eBOOK

www.security-insider.de

SECURITY INSIDER

Ganzheitliche Security für Industrie 4.0

Digitale Transformation in der Industrie

Sicherheitsstrategien für OT und IIoT

Der Weg zur ganzheitlichen IIoT Security

Powered by:

TREND MICRO™

Inhalt

3 Digitale Transformation in der Industrie
Keine Smart Factory ohne Security

8 Sicherheitsstrategien für OT und IIoT
Mehr Schutz für Industrie 4.0

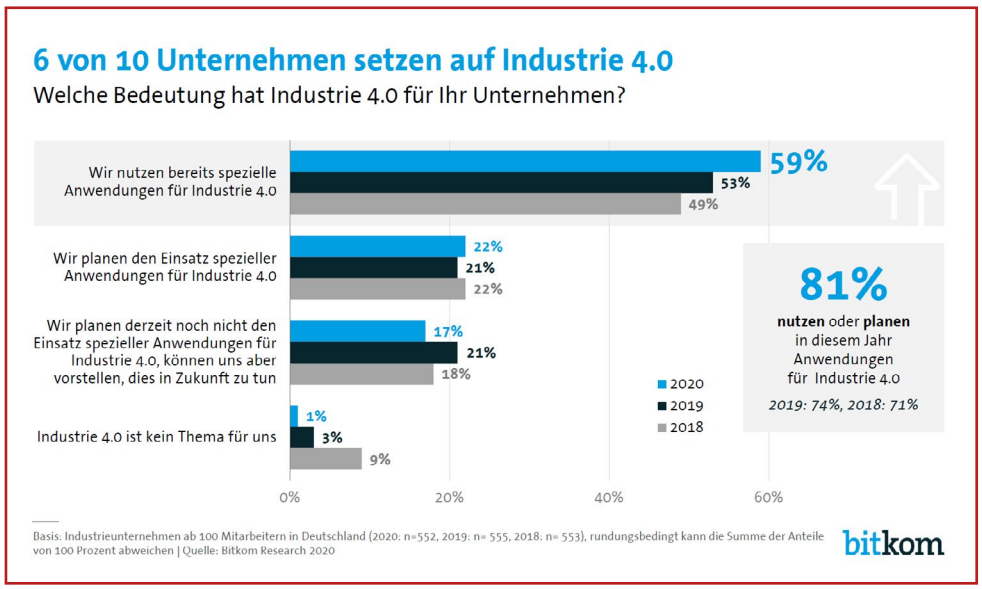
11 Der Weg zur ganzheitlichen IIoT Security
Neue Ansätze für die Industrial Security

14 OT-Security schrittweise umsetzen
Trend Micro TXOne

Vogel IT-Medien GmbH
Max-Josef-Metzger-Str. 21
86157 Augsburg
Telefon +49 (0) 821/2177-0
E-Mail redaktion@security-insider.de
Web www.Security-Insider.de
Geschäftsführer: Werner Nieberle
Chefredakteur: Peter Schmitz, V.i.S.d.P.,
peter.schmitz@vogel-it.de
Erscheinungstermin: Februar 2021
Titel: WrightStudio/stock.adobe.com

Digitale Transformation in der Industrie

In der Industrie 4.0 verzahnt sich die Produktion mit moderner Informations- und Kommunikationstechnik. Dadurch kommen industrielle Anlagen und Systeme aber auch in direkten Kontakt mit Cyberrisiken. Konzepte für Industrie 4.0 müssen deshalb immer auch eine Cybersicherheitsstrategie umfassen. Wie diese aussehen kann, zeigen verschiedene Branchenstandards für die Industrial Cyber Security.



Digitalisierung auf dem Vormarsch: Fast 6 von 10 Industrieunternehmen mit mehr als 100 Mitarbeitern in Deutschland nutzen Anwendungen aus dem Bereich Industrie 4.0. (Bild: Bitkom)

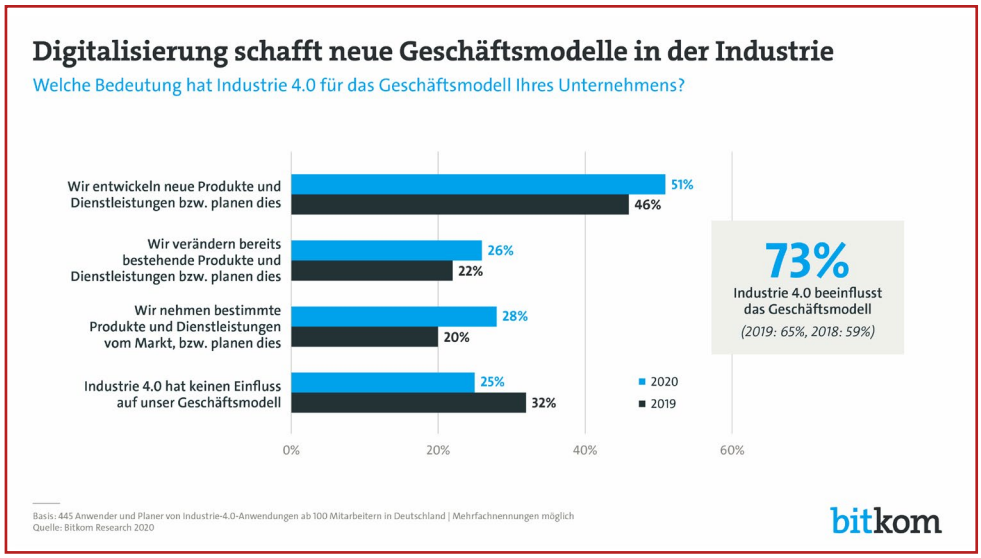
Wandel der Geschäftsmodelle bei Industrieunternehmen

Vernetzte Produktionsanlagen, Echtzeit-Kommunikation zwischen Maschinen, individuelle Unterstützung vom Kollegen Roboter: Die Digitalisierung der Industrieunternehmen in Deutschland macht Fortschritte, so der Digitalverband Bitkom. Fast 6 von 10 Industrieunternehmen mit mehr als 100 Mitarbeitern in Deutschland (59 Prozent) nutzen spezielle Anwendungen aus dem Bereich Industrie 4.0. Vor zwei Jahren waren es erst 49 Prozent.

