23 Experten teilen ...

ihre Meinung zu **Entwicklung und Trends**

Industrial- und IoT-Security Jahresrückblick

2022

Sichere Industrie

Vorwort

In diesem Jahr konnte man den Eindruck bekommen, dass die Welt Kopf steht. Kaum dass die Folgen der Pandemie ihre volle Wirkung erzielten und die Weltmärkte vor riesige Herausforderungen stellten, folgte ein Krieg in Europa, der nach wie vor anhält und dessen Auswirkungen wir alle spüren.

Unser traditioneller Jahresrückblick fasst die Ereignisse und Entwicklungen des Jahres aus Security-Sicht zusammen und dabei ist uns wichtig, ein möglichst umfassendes Bild aus den persönlichen Blickwinkeln unserer Experten aufzuzeigen. Die meisten Beiträge nennen den russischen Angriffskrieg und die besondere Gefährdungslage, die sich daraus für **Kritische Infrastrukturen** ergibt, als eines der bestimmenden Themen in diesem Jahr. Auch wenn die Befürchtungen sich bisher nicht bewahrheitet haben und große Cyberangriffe in diesem Kontext noch ausgeblieben sind, so wird uns doch deutlich vor Augen geführt, was für alle Beteiligten Priorität haben muss:

IT-Infrastrukturen auch in OT-Bereichen ausreichend gegen Gefahren egal welchen Ursprungs abzusichern.

Das geht nach wie vor nur schleppend voran, vor allem bei Unternehmen, die keiner Regulierung unterliegen und noch immer hoffen, dass der Blitz im Nachbarhaus einschlägt, aber nicht im eigenen. Die Unternehmen der Kritischen Infrastrukturen hingegen stehen durch die **Angriffserkennung,** die der Gesetzgeber ab **1. Mai 2023** für sie vorschreibt, gewaltig unter Handlungsdruck. Und das wird sich fortsetzen, wenn die Europäische Regulierung etwa mit der **NIS2 Richtlinie** und dem **Cyber Resilience Act** nachlegt und Cybersecurity für die gesamte Lieferkette verbindlich vorgibt. Dabei lassen wir einmal außer Acht, wie und von wem diese stärkere Regulierung im Zweifel in Zukunft nachverfolgt werden soll.

Der Markt kommt durch eine veränderte Nachfrage in Bewegung. Weil Produktsicherheit für Betreiber eine immer größere Rolle spielt, sind die Hersteller und Zulieferer in der Pflicht. Themen wie sichere Software Supply Chains durch die Software Bill of Materials **(SBOM)** und Schwachstellenmanagement nach dem **CSAF Standard** (Common Security Advisory Framework) nehmen immer mehr an Fahrt auf.

Um Security für vernetzte heterogene Industrieumgebungen wirksam zu implementieren, braucht man Expertinnen und Experten. Diese fehlen leider nach wie vor - der Fachkräftemangel limitiert die Handlungsspielräume. Umso wichtiger ist es, die vorhandene Expertise bestmöglich zu nutzen und einen Wissenstransfer in alle Richtungen aktiv zu fördern.

Ich freue mich sehr über die vielen interessanten und persönlichen Einblicke der Experten aus den ganz unterschiedlichsten Bereichen, die wir im vorliegenden Jahresrückblick zusammengefasst haben. Beim Lesen wünsche ich Ihnen viel Spaß!

Außerdem wünsche ich Ihnen einen erfolgreichen Jahresabschluss und ein gutes und gesundes Jahr 2023.

Max Weidele
Gründer
»Sichere Industrie«

Manuel Atug
HiSolutions AG

Was war für Sie bemerkenswert in Ihrem Security-Jahr 2022?

In den Parteien der Ampel wird deutlich öfter über Digitalisierung und Security-Themen und auch über den Schutz von Kritischen Infrastrukturen gesprochen, als es noch in der GroKo der Fall war. Das Ganze nimmt also so langsam auch in den seriösen Bereichen, abseits von Glitzer wie Blockchain- und KI-Hypes oder Schaufenster- und Leuchtturm-Projekten zum Profilieren, Fahrt auf, was ich sehr begrüße.

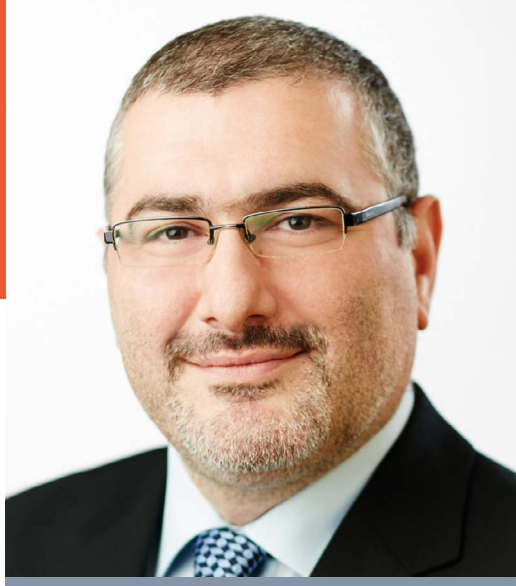
Bei welchem Thema haben Sie mehr Entwicklung erwartet, als tatsächlich eingetreten ist?

Angriffserkennungssysteme, denn das IT-SIG2.0-Gesetz schreibt den Einsatz für KRITIS ja ab Mai 2023 vor und eigentlich hätte es da mehr Entwicklung und Kommunikation zu geben müssen. Das BSI hat mit einer guten Orientierungshilfe vorgelegt, aber von den Anbietern kommt da nicht viel mehr als ein wenig Werbung und Marketing.

Gab es für Sie ein Trendthema der Digitalisierung, das aus Security-Perspektive für ordentlich Stress gesorgt hat?

„Cyberwar“ hat aufgrund des Angriffskrieges von Putin auf die Ukraine für viel Stress und Aufregung gesorgt. Tatsächlich waren es aber eher 1.000 kleine Nadelstiche wie DDoS-Angriffe auf Webseiten oder ähnliches. Und die Maßnahmen, die von den Sicherheitsbehörden empfohlen wurden, wie Patchen der aus dem Internet erreichbaren Systeme und Vorhalten von Offline-Backups, waren die üblichen, die auch vor dem Krieg akut waren und sie sind es nach dem Krieg immer noch. Insofern hat der Cyberwar, welcher im Wesentlichen nur auf den Powerpoint-Folien von alten, weißen Männern aus der Rüstungsindustrie und von unseriösen Sicherheitsproduktanbietern existiert, viel Stress gemacht, aber nicht wirklich zu einem Mehrwert in der Industrie-Sicherheit geführt.

»Am Ende geht es uns alle etwas an, ob wir eine sichere Industrie haben und ob morgen noch Strom und Wasser aus den Leitungen kommt.«



Manuel Atug
Head of Business Development

HiSolutions AG

Was ist Ihr persönlicher Wunsch im Kontext Security für 2023?

Dass wir ein sinnvolles und wirksames KRITIS Dachgesetz für den physischen Schutz von Kritischen Infrastrukturen erhalten und dass eine gute Umsetzung der EU NIS2 Richtlinie vorgenommen wird. Damit könnten wir eine defensive Cybersicherheitsstrategie EU-weit vorleben und umsetzen und die Kritischen Infrastrukturen dadurch resilienter machen, statt Compliance-Papiertiger zu schaffen, populistische und offensive Maßnahmen einzufordern oder wirkungslose Befugniserweiterungen für die Sicherheitsbehörden zu schaffen, die den Schutz von KRITIS tatsächlich reduzieren.

Das geht alles natürlich nur, wenn die Expertinnen aus Wissenschaft und Zivilgesellschaft auch mit an den Tisch geholt werden, statt nur im Kreis des Ministeriums zu agieren und Wirtschaftsverbände anzuhören.

Am Ende geht es uns alle etwas an, ob wir eine sichere Industrie haben und ob morgen noch Strom und Wasser aus den Leitungen kommt. Egal ob es ein Naturereignis, eine Ransomware oder ein (Cyber-)Angriff als Sabotageakt aus politischer Motivation getrieben war, das die Bedrohung auslöst. Wenn solche Ereignisse durch geeignetes Risiko- und Notfallmanagement statt zu einer Katastrophe lediglich zu einer Störung reduziert werden können, benötigen wir nicht 100%ige Sicherheit. Wir haben dann verfügbare kritische Dienstleistungen für das Gemeinwohl der Bevölkerung.

Ron Brash
aDolus Technology Inc.

What was remarkable for you in your security year 2022?

The number of software supply chain discussions surrounding product development was remarkable. There was a growing awareness of the complexity of all that goes into a software package, including inherited weaknesses. Standards and legislation have pushed for Software Bills of Material (SBOMs) and transparency in the software supply chain, but industry isn't ready for the tsunami of issues that will arise from greater visibility. Vulnerability management will require an organizational rethink on the influx of red in risk dashboards.

There was a monumental increase in software supply chain attacks recently. The resulting emphasis on SBOMs has been energizing, but I worry that the risk contained in inherited flaws is underappreciated.

If I already own risky assets and I lack resources, I'm going to struggle. If the average 40 MB firmware has 100 subcomponents, 70+ CVEs, and 5000+ child files, imagine the risks embedded in a 5 GB SCADA application? Supply chain security is complicated, but we have momentum. For example, a large integrator came to us with a vision and technical roadmap for tackling supply chain issues to answer both an organizational and a customer need. This integrator's mindset was a good surprise for my engineer-like heart.

On which topic did you expect more development than actually occurred?

I expected more convergence between Vulnerability Exploitability eXchange (VEX) information and asset management solutions in 2022. It is one thing to obtain a product SBOM, but operators want frequent, accurate associations of vulnerabilities on their assets — especially those inherited from vulnerable subcomponents. And they need to know which vulnerabilities do NOT affect them so they can sleep easy when a CVE is published warning of Armageddon-like impacts.

Getting full value from SBOMs requires more work, like combining OEM information with asset and vulnerability management systems to make informed risk decisions. Happily, for asset owners who are struggling to obtain SBOMs from their OEMs, technologies exist for creating them on their own (even for legacy software where there's no source code). Asset owners and integrators just need to yell louder to get their asset management solutions to ingest VEX and SBOM documents.

