute Ausgangsbasis, um Lösegeld zu erpressen. Auch Safetysteuern, die Gefahr für Leib und Leben abwenden sollen, lassen sich zielführend anvisieren, um großen Druck aufzubauen. Wo immer sich ein lukratives Preisschild dranschreiben lässt, dann werden wir es erleben!

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

Licht ins Dunkel bringen und back-to-the-roots: **Asset- und Inventory-Management sowie die Segmentierung von flachen Netzwerkstrukturen führen unter anderem zu echter Sichtbarkeit**. Es braucht volle Transparenz, denn Du kannst nur schützen, was Du kennst. Best Practices, erprobte Methoden und Standards gibt es mehr als genug, die aber auch angewendet und umgesetzt werden wollen.

Errungenschaften in der Gebäudeautomation, wie deutlich sicherere Protokolle sollten als das angesehen werden, was sie sind: Ein kleiner Teil in einer umfänglichen Security-Policy. Und auch hier gilt: Wird die Basisarbeit nicht erledigt, schützt mich kein Protokoll.

„Sprungbrett für eine Kompromittierung der IT-Systeme sind zunehmend Nebenanlagen und Geräte im Schatten, die nicht typischerweise der IT-Abteilung oder der Produktion [...] zugewiesen sind.“



Mirco Kloss

Business Development
Manager OT DACH
Fortinet Inc.



Daniel Buhmann

Systems Engineer OT/
IoT
Fortinet Inc.



Gab es 2020 einen Security-Vorfall im Industriebereich, der Ihrer Meinung nach besonders relevant war?

[Buhmann] Wie auch schon 2019 hat im Jahr 2020 die **Anzahl der Ransomware Vorfälle im Industriebereich weiter zugenommen**. Aus der Anzahl dieser Vorfälle sticht besonders die **EKANS Ransomware** hervor, die neben Honda und Fresenius noch einige weitere Unternehmen im Industrieumfeld befallen hat. EKANS, oder auch SNAKE, wie die Schadsoftware von manchen Security-Forschern genannt wird, verschlüsselt nicht nur die betroffenen Systeme, sondern sucht gezielt nach Prozessen von SCADA oder ICS Systemen und beendet diese. Außerdem verschlüsselt die Schadsoftware neben den Systemdateien von Server und Clients gezielt Daten von Steuerungssystemen.

Der Vorfall zeigt einmal mehr, **wie wichtig ein vollumfängliches Securitykonzept und die durchgehende Segmentierung im OT Umfeld ist**, und ist meiner Meinung nach erst der erste von vielen gezielten Ransomware-Angriff auf Industrieumgebungen.

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

[Kloss] **Trotz Corona hat sich die Industrial Security weiterentwickelt und wird wesentlich stärker wahrgenommen**. Einige Unternehmen suchen nun gezielt Cybersecurity Mitarbeiter für OT und auch die CISOs haben dieses Verantwortungsfeld immer mehr im Blick.

Des Weiteren haben **einige Anlagenbetreiber die Corona-Krise genutzt, um lange aufgeschobene Umbauten und Security-Implementierungen umzusetzen**, während ein Großteil des Personals in Kurzarbeit war. Außerdem hat der großflächige Einsatz von Homeoffice Arbeit ein Umdenken bei der Absicherung der Unternehmensnetzwerke und -systeme erfordert, was sich bis in die Steuerungssysteme durchgezogen hat. Remote Zugänge und Fernwartung sind wichtiger denn je.

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

[Buhmann] Wir werden leider im nächsten Jahr weiterhin von Ausfällen von Industrieanlagen durch Ransomware hören. **Gezielte Angriffe auf Industriesysteme werden zunehmen**, da die Betreiber hier besonders hart getroffen werden können und eher bereit sind, über die Zahlung von Lösegeld nachzudenken, um die Produktion wieder zum Laufen zu bringen.

Die Systemhersteller verstehen die Brisanz von Securitymaßnahmen in Industrieanlagen inzwischen auch und sehen sie nicht mehr als Mehraufwand in Ihren Systemen.

Leider wird es noch einige Jahre dauern, bis sich diese Entwicklung überall zeigt, und wir werden die bestehenden Industriesysteme zukünftig noch besser mit Securitymaßnahmen versehen müssen.

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

[Kloss] **IT und OT müssen noch stärker zusammenarbeiten**, um die Herausforderung gemeinsam meistern zu können. Es macht wenig Sinn, dieselben Lösungen auf beiden Seiten aufzubauen und zu betreiben, wenn eh schon beide Seiten über Personalmangel klagen. In einigen Unternehmen sehen wir diesen Trend bereits auch dahingehend, dass nicht mehr von IT und OT gesprochen wird, sondern von Office-IT und Production-IT.

Aber nicht nur das Personal, sondern auch die **Lösungen müssen stärker integriert werden und miteinander interagieren können**. Es werden zukünftig nicht mehr nur Einzellösungen die Anforderungen der Security erfüllen können. Der „Best of Integration“ Ansatz hilft dabei, die eingesetzten Lösungen effizienter zu nutzen und genug Ressourcen freizumachen, um das Securitylevel weiter zu erhöhen.

„[...] viele Anlagenbetreiber [haben] die Corona-Krise genutzt, um lange aufgeschobene Umbauten und Security-Implementierungen umzusetzen.“



Manuel Atug

Senior Manager
HiSolutions AG



Gab es 2020 einen Security-Vorfall im Industriebereich, der Ihrer Meinung nach besonders relevant war?