94 Prozent sehen in der Industrie 4.0 die Voraussetzung für den Erhalt der Wettbewerbsfähigkeit der deutschen Industrie. Mehr als jeder Zweite (55 Prozent) betont, Industrie 4.0 gebe dem eigenen Geschäft generell neuen Schub. Insgesamt sieht eine überwältigende Mehrheit von 93 Prozent der Industrieunternehmen Industrie 4.0 als Chance.

Bei fast drei Viertel (73 Prozent) der deutschen Industrieunternehmen werden im Zuge von Industrie 4.0 nicht nur einzelne Abläufe oder Prozesse verän-

dert, sondern ganze Geschäftsmodelle – eine deutliche Zunahme gegenüber 2018 (59 Prozent). Etwas mehr als jedes zweite Unternehmen (51 Prozent) entwickelt neue Produkte und Dienstleistungen oder plant dies (2018: 39 Prozent). Jedes Vierte (26 Prozent) verändert bestehende Produkte oder hat dies vor (2018: 18 Prozent).



Die Digitalisierung schafft neue Geschäftsmodelle in der Industrie, aber auch neue Risiken, insbesondere Cyberrisiken. Industrie 4.0 benötigt deshalb Industrial Cyber Security als Basis. (Bild: Bitkom)

Security als Herausforderung der Digitalisierung in der Industrie

Industrie 4.0 funktioniert aber nur mit Sicherheit, betont der Digitalverband Bitkom. Denn die Vernetzung von Produktionsmaschinen und Prozessen birgt auch neue Risiken. Während nach einer Bitkom-Studie etwa jedes zweite Unternehmen in Deutschland Opfer von Datendiebstahl, Sabotage und Spionage wurde, ist die Zahl für die Industrieunternehmen höher.

Auch das BSI (Bundesamt für Sicherheit in der Informationstechnik) berichtete im Jahr 2020 von Cyberattacken, die die deutsche Industrie betreffen. Nicht nur große Industrieanlagen können gefährdet sein. Auch kleine und mittelständische Unternehmen, die sich durch Alleinstellungsmerkmale wie zum Beispiel die Produktion spezieller Komponenten im Maschinenbau auszeichnen, wurden Opfer von Cyber-Angriffen, so das BSI.

Um die Vorteile von Industrie 4.0 nachhaltig nutzen zu können, müssen Industrieunternehmen deshalb eine Sicherheitskultur in der Digitalisierung etablieren. Die Handlungsempfehlungen nach Auffassung des Bitkom für die Umsetzung von Sicherheit in Industrie 4.0 müssen deshalb sein:

- Security by Design bei allen Schnittstellen und vernetzten Geräten: Es muss sichergestellt sein, dass die richtigen Geräte miteinander sinnvoll sprechen.
- Individuelle SIEM-Lösungen (Security Information and Event Management): Intelligente Software muss die ausgetauschten Informationen der vernetzten Geräte überwachen und Anomalien in der Kommunikation erkennen.
- Ein präventives und permanentes Risikomanagement muss die Gefahren und Auswirkungen konkret benennen, um die Schwachstellen zu kennen und Lücken zu schließen, bevor sie ausgenutzt werden.

- Internationale Sicherheitsstandards bei der Vernetzung von Geräten müssen formuliert und umgesetzt werden.

Schwachstellen bei Industrie 4.0 gibt es reichlich

Sicherheitslücken zum Beispiel in den Steuerungssystemen industrieller Anlagen gab es schon vor Industrie 4.0, doch durch die Vernetzung der Maschinen und Systeme und insbesondere die Verbindung mit Online-Diensten sind diese Schwachstellen auch über das Internet und für Cyberattacken zugänglich. Zusätzlich sind durch die digitalen Systeme auch neue Sicherheitslücken in die industriellen Anlagen eingezogen.
Die Top 10 Bedrohungen für Industrial Control Systems (ICS), die von der Allianz für Cybersicherheit veröffentlicht werden, geben einen Überblick darüber, wie vielfältig die Angriffsmöglichkeiten sind:

- Einschleusen von Schadsoftware über Wechseldatenträger und externe Hardware
- Infektion mit Schadsoftware über Internet und Intranet
- Menschliches Fehlverhalten und Sabotage
- Kompromittierung von Extranet und Cloud-Komponenten
- Social Engineering und Phishing
- (D)DoS-Angriffe
- Internet-verbundene Steuerungskomponenten
- Einbruch über Fernwartungszugänge
- Technisches Fehlverhalten und höhere Gewalt
- Kompromittierung von Smartphones im Produktionsumfeld

Als Folgeschäden nennt das BSI insbesondere:

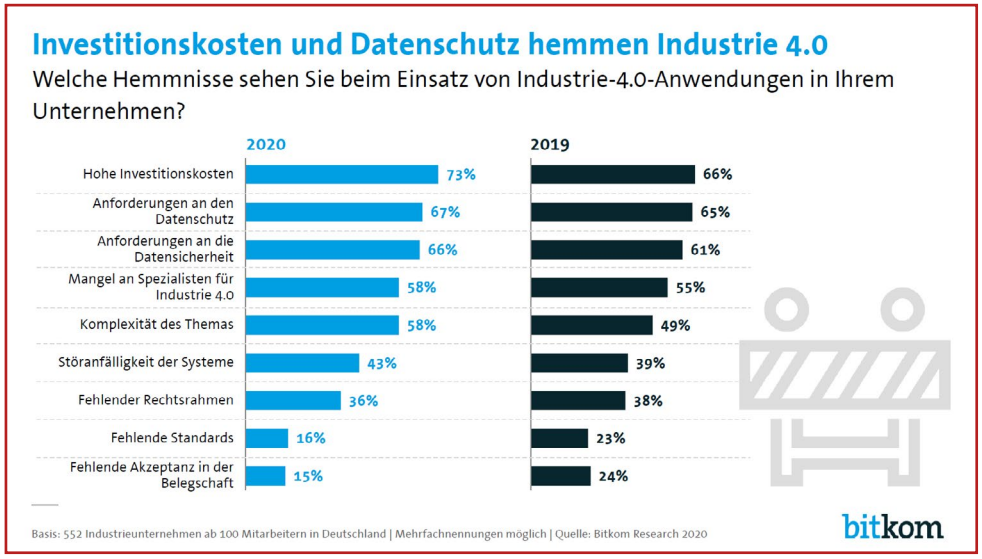
- Verlust der Verfügbarkeit des ICS / Produktionseinbußen
- Datenabfluss / Verlust von Know-how (Intellectual Property)
- Herbeiführen von physischen Schäden an Anlagen
- Auslösen von Safety-Prozeduren oder Beeinträchtigung von Safety-Systemen
- Minderung der Qualität der Erzeugnisse