Was there a trendy topic in digitalization that caused a lot of stress for you from a security perspective?

SBOMs were the trendy topic in 2022 and were often characterized as a panacea to the world's cybersecurity woes. Truthfully, standalone SBOMs are simply an ingredients list. They require enrichment to be useful — enrichments like aggregation of risks, prioritization, namespace problem correction, vulnerability associations, component vendor detection, and file similarities.

Most people are looking for a way to understand what is in a product and without doubt, SBOMs are a software supply chain imperative. However, be sure to clarify how they are to be practically used, and determine if they can be used at scale and in an organization-friendly manner.

»I would like to have more honest conversations about the condition of our critical infrastructure assets.«

Ron Brash
VP of Technical Research & Integrations

aDolus Technology Inc.

What is your personal wish in the context of security for 2023?

I would like to have more honest conversations about the condition of our critical infrastructure assets. We generally take good care of revenue-generating systems (e.g., a turbine), but we are dropping the ball on networking infrastructure upgrades, tombstoning and virtualizing hardware, and most cybersecurity basics. I'd like to see that corrected.

Security can be done affordably and intelligently. We just need to apply common sense, avoid run-to-fail situations, and approach technology as an ongoing transition.

Fred Gordy
Michael Baker International

What was remarkable for you in your security year 2022?

This is the first year I have seen firsthand the type of attacks and misuse we've seen. All of these happened in the third quarter of 2022.

- Russian-based malware infiltrated a commercial real estate property's HVAC system.
- Crypto mining installed on the building control system had been running for most of 2022.
- Access control service provider did not have hardware and backups as documented in the service agreement. The server died and the service provider did not have a server ready. Once a server was procured the service provider's most recent copy of the backup was in October of 2008.
- A service provider fired an employee. Because the service provided remote access and used only one username and password, the ex-employee was able to get into a customer's system and brick/disable several controllers and also wiped three servers clean.

On which topic did you expect more development than actually occurred?

There is a lot of work being done on cybersecurity standards for building control systems. However, the people who service, install, and run these systems are entrenched in 40+ years of culture that do not include cybersecurity.

Work must be done to change the culture. If this is not done, the adoption of these standards will be slowed down greatly.

Was there a trendy topic in digitalization that caused a lot of stress for you from a security perspective?

Interoperability between systems is a good thing, however, if done without cybersecurity at its core, the systems are left extremely vulnerable. ISA 62443 has a method called Zones and Conduits to define and secure systems in a building. Each is assessed to determine what Zone they are in. When communication between systems is needed, the systems are usually wide open to each other. This means infiltration of one could mean infiltration of all systems. Conduits define the path and the specific points required and only they are allowed.

»The foundation for cybersecurity is knowing what you have, knowing how it is connected, and knowing who has access.«

What is your personal wish in the context of security for 2023?

The foundation for cybersecurity is knowing what you have, knowing how it is connected, and knowing who has access. These have to be starting points before you begin building your cybersecurity program.

It is my wish that everyone answer for themselves these three questions. We see it all the time. None of the three is known fully by most building system owners.

Fred Gordy
Director –
OT Risk Assessments

Michael Baker International

Sebastian Fritsch - Mirco Weber
secuvera GmbH

Was war für Sie bemerkenswert in Ihrem Security-Jahr 2022?

Im Gegensatz zu früheren Jahren ist die IEC 62443 nun als OT-Security-Norm im Markt klar angekommen. Es besteht nun weniger die Frage, nach welchem Standard man vorgehen soll oder ob überhaupt etwas getan werden muss. Stattdessen wird nun explizit die Frage gestellt, wie setze ich die Anforderungen der IEC 62443 in meinem Unternehmen effizient um.

Ein Grund ist hier mit Sicherheit, dass immer mehr Unternehmen Lieferketten-Security einfordern, und zwar entweder die Einhaltung der gesamten IEC 62443-4-1 (Anforderungen an den sicheren Produktentwicklungsprozess) oder erstmal nur Teile dieser Norm.

Bei welchem Thema haben Sie mehr Entwicklung erwartet, als tatsächlich eingetreten ist?

Im Bereich der Security hat man sich leider über die Jahre daran gewöhnt, dass wir nur sehr langsam vorankommen. Das liegt sicherlich daran, dass Security ein Qualitätsmerkmal ist, und kein funktionales Feature darstellt. Daher ist es wichtig, dass Security als zentrale Anforderung definiert und über Management-Ansätze verwaltet wird. Dennoch zeigt sich, dass Security auch von externen Stellen immer mehr eingefordert wird (u.a. Lieferketten-Security, Regulierungsinitiativen) und im Angesicht zahlreicher medienwirksamer Angriffe auch immer mehr in den Fokus rückt.

Gab es für Sie ein Trendthema der Digitalisierung, das aus Security-Perspektive für ordentlich Stress gesorgt hat?

5G-Campus-Technik macht der WLAN-Technologie zunehmend Konkurrenz. Die Komplexität ist zwar deutlich höher, aber dafür hat die Technologie viel Potential, zum Beispiel hinsichtlich Echtzeitfähigkeit und damit verbundener Use-Cases.

5G-Netze werden derzeit realisiert, Security jedoch wird wenig betrachtet. Dies bedeutet aber, dass wir nachträglich 5G-Campus-Netze abzusichern haben, die zunächst Testnetze waren und dann schleichend doch produktiv genutzt werden.

»Im Gegensatz zu früheren Jahren ist die IEC 62443 nun als OT-Security-Norm im Markt klar angekommen.«

Sebastian Fritsch
Leiter Industrial Security/Prüfstelle

Was ist Ihr persönlicher Wunsch im Kontext Security für 2023?

In den letzten Jahren wurden an verschiedenen Stellen durch den europäischen Gesetzgeber viele Initiativen gestartet, die bis heute noch nicht abgeschlossen sind und zum Teil relevante Kapazitäten der Security Community binden.

Die europäischen Initiativen im Kontext Cybersecurity sind seit 2018 der Start der Umsetzung des Cybersecurity Act (CSA), dann seit 2021 die Ergänzung von Security Anforderungen im Rahmen der RED Directive und nun noch seit 2022 der Beginn der Diskussion zum Cyber Resiliance Act (CRA).

Es wäre wünschenswert, wenn Teile dieser Initiativen 2023 abgeschlossen werden, sodass die Praktiker endlich übernehmen können, und die Ergebnisse in den Markt tragen, um damit den Zielen der Initiativen näher zu kommen: Security-Qualität in Produkte zu bringen.

Mirko Weber
Industrial Security Experte

secuvera GmbH

Sichere Industrie

Andreas Harner
CERT@VDE

Was war für Sie bemerkenswert in Ihrem Security-Jahr 2022?

Security-Anforderungen werden mehr und mehr durch die Betreiber von Automatisierungstechnik in Ausschreibungen gefordert. Das bringt Herausforderungen für Zulieferer entlang der gesamten Lieferketten.

Lieferanten und Hersteller spüren diesen Druck: Security umsetzen und machen heißt nun die Devise! Dazu gehört auch das Veröffentlichen von klar strukturierten und aussagekräftigen Warnmeldungen (Advisory) der Hersteller.

Zudem zeigt der Russland-Ukraine-Krieg, wie anfällig moderne Gesellschaften für Angriffe auf Kritische Infrastrukturen sind und wie wichtig deren Schutz vor Angriffen auch aus dem Cyberraum sind. Und weil es in diesen Strukturen eben nicht nur IT, sondern auch sehr viel OT gibt, rückt das Thema „OT-Security“ mehr und mehr in das Wahrnehmungsfeld der Öffentlichkeit.

Bei welchem Thema haben Sie mehr Entwicklung erwartet, als tatsächlich eingetreten ist?

Ich vermisse eine Art „Wumms“ im Bereich der Cybersecurity im Rahmen der Ausbildung in Deutschland. Vielleicht sehe ich relevante Anstrengungen und Initiativen auch nicht, aber wo bitte bleiben Ausbildungsoffensiven und Kampagnen, um den so dringend benötigten „Security Nachwuchs“ aufzubauen? Das muss in den Schulen und erst recht in den Hochschulen adressiert werden!

Gab es für Sie ein Trendthema der Digitalisierung, das aus Security-Perspektive für ordentlich Stress gesorgt hat?

Ja, das starke, zum Teil exponentielle Wachstum der gefundenen Schwachstellen in den Produkten der Automatisierungstechnik. Dies macht das Umsetzen von Maßnahmen, die die Effizienz steigern, in unserem CERT-Umfeld unumgänglich:

Die Einführung von maschinenlesbaren Warnmeldungen der Hersteller nach dem CSAF Standard (www.csaf.io) ist hierbei ein wesentlicher Meilenstein.

»[Der] Russland-Ukraine-Krieg [zeigt], wie anfällig moderne Gesellschaften für Angriffe auf Kritische Infrastrukturen sind und wie wichtig deren Schutz vor Angriffen auch aus dem Cyberraum ist.«

Andreas Harner
Abteilungsleiter
CERT@VDE &
Cybersecurity

DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE

Was ist Ihr persönlicher Wunsch im Kontext Security für 2023?

Cybersicherheit muss, wie beispielsweise in der IEC 62443-4-1 gefordert, ein wesentlicher Bestandteil eines sicheren Produktentwicklungszyklus bei den Herstellern sein und werden. Ansonsten wird eine Art „Darwinismus“ einsetzen mit der Konsequenz, dass viele Hersteller auch in Deutschland und Europa an der Digitalisierung scheitern.

Sichere Industrie

Dr.-Ing. Lutz Jänicke
PHOENIX CONTACT GmbH & Co. KG

Was war für Sie bemerkenswert in Ihrem Security-Jahr 2022?

Die geopolitische Lage hat die Herausforderungen zur Security aufgezeigt. Neben der Vielzahl öffentlich gewordener Fälle von Ransomware-Erpressung ist die Cyberbedrohung durch staatliche Akteure in die Wahrnehmung gerückt worden.

Dass es durch zwei gezielte Angriffe auf Glasfaserverbindungen möglich war, den Bahnverkehr in Norddeutschland zum Erliegen zu bringen, zeigt den Bedarf an weitergehenden Maßnahmen. Dabei ist es unwichtig, wer die Anschläge und mit welcher Motivation verübt hat. Wir sehen die Verwundbarkeit (Schadenshöhe) und immer mehr Vorfälle (Eintrittswahrscheinlichkeit). Das Risiko, selbst betroffen zu sein, steigt.