Der Fall vom **Uniklinikum Düsseldorf** war insofern besonders relevant, da er zwei wichtige Problemstellungen aufzeigt, die alle Industrieumgebungen immer stärker betreffen werden. **Systeme für Fernzugriffs- und Fernadministration erlauben einen Zugriff bis in kritische Produktionsumgebungen hinein.** Sind diese schlecht administriert oder sogar unsicher konfiguriert, dann fällt auch Produktion aus, da die organisierte Kriminalität sich da nicht zweimal bitten lässt.

In diesem Fall ist der zweite Aspekt aber auch ein Wesentlicher. Der Hersteller Citrix hat für das Netscaler System offenbar eine **schlechte Softwareentwicklung** an den Tag gelegt, denn mit einfachen Tests wären diese Defizite schnell aufgefallen. Aber darüber hinaus wurde auch eine **unzureichende Informationspolitik und ein schlechtes herstellereitiges Patchmanagement** betrieben. Man hat viele Wochen benötigt, der Workaround und die Patches waren fehlerhaft. So musste bei beidem nachgebessert werden. Das versteht die Industrie nicht unter „Enterprise“ Software Hersteller!

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

Es wurde sehr viel darauf geachtet, wer welche APT-Gruppe sein könnte und welcher Angreifer in welcher kriminellen Bande aktiv ist. Ja, das ist gut und schön, für Ermittlungsbehörden. Es wird deswegen aber auch sehr viel Marketinghype von einigen Herstellern von Systemen zur Anomalieerkennung gemacht, vor allem aus den USA.

Allerdings hilft beides der Erhöhung einer Cyberresilienz der kritischen Infrastrukturen und der Industrie halt nicht wirklich. **Wichtiger wäre, die „langweiligen“ Themen der echten Industrial Security zu kommunizieren und umzusetzen.** Also sowas wie Asset Management, Sicherheitsupdates einspielen, Trennung und Segmentierung der Netze, Zugriffsrechte und Firewall Regeln aufräumen, sichere Fernzugriffe, Multi-Faktor-Authentifizierung für Administratoren, Backups, auch offline und mit Restore-Tests oder auch den Ernstfall üben. **Klassisch also und nicht „on the edge“.** Denn das hilft ganz konkret zur Abwehr von Cyberbedrohungen.

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

Ransomware ist kontinuierlich und seit Jahren stark im Aufwind, denn damit machen kriminelle Banden viel Geld. Diese Bandenkriminalität wird sich noch weiter verstärken, so dass immer mehr Konzerne und Mittelständler davon betroffen sein werden. Sie etablieren sich halt gerade als bevorzugte VIP-Kundschaft für Cyberkriminelle.

Denn die Ermittlungsbehörden fixieren sich lieber darauf, weitere Cyberagenturen und Behörden ins Leben zu rufen, Stichwort Verantwortungsdiffusion, die Vorratsdatenspeicherung zu fordern oder General-schlüssel für verschlüsselte Messenger zu erhalten, statt sich **mittels**

Ausbildung und Ausstattung sowie einheitlicher Vorgehensweisen gegen Cyberkriminelle aufzustellen und zu wappnen.

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

Back to the roots, statt „jumbawumba“ Security. Also die oben erwähnten Sicherheitsmaßnahmen als Basics aber dafür konsequent umsetzen, und **nicht dem neuesten Marketinghype** (von Herstellern) hinterherzurennen.

Darüber hinaus sollte immer hinterfragt werden, **wofür man digitalisiert.** Für mehr Automatisierung im Produktionsprozess macht es Sinn, dann aber bitte mit den 1 x 1 Security Maßnahmen. Nur weil der CEO in der Managementzeitschrift gelesen oder von anderen Geschäftsführern davon gehört hat, dass die anderen das auch machen, vielleicht lieber nicht.

„Wichtiger wäre, die „langweiligen“ Themen [wie beispielsweise Asset Management, Netzwerksegmentierung oder Absicherung der Fernzugriffe] umzusetzen.“

Lisa Unkelhäußer

IBM Deutschland



Lisa Unkelhäußer

Security Channel Leader
DACH
IBM Deutschland GmbH



Gab es 2020 einen Security-Vorfall im Industriebereich, der Ihrer Meinung nach besonders relevant war?

Es gab mehrere drastische Stillstände von Produktionen inklusive großer Auswirkungen auf deren Lieferketten und Kunden, vor allem die **Ransomware Attacken haben deutlich zugenommen**.

Allerdings war der einprägsamste Fall für mich der **Angriff auf das Uniklinikum Düsseldorf**, der für einen breiten Aufschrei in den Medien gesorgt hat, und auch der Bevölkerung noch mal gezeigt hat, wie anfällig die kritischen Infrastrukturen sind.

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

Der Markt fängt an sich auf der Hersteller / Lösungsseite zu konsolidieren. **Viele kleinere Vendoren werden übernommen und aufgekauft**, das ist unter anderem ein Zeichen dafür, dass das Marktwachstum weiterhin stark zunehmen wird.

Bei den Industrieunternehmen konnte ich mehr und mehr beobachten, wie erste Testinstallationen gemacht wurden und an Konzepten für die Fertigung gearbeitet wurde.

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

Die Störfälle werden sich durch die weitere Vernetzung sowohl in der Anzahl als auch in der Heftigkeit weiter erhöhen.