Cyber Security in der Industrie: Internationale Ansätze sind erforderlich

„Um in den datengetriebenen industriellen Wertschöpfungsnetzwerken der Zukunft erfolgreich zu sein und das notwendige Vertrauen bei den Akteuren zu schaffen, brauchen wir Transparenz und ein gemeinsames Verständnis von den Herausforderungen für die IT-Sicherheit“, so das Bundesministerium für Wirtschaft und Energie. „Entscheidend ist dabei, Sicherheitsanforderungen und -konzepte in globalen Industrie-4.0-Wertschöpfungsketten zu standardisieren und staatliche Regulierungen zu synchronisieren.“
Die Industrieanlagensicherheit sollte in der Unternehmensstrategie verankert sein, so auch KPMG. Hier besteht noch großer Nachholbedarf. Eine Kurzstudie von KPMG zeigt, dass 60 Prozent der befragten Unternehmen nicht über ein ganzheitliches Security-Konzept für Operational Technology (OT) verfügen.

Standards, Normen und Empfehlungen zur Industrial Cyber Security

Tatsächlich gibt es bereits eine Reihe von Standards, Normen und Empfehlungen zur Industrial Cyber Security. An Vorgaben mangelt es somit nicht, wohl aber an der Kenntnis dieser Vorgaben und an der Umsetzung. Deshalb soll an dieser Stelle ein Überblick über wichtige Standards, Normen und Empfehlungen zu Industrial Cyber Security gegeben werden.



Neben den Investitionskosten sind es Datenschutz und Datensicherheit, die als große Herausforderung bei Industrie 4.0 gesehen werden. Wer die Vorteile der digitalisierten Industrie nutzen möchte, kommt an Security nicht vorbei. (Bild: Bitkom)

Wenn Industrieunternehmen an ihren Konzepten für Industrie 4.0 arbeiten, müssen sie nicht von Beginn an neu eine eigene Cybersicherheitsstrategie entwickeln, wohl aber die verfügbaren Normen, Richtlinien und Standards auf das eigene Vorhaben anwenden:

IEC62443/ISA99

Die internationale Normenreihe IEC 62443 behandelt die Cyber Security von „Industrial Automation and Control Systems" (IACS) und richtet sich an Betreiber, Integratoren und Hersteller. Ursprünglich wurden sie als ANSI/ISA-99 oder ISA99-Standards veröffentlicht.

Gegenstand der Normenreihe sind „Industrial Automation and Control Systems" (IACS), also alle Bestandteile, die für den zuverlässigen und sicheren Betrieb einer automatisierten Produktionsanlage erforderlich sind. Dazu gehören sowohl Hardware- als auch Softwarekomponenten, ebenso die organisatorischen Prozesse für die Errichtung und den Betrieb.

Behandelt werden Konzepte wie Defense-in-Depth, die Umsetzung von organisatorischen Maßnahmen wie Patch-Management, technische Aspekte wie Securitylevel und Sicherheitsanforderungen sowie die Produkt- und Komponentensicherheit (wie Sensoren, Schnittstellen, Chips).

ICS Security Kompendium des BSI

Das ICS Security Kompendium des Bundesamtes für Sicherheit in der Informationstechnik (BSI) versteht sich als Grundlagenwerk für die IT-Sicherheit in ICS.

Der erste Teil richtet sich an Betreiber von industriellen Steuerungsanlagen. Dort finden sich auch eine Sammlung von Maßnahmen und eine Vorgehensweise, um die Umsetzung zu prüfen.

Der zweite Teil richtet sich an Hersteller von ICS-Komponenten. Der Teil beschreibt Anforderungen an ICS-Komponenten sowie Rahmenbedingungen, die bei der Entwicklung beachtet werden sollten. Zur Unterstützung einer sicheren Entwicklung wurden Fragestellungen formuliert, um Komponenten testen zu können.

Weitere BSI-Richtlinien mit Bezug zur industriellen Cybersicherheit

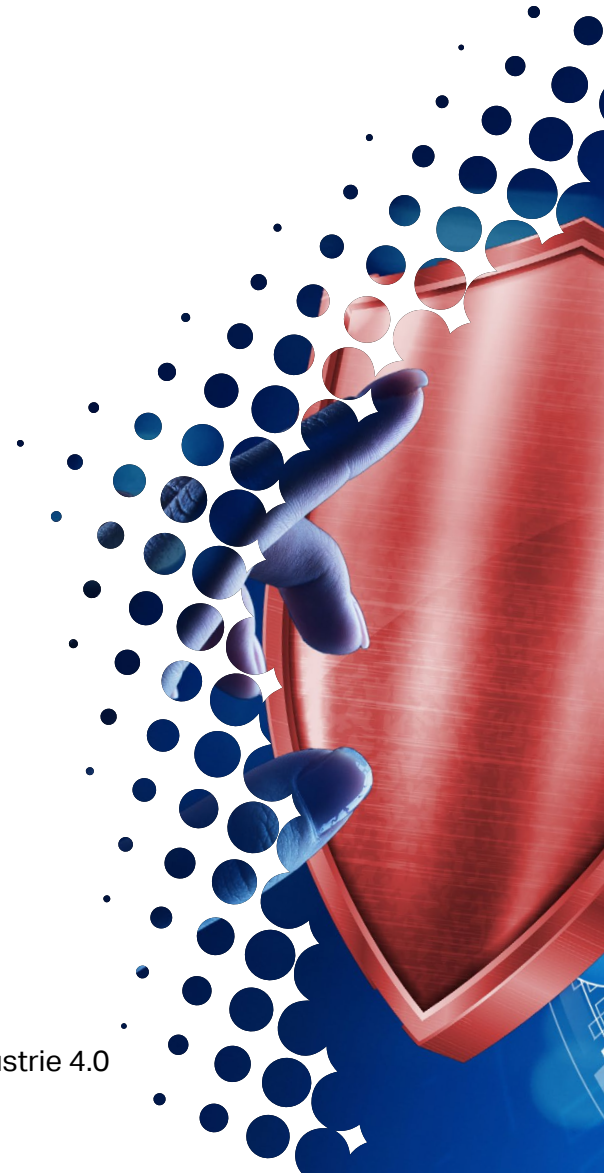
In der Empfehlung „Sicherer Einsatz von ICS-spezifischen Apps" geht es um den Trend, für industrielle Anlagen wie der Fabrikautomation oder Prozesssteuerung zunehmend Apps auf Smartphones und Tablets zur Visualisierung und Parametrierung einzusetzen. Die Empfehlung nennt Maßnahmen, um einen hinreichend sicheren Einsatz von Apps im Kontext von ICS zu ermöglichen.