Bei welchem Thema haben Sie mehr Entwicklung erwartet, als tatsächlich eingetreten ist?

Was in der Breite in vielen Unternehmen zur Cybersecurity unternommen wird, lässt sich schwer beurteilen. Das Bewusstsein wächst aber sicher.

Grundsätzlich war noch für 2021 die Verordnung zu wirtschaftlich relevanten „Unternehmen im besonderen öffentlichen Interesse“ im Kontext des IT-Sicherheitsgesetzes 2.0 erwartet worden. Dies hätte sicher zu zusätzlichem Handlungsdruck geführt. Mittlerweile steht die Version 2 der europäischen Richtlinie zur Netzwerk- und Informationssicherheit (NIS 2.0) vor der Verabschiedung und wird deutliche Anforderungen setzen.

Gab es für Sie ein Trendthema der Digitalisierung, das aus Security-Perspektive für ordentlich Stress gesorgt hat?

Eigentlich nicht. Vielmehr könnte man zu der Einschätzung kommen, dass mehr Digitalisierung mitunter helfen würde, wenn sie denn professionell erfolgt, also die Cybersicherheit berücksichtigt.

Dass Kommunen oder zum Beispiel die Industrie- und Handelskammern langfristig durch Cyberangriffe lahmgelegt werden können, ist ein Unding. Und hier würde man sicher nicht zu viel Digitalisierung unterstellen. In zahlreichen Unternehmen geht die Digitalisierung mit Security-Maßnahmen Hand in Hand.

»Die Bedrohungslage nimmt permanent zu und jede Organisation sollte die notwendigen [Security-]Maßnahmen aus eigenem Interesse umsetzen.«

Dr.-Ing.
Lutz Jänicke
Corporate Product & Solution Security Officer

PHOENIX CONTACT GmbH & Co. KG

Was ist Ihr persönlicher Wunsch im Kontext Security für 2023?

Dass die sichtbaren Fortschritte zur Cybersecurity mit hoher Geschwindigkeit ausgebaut werden. Die Bedrohungslage nimmt permanent zu und jede Organisation sollte die notwendigen Maßnahmen aus eigenem Interesse umsetzen.

Zusätzlicher Druck kommt aus der nationalen und internationalen Regulierung. Der europäische Gesetzgeber hat mit der NIS 2.0-Richtline und dem gerade neu vorgeschlagenen Cyber Resilience Act große Schritte gemacht. Es wird für alle Beteiligten eine Herausforderung werden, diese Anforderungen zeitgerecht zu realisieren.

Klaus Jochem
Klaus Jochem Unternehmensberatung

Was war für Sie bemerkenswert in Ihrem Security-Jahr 2022?

Die Assessments und Beratungen, die ich in diesem Jahr durchgeführt habe, zeigen deutlich, dass in der OT und in der IT die grundlegenden Dinge immer noch nicht gemacht werden. Viele Unternehmen arbeiten an der Einführung von “Fancy Tools” wie Privileged Account Management und Anomalie-Erkennung, also an den letzten 10% des Sicherheitsniveaus. Die ersten 50%, die zudem fast ohne zusätzliche Investitionen erreichbar sind, werden vielfach nicht oder unzureichend umgesetzt. Nur zwei Beispiele:

[1] Patchen von Anwendungen ist die vielleicht unbeliebteste Aktivität bei IT- und OT-Security-Teams überhaupt. Dabei sind es nicht-gepatchte Schwachstellen (z.B. Log4Shell) auf Systemen, die vom Internet oder vom Firmennetzwerk erreicht werden können, über die Angreifer in Firmen- oder Produktionsnetzwerke einsteigen. Für Systeme an Netzwerkübergängen sollte mindestens Vulnerability-Management gemacht werden, damit eine schnelle Behandlung von Schwachstellen ermöglicht werden kann.

[2] RDP und psexec sind mit die beliebtesten Transportwerkzeuge bei Angreifern, insbesondere mit lokalen Accounts. Seit Jahren empfiehlt Microsoft, jeden Netzwerkzugriff mit lokalen Accounts zu unterbinden. Das kann per Group-Policy ohne großen Aufwand zentral durchgeführt werden, stoppt viele Angriffe bereits nach der initialen Übernahme eines Systems, und ist kaum implementiert.

Fancy Tools benötigen eine sichere Grundlage damit sie die geplanten Ergebnisse liefern können. Privileged Account Management wirkt nur dann, wenn die Möglichkeit, lokale Accounts einzurichten und mit ihnen im Netzwerk zu arbeiten, beschränkt ist. IT-/OT-Security, die auf tönernen Füßen steht, wird Angriffen nicht dauerhaft standhalten können.

Bei welchem Thema haben Sie mehr Entwicklung erwartet, als tatsächlich eingetreten ist?

Einige Hersteller von Automatisierungslösungen unterstützen nun Microsoft Defender als Antimalware-Lösung, leider nur die im Betriebssystem eingebaute Lösung. Das genügt bei weitem nicht, um modernen Bedrohungen effektiv und effizient begegnen zu können. Aus Sicht der IT-Security sind wir beim Thema Anti-Malware-Lösungen im Automatisierungsumfeld noch in den 1990er Jahren. Hier muss sich dringend etwas tun, gerade im Hinblick auf Digitalisierung und Cloud.

Gab es für Sie ein Trendthema der Digitalisierung, das aus Security-Perspektive für ordentlich Stress gesorgt hat?

Das Thema IT-/OT-Konvergenz hat für viel Stress gesorgt, jedoch eher für Eustress als Distress. Ich bin ein Befürworter von IT-/OT-Konvergenz, da durch IT-Automatisierung im Produktionsumfeld Personalkapazitäten frei werden, die wir dringend im Umfeld Digitalisierung benötigen.

IT-/OT-Konvergenz funktioniert sehr gut, sobald IT- und OT-Personal die gleiche Sprache sprechen. Dieses gemeinsame Verständnis zu erreichen, ist für einen Moderator teilweise anstrengend.

»IT-/OT-Konvergenz funktioniert sehr gut, sobald IT- und OT-Personal die gleiche Sprache sprechen.«

Klaus Jochem

IT / Security Strategist

Klaus Jochem Unternehmensberatung

Was ist Ihr persönlicher Wunsch im Kontext Security für 2023?

Mein persönlicher Wunsch ist “mehr Automatisierung” in der IT-/OT-Security. Warum?

Aus meiner Sicht braucht man Security, um das vorhandene Geschäft zu sichern. Security erzeugt weder Innovation, noch erhöht sie die Produktivität. Schlecht gemacht behindert sie Innovation und reduziert Produktivität. Der Ökonom Peter F. Drucker würde bei einem solchen Produkt die Frage stellen: „How do we get out and how fast?“ Schlimmer noch, Security bindet die smarten Leute, die wir dringend für Digitalisierung und Innovation benötigen.

Leider können wir nicht aus der Security aussteigen, aber wir können durch verstärkte Automatisierung verhindern, dass noch mehr Personal durch diese Aktivitäten gebunden wird.

Peter F. Drucker mein dazu: „Economic results require also that staff efforts be concentrated on the very few activities that a capable of producing truly significant business results – with as little staff work and staff effort as possible spent on the others.“

Sichere Industrie

Isiah Jones, GICSP, CISSP
AIT Applied Integrated Technologies

What was remarkable for you in your security year 2022?

Learning about ObjectSecurity's ability to scale and automate binary reverse engineering steps.

I collaborated with them, to map discovered weaknesses and vulnerabilities to ISA/IEC 62443 part 4-2 component security requirements. Had those component requirements been designed into the embedded hardware, firmware and or software capabilities in the beginning it could have prevented, removed or at least minimized those discovered weaknesses (CWE) and or vulnerabilities (CVE).

On which topic did you expect more development than actually occurred?

More focus didn't happen on automating the discovery and testing of PLC top 20 security coding practices for Ladder Logic, Function Block Diagram, Function Chart etc.

I had hoped that the PLC programming vendors would have updated their programming software and publically documented or advertised how many of the top 20 practices were already automatically flagged and checked for the programmers and end users. That didn't happen.

Was there a trendy topic in digitalization that caused a lot of stress for you from a security perspective?

Virtualization of PLCs, IO, safety systems. Putting ICS OT protocols into Cloud edge connector gateway software and essenstially taking protocols like Modbus and extending them to the Cloud directly. Pushing Cloud and virtualization down to Purdue Model level 1 and sometimes even level 0 devices in the field has unnecessary safety implications yet to be fully realized. Is the juice really worth the squeeze?

»Secure Design is not optional, it's the purpose of doing security in the first place.«

Isiah Jones, GICSP, CISSP

Cyber Engineer (ICS OT IIoT IoT Cyber-Physical)

AIT Applied Integrated Technologies

What is your personal wish in the context of security for 2023?

For 2023 I wish for the following:

- PLC programming and change management software all implement automated logic checking and flagging features for programmers, end users and security consultants to easily check and verify which PLC top 20 practices were implemented in the logic.

- More persistent, frequent and aggressive full spectrum offensive red team as a service engagements across all sectors using ICS OT IIoT IoT embedded components and Cyber-Physical systems. Narrow scope pentration tests once a year or every other year is not good enough.

- More scaling and integration of automated binary reverse engineering, decompiling and disassembly and asset owners doing a mapping of tools like ObjectSecurity in their supply chain security. More efforts by systems integrators and security consulting in their services and as well by product suppliers and OEMs in their product development lifecycle to rapidly improve design weaknesses and vulnerabilites.
  I'd like to see security level 3 (SL-3) in ISA/IEC 62443 part 4-2 for component requirements become the international baseline that all components are designed to.
  That'd be my wish for 2023.

Sichere Industrie

Hans-Peter Käser
Bundesamt für wirtschaftliche Landesversorgung BWL

Was war für Sie bemerkenswert in Ihrem Security-Jahr 2022?