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

Es müssen **noch mehr Kooperationen** geschaffen werden, vor allem **zwischen den Platzhirschen der Produktionswelt und der IT**.

Außerdem ist das Thema Awariness immer noch entscheidend, je mehr Verständnis und Aufklärung geschaffen wird, desto mehr gewinnt das Thema an Relevanz.

„Es müssen noch mehr Kooperationen geschaffen werden, vor allem zwischen den Platzhirschen der Produktionswelt und der IT.“



Martin Zappe

Business Unit Manager
Industrial Engineering
ICS GmbH



Sebastian Stürzl

IT-Security Consultant
ICS GmbH



Patric Birr

Head of Business Center
Security
ICS GmbH

Gab es 2020 einen Security-Vorfall im Industriebereich, der Ihrer Meinung nach besonders relevant war?

Durch die Vielzahl der täglichen Cyber-Angriffe ist es schwierig, nur einen einzigen Vorfall in 2020 zu benennen. Geht man von der Schwere des Angriffs aus, könnte man die **Ransomware-Attacke auf die Software AG** als einen der schlimmsten dieses Jahr bezeichnen. Die Software AG ist dabei der zweitgrößte Anbieter von Software Lösungen und Dienstleistungen in Deutschland und wurde Anfang Oktober zum Ziel eines „DoubleExtortion“ Angriffs. Dabei nutzte die „Clop“ Hackergruppe eine Ransomware, um erst Daten von den Servern der Software AG zu stehlen und diese danach zu verschlüsseln. Verlangt wurde anschließend ein Lösegeld von 23 Mio. Euro, um eine Veröffentlichung dieser Daten durch „Clop“ zu verhindern. Die Software AG weigerte sich, und so waren kurz darauf interne Daten des Unternehmens im Darknet einsehbar. Zwar sparte man sich seitens der Software AG das Lösegeld, der Image Schaden und der folgende Einbruch des Aktienkurses wogen dabei aber nicht weniger schwer. Ähnliches ereignete sich zur gleichen Zeit übrigens auch beim **Navigationssystem Anbieter Garmin**.

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

Durch die schlechte Verfolgbarkeit der Angreifer, die lukrativen Ziele und das geringe Risiko **nahmen speziell Angriffe durch Ransomware deutlich zu**. Die Unternehmen reagierten u.a. durch die Vorfälle der letzten Jahre mittlerweile etwas sensibler auf das Thema Industrial Security. Allerdings ist weit noch nicht allen Unternehmen klar, wie wichtig das Thema ist und wie existenzbedrohend ein solcher Angriff sein kann. Unsere täglichen Gespräche mit Kunden, Interessierten und Teilnehmern aus den unterschiedlichsten Arbeitskreisen spiegeln dies leider auch mehr als deutlich wieder.

Die **zunehmende Verbreitung von IIoT-Geräten** und Cloud Services, stellte die Firmen dieses Jahr vor zusätzliche Herausforderungen. Desweiteren sind immer noch viele GeschäftsführerInnen im **Irrglauben, dass die hauseigene IT sich schon darum kümmert**, dabei sind die Abteilungen mit dem täglichen operativen Geschäft vollkommen ausgelastet.

Die **Entwicklung auf dem Arbeitsmarkt für Security-Experten** verschärfte die Situation noch weiter, da das Angebot an Personal nicht mit dem Bedarf gedeckt werden konnte. In den nächsten Jahren werden IIoT und Cloud daher weiter in den Vordergrund rücken, aber auch Cyber-Attacken werden weiter zunehmen.

Eine interessante Entwicklung wird sicherlich auch der **vermehrte Einsatz von Künstlicher Intelligenz in Abwehrsystemen** werden, welche sich aber auch schon Angreifer zunutze machten.

Zu beobachten ist der **vermehrte Einsatz und Etablierung der IEC 62443** in der Prozess- und Automatisierungsindustrie, um insbesondere Prozesse, aber auch Produkte zu zertifizieren. Die Situation der Industrial Security bleibt also die nächsten Jahre nicht nur spannend, sondern vor allem auch angespannt.

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

Wie schon erwähnt ist Ransomware auch weiterhin eine der größten Bedrohungen für die Industrie, hatte aber bisher „nur“ Auswirkungen auf die Verfügbarkeit der Systeme. Besorgniserregend ist daher eine Entwicklung, welche 2017 erstmals mit „TRITON“ in Erscheinung trat, in der **industrielle Kontrollsysteme (ICS) gezielt angegriffen** werden. TRITON wurde entwickelt, um mit einer bestimmten Art von Kontrollsystem, sog. „sicherheitsinstrumentierten Systemen“ (SIS) zu kommunizieren. Diese Systeme sind meist als Überwachung von z.B. Temperatur oder Drucksensoren im Einsatz und daher auch sicherheitsrelevant. **Eine Manipulierung der Controller-Logik hätte somit Auswirkungen auf die funktionale Sicherheit von Industrieanlagen** und damit auch kritischer Infrastruktur. TRITON ist somit der erste Nachweis eines gezielten Angriffs auf SIS-Systeme.