Zu nennen sind auch die technischen Richtlinien des BSI. Das Ziel der technischen Richtlinien des BSI (BSI-TR) ist die Verbreitung von angemessenen IT-Sicherheitsstandards.

Guidelines von ENISA

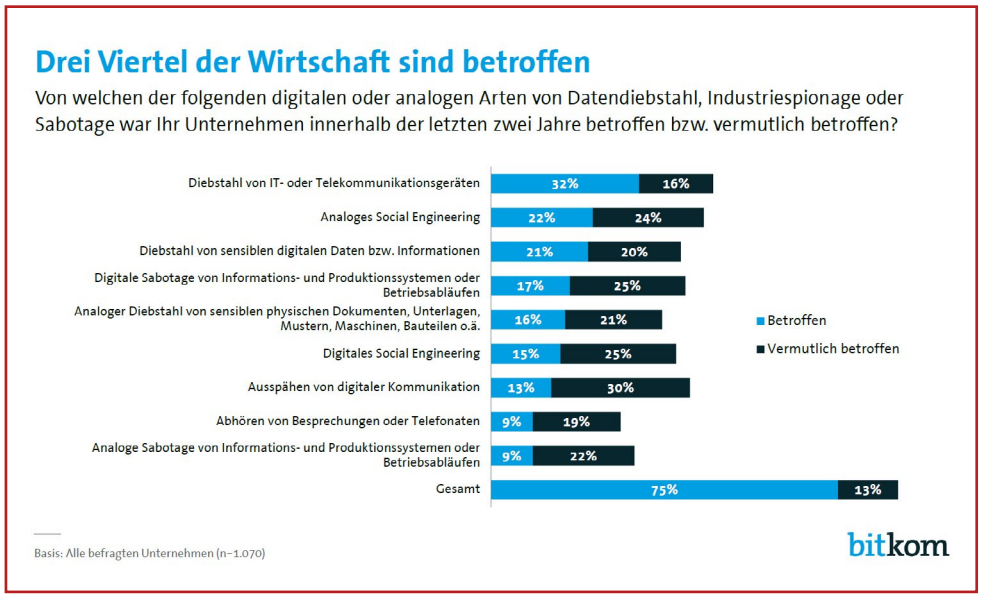
Die EU-Agentur für Cybersicherheit ENISA veröffentlicht ebenfalls Richtlinien, die bei der Etablierung einer sicheren Industrie 4.0 hilfreich sein können, darunter „Good Practices for Security of Internet of Things in the context of Smart Manufacturing".

Oliver Schonschek



Sicherheitsstrategien für OT und IIoT

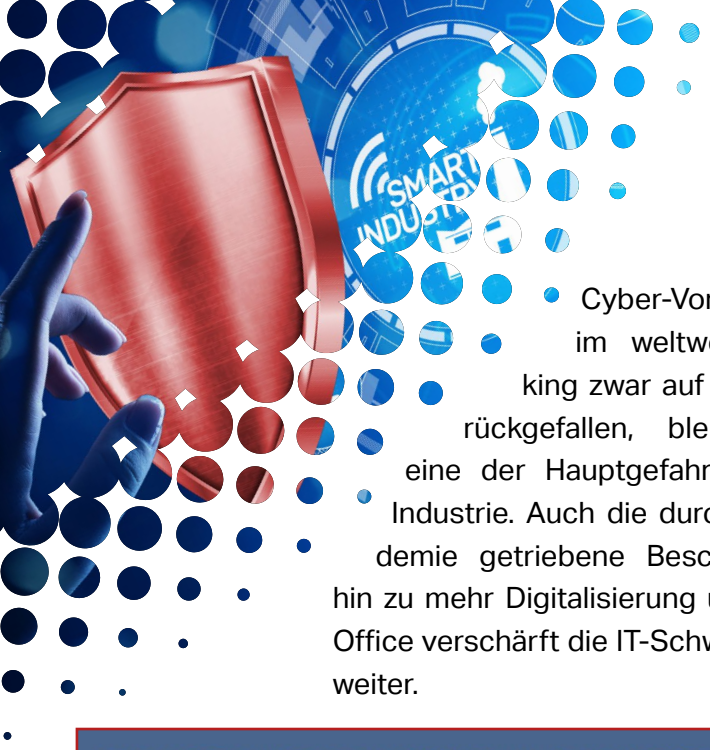
Die Zahl und Vielfalt der erfolgreichen Attacken auf Industrieunternehmen zeigt, dass es noch deutliche Lücken in den industriellen Schutzkonzepten gibt. Es bleibt viel zu tun für die Sicherheit von OT (Operational Technology) und IIoT (Industrial Internet of Things), damit aus einer Smart Factory eine Secure Smart Factory wird. Doch ohne die Maßnahmen der Industrial Cyber Security kann keine Smart Factory bestehen.