Die massive Zunahme der Cyberangriffe auf Kritische Infrastrukturen. Mit dem Ausbruch des Ukraine-Konflikts sind noch weitere Bedrohungen dazugekommen. Angriffe, die auf ViaSat (USA) gemacht worden sind, hatten Auswirkungen auf Windparkanlagen in Deutschland. Das heißt, dass lokale Angriffe Auswirkungen auf andere Kontinente haben können. Ein neuer Faktor, der dazugekommen ist, sind Sabotageakte auf Kabelverbindungen (Deutschland und Frankreich), die massive Auswirkungen auf den Betrieb von Kritischen Infrastrukturen haben.

Die Verwundbarkeiten haben nun auf allen möglichen Ebenen zugenommen und stellen uns vor neue Herausforderungen. Gleichzeitig bleiben die Herausforderungen aus den Covid-Jahren weiter bestehen: Schlecht definierte Homeoffice-Prozesse mit vielen neuen Angriffsvektoren und global gestörte Lieferketten mit immer noch sehr großen Lieferschwierigkeiten bei Hardwareelementen.

Bei welchem Thema haben Sie mehr Entwicklung erwartet, als tatsächlich eingetreten ist?

Die ganzen Digitalisierungsprozesse sind noch nicht so weit gekommen, damit diese für die Anwender akzeptiert und anwendbar sind.

Ein gemeinsames Verständnis für Sicherheitsanforderungen fehlt ebenso, wie ein Bewusstsein für den Wert und die möglichen Zusatznutzen von Daten. Der Fokus scheint mir da etwas einseitig auf die Datenschutzthematik ausgelegt zu sein, anstatt auch den Mehrwert der Daten zu berücksichtigen. Das neue Datenschutzgesetz spielt hier eine wesentliche Rolle. Viele Firmen lassen sich bei der Umsetzung noch zu viel Zeit, da dieses Thema zu wenig priorisiert wird.

Gab es für Sie ein Trendthema der Digitalisierung, das aus Security-Perspektive für ordentlich Stress gesorgt hat?

Stress nicht, aber die Verfügbarkeit der IT-Anwendungen, die in die Cloud verschoben werden. Wenn wir die aktuelle Situation mit der Energieversorgung anschauen, wäre es durchaus möglich, dass Firmen bei einer Strommangellage nicht mehr auf ihre Daten zugreifen können, da die Datenleitungen nicht mehr zur Verfügung stehen. Da befürchte ich, dass das Business Continuity Management (BCM) noch nicht überall gemacht worden ist.

Ebenso wird Cybersecurity zu oft noch aus einer ichbezogenen Perspektive betrieben. Unternehmen beurteilen die Risiken an ihren Standorten, aber ohne auch die Abhängigkeiten von Energie, Lieferanten, Herstellern und Telekommunikations-Dienstleistern angemessen zu berücksichtigen.

»Ein gemeinsames Verständnis für Sicherheits-anforderungen fehlt ebenso, wie ein Bewusstsein für den Wert und die möglichen Zusatznutzen von Daten.«

Hans-Peter Käser

Projektleiter Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken

Bundesamt für wirtschaftliche Landesversorgung BWL

Was ist Ihr persönlicher Wunsch im Kontext Security für 2023?

Dass Security als laufender Prozess wahrgenommen wird, der immer wieder neu beurteilt werden muss. Dieses Thema ist noch nicht überall im Management angekommen.

Da wünsche ich mir, dass es uns gelingt, dass dieses Thema nun ernst genommen wird. Die Investitionen müssen nicht nur in Technik gemacht werden, sondern auch in Mitarbeiter:Innen, damit Awareness laufend geschult und trainiert wird (z.B. Feuerwehr).

Prof. Dr. Dennis-Kenji Kipker
Hochschule Bremen

Was war für Sie bemerkenswert in Ihrem Security-Jahr 2022?

Mit Sicherheit kann man den Russland-Ukraine-Krieg als ausschlaggebendes Ereignis auch für die Cybersecurity betrachten. Mit ihm wurde die nationale und europäische Cybersecurity-Landschaft gehörig durcheinandergewirbelt. Nicht nur, dass wir feststellen konnten, wir vulnerabel wir sind, sondern auch, dass Cybersecurity eben nicht alles ist und sein kann, um Kritische Infrastrukturen zu schützen. Stichwort ist da die sogenannte „hybride Kriegsführung".

Andererseits haben wir aber auch gesehen, dass das Thema „Cyberwar" weniger heiß gegessen als gekocht wird – Deutschland befindet sich nämlich nach wie vor nicht in einem Cyberkrieg. Und wir haben gesehen, dass Themen wie Desinformation auch unmittelbare Auswirkungen auf die Cybersecurity haben können.

Bei welchem Thema haben Sie mehr Entwicklung erwartet, als tatsächlich eingetreten ist?

Ich hätte mir tatsächlich vom Bund politisch wie gesetzgeberisch mutigere Schritte zur Stärkung der nationalen Cybersicherheit erhofft. Weder beim Thema „Hackback" beziehungsweise „digitaler Gegenschlag" konnte man bislang politisch einen sinnvollen Durchbruch erzielen noch beim staatlichen Umgang mit Schwachstellen und verschlüsselter Kommunikation. Die aus dem Bundesinnenministerium vorgestellte „Cybersicherheitsagenda" war inhaltlich eine absolute Enttäuschung und zeigt, dass das Thema trotz seines hohen Stellenwertes für Bürger und Industrie noch immer nicht die Bedeutung genießt, die es eigentlich haben müsste.

Gab es für Sie ein Trendthema der Digitalisierung, das aus Security-Perspektive für ordentlich Stress gesorgt hat?

Definitiv! Die Veröffentlichung des Entwurfs des neuen „Cyber Resilience Act" durch die Europäische Kommission im September. Cybersecurity wird nun endgültig zu einem Standard-Feature über alle Produkte und Branchen hinweg, gleichgültig ob B2B oder B2C.

Cybersicherheit muss über die gesamte (digitale) Lieferkette hinweg gedacht werden und wir haben ja bereits in der Vergangenheit mehr und mehr gesehen, wie angreifbar diese Lieferkette ist.

»Cybersecurity wird nun endgültig zu einem Standard-Feature über alle Produkte und Branchen hinweg, gleichgültig ob B2B oder B2C.«

Was ist Ihr persönlicher Wunsch im Kontext Security für 2023?

Ich würde mir deutlich mehr Verlässlichkeit und Rechtssicherheit beim Thema Cybersicherheit von Politik und Behörden wünschen, als dies bislang der Fall ist. Cybersicherheit ist kein Selbstzweck, sondern dient dem Schutz und Wohlergehen aller. Und das ist in diesem Jahr bei mancher politischen Entscheidung offensichtlich missverstanden worden.

Last but not least ein weiterer Aspekt: Der Gesetzgeber muss endlich Klarheit für den rechtlichen Umgang mit Penetration Testing schaffen und das Computerstrafrecht entsprechend reformieren! Es kann nicht sein, dass Sicherheitsforscher für legitime Interessen stets an der Grenze zur Strafbarkeit arbeiten.

Prof. Dr. Dennis-Kenji Kipker

Professor für IT-Sicherheitsrecht

Hochschule Bremen

Mirco Kloss - Daniel Buhmann
FORTINET, Inc.

Was war für Sie bemerkenswert in Ihrem Security-Jahr 2022?

Bemerkenswert ist nach wie vor die Abwehrhaltung, die einige Verbände gegenüber Regularien, Standards und Gesetzen leider an den Tag legen. Damit meine ich den Ansatz, sich gegen Vorschriften für Security zu wehren, anstatt diese umzusetzen.

Die Energie und der Aufwand, der betrieben wird, um „Schlupflöcher“ zu finden, um beispielsweise nicht unter KRITIS zu fallen, ist beachtlich. Warum wird diese Energie nicht einfach in die Umsetzung von Maßnahmen gesteckt? Das würde uns allen und vor allem den Unternehmen mehr nutzen und die Welt ein Stück weit sicherer machen.

Bei welchem Thema haben Sie mehr Entwicklung erwartet, als tatsächlich eingetreten ist?

Leider fehlt in den meisten Pflichtenheften immer noch das Thema Security. Ein Beispiel ist der Maschinenbau. Es ist nach wie vor schwierig, dass Sicherheit von vorne gedacht und einfach mit eingebaut wird. Dabei würde es viele Verbesserungen für die Sicherheit geben, wenn Maschinen schon mit Sicherheitskomponenten ausgeliefert würden.

Es muss dringend etwas passieren: Nur wenn Security verbindlich in Ausschreibungen steht, wird Security auch mit verbaut werden. Nehmen wir das Beispiel Sicherheit in Fahrzeugen: Auch Airbags sind mittlerweile serienmäßig in den Fahrzeugen verbaut, einfach weil es Sinn macht und weil Kunden es erwarten!

Gab es für Sie ein Trendthema der Digitalisierung, das aus Security-Perspektive für ordentlich Stress gesorgt hat?

Das Thema der vernetzen Gebäude. Gebäude sind weltweit für ca. 40% der CO2-Emissionen verantwortlich. Um hier gegenzusteuern und den Ressourceneinsatz zu optimieren, werden viele Gebäude nun „smartifiziert“, also technisch hochgerüstet, mit der Cloud verbunden, und vieles mehr.

Leider wird bei Smart Buildings häufig die Security außer Acht gelassen. Das führt zu einer zusätzlichen Erweiterung der Angriffsfläche und hat Auswirkungen auf die Safety. Wenn beispielsweise Fahrstühle betroffen sind, kann fehlende Security im günstigsten Fall nur einen Stillstand verursachen, aber im schlimmsten Fall kann leider auch ein Absturz die Folge sein. Gebäude müssen Secure Smart Buildings werden.

»Leider wird bei Smart Buildings häufig die Security außer Acht gelassen. Das führt zu einer zusätzlichen Erweiterung der Angriffsfläche und hat Auswirkungen auf die Safety.«

Was ist Ihr persönlicher Wunsch im Kontext Security für 2023?

Dass der §8 (1a) BSIG-E ganzheitlich gelesen wird. Aktuell sprechen die meisten davon, dass sie bis zum 1. Mai 2023 eine „Angriffserkennung" benötigen, weil das IT-Sicherheitsgesetz 2.0 (IT-SiG 2.0) die entsprechende Anforderung enthält.