Unsere Vermutung ist, dass wir in dieser geopolitisch kühlen Phase **vermehrt Angriffe dieser Art auch in Europa** sehen werden. Momentan schützt uns hier nur der Fakt, dass diese Art Malware speziell für einen Controller, in diesem Fall eine Triconex-Sicherheitssteuerung, zugeschnitten sein muss und daher sehr aufwendig zu entwickeln ist bzw. nur einen schmalen Angriffsvektor bietet. Künftig könnten solche Angriffe aber auch breitgefächert stattfinden und alle verwundbaren Systeme zum Ziel haben, was eine neue Dimension von Cyber-Angriffen ermöglichen würde.

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

Standards sollten nicht nur bekannt sein, sondern auch gelebt werden. Insbesondere die ersten „Schritte“, getreu dem Motto **„Mitarbeiter sind die beste Firewall“**, sind oftmals mit verhältnismäßig „einfachen“ Mitteln, aber großer Wirkung zu realisieren. Berichte zeigen, dass zwar über 80% der Unternehmen gängige Standards kennen, doch nur 40% davon diese auch nachweislich umsetzen. Vor allem menschliches Versagen ist weiterhin der Hauptgrund für Sicherheitslücken und erfolgreiche Cyber-Attacken. Ein prominentes Beispiel dafür ist das Patchmanagement. Trotz lautstarker Warnungen von Seiten des BSI werden **Updates oftmals immer noch verzögert oder gar nicht eingespielt**, was dem Angreifer seine Arbeit deutlich erleichtert.

Ein erfolgreicher Schutz ist also immer auch mehrstufig in einer Verschmelzung von Mensch und Technik zu finden. Auf der einen Seite steht dabei die **Sensibilisierung von Mitarbeitern**, um deren Awareness zu schulen und auf der anderen Seite eine **dedizierte Sicherheitslösung der Systeme sowie einer gut gesicherten Kopplung von OT und IT**. Gerade diese zunehmende Verbindung von OT und IT sowie deren Prüfung auf Schwachstellen wird eine der Hauptaufgaben für die Security der nächsten Jahre werden.

„Insbesondere die ersten Schritte, getreu dem Motto „Mitarbeiter sind die beste Firewall“, sind oftmals mit verhältnismäßig einfachen Mitteln, aber großer Wirkung zu realisieren.“



Fred Gordy

Intelligent Buildings, LLC



Fred Gordy

Director of
Cybersecurity
Intelligent Buildings, LLC



Which ICS security incident in 2020 was particularly relevant for you and why?

There is not one specific event but rather a reoccurring attack type which is **ransomware taking control of the application host**. Ransomware accounts for over 80% of the attacks but one that is almost 100% avoidable. Operators are using the application host to check social media and email. The application host should never be used for any purpose other than what it was designed to do.

How did you perceive the development of the ICS security scene this year?

There has definitely been growing interest, however, there is a **great deal of maturity needed** in technology, the people responsible for the systems, and policies and processes to govern.

What's your best guess on how the threats and incidents will develop next year?

There have been a couple of cases of injury and even death that is loosely attributed to attacks. We could begin to see more of these. Additionally, there will most likely be an **increase in OT focused attacks** to cause interruption of services and to use as a means to see if there are opportunities to pivot to corporate networks.

How should security adapt to this development?

The primary areas that need addressing are the continued advancement of **OT monitoring** and **assessment management** tools, developing security professionals that have **knowledge of both OT and IT** environments, and appropriate level of **policies** to empower facility management and the vendors that serve them to do their part in the cyber protection chain.

„Ransomware accounts for over 80% of the attacks but one that is almost 100% avoidable.“

Siegfried Müller

MB connect line GmbH



Siegfried Müller

Geschäftsführer
MB connect line GmbH



Gab es 2020 einen Security-Vorfall im Industriebereich, der Ihrer Meinung nach besonders relevant war?

Die meisten Vorfälle im Unternehmensbereich waren für mein Empfinden sehr geprägt von **Ransomware**. Wenn auch diese nicht primär auf den Produktionsbereich ausgerichtet waren, so war es bestimmt für viele Opfer eine „neue“ Erfahrung und mit Sicherheit schmerzhaft.

Mehr Sorge macht mir hingegen die **immer bekannter werdenden Schwachstellen von Softwarebibliotheken in Industriegeräten**, wie z.B. Ripple20. Denn auch wenn die Schwachstellen beseitigt werden, so besteht die große Herausforderung darin, alle betroffenen Geräte zu patchen.

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

Gut, mit Luft nach oben! Organisationen und Verbände mobilisieren immer stärker das Thema IT-Sicherheit in der Industrie. Dadurch steigt natürlich das Bewusstsein für Anwender, Integratoren und Hersteller. Das ist äußerst positiv anzusehen.

Die **IEC 62443 bekommt mehr Zuspruch** und einige Arbeitsgruppen in der Industrie versuchen die Inhalte zu verstehen und umzusetzen. Wir dürfen hier nicht an Fahrt verlieren und alle sollten erkennen, dass die Verbesserung der IT-Sicherheit eine langfristige Investition ist.

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

Die Angriffszahlen werden steigen! Die **zunehmenden Homeoffice Arbeitsplätze bieten zusätzliche Angriffsvektoren**, und wir haben es hier mit einem deutlich höheren Risiko zu tun.

Ich erwarte einen **deutlichen Zuwachs an Ransomware Angriffen** in allen Bereichen wie z.B. Gebäudemanagement, Produktion und KRITIS. Dedizierte Angriffe auf Automatisierungsanlagen schätze ich als eher selten ein.