Durch Sabotage, Datendiebstahl oder Spionage entsteht der deutschen Wirtschaft jährlich ein Gesamtschaden von 102,9 Milliarden Euro – analoge und digitale Angriffe zusammengenommen. Dabei sind Industrieunternehmen besonders gefährdet. (Bild: Bitkom)

Industrieunternehmen im Fadenkreuz der Online-Kriminellen

Laut Umfrage des Digitalverbands Bitkom entsteht der deutschen Wirtschaft durch Sabotage, Datendiebstahl oder Spionage jährlich ein Schaden von mehr als 100 Milliarden Euro. Drei von vier Unternehmen (75 Prozent) sind in den vergangenen zwei Jahren Opfer geworden, jedes achte Unternehmen (13 Prozent) vermutet dies. Die möglichen, hohen Schäden sind den besonders betroffenen Industrieunternehmen durchaus bewusst. So berichtet der Industrieversicherer Allianz Global Corporate & Specialty (AGCS) in dem Allianz Risk Barometer 2021, dass Betriebsunterbrechung (BU), Pandemie-Ausbruch und Cyber-Vorfälle die drei wichtigsten Geschäftsrisiken für 2021 sind. In Deutschland dominieren BU (Platz 1 mit 50%), Cyber-Vorfälle (48%) und Pandemie-Ausbruch (35%) das Ranking – wobei deutsche Unternehmen das Risiko eines Cyber-Vorfalls (Platz 2) noch größer einschätzen als die Folgen der Pandemie (Platz 3).



Cyber-Vorfälle sind im weltweiten Ranking zwar auf Platz 3 zurückgefallen, bleiben aber eine der Hauptgefahren für die Industrie. Auch die durch die Pandemie getriebene Beschleunigung hin zu mehr Digitalisierung und Home-Office verschärft die IT-Schwachstellen weiter.

Das Allianz Risk Barometer 2021 wird von dem sogenannten „Covid-19-Trio" dominiert. Betriebsunterbrechung, Pandemie und Cyber sind stark miteinander verknüpft und zeigen die wachsende Verwundbarkeit der hochgradig globalisierten und vernetzten Welt auf. (Bild: AGCS)

Covid-19-bezogene Malware- und Ransomware-Vorfälle haben während des Lockdowns stark zugenommen, während Cyberkriminalität mittlerweile die Weltwirtschaft mehr als eine Billion US-Dollar kostet. Die ohnehin schon häufigen Ransomware-Angriffe nehmen weiter zu und nehmen mit hohen Erpressungsforderungen zunehmend Großunternehmen ins Visier, wie der aktuelle AGCS-Bericht zu Cyber-Risikotrends zeigt.

Schäden durch Distributed Denial of Service (DDoS) oder Phishing- und Ransomware-Angriffe machen heute demnach einen Großteil des Schadenvolumens in der Cyberversicherung aus.

Mehr Sicherheit für die Industriebranchen

Für Deutschlands global vernetzte Industrie sind alle Dimensionen von Sicherheit entscheidend – analog wie digital, so der BDI (Bundesverband der Deutschen Industrie). Mit voranschreitender Digitalisierung und der damit einhergehenden stärkeren Vernetzung nimmt die Zahl möglicher Angriffe stetig zu. Neun von zehn Industrieunternehmen waren in den vergangenen zwei Jahren von analogem wie digitalem Datendiebstahl, Industriespionage oder Sabotage betroffen, berichtet der BDI. Etwa die Hälfte aller Industrieunternehmen verzeichnet wöchentlich Angriffe. Hierfür wird meist ein dauerhafter Zugang gesucht, um Daten zu stehlen, zu verändern oder zu zerstören und Produktionsprozesse zu beeinflussen.

Ein Großteil der deutschen Unternehmen ist sich der potenziellen Gefahren im analogen und digitalen Raum bewusst und ergreift organisatorische,

personelle und technische Sicherheitsmaßnahmen. Die Firmen investieren zudem bereits heute in die Sicherheit von Produkten, Prozessen und Personen, so der BDI. Doch es gibt weiterhin Bedarf an Sicherheitsmaßnahmen in der Industrie. So fordert der Bundesverband der Deutschen Industrie:

- Mehr personelle Ressourcen in Behörden für die Sicherheitsüberprüfung
- Eine eindeutige Benennung von Ansprechpartnern in Behörden
- Ein besser auf die Bedürfnisse der deutschen Industrie abgestimmtes „Zweites IT-Sicherheitsgesetz"
- Die Einführung staatlicher Gegenmaßnahmen auf Cyberangriffe (Hackback)
- Eine vertiefte Kooperation von Staat und Wirtschaft

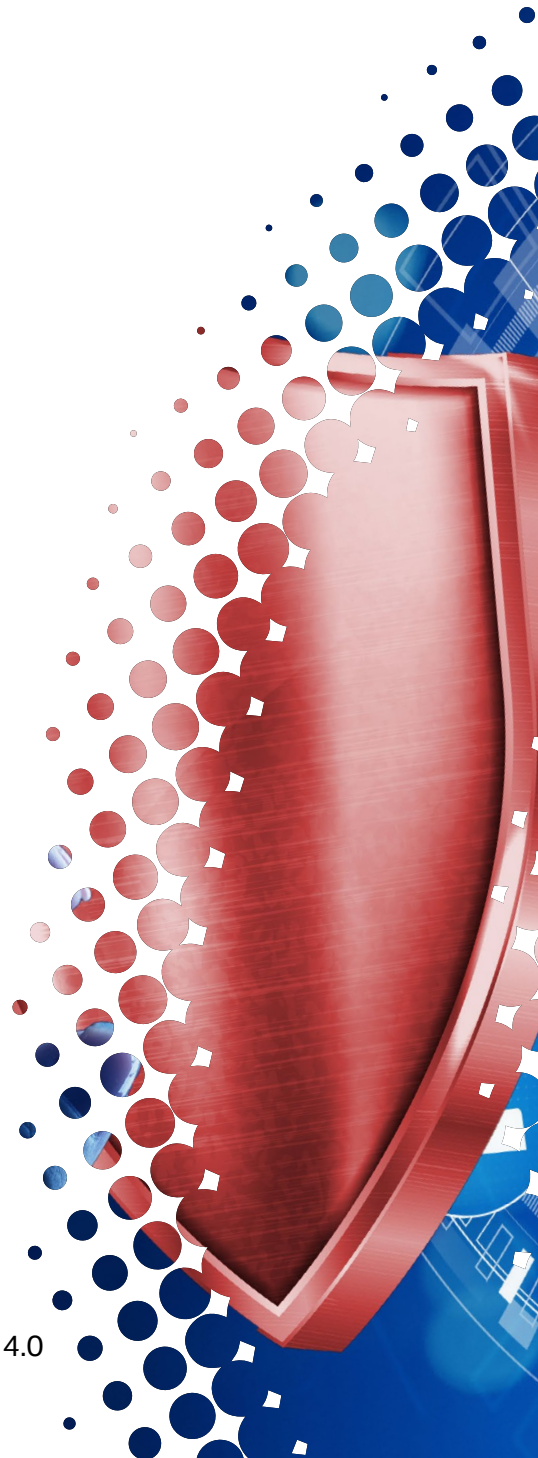
Lücken in der Industrial Cyber Security schließen