Das bloße Erkennen eines Angriffs ist jedoch nicht ausreichend. Im Gesetzestext geht es auch um die Vermeidung von Bedrohungen und um geeignete Maßnahmen, um angemessen auf Störungen zu reagieren. Oder anders ausgedrückt: worin besteht der Nutzen, wenn ich vor meinem brennenden Betrieb stehe und zusehe, wie es brennt? Es muss der Brand dann auch gelöscht werden! Und am besten ist es doch, wenn es gar nicht erst so weit kommt, weil man auf die richtige Prävention gesetzt hat.

Mirco Kloss
Team Lead Business Development - Operational Technology D-A-CH

FORTINET, Inc.

Daniel Buhmann
Principal Systems Engineer OT/IoT

FORTINET, Inc.

Sichere Industrie

Peter Lukesch
ondeso GmbH

Was war für Sie bemerkenswert in Ihrem Security-Jahr 2022?

Dieses Jahr wurden unterschiedlichste Branchen und Unternehmen wie Bridgestone, Fendt, Knauf, Weidmüller, aber auch Energieversorger gezielt angegriffen. Dabei handelte es sich überwiegend um Ransomware, verteilt beispielweise über Supply Chain Attacks mit insgesamt sehr gravierenden Auswirkungen.

Bemerkenswert daran ist aber das Ergebnis. Es scheint so, als würden sich nur diese betroffenen Firmen danach intensiv mit grundlegenden Themen wie zum Beispiel einem Asset-Management oder einer sicheren Backup-Strategie auseinandersetzen. Andere atmen auf, weil sie nicht betroffen waren und priorisieren weiter die Hype-Themen, welche sich entweder direkt finanziell oder marketingtechnisch positiv auf das Unternehmen auswirken können. Eine interessante Wende könnte hier beispielsweise die NIS2 Direktive oder auch der Cyber Resilience Act vorantreiben.

Bei welchem Thema haben Sie mehr Entwicklung erwartet, als tatsächlich eingetreten ist?

Im Rahmen einiger Projekte und bei der gezielten Nachwuchssuche an Hochschulen und Universitäten ist mir dies wieder verstärkt aufgefallen: IT- und Security-Themen werden immer noch als reine IT-Aufgaben angesehen und halten nicht Einzug in die täglichen Unterstützungsaufgaben der Instandhaltung oder gar in einer eigenen OT-Organisation.

Dabei ist es in der heutigen Zeit unerheblich, ob eine Maschine nicht betriebsbereit ist, weil ein mechanisches Teil ausgefallen ist, oder eine Fehlkonfiguration vorliegt – oder gar das eine das andere zur Konsequenz hat, wenn beispielsweise eine Ersatzbaugruppe nicht vom System erkannt wird.

Gab es für Sie ein Trendthema der Digitalisierung, das aus Security-Perspektive für ordentlich Stress gesorgt hat?

Ein spannender Punkt ist immer wieder, mit welcher Akribie Unternehmen Produktionsdaten sammeln, auswerten und danach in der Cloud mit neuesten AI-Algorithmen verproben. Bei einem Vorfall wie Log4J zum Jahreswechsel oder den kürzlichen OpenSSL-Schwachstellen wird dann aber festgestellt, dass es an der Basis knirscht: Welche Geräte sind überhaupt im Einsatz? Welche Software ist installiert? Und in welchen Versionen? Geeignete Maßnahmen können zügig definiert werden. Bis man aber weiß, wo und wie man diese anwendet, kann eine Menge Zeit vergehen.

Auch wenn es uns in Deutschland mit dem Hang zu primär amerikanisch betriebenen Cloud-Plattformen nicht direkt betroffen hat, haben wir dieses Jahr auf sehr drastischem Weg erfahren, wie durch staatliche Auseinandersetzungen auch kurzfristig die Zusammenarbeit mit vorher noch legal verbundenen Unternehmen ausgesetzt oder gar untersagt werden kann.

Dabei sollte jedes Unternehmen für sich noch einmal genau bewerten, welche Daten mit welcher Businesskritikalität sich außerhalb des eigenen Zugriffs befinden und ob dies immer sinnvoll sein muss. Können Daten/Dienste beispielweise auch relativ kurzfristig wieder übernommen und selbst betrieben werden? Definierte SLAs sind nett, solange diese nicht durch staatliche Maßnahmen unterbunden werden.

»IT- und Security-Themen werden immer noch als reine IT-Aufgaben angesehen […].«

Peter Lukesch

COO

ondeso GmbH

Was ist Ihr persönlicher Wunsch im Kontext Security für 2023?

An meinem Wunsch hat sich gegenüber den letzten Jahren nicht viel geändert: Ich wünsche mir, dass die OT-Themen jetzt einfach angefangen werden.

In meinem Arbeitsalltag bei ondeso erlebe ich immer wieder, dass in den Unternehmen die wichtigen Themen selbst erkannt werden und es auch bekannt ist, woran mit welcher Priorität gearbeitet werden muss. Ein aus meiner Sicht großer Fehler dabei ist allerdings zu versuchen, in einem Megaprojekt die eine Lösung zu finden, die alle Herausforderungen ohne zusätzlichen Aufwand löst – in einem beratungsintensiven 2-Jahres-Projekt. Zielführender wäre es, das eine essenzielle Thema mit dem größten Mehrwert gezielt anzugehen, umzusetzen und dann Folgelösungen an dieser Strategie auszurichten. Dabei sollten im Speziellen die Mitarbeiter eingebunden werden, die am Ende auch damit arbeiten.

Prof. Dr.-Ing. Dominik Merli
Hochschule Augsburg - Institut für innovative Sicherheit

Was war für Sie bemerkenswert in Ihrem Security-Jahr 2022?

Für mich waren besonders die zahlreichen Vorfälle im ländlichen Raum bemerkenswert. Darunter waren auch einige Organisationen aus unserer Region Bayerisch-Schwaben, wie zum Beispiel die Reitzner AG aus Dillingen, die Donau-Stadtwerke Dillingen-Lauingen, die Produktion von AGCO/Fendt in Asbach-Bäumenheim und die Verwaltung der Marktgemeinde Bissingen.

Für die Zukunft bedeutet das: Angriffe auf KMUs, Produktionsstätten sowie Behörden sind nicht mehr nur Theorie, sondern tagtägliche Realität. Die Auswirkungen spürt jeder von uns: IT-Infrastrukturen stehen still, tausende Mitarbeitende müssen in Kurzarbeit und Kommunen können plötzlich ihre Services nicht mehr bereitstellen.

Auch die Vernetzung und Digitalisierung nimmt in vielen Organisationen zu. Dadurch vergrößert sich die Angriffsfläche noch mehr. Aus meiner Sicht ist es jetzt wichtiger denn je, Bewusstsein für die Risiken zu schaffen und praxisnahe Unterstützung anzubieten, auch in Branchen, die bisher wenig digital waren.

Bei welchem Thema haben Sie mehr Entwicklung erwartet, als tatsächlich eingetreten ist?

Ich hatte eine Aufbruchsstimmung bei der Entwicklung von sicheren Produkten in der Industrie erwartet. Mit dem Cyber Security Act und dem Cyber Resilience Act auf europäischer Ebene, aber auch der soliden Normengrundlage im Teil 4 der IEC 62443 gibt es hierfür gute Impulse.

Allerdings sind einige Unternehmen bei dieser Entwicklung hinter meinen Erwartungen geblieben. Investitionen in einen sicheren Entwicklungsprozess oder in starke Security Features für Produkte sind selten. Und das, obwohl sowohl die Bedrohungslage als auch die Anforderungen von Kunden und Gesetzgebern steigen. Statt proaktiv zu handeln, höre ich oft, dass die Konkurrenz auch noch nichts in diese Richtung unternimmt, dass Kunden für sichere Produkte nicht zahlen würden und dass einfach niemand im Unternehmen Zeit für diese Themen hat. Dabei sollte es meiner Meinung nach viel mehr um strategische Entscheidungen gehen, wie sich die Sicherheit von Komponenten in der Industrie, aber auch in anderen Bereichen, entwickeln soll und muss. Zudem können Schutzmaßnahmen auch durchaus positiv zur Differenzierung beitragen.

»Steigt der Grad der Digitalisierung, ist es aus meiner Sicht unabdingbar, dass auch in die Absicherung dieser IT-Systeme investiert werden muss.«

Prof. Dr.-Ing. Dominik Merli

Professor für IT-Sicherheit an der Fakultät für Informatik

Hochschule Augsburg - Institut für innovative Sicherheit

Gab es für Sie ein Trendthema der Digitalisierung, das aus Security-Perspektive für ordentlich Stress gesorgt hat?

Digitalisierung steht mittlerweile nicht mehr nur in der Wirtschaft auf der Tagesordnung. So geraten zunehmend auch Behörden, Schulen und kommunale Verwaltungen ins Fadenkreuz von Cyberkriminellen. 2022 legte ein Angriff die Stadtverwaltung Dingolfing lahm, womit das Rathaus 14 Tage lang nur telefonisch erreichbar war. Eine Phishing-Mail machte die Datenverarbeitung des Medienzentrums München-Land und damit 75 Schulen arbeitsunfähig und viele Kommunen wurden Opfer von Ransomware.

Steigt der Grad der Digitalisierung, ist es aus meiner Sicht unabdingbar, dass auch in die Absicherung dieser IT-Systeme investiert werden muss. Sonst drohen Ausfälle und starke Einschränkungen wie zum Beispiel durch Datenverlust. Und das spüren dann vor allem die Bürgerinnen und Bürger.

Was ist Ihr persönlicher Wunsch im Kontext Security für 2023?

Die Security-Branche arbeitet oft mit negativen Szenarien. Dabei lenken wir viel zu selten den Blick auf das, was tatsächlich gut funktioniert. Ich wünsche mir, dass positive Beispiele für sichere Produkte und vorbildliche Umsetzungen von sicheren Entwicklungsprozessen mehr Anerkennung und Sichtbarkeit bekommen. Denn nur über Security zu sprechen, wenn wieder etwas schief gegangen ist, sollte nicht unser Ziel sein.

Ein weiterer Vorteil: Wenn Unternehmen offen über ihre Erfolge in Sachen Sicherheit sprechen, schaffen sie Vertrauen bei ihren Kunden und geben dem Wettbewerb das klare Signal: an Security kommt man heute nicht mehr vorbei!