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

Security muss einfach anwendbar werden! Auch wenn Anwender gerne ihre Arbeit und das Umfeld sicherer machen möchten, so **fehlt es den Systemen oft noch an der einfachen Umsetzung**, um das Security-Niveau zu erhöhen. Dafür müssen wir als Security-Community weiter an Aufklärung und Bewusstsein arbeiten. Es gibt noch viel zu tun, packen wir es an!?

„Auch wenn Anwender gerne ihre Arbeit und das Umfeld sicherer machen möchten, so fehlt es den Systemen oft noch an der einfachen Umsetzung [...]“

Dr. Lutz Jänicke

Phoenix Contact



Dr. Lutz Jänicke

Corporate Product &
Solution Security Officer
**Phoenix Contact GmbH
& Co. KG**



Gab es 2020 einen Security-Vorfall im Industriebereich, der Ihrer Meinung nach besonders relevant war?

Einen besonderen Vorfall, der sich speziell auf die Automatisierungsumgebung bezieht, kann ich nicht sofort abrufen. Vielmehr war die **Automatisierungsbranche also solche in 2020 offensichtliches Ziel diverser Ransomware-Angriffe.**

Dabei waren die Angreifer mindestens technisch erfolgreich, die angegriffenen Unternehmen litten unter schweren Störungen. Zur Frage, ob die Angreifer auch kommerziell erfolgreich waren, also Gelder einnehmen konnten, habe ich keine Informationen.

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

Diskussionen und Gespräche in Gremien oder Workshops zeigen diverse Aktivitäten, in denen wenigstens **größere Betreiber intensiv am Aufbau eines Security-Assetmanagements** arbeiten und/oder **Security-Anforderungskataloge** ausarbeiten oder konkretisieren. Ich erwarte hier zeitnah deutliche Fortschritte.

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

Die Entwicklungen im Kontext Ransomware belegen die **Professionalisierung der Cybersecurity-Angriffe**. Dass bei entsprechenden Angriffen vorher auch Informationen ausgeleitet werden, um mit der Drohung der Veröffentlichung das Erpressungspotential zu erhöhen, belegt die technische Qualität der Angriffe. Tätergruppen werden ihr Wissen und ihre Angriffswerkzeuge weiterentwickeln, so dass mit mehr oder heftigeren Angriffen zu rechnen ist.

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

Wenn die sichtbaren Schäden wachsen, halten offensichtlich die Security-Maßnahmen nicht mit der Bedrohungslage Schritt. Da sich die Security-Qualität von Produkten und Systemen nicht kurzfristig massiv erhöhen lässt, müssen die **kompensierenden Gegenmaßnahmen entsprechend gesteigert werden**. Da ein Schadensfall nicht komplett ausgeschlossen werden kann, sollten Fragen der **Schadensbegrenzung und der Resilienz** einen zentralen Platz einnehmen.

Bezogen auf die Industrial Security ist zu beachten, dass etwa ein Ransomware-Angriff die ganze Firma betrifft und Cybersecurity daher auch gemeinschaftlich angegangen werden sollte: **IT und OT gemeinsam!**

„[...] ein Ransomware-Angriff [betrifft] die ganze Firma und Cybersecurity [sollte] daher auch gemeinschaftlich angegangen werden: IT und OT gemeinsam!“

Tobias Glemser

secuvera GmbH



Tobias Glemser

Geschäftsführung
secuvera GmbH



Gab es 2020 einen Security-Vorfall im Industriebereich, der Ihrer Meinung nach besonders relevant war?

Einen? Während 2019 noch einzelne Ausfälle und der Stillstand ganzer Unternehmen noch "Highlights" waren - man denke nur an die Pilz GmbH & Co KG - so sind es **2020 schon zu viele geworden, um diese noch zu nennen**. Außerhalb des Industriebereichs hat mich das gezielte **Spearphishing auf Teilnehmer der Münchner Sicherheitskonferenz** dann doch beeindruckt.

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

Ein spannendes Jahr! Wir als Anbieter von Beratung und Prüfung von Sicherheitseigenschaften in IIoT-Produkten nach Standards wie IEC 62443 haben zwei Dinge wahrgenommen:

1. Die **Standardisierung schreitet zum Glück weiter voran**. Die Zusammenarbeit der deutschen Verbände und deren aktiver Mitglieder empfinden wir als konstruktiv und zielführend, um ein einheitliches und ansteigendes Sicherheitsniveau schaffen zu können.
2. Die **Hersteller aller Bereiche, nicht nur in der Industrie, stehen auf der Bremse**. Es gibt einige wenige Coronakrisen-"Gewinner", wie z. B. Hersteller von Videokonferenzsoftware, die weiter an der Verbesserung der Cyberresilienz ihrer Produkte arbeiten. Bei vielen sind Budgets schlicht geschoben worden und Prioritäten verändert. Optionale Sicherheitseigenschaften fallen seit jeher als einer der ersten Aspekte aus den Budgets heraus. Daher sind Standardisierung und einheitliche, verbindliche Anforderungen so wichtig. Man stelle sich das Sicherheitsniveau von Autos vor, wenn die Sicherheitseigenschaften nicht reguliert wären!

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

Cyberkriminelle werden wie in den letzten Jahren immer häufiger und gleichzeitig tiefer in Netze vordringen. **Erpressung nach Befall ist keine Ausnahme mehr**, sondern ein etabliertes, rentables und vergleichsweise risikofreies Verbrechen. Es werden sicherlich auch noch skrupelloosere Attacken kommen, bei denen die Angreifer auch die Gefahr für Leib und Leben von Menschen in Kauf nehmen.