Die EU-Agentur für Cybersicherheit ENISA hat aufgezeigt, was zu tun ist, um aus einer Smart Factory eine Secure Smart Factory zu machen, was also in der und für die Industrie 4.0 getan werden sollte, um die Cybersicherheit zu erhöhen, darunter nicht nur technische Schutzmaßnahmen, sondern auch:

- Förderung des funktionsübergreifenden Wissens über IT- und OT-Sicherheit
- Sichere Supply-Chain-Management-Prozesse
- Erstellen von Industrie-4.0-Baselines für die Interoperabilität der Sicherheit
- Klärung der Haftung der Industrie-4.0-Akteure
- Harmonisierung der Bemühungen um Sicherheitsstandards für Industrie 4.0

Doch auch in der technischen Cybersicherheit muss noch einiges geschehen, um das Ziel einer Secure Smart Factory erreichen zu können. Dies wird im nächsten Kapitel näher betrachtet.

Oliver Schonschek



Der Weg zur ganzheitlichen IIoT Security

Die steigenden Cyberrisiken bei Industrie 4.0 zeigen, dass auf allen Ebenen der Sicherheit neue Wege beschritten werden sollten: organisatorisch, regulatorisch und auch technisch. Dazu gehören Konzepte wie ein übergreifendes Security Monitoring im Industrial IoT, die Nutzung von spezifischer Threat Intelligence und der Ansatz, die Security direkt in die Geräte der OT (Operational Technology) zu bringen.

Sicherheit gehört fest zum Leitbild 2030 für Industrie 4.0. (Bild: Plattform Industrie 4.0 / INFOGRAFIK PRO)

Besserer Schutz für Industrieumgebungen

Die IT- und OT-Konvergenz in intelligenten Fabriken hat nicht nur Produktivitätsvorteile gebracht, sondern auch die Cybersicherheitsrisiken durch Malware-Infektionen und unbefugten Zugriff erhöht. Aufgrund der flachen Netzwerkarchitektur und der damit verbundenen Anfälligkeit für Angriffe kann eine ganze Produktion völlig zum Erliegen kommen. Passende Lösungen für die Netzwerksicherheit, inklusive Netzwerksegmentierung, müssen sowohl eine Produktivitätssteigerung ermöglichen als auch effiziente Sicherheit garantieren.

Auf der einen Seite sind IT-Netzwerksicherheitslösungen bei weitem nicht so anpassungsfähig, insbesondere bei der Unterstützung von industriellen Netzwerkprotokollen, wie es die OT erfordert. Auf der anderen Seite haben bestehende industrielle Netzwerksicherheitslösungen oft mit der zentralen Verwaltbarkeit zu kämpfen, wenn Sicherheitsrichtlinien für Hunderte von Anlagen und Netzwerken einzeln verwaltet und ausgerollt werden müssen.

Entsprechend empfiehlt sich die Nutzung von speziellen Lösungen zur erweiterten Netzwerksegmentierung, sodass Angriffe auf Schwachstellen im IT-Bereich nicht auf den OT-Bereich übergreifen können oder umgekehrt.

Kommunikation im Industrial IoT besser absichern

Um die Cyberrisiken in vernetzten industriellen Umgebungen besser erkennen zu können, gilt es zudem, die industriellen Netze spezifisch zu überwachen, also die bei Industrie 4.0 vorherrschenden Kommunikationsprotokolle in das Security Monitoring und in die Netzwerkkontrolle zu übernehmen.

Möglich wird dies mit einer speziellen Industrial Firewall und einem dedizierten Intrusion-Prevention-System (IPS), sowie mit einer Security-Management-Konsole, die auch Transparenz über installierte OT-Geräte ermöglicht und sich nicht nur auf den IT-Bereich beschränkt.

Spezielle Security-Probleme benötigen spezifische Lösungen

Die Industrial Cybersicherheit muss zudem Antworten finden auf weitere, OT-spezifische Probleme, die im IT-Bereich in der Form nicht auftreten, wie das Problem, Maschinen nicht zeitnah mit Patches versorgen zu können, da ihr Betrieb nicht unterbrochen werden darf, oder die oftmals schwache Zugangskontrolle bei industriellen Systemen.

Eine umfassende Cybersicherheitslösung für die Smart Factory sollte deshalb Schutz bieten für industrielle Endpunkte, Netzwerke, Server und Cloud-Workloads. Gleichzeitig sollten XDR-Funktionen (Extended Detection and Response) für Erkennung und automatische Reaktion auch im OT-Netz verfügbar sein. Um dem Mangel an Fachkräften in der Security, der auch Industrieunternehmen betrifft, begegnen zu können, empfehlen sich zudem Security-Dienstleistungen, etwa Services für die Reaktion auf Vorfälle (Incident Response).