Sichere Industrie

Patrick Miller
Ampere Industrial Security

What was remarkable for you in your security year 2022?

Executive awareness of cybersecurity. I have seen a much greater degree of understanding and capability at the board, executive and senior leadership levels. Better, more informed questions are being asked by the right people to make risk decisions for the organization.

I am even seeing cybersecurity as a key component of merger and acquisition activity.

On which topic did you expect more development than actually occurred?

The Cyber Insurance market was less stable and more inconsistent than I expected. I had hoped both the asset owners and the insurers (including re-insurers) would stabilize on some better risk frameworks, questionnaires and actuarial tables but that hasn't happened.

I believe the impacts from ransomware in 2020-2021 have caused a serious shift. Many insurers no longer offer cyber insurance and those that do have increased premiums and made many of the necessary coverages additional packages at higher costs. Further, with the fluid definitions of war and force majeure, there is less certainty that they will even pay a claim if you submit one.

Was there a trendy topic in digitalization that caused a lot of stress for you from a security perspective?

The Zero Trust trend is confusing for many. I spend more time than I should helping management understand what it is, and what it isn't. Many have been sold on a panacea solution without a full understanding of how much impact it can have on operations during the implementation stage. It takes far more planning than most imagine.

»I am even seeing cybersecurity as a key component of merger and acquisition activity.«

Patrick Miller
Chief Executive Officer

Ampere Industrial Security

What is your personal wish in the context of security for 2023?

We figure out breach notification regulations. Starting with a solid decent definition for „incident“ and reasonable timeframes for reporting to authorities.

We should agree on a minimum set of data that must be reported and also provide safe harbor for those that report, with possible penalties for those that don’t. This will help organizations mature their programs as well as provide everyone with metrics/data on which measures are working and which are not.

Siegfried Müller
MB connect line GmbH

Was war für Sie bemerkenswert in Ihrem Security-Jahr 2022?

Auf das ganze Jahr gesehen hat mich doch die Vielzahl an Meldungen zu Angriffen in Unternehmen überrascht. Viele dieser Angriffe haben es auch in die Medien geschafft und somit wurde auch die Öffentlichkeit endlich mal intensiver informiert.

Gerade auch die Auswirkungen auf die Lieferketten waren doch schwerwiegend und teilweise nachhaltig. Manche der betroffenen Unternehmen sind auch nach Monaten noch nicht richtig wieder auf Kurs und andere hat es in kurzer Zeit gleich zweimal „erwischt".

Bei welchem Thema haben Sie mehr Entwicklung erwartet, als tatsächlich eingetreten ist?

Die gesamte Security-Community bietet eine große Anzahl an Informationsveranstaltungen, tiefe Einblicke in die Fachthemen und umfassendes Expertenwissen. Das Ziel ist dabei, viele Personen aus dem nicht-IT-Umfeld zu erreichen und für das Thema IT-Sicherheit in der OT zu sensibilisieren. Dennoch wird für mein Empfinden das Angebot noch nicht ausreichend wahrgenommen und das könnte sich in der Zukunft fatal auswirken. Denn die ohnehin wenigen Fachleute werden künftig stärker in aktuellen Herausforderungen eingebunden sein und keine Zeit mehr für Informationsveranstaltungen haben.

Gab es für Sie ein Trendthema der Digitalisierung, das aus Security-Perspektive für ordentlich Stress gesorgt hat?

Im Maschinen- und Anlagenbau geht es nach wie vor um IIoT und Edge, mit dem Ziel, den „goldenen" Datenschatz zu heben und zu verwerten. Und da wird einfach eingebaut, was die Funktion erfüllt, meist ohne Sicht auf die Security.

Für Stress hat das vermutlich im Moment noch nicht gesorgt, aber es wird noch dafür sorgen, davon bin ich überzeugt. Ich sehe das als eine der wichtigsten Herausforderungen in unserem Umfeld, denn die Netzwerke aus dem sogenannten Brownfield oder dem Maschinenbestand wurden nicht im Hinblick auf Security konstruiert. Wenn hier Komponenten für die Kommunikation installiert werden, die außerhalb der Maschinen stattfindet, dann muss dafür die Security ganz klar betrachtet und berücksichtigt werden.

»Wichtig ist, dass wir alle dieselbe Sprache sprechen und Verständnis für die unterschiedlichen Welten der IT und OT aufbringen.«

Siegfried Müller

VP Advanced Technologies

MB connect line GmbH

Was ist Ihr persönlicher Wunsch im Kontext Security für 2023?

Eine Basis-Regulierung der Cybersicherheit für Hersteller, Integratoren und Betreiber gleichermaßen. Ich könnte mir beispielsweise vorstellen, dass man mit entsprechend absolvierten Trainings zu den Security Basics schon eine Basis schaffen könnte.

Wichtig ist, dass wir alle dieselbe Sprache sprechen und Verständnis für die unterschiedlichen Welten der IT und OT aufbringen. Wir sollten unsere wenigen Fach-Ressourcen nicht damit verschwenden, irgendwelche Fragenkataloge zu beantworten, nur um herauszufinden, wieviel Security der „andere“ im Unternehmen lebt oder berücksichtigt.

Simeon Mussler - Jannis Stemmann - Philipp Pelkmann
Bosch CyberCompare

Was war für Sie bemerkenswert in Ihrem Security-Jahr 2022?

Der Versuch, das Jahr 2022 aus Security-Perspektive einzuordnen, ist in vielerlei Hinsicht komplex. Die Sicherheitslage schien sich durch die aktuellen globalen Krisen wesentlich zu verschlimmern und es wurden viele Warnungen ausgesprochen. Die große Welle hat sich, zumindest zu dem Zeitpunkt, als diese Zeilen geschrieben wurden, nicht eingestellt. Eine Einschätzung bleibt schwierig.

Positiv ist zu verzeichnen, dass viele Unternehmen wichtige Schritte hin zu mehr Security gemacht haben, und zwar sowohl in organisatorischer als auch in technischer Hinsicht. Die Einsicht nimmt zu, dass man sich auf IT-Störfälle vorbereiten und jetzt gezielte Aktionen für angemessene Reaktionen starten muss. Diese Erkenntnis haben wir in vielen Gesprächen gesehen, die wir über das Jahr hinweg mit unseren Kunden geführt haben.

Allerdings hat die wirtschaftliche Entwicklung zu einer absinkenden Marktlage in Q3 und Q4 geführt und die Budgets der Anwender entsprechend beschränkt. Auch auf Anbieterseite wird die angespannte Situation vermutlich Spuren hinterlassen, weil weniger in neue Technologien investiert wird.

Wenn man die Sicherheitslage betrachtet, gab es im Jahr 2022 aus unserer Sicht weniger Bemerkenswertes als befürchtet. Im Kontext von Security war es aber auch weniger als erhofft.

Bei welchem Thema haben Sie mehr Entwicklung erwartet, als tatsächlich eingetreten ist?

In den Enterprise IT-Bereichen standen in diesem Jahr vor allem die Themen der Endpunkt-Security im Fokus – nach den starken Investitionen im Markt in den letzten Jahren (Stichwort EDR, XDR, MDR, und weitere) hat das noch nicht alle Kunden überzeugt. Wir sehen die EDR-Lösung als Erweiterung im EPP-Bereich noch am ehesten im Kundenfokus.

Bei KRITIS-Unternehmen gab es zudem durch die BSI-Orientierungshilfe für Angriffserkennung viel Bewegung. Aus der Bewegung ist teilweise auch leichte Hektik geworden, was Organisationen fordert und dem Ziel – der Reduzierung von Angriffsrisiken – nur bedingt zuträglich ist. Wir waren im ersten Halbjahr überrascht, wie ruhig es hier war und im zweiten Halbjahr nach der Veröffentlichung umso überraschter, dass doch einige nun erst gestartet sind. Das wird nun herausfordernd bis Mai, aber wir unterstützen unsere Kunden dabei nach Kräften.

Wo sich noch viel zu wenig getan hat, ist die OT-Security in Unternehmen, die nicht KRITIS sind. Diese gehen weiterhin noch relativ unbedarft mit dem Thema um. Einige Unternehmen machen erst jetzt langsam kleine Schritte.

»Wir müssen in der Community gemeinsam an den vielen Rädchen der Security drehen, um insgesamt eine bessere Absicherung von Industrieumgebungen zu erreichen.«

Simeon Mussler
Chief Operating Officer / Director

Gab es für Sie ein Trendthema der Digitalisierung, das aus Security-Perspektive für ordentlich Stress gesorgt hat?

Die Cloud ist für viele Unternehmen derzeit ein übergreifendes Thema, weil sie als Enabler für zahlreiche Use Cases in der Digitalisierung gilt. Bei der Umsetzung von Cloud-Lösungen werden jedoch wichtige Aspekte wie sichere Zugänge und eine saubere Konfiguration nach wie vor unterschätzt.

Die Suche nach geeigneten Wegen, um die OT-Bereiche sicher anzubinden, wird uns in den kommenden Jahren noch reichlich beschäftigen.

Jannis Stemmann
Chief Executive Officer

Was ist Ihr persönlicher Wunsch im Kontext Security für 2023?

Wir müssen in der Community gemeinsam an den vielen Rädchen der Security drehen, um insgesamt eine bessere Absicherung von Industrieumgebungen zu erreichen. Wir wünschen uns, dass sich weiterhin jeder einbringt, der einen konstruktiven Beitrag leisten kann. Wenn jeder sein Süppchen selber kocht und alleine löffelt, dann sind die Aussichten auf Erfolg nämlich sehr begrenzt!

Philipp Pelkmann
Chief Technology Officer

Bosch CyberCompare

Sichere Industrie

Frank Polky
Mars Global Services

Was war für Sie bemerkenswert in Ihrem Security-Jahr 2022?

Visibility – Durch die konsequente Nutzung und Integration von Tools wurde eine wertvolle Datenbasis für die OT-Security geschaffen, aber auch für weitere Schritte im Bereich OT Operations.

Daten sind das neue Gold, heißt es so schön, aber sie sind auch der Grundstein für die Integration der Digitalen Fabrik. Ohne einen klaren Blick auf den aktuellen Status in der OT sind weitere Integrationen der Digitalen Fabrik vergleichbar mit Sandburgen am Strand.