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

Hersteller, Integratoren und Betreiber sollten daran arbeiten, durch gemeinsame Anstrengung angepasste Profile für ihre jeweiligen Anwendungsbereiche zu entwickeln. Gleichzeitig sollten sowohl **sinnvolle als auch maßvolle Sicherheitsanforderungen** etabliert werden. Einheitliche Standards helfen dabei, das Rad nicht jeweils neu zu erfinden.

„Erpressung nach Befall ist keine Ausnahme mehr, sondern ein etabliertes, rentables und vergleichsweise risikofreies Verbrechen.“

Björn Eibich & Matthias Groß

TÜV Hessen



Björn Eibich

Bereichsleiter Cyber- &
Informationssicherheit
TÜV Hessen



Matthias Groß

Cybersecurity Expert
TÜV Hessen



Gab es 2020 einen Security-Vorfall im Industriebereich, der Ihrer Meinung nach besonders relevant war?

[Eibich] Der **Datenleak bei Rheinmetall** fällt mir hierzu ein: Interne Unterlagen u.a. zu Panzerfahrzeugen geleakt, Bußgeld und Imageschaden droht! Der Leak entstand angeblich durch einen Zulieferer. Daher sehe ich ihn als relevant zum Thema **Security in der Supply Chain** an.

[Groß] Mir fällt ein Beispiel nicht direkt aus der produzierenden Industrie ein, sondern der Vorfall im **Universitätsklinikum Düsseldorf**. Hier musste nach der Lahmlegung durch eine Cyberattacke (shitrix) ein Rettungswagen in der Anfahrt zu einer anderen Klinik umgeleitet werden. Dass der Patient, der transportiert wurde, verstarb, wird diesem Sicherheitsvorfall zugeschrieben.

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

[Eibich] Meiner Meinung nach gibt es leider insgesamt **immer noch zu wenig „Awareness“**. Es zieht zwar langsam an, wenn man es aber mit IT-Security vergleicht, würde ich die Entwicklung mit dem Stand von 2008 beschreiben.

[Groß] Es gab eine **steigende Awareness** hin zur Security, sowie eine **Zunahme der Vernetzung und der Security Standards**. Big Player greifen das Thema mehr und mehr auf, was andere motiviert mitzuziehen. Das ist eine sehr positive Entwicklung.

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

[Eibich] Ich denke, wir werden noch **mehr Ransomware Vorfälle in der Industrie** sehen. Schnelles und angemessenes Patchen ist dort ja quasi unmöglich.

[Groß] Wie bereits in den letzten Jahren erkennbar wurde, wird es einen weiteren Anstieg von Störfällen geben. Trotz gewisser bestehender Awareness rechne ich bei der Bedrohung weiterhin mit **Schwerpunkt Ransomware**.

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

[Eibich] Das sehen wir beim TÜV Hessen klar so, dass zukünftige **Verfügbarkeit nur noch durch höhere Security erreichbar** ist.

[Groß] Es sollte Klarheit darüber herrschen, dass **Verfügbarkeit nur durch eine Erhöhung des Securityniveaus erreichbar** ist.

„[...] zukünftige Verfügbarkeit [ist] nur noch durch höhere Security erreichbar [...].“

Ron Brash Verve Industrial Protection



Ron Brash

Director of Cyber Security
Insights
Verve Industrial Protection



Which ICS security incident in 2020 was particularly relevant for you and why?

The **Honda cyber security attack** was most relevant for me as I found it to be an interesting case where **cascading effects** went from one part of the organization, all the way to other subsidiaries, and even outsourced contractors responsible for logistics. This highlights an interesting challenge where just-in-time manufacturing, ERPs, and overall IT infrastructure can grind a business to a halt even if actual safety or visibility on process control is left untouched, but **also how the media can often misconstrue such an attack as being OT**, when in reality it is far less insidious. Regardless of that, expect more “OT attacks” when they are likely IT in nature, provide services or functionality to Operations, and the good news is that a number of solutions exist to reduce risk in those areas (should organization’s implement them).

On another note, while **ransomware** is “oldhat” and circa from the 1990s – it is a growing threat, but it is a very relevant concern when an organization wishes to avoid disruptions. 2020 (and probably for some time to come) will have several unintended consequences including a lack of spare capital, and so criminal groups may also wish to cash in on that (they too may need the ransom to finance their operations). Therefore, even if ransomware is for the purposes of ransom (targeted or opportunistically) or for hiding the tracks of an insidious nation state attack, it’s a risk to be reckoned with, and Honda merely reminded us that an attack can have cascading collateral damage.

How did you perceive the development of the ICS security scene this year?

2020 was not overly notable from an incident perspective, but truthfully there is some evidence that a few **vendors may exit the market for a variety of reasons**. Alternatively, there were some notable **supply-chain related software vulnerabilities** (such as URG11 or Ripple20) that had a positive effect on raising the challenges when assessing whether they are applicable to X devices, determining risk exposure, and understanding their nuances. Unfortunately, the media further embellished upon the researcher’s claims regarding the sheer numbers of affected devices, but, awareness on the topic of components within a “closed product” or understanding the shortfalls of the CVSS scoring system in OT/ICS is very important from a number of perspectives. For example, product management from the OEM perspective can be challenging due to component ecosystem complexity, gaps in product security, and immature secure development lifecycle management. In fact, most vendors do not know the exact software materials within their products, and asset owners are also unaware of potential flaws left unmitigated.