Mit einer geeigneten Lösung für Industrial Cyber Security und damit für die Absicherung der Smart Factory lassen sich die Maßnahmen ergreifen, die die diskutierten offenen Flanken in der Sicherheit von Industrie 4.0 schließen können, darunter:

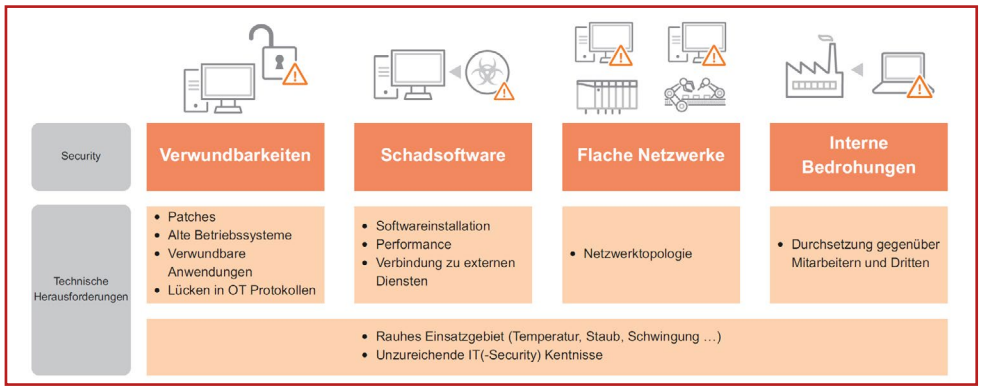
- Perimeterschutz im OT-Bereich zur Verhinderung von Cyberangriffen auf Schwachstellen
- Serversicherheit zum Schutz der Industrie-Server vor einer Malware-Infektion
- Schutz für IIoT-Geräte, etwa industrielle IoT-Gateways, die in Industrieservices verwendet werden
- Frühzeitige Identifikation interner Aktivitäten von Cyberangriffen in der OT-Umgebung

- Überwachung des Netzwerkverkehrs auch aus OT-Perspektive
- Schutz für industrielle Steuergeräte
- Netzwerksegmentierung zur Verhinderung der Ausbreitung einer Infektion zwischen OT und IT
- Schutz für kritische Geräte auf Netzwerkebene
- Verhinderung der Ausführung von Malware und unzulässigen Programmen (Sperrung)
- Scan und Bereinigung von Malware auf OT-Geräten, auf denen keine Sicherheitssoftware installiert werden kann
- Transparenz über Produktionsgeräte und Sicherheitsereignisse auch im OT-Bereich

Secure Smart Factories sind somit möglich, mit einer smarten Industrial Cybersicherheit. *Oliver Schonschek*

OT-Security schrittweise umsetzen

Selbst wenn man sich in der Vergangenheit „darum drücken“ und die Verantwortung an den Integrator oder Betreiber abgeben konnte – inzwischen ist Security Bestandteil vieler Lastenhefte. Und selbst bei Alt-Anlagen mehren sich die entsprechenden Anfragen. Trotzdem ist die übereilte Einführung von technischen Lösungen nicht zielführend. Egal ob nun IEC62443, BSI-ICS-Kompendium, NIST SP800-82 oder sonstige Rahmenwerke: Bei allen ist ein (kontinuierlicher) Risikobewertungsprozess Teil des Konzepts.



IT-Sicherheitsherausforderungen in der Produktion (Bild: Trend Micro)

Es gilt Risiken zu evaluieren und sich dann erst Gedanken um mögliche Gegenmaßnahmen zu machen. Diese *können* technischer Natur sein, *müssen* es aber nicht. Entscheidet man sich für technische Ansätze, hat sich in der Praxis ein Sicherheitskonzept aus den drei Phasen Prävention, Erkennung und Resilienz bewährt.

Herausforderungen bei Security und Implementierung

Im Vergleich zur Office-IT, stellt die Betriebsumgebung bewährte Vorgehensweisen aber auch technologische Lösungen auf den Prüfstand. Von den rauen Umweltbedingungen ganz zu schweigen.

Verwundbarkeiten

Während in der Office-IT das zeitnahe Patchen von Systemen üblich ist, stellt dies in der Produktion aus verschiedenen Gründen (Lebens-/Betriebsdauer, Verfügbarkeit, Support) ein großes Problem dar. Trotz der größeren Angriffsfläche aufgrund unsicherer Protokolle, alter Komponenten und Konfigurationen.

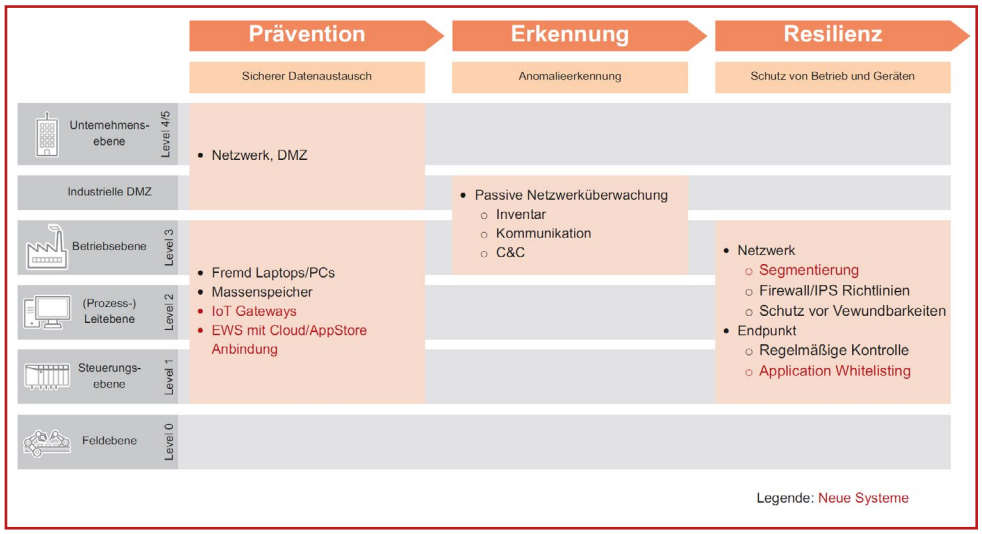
Schadsoftware

Selbst wenn Schutzsoftware installiert werden darf, stellt sich zwangsläufig die Frage nach der Verfügbarkeit und Beeinträchtigung der System-Performance. Normale, aus der Office-IT kommende Software verlangt ein einigermaßen modernes System. Etwas, das auf

ein in die Jahre gekommenes HMI oder einen anderen Steuerungs-PC in vielen Fällen nicht mehr zutrifft.