Durch die neu gewonnene „visibility“ rückt aber auch klar der Mensch wieder in den Mittelpunkt. Die besten Tools nützen wenig, wenn der Benutzer sie nicht nutzt oder umgeht. Hier zeigt sich ein klares Problem der IT auf, die jahrelang die neue Bequemlichkeit propagiert hat. Die Praktiken hatten sich auch im OT-Umfeld über die Jahre eingeschlichen und so wurden aus praktischen Hintergründen Tools der OT und der IT vermischt. OT-Security wird nun aber als Hürde gesehen, da aus Security-Sicht wieder eine Trennung erfolgen muss.

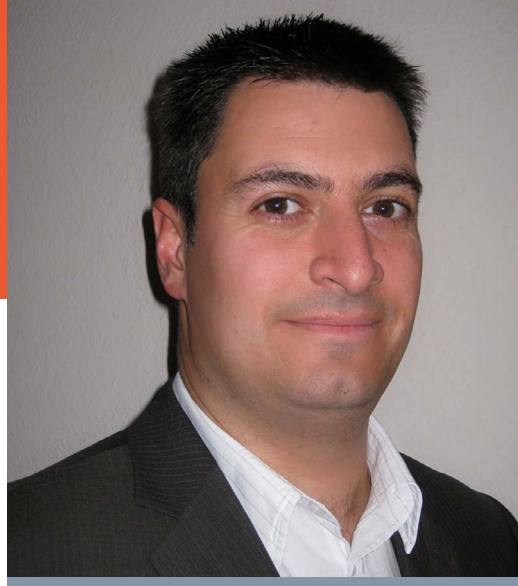
Ein weiterer bemerkenswerter Punkt ist die Tatsache, dass OT mehr und mehr zum Ziel wird. Wir sehen einen Anstieg an Schwachstellen, die aufgedeckt werden und zeitgleich eine Professionalisierung der Angriffstools. Toolkits wie Chernovite zeigen, dass ein Markt vorhanden ist für diese spezifische Art von Tools, die es auch ohne detaillierte Kenntnisse möglich machen, Schaden im OT-Umfeld anzurichten. Bedurfte es vor einigen Jahren noch Expertenwissens im Bereich OPC oder ModbusTCP, um nur zwei Beispiele zu nennen, lässt sich dies nun per „Rundumsorglos-Tool“ erledigen.

Bei welchem Thema haben Sie mehr Entwicklung erwartet, als tatsächlich eingetreten ist?

Bessere Integration der Tools. Es gibt im Bereich der OT Security einen bunten Blumenstrauß an Tools. Viele klassische OT-Hersteller und IT-Player verfolgen eine muntere Einkaufsstrategie. Der Schlüssel zum Erfolg, die Integration dieser Produkte, bleibt dabei leider oft auf der Strecke. Ein bunter Blumenstrauß an Tools ist sicher eine hervorragende Sache, macht die Suche nach relevanten Informationen aber zur bekannten Nadel im Heuhaufen.

Bemerkenswert ist weiterhin die limitierte Verfügbarkeit von Fachkräften und speziell jungen Talenten im Bereich OT-Security. Die Experten sind überschaubar und die Akteure sind im OT-Bereich mehr und mehr vernetzt. Nachwuchsarbeit in diesem Bereich scheint immer noch eine Nische zu sein und wenige Universitäten und Hochschulen spezialisieren sich auf den Bereich OT-Security.

»Daten sind das neue Gold, heißt es so schön, aber sie sind auch der Grundstein für die Integration der Digitalen Fabrik.«



Frank Polky
Director OT Security

Mars Global Services

Gab es für Sie ein Trendthema der Digitalisierung, das aus Security-Perspektive für ordentlich Stress gesorgt hat?

Trendthema Nr. 1 – Cloudintegration. Wie integriere ich moderne Cloud-Technologie in existierende Fabriken und Infrastrukturen? Wie harmonisiere ich Technik und Daten? Wie gestalte ich eine sichere Integration von Technologien, die „unsecure by Design“ sind?

Trendthema Nr. 2 – IOT. Geräte von verschiedensten Playern überschwemmen den Markt. War es vor Jahren noch die MES-Flagge, die über jedem Stand der SPS-Messe wehte, so schwebt dort nun die IOT-Wolke. Hersteller werfen mit Lösungen für Probleme um sich, die bisher noch nicht einmal vorhanden sind.

Bei den zu lösenden Problemstellungen wird zunehmend eine Abhängigkeit von Cloud-Technologien kreiert. Nachdem am Anfang Daten in der Cloud gesammelt und ausgewertet werden sollten, sehen wir uns mehr und mehr der Frage nach dem Eingriff in die Automatisierung gegenübergestellt. Dem entgegen steht das technische Design dieser Lösungen. Basis-Funktionalitäten der Automatisierung wie beispielsweise store and forward stehen zumeist nicht zur Verfügung.

Die technische Umsetzung ist teils kritisch zu sehen, genauso wie auch die zu lösende Problemstellung. Technisch ergeben sich Fragen wie zum Beispiel ob Raspberry PI´s als ein geeignetes IOT-Gateway dienen können. Ist ein ESP-Chip für 1$ sicher zu konfigurieren und im industriellen Umfeld zu betrieben?

Was ist Ihr persönlicher Wunsch im Kontext Security für 2023?

Es muss uns gelingen, noch mehr Awareness zu erzeugen: Es braucht ein starkes Team, das in Zusammenarbeit mit den lokalen Fabriken ein Security-Verständnis schafft. Mitarbeiter in der Fabrik sind unsere „First line of defence“. Hier gilt es die Mitarbeiter zu sensibilisieren. Kampagnen, die im Büro durchgeführt werden, müssen für die speziellen Anforderungen der Fabrik-Mitarbeiter angepasst werden.

Dipl. Phys. Jens Wiesner
Bundesamt für Sicherheit in der Informationstechnik

Was war für Sie bemerkenswert in Ihrem Security-Jahr 2022?

Der Konflikt in der Ukraine hat sehr viel Unruhe, aber bisher wenig gezielte Vorfälle in Deutschland mit sich gebracht. Es gibt einen starken Anstieg an Hacktivismus, der dazu führt, dass direkt mit dem Internet verbundene Systeme angegriffen und ihre Konfiguration manipuliert wird, was zu längeren Produktionsausfällen führen kann.

Weiterhin gibt es einen starken Drang von Produktionssystemen in die Cloud, wobei die Grenzen zu IoT verschwimmen. Einer internationalen Umfrage zufolge sollen schon ca. 25% der Systeme in der Cloud sein, wobei nicht eindeutig definiert wurde, was das für Systeme sind und wie die Cloudnutzung konkret aussieht.

Bei welchem Thema haben Sie mehr Entwicklung erwartet, als tatsächlich eingetreten ist?

Um das Thema Industrie 4.0 scheint es etwas stiller geworden zu sein, wobei die Entwicklung von Produkten Zeit dauert und das Thema intelligente Produktion zu einer Selbstverständlichkeit geworden ist.

Ransomware in der Produktion oder in der Gebäudetechnik ist glücklicherweise bisher eher zufällig. Gezielte Angriffe sind hier noch nicht signifikant feststellbar. Das kann sich allerdings in Zukunft ändern, da sich die verwendeten OT-Systeme immer mehr klassischen IT-Systemen annähern und Angreifer sich nicht mehr so stark umstellen müssen.

Gab es für Sie ein Trendthema der Digitalisierung, das aus Security-Perspektive für ordentlich Stress gesorgt hat?

Supply-Chain-Sicherheit wird Teil Europäischer Gesetzgebung. Die genaue Ausgestaltung steht noch aus und das BSI arbeitet intensiv daran, dass neben der Software Bill of Materials (SBOM) auch das Common Security Advisory Framework (CSAF) akzeptiert wird. Während die SBOM für Hersteller verpflichtend wird, wird CSAF insbesondere für Betreiber, Wartungspersonal und Integratoren große Verbesserungen bringen. Der CSAF-Standard ist jetzt final veröffentlicht, jetzt brauchen wir mehr Hersteller, die Advisories in CSAF anbieten, und Asset-Management-Systeme, die CSAF verarbeiten können.

»Supply-Chain-Sicherheit wird Teil Europäischer Gesetzgebung.«

Was ist Ihr persönlicher Wunsch im Kontext Security für 2023?

Dass der Krieg gegen die Ukraine nicht weiter eskaliert und es zu keinem signifikanten Vorfall in KRITIS kommt.

Und dass der Erfolg von CSAF zu einer weltweiten Nutzung führt. Konsequentes Patch- und Updatemanagement reduziert zwar nur eines von vielen Problemen in der Industrie, aber dieses wird mit Hilfe von CSAF für Betreiber vergleichsweise einfach beherrschbar. Voraussetzung für eine Bereitstellung durch Hersteller ist, dass Betreiber in Ausschreibungen und Gesprächen Informationen über Patches und Updates gemäß dem CSAF Standard einfordern.

Dipl. Phys.
Jens Wiesner
Referatsleiter TK15
Industrielle Steuerungs- und Automatisierungssysteme

Bundesamt für Sicherheit in der Informationstechnik

Markus Woehl
VIDEC Data Engineering GmbH

Was war für Sie bemerkenswert in Ihrem Security-Jahr 2022?

Wir betrachten die aktuelle Entwicklung der IT- und OT-Security-Bemühungen in den KRITIS Brachen mit einem lachenden und einem weinenden Auge. Grundsätzlich freuen wir uns, dass das Thema in den Köpfen der Entscheider angekommen ist. Wir bedauern jedoch, dass die meisten erst durch Vorfälle im eigenen Unternehmen oder durch Angriffe in der unmittelbaren Nachbarschaft zum Handeln bewegt wurden oder als Reaktion auf den gestiegenen Druck durch die gesetzlichen Vorschriften.

Viele Vorfälle in den vergangenen Jahren hätten nicht passieren müssen, wenn die Betreiber vorher reagiert und bereits vor Jahren eine Anomalieerkennung etabliert hätten.

Bei welchem Thema haben Sie mehr Entwicklung erwartet, als tatsächlich eingetreten ist?