ICS security is also beginning a return to reality where the consumers of security products (the asset owners) are moving towards practical solutions that reduce their cyber risk, and **help them solve problems vs. add more information on the fires of overload or wasted investments**. This includes focusing only on passive detection technologies or threat intelligence feeds which often have little value **when other basics have been neglected or the organization is not at an adequate**

Ron Brash Verve Industrial Protection

state of maturity. And as a result, I have observed organizations focusing on more intelligent expenditures, which will hopefully alter the security landscape for 2021.

What's your best guess on how the threats and incidents will develop next year?

I think the biggest threats to many organizations (especially the small and medium-sized businesses) are their **inability to tolerate disruptions from a financial perspective and the difficulties they often have when maintaining their cyber-infrastructure**. The latter being another point where several outstanding vulnerabilities may be left exposed and exploited by common malware, which results in figuratively unrecoverable financial demise in a number of industries where insurance is not a sufficient bailout plan.

In OT security, we have not seen ransomware attack ICS devices yet, but some **embedded IT-esque devices such as NAS devices have had some forms of ransomware affect them as well**. This is very interesting because recovering from a physical attack at a plant-floor level and actual hardware is immensely difficult to recover from – there can be tens or hundreds of devices, and they may be EoL, available in small quantities, or distributed across an organization and not immediately on hand. This will surely be an insurance-related event as remediation is not as simple as rebuilding workstations or active directory type infrastructure.

I also predict there could be more **software supply chain related vulnerabilities** where malicious entities use trojan horse style attack strategies to gain access to unsuspecting asset owners. **As budgets are tight from COVID-19, there will likely be a reluctance for upgrades, changes that result in more security, and likely a lack of verification where software has originated from**. This also will rear its head as a challenge for OEMs who integrate software and package it into a product. They too will operate on a budget or have a myriad of constraints.

How should security adapt to this development?

I do not think there will be a race to the bottom when trying to obtain security products or services, but **many organizations may choose to employ and build up individuals internally**. Most security issues are not from a lack of manpower, but from a combination of lack of visibility, inability to leverage current investments, invest in technology upgrades that provide more than just security, and ill-defined (non-existent) policy or procedures. As a result, organizations should adapt by making intelligent investments, ensure full operationalization to obtain maximum benefits, and commit to maintaining their assets (logical or physical). **Security always degrades over time, and asset management should evolve to reflect this change in thinking**.

For physical ICS device failures relating to device-based ransomware, this will be an extension of existing processes (potentially), but the scale of replacement will be a challenge. However, this may result in OT obtaining larger (much needed) security-enhancement budgets, spare device inventories, the inclusion of security from a maintenance

Ron Brash Verve Industrial Protection

/ response perspective into relevant OT processes, and increases in organizational awareness regarding current ICS assets.

You may also see **insurance being more applicable in these cases** as a mechanism to recover some of the lost costs so there may be an uptick in this type of insurance as PART of an organization’s cyber strategy.

Regarding Software Bills of Materials (SBoMs) and the handling of embedded vulnerabilities, security will adapt to a model similar to a publicly available annex, or some sort of PKI-like model where there are channels and authoritative sources. Product development needs to change moving forward, and there will need to be a significant effort towards deriving SBoMs for legacy or abandoned products to ensure asset owners can adequately assess any risks and their mitigations. Industry organizations that provide services such as the National Vulnerability Database (NVD) will need to ensure synchronization between the vendor/OEM and their security portals too. It is currently very difficult to map CPEs to affected OT/ICS products.

„[...] (the asset owners) are moving towards practical solutions that reduce their cyber risk, and help them solve problems vs. add more information on the fires of overload or wasted investments.“



Airbus CyberSecurity
Jörg Schuler



AK: ITSGA
Tim Bauer



FORTINET
M. Kloss, D. Buhmann



HiSolutions AG
Manuel Atug



IBM
Lisa Unkelhäuser



ICS GmbH
M. Zappe, S. Stürzl, P. Birr



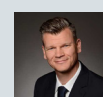
Intelligent Buildings
Fred Gordy



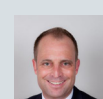
MB connect line GmbH
Siegfried Müller



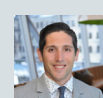
Phoenix Contact
Dr. Lutz Jänicke



secuvera GmbH
Tobias Glemser



TÜV Hessen
B. Eibich, M. Groß



Verve Industrial Protection
Ron Brash

Die Einschätzungen unserer Expertinnen und Experten aus unterschiedlichen Branchen und Bereichen vermitteln ein realistisches Bild über die aktuelle Bedrohungslage und den Zustand der Industrial Security in den Unternehmen. Aber auch das, was ihnen im Gedächtnis bleibt von diesem bemerkenswerten Jahr und ihre Empfehlungen für praktikable Lösungsansätze wollen wir zu einem Gesamtbild zusammenfassen.

Die Gefahr wird spürbar

Cyberangriffe sind keine seltenen Ereignisse und so wurden auch in diesem Jahr viele Unternehmen von Cyberkriminellen ins Visier genommen, mit anwachsender Entwicklung.

Bemerkenswert ist, dass die Attacke auf das Universitätsklinikum Düsseldorf für die meisten unserer Expertinnen und Experten eine prägende Erfahrung war. Krankenhäuser und andere Einrichtungen im medizinischen Bereich sind in ganz besonderer Weise essenziell für Leib und Leben. Ein Cyberangriff auf solche Ziele ausgerichtet, kann nicht nur wirtschaftlichen Schaden anrichten oder Daten ins Licht der Öffentlichkeit zerren, die dort nicht hingehören, sondern kann Menschenleben unmittelbar gefährden. Dieser Fall macht Angst, auch wenn es daneben einige andere Vorfälle mit weitreichenden Folgen für die betroffenen Unternehmen gab, wie z.B. Ransomware-Angriffe auf die Software AG oder Fresenius und Honda. Die hohe Gefährdungslage für kritische Infrastrukturen, wo die Administration und Konfiguration von IT-Infrastruktur für eine sehr hohe Anzahl verschiedener Systeme viel Optimierungspotenzial aufweist, wird uns hier sehr eindringlich vor Augen geführt!

Als präferierte Ziele der Angreifer machen unsere Expertinnen und Experten zunehmend Industrieunternehmen aus, die durch die Lahmlegung ganzer Produktionsbereiche empfindlich getroffen werden und entsprechend erpressbar sind. Vor allem Attacken mit Ransomware, die zum Beispiel über ungepatchte Systeme in Produktionsumgebungen eingeschleust werden kann, sind zu einem profitablen Geschäftsmodell geworden, das Kriminellen für wenig Aufwand und Risiko hohe Gewinne einbringt.

Worauf wir uns einstellen müssen und wie wir das tun

Die einhellige Meinung der befragten Expertinnen und Experten ist, dass sich Cyberattacken kommerzialisiert haben und deswegen das neue Geschäftsmodell Ransomware weiter anwachsen wird. Dabei werden wir vermehrt mit zielgerichteten Angriffen auf OT-Bereiche von Unternehmen rechnen müssen.

Allerdings ist bei Betreibern inzwischen eine wachsende Gegenwehr zu sehen. Die Notwendigkeit einer umfassenden Absicherung von IT-Infrastruktur in der Betriebstechnik ist im Management ganz oben angekommen. Es wird in Assetmanagement Lösungen investiert und bei den Herstellern stehen die ersten Produkt- und Prozessertifizierungen nach IEC 62443 auf der Tagesordnung. Wesentliche Herausforderungen bestehen dabei zum einen in einer noch immer nicht aus-

reichend etablierten Awareness und zum anderen auch in zunehmend fehlenden personellen Ressourcen, um Projekte vorantreiben und umsetzen zu können. Es gibt nach wie vor zu wenige Security-Experten auf dem Markt.

Und dann ist da noch Corona. Die Pandemie hat die finanziellen und personellen Ressourcen weiter verknüpft und Security Projekte dadurch ausgebremst. Allerdings liegt in der Situation auch eine große Chance, denn die Anforderung Remotezugänge einzurichten und der Nutzen, den sie bieten, treibt die Digitalisierung massiv voran.

Gemeinsam in die richtige Richtung

Dass umfassende Sicherheitskonzepte in den Unternehmen nicht von heute auf morgen verfügbar sind, liegt auf der Hand. Die Entwicklung hin zu einer praxistauglichen Vorgehensweise ist eine langwierige Angelegenheit. Wie schwierig es sein kann, einen zeitgemäßen Umgang mit Security zu finden, lässt sich an den derzeit oftmals hitzig geführten Diskussionen um den kürzlich veröffentlichten neuen Referentenentwurf des IT-Sicherheitsgesetzes (ITSiG) für kritische Infrastrukturen verfolgen. Gut Ding will eben Weile haben.

Es gilt, aktuell die Widerstandsfähigkeit von Organisationen, Prozessen und Infrastrukturen zu stärken und den möglichen Schaden durch Cyberangriffe, die dennoch einen Weg ins Unternehmen finden, zu begrenzen. Das gelingt am besten – darin herrscht große Einigkeit – wenn die „Basics“ der Industriellen Sicherheit umgesetzt werden. Dabei geht es nicht um den neuesten Hype auf der technologischen Spielwiese, sondern vielmehr um die weniger spektakulären, aber bewährten Maßnahmen wie Patchmanagement, Zutrittskontrolle und Multifaktor-Authentifizierung, Segmentierung von Netzen, Asset Management, et c. Um ein möglichst hohes Maß an Sicherheit zu erreichen, sollten die einzelnen Maßnahmen im Rahmen eines mehrstufigen Schutzkonzeptes realisiert werden.

Dabei ist es unerlässlich, dass Betreiber, Integratoren und Hersteller an einem Strang ziehen und Security-by-Design-Ansätze vorantreiben und umsetzen. Die gemeinsame Ausrichtung beginnt aber bereits in den Unternehmen selbst mit einer wertvollen Kombination von Expertise und Erfahrung, nämlich in einer engen Zusammenarbeit von IT-Abteilung und OT-Bereichen.

Und meine ganz persönliche Meinung ist, dass wir unsere Hands-on-Mentalität weiter ausbauen und aktiv nach funktionierenden Wegen suchen und diese miteinander teilen müssen. Es ist ein gemeinsames Ziel, das wir verfolgen, die erforderliche Anstrengung ruht auf vielen Schultern.

Max Weidele



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:
info@sichere-industrie.de

Online:
<https://sichere-industrie.de>



sichere* *industrie 
simplified industrial security