Der Einsatz von KI-Funktionen in der Angriffserkennung könnte durchaus weiter sein, jedoch zeigt sich immer mehr, dass die herkömmlichen Verfahren der Angriffserkennung den Anwendern heute schon gute Dienste leisten. Die Transparenz in den Netzwerken wird durch den Einsatz dieser Werkzeuge erheblich gesteigert und der Aufwand wird dabei extrem minimiert.

KI-Funktionen, so wichtig sie aufgrund der Terminologie erscheinen, sind wertlos, wenn der Betreiber nicht mit einfachen Mitteln an die Bereiche herangeführt wird. Für uns ist daher ein reger Austausch mit den Betreibern wichtig, damit sich durch die Umsetzung ein echter Mehrwert ergibt.

Gab es für Sie ein Trendthema der Digitalisierung, das aus Security-Perspektive für ordentlich Stress gesorgt hat?

Digitalisierung und dezentrale Netzwerkinfrastrukturen der Kritischen Infrastrukturen sind seit Beginn des Jahrtausends ein Trendthema für uns. Das Fortschreiten des IIoT und die zum Teil haarsträubende Umsetzung in Low-Cost-Netzwerkteilnehmern mit veralteten und nicht patchbaren Betriebssystemständen sowie fest vergebenen Kennwörtern lässt die Sorge um die Versorgungssicherheit nicht gerade kleiner werden.

Security by Design und ein sicherer Entwicklungsprozess sind überfällige Ansätze, um die zunehmende Vernetzung und das IIoT sicher zu gestalten, dabei sind alle Beteiligten der Lieferkette in der Pflicht.

»Angriffserkennung, Risikomanagement und Netzwerküberwachung müssen als Sicherheitsstandard für alle industriellen Netzwerke festgelegt werden, wenn wir ernsthaft die Umsetzung der Digitalisierung vorantreiben wollen.«

Markus Woehl
Geschäftsführer

VIDEC Data Engineering GmbH

Was ist Ihr persönlicher Wunsch im Kontext Security für 2023?

Angriffserkennung, Risikomanagement und Netzwerküberwachung müssen als Sicherheitsstandard für alle industriellen Netzwerke festgelegt werden, wenn wir ernsthaft die Umsetzung der Digitalisierung vorantreiben wollen. Sie bilden die Grundlage für zukünftige Themen wie zum Beispiel KI, Risikobetrachtungen und transparente sichere Prozesse (ISO 27001 und IEC 62443).

Die eingesetzten Intrusion-Detection-Systeme sind aber nicht nur Kostenfaktor und Absicherung. Sie bieten auch einen erheblichen Mehrwert, der in der Transparenz und dem sicheren Betrieb der Netzwerke verankert ist. Allein die gestiegene Kenntnis der Vorgänge in den Netzwerken kann auch im Fehlerfall sicher und effizient helfen. Und wenn das System dann noch eine eindeutige Beziehungsübersicht der Netzwerkteilnehmer mit den verwendeten Adressen und Ports mit ausgibt, was auch eine hervorragende Grundlage für eine Firewall Konfiguration darstellt, dann ist schon sehr viel erreicht.

Sichere Industrie

Manuel Atug
HiSolutions AG

Ron Brash
aDolus Technology Inc.

Fred Gordy
Michael Baker International

Sebastian Fritsch - Mirco Weber
secuvera GmbH

Andreas Harner
CERT@VDE

Dr.-Ing. Lutz Jänicke
PHOENIX CONTACT GmbH & Co. KG

Klaus Jochem
Klaus Jochem Unternehmensberatung

Isiah Jones, GICSP, CISSP
AIT Applied Integrated Technologies

Hans-Peter Käser
Bundesamt für wirtschaftliche Landesversorgung BWL

Prof. Dr. Dennis-Kenji Kipker
Hochschule Bremen

Mirco Kloss - Daniel Buhmann
FORTINET, Inc.

Peter Lukesch
ondeso GmbH

Prof. Dr.-Ing. Dominik Merli
Hochschule Augsburg - Institut für innovative Sicherheit

Patrick Miller
Ampere Industrial Security

Siegfried Müller
MB connect line GmbH

Simeon Mussler - Jannis Stemmann - Philipp Pelkmann
Bosch CyberCompare

Frank Polky
Mars Global Services

Dipl. Phys. Jens Wiesner
Bundesamt für Sicherheit in der Informationstechnik

Markus Woehl
VIDEC Data Engineering GmbH

Zusammenfassung

Ein bemerkenswertes Security-Jahr 2022

Stockende Lieferketten, ein anhaltender Fachkräftemangel und wachsende Bedrohungen im Cyberraum – es ist gerade nicht einfach. Die Beiträge unserer Experten machen deutlich, wie groß die Herausforderungen beim Thema Security sowohl für Hersteller als auch für die Betreiber aktuell sind und vermutlich weiter bleiben werden.

Die Cyberangriffe, die es über die Medien in ein breites öffentliches Bewusstsein geschafft haben, zeigen die Verwundbarkeit global vernetzter Supply Chains auf und gleichzeitig unsere Abhängigkeit davon. In Unternehmen, die nicht reguliert sind, passiert im Hinblick auf Security bisher immer noch zu wenig. Unsere Experten zeigen sich darüber besorgt, weil Cyberkriminelle zunehmend auch OT-Bereiche direkt ins Visier nehmen und dabei ihre Methoden immer weiter professionalisieren.

Für Kritische Infrastrukturen baut der Gesetzgeber den Schutz mit einer ab dem 1. Mai 2023 verpflichtenden Angriffserkennung weiter aus und auch die Europäische Gesetzgebung bringt neue Security-Richtlinien auf die Zielgerade. Der Handlungsdruck wächst also weiter. Mit Spannung bleibt zu erwarten, ob diese neuen Regularien auch angemessen verfolgt werden können und nicht nur ein zahnloser Tiger bleiben.

Die Themen im Fokus

Innovative datenbasierte Technologien halten mit einer steigenden Anzahl von Anwendungen immer weiter Einzug in Automationsumgebungen. Damit die Trends rund um die Nutzung von Daten auch echte Mehrwerte und einen nachhaltigen Nutzen bringen, müssen Unternehmen konkrete Use Cases definieren und IoT und Cloud-Anwendungen sicher integrieren. Wie unsere Experten betonen, ist Security ein wichtiger Erfolgsfaktor der Digitalisierung. Jedoch sind die meisten technologischen Basics in den IT-/OT-Infrastrukturen nicht vorhanden, so dass das stabile Fundament für erfolgreiche Digitalisierungsprojekte oftmals fehlt.

Ein besonderes und weiter wachsendes Augenmerk liegt aktuell auf dem Thema Produktsicherheit und Schwachstellenmanagement. Für mehr Sicherheit in der Softwarelieferkette soll die Software Bill of Materials (SBOM) sorgen. Sie liefert Transparenz über die Softwarekomponenten in Open-Source-Paketen und über die Schwachstellen.

Ein Meilenstein ist nach den Experten die Verabschiedung des CSAF Standards (Common Security Advisory Framework), in dem Sicherheitsmeldungen in einheitlichen Formaten maschinenlesbar verfügbar gemacht werden können. SBOMs und CSAF helfen Betreibern dabei, die wachsende Zahl an Schwachstellen in der Automationstechnik schnell zu erkennen, zu bewerten und Ihr Patchmanagement an der Kritikalität für ihre Anlagenverfügbarkeit auszurichten.

Entscheidend wird sein, wie beides über die gesamte Lieferkette bis zum Betreiber zur Verfügung gestellt werden kann. Und außerdem: Nutzen kann dies nur, wer Assets und ihre Patchstände in einem vollständigen OT-Asset-Management aktuell verfügbar hat. Stichwort: Umsetzung von OT-Basics.

Ein anderes Thema auf der Agenda ist die zunehmende Vernetzung der Gebäudeautomation und die Risiken, die sich daraus ergeben. Eine der großen Herausforderungen im Bereich der Smart Building Security ist die Verbindung mit wachsenden Safety-Anforderungen. Dies erfordert, genau wie für andere OT-Bereiche auch, einen ganzheitlichen Ansatz, vor allem aber, bisher vernachlässigte Zielgruppen wie beispielsweise aus dem Facility-Management ins Boot zu holen.

Was wir in 2023 brauchen, um Security voranzubringen

Wenig überraschend sind die altbekannten Themen, die auf der Wunschagenda für das nächstes Jahr sind:

Im Management muss sich weiter das Bewusstsein etablieren, dass Security ein kontinuierlicher Prozess ist und fortwährend angepasst werden muss. Dazu gehört auch, sich vermehrt auf die wichtigen Basics zu konzentrieren, statt auf bunte Folien, und schneller in die eigentliche Umsetzung zu kommen. In den meisten Fällen sind diese Basics für einen Großteil des erforderlichen Sicherheitsniveaus verantwortlich.

Ein weiterer wichtiger Hebel liegt bei den Betreibern: Wenn Security in Ausschreibungen und in Einkaufsprozessen zu den üblichen Kriterien zählt, müssen Hersteller sie als zentrale Anforderung betrachten und bei der Produktentwicklung entsprechend berücksichtigen.

Die Experten sehen in einem baldigen Inkrafttreten der NIS 2 Richtlinie und der Verabschiedung des EU Cyber Resilience Act einen wichtigen Schritt, um das Security-Niveau an die aktuelle Bedrohungslage anzupassen. Unternehmen müssen bereit sein, mit der Umsetzung zeitnah starten zu können.

Was unsere Experten sich außerdem wünschen, sind starke Initiativen, um dem Fachkräftemangel entgegenzuwirken. Es braucht dringend mehr Nachwuchskräfte, die über Expertise sowohl für IT-Security als auch für die Anforderungen in Automationsumgebungen verfügen. Derweil ist die Community gefragt, damit Verständnis für die Anforderungen in IT und OT aufgebaut wird und an der gemeinsamen Zielsetzung mit vereinten Kräften gearbeitet wird.

Für mich persönlich ist entscheidend, dass wir noch mehr in die Umsetzung kommen, anstatt nur mit der immer gleich aussehenden bunten Risikomatrix zu agieren. Wir brauchen Menschen, die aktiv im Feld technische Projekte umsetzen und in den Betrieb überführen.

Max Weidele
Gründer
»Sichere Industrie«

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 Interveiws, 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: jahresrueckblick@sichere-industrie.de