Flache Netzwerke

In vielen Umgebungen sind flache (Layer 2-) Netzwerke immer noch die Regel. In Kombination mit den immer gleichen IP-Adresskreisen und „Standard-IPs" für bestimmte Geräte war und ist dies leider immer noch üblich. Bei einem Vorfall ist die Größe des „Einschlagkraters" dann aber auch gleich dem gesamten Netzwerk.



Lösungsansätze zur Prävention, Erkennung und Resilienz (Bild: Trend Micro)

Interne Bedrohungen

Eingebrachte (Fremd-) Geräte wie Laptops oder Mobilgeräte (die zum Beispiel am USB-Port des HMIs geladen werden) stellen einen Eintrittspunkt für Schadsoftware dar. Richtlinien und Vorgaben definieren vielleicht, was verboten/eingeschränkt/kontrolliert ist. Dies bedarf dann aber auch der Kontrolle. Und bei der Durchsetzung treten durchaus Nebeneffekte auf, die sich beispielsweise aufgrund des Zeitaufwandes in höheren Wartungskosten niederschlagen.

Verteidigungsstrategien in drei Schritten

Als erster Schritt steht in vielen Fällen das Herstellen von Visibilität. Dies kann unter Umständen sogar als Teil der Risikobewertung gesehen werden und umfasst eine Inventarisierung der verbauten Komponenten, aber auch die Erfassung des Kommunikationsverhaltens. Nach der Risikobetrachtung haben sich in der Praxis bei der Implementierung von technischen Security-Maßnahmen im Produktionsumfeld drei Phasen bewährt: Bei bestehenden Anlagen steht ganz klar Prävention und Erkennung im Vordergrund. Neuere Anlagen können um eingebaute Resilienz erweitert werden.

Prävention

Bei der Prävention geht es primär um den sicheren Datenaustausch. Eintrittstore für Schädlinge müssen (soweit möglich) minimiert werden. Dabei gilt es, verschiedene Herausforderungen in den verschiedenen Ebenen der Produktion zu betrachten:

Netzwerk und DMZ: Normale Firewalls zwischen der Office-IT und der Produktion sind in der Regel blind in Bezug auf OT-spezifische Protokolle. Aber selbst bei Office-IT-Protokollen gibt es Besonderheiten: Während zum Beispiel

SMBv1 im Office-Bereich seit Jahren standardmäßig deaktiviert ist, ist SMBv1 in der Produktion (unter anderem zum Verteilen von Rezepturdateien) durchaus üblich. Wird also einfach nur SMB gefiltert, so ist die Office-IT nicht für Angriffe wie EternalBlue anfällig – in der Produktion schlägt dies aber voll durch. Hier haben sich IPS-Systeme (Intrusion-Prevention-Systeme) bewährt, die auch innerhalb der zulässigen Kommunikation mögliche Angriffe abwehren können. Dies ist insbesondere deshalb wichtig, da in der Produktionsüberwachung und -steuerung oft „normale" Desktop/Server-Systeme im Einsatz sind. Bei diesen Office-IT-nahen Systemen, die in der Regel auch nicht hart echtzeitkritisch sind, lassen sich häufig mit aus der Office-IT üblichen Security-Lösungen mögliche Eintrittspunkte minimieren.

Wartung: Vor der Einbringung fremder Geräte in das Netz oder an Maschinen gilt es, diese zu überprüfen. Theoretisch kann das durch eine „Rettungs-CD" mit Virenscannern geschehen. Aufgrund fehlender Updates, die dank Air Gap auch nicht online gezogen werden können, haben sich in der Praxis andere Lösungen bewährt. Dazu zählen spezielle USB-Sticks, die mit aktuellen Signaturen fremde Systeme ohne Reboot und Installation von Software schnell scannen können.

Erkennung

Da Prävention keinen vollständigen Schutz garantieren kann, bietet sich im zweiten Schritt die Anomalie-Überwachung an. Anomales Verhalten muss nicht zwangsläufig ein Angriff sein. Es kommen auch andere Fehlerquellen in Betracht. Dabei gilt es, die ganze Bandbreite von sehr OT-spezifischen bis zu Office-IT-spezifischen Anomalien abzudecken: Das Auftauchen oder Verschwinden von Geräten, die nicht durch die Inventurliste gedeckt sind, ist beispielsweise auf jeden Fall eine Nachforschung wert. Aber auch Änderungen an Konfigurationen, Projektierungs- oder Rezepturdaten sollten verifiziert werden. Selbst Änderungen im Kommunikationsverhalten (Volumen, Frequenz, Anzahl) können einen Hinweis geben. In der Praxis haben sich Lösungen bewährt, die das OT-Inventar und dessen Kommunikationsverhalten dynamisch erfassen und Abweichungen melden. Aber auch die Suche nach Office-IT-spezifischem Verhalten (C&C-Kommunikation, Brute-Force-Attacken, etc.) ist auf jeden Fall zu empfehlen.

Resilienz

Bei neuen Umgebungen, bei denen man keine Wechselwirkungen durch nachträglich eingebrachte Sicherheit fürchten muss, sind wenig überraschend umfangreichere Maßnahmen denkbar:

Im Netzwerk empfiehlt es sich, die Umgebung soweit wie möglich zu segmentieren. Für kleinere Umgebungen gibt es IPS-Geräte, die bequem im Schaltschrank verbaut werden können und somit ein Gerät, ein Segment oder auch eine Linie schützen können. Mit der Unterstützung von OT-Protokollen, Netzwerktransparenz (Layer 2), Rückfall in einen sicheren Zustand bei Stromausfall

(Fail-Open) und einem robusten Formfaktor unterscheiden sie sich deutlich von Geräten in der Office-IT. In größeren Umgebungen kommen Geräte mit ähnlichem Funktionsumfang, aber höherer Portdichte (2x WAN, 8x LAN) zum Einsatz. Eingebaut im Schaltschrank schützen diese dank ihrer Portanzahl mehr Segmente. Wird der Netzwerkzugang zentral bereitgestellt, empfehlen sich IPS-Array-Lösungen, die zentral aus dem Rack (ähnlich einem Core Switch) OT-Sicherheit für eine große Anzahl von Segmenten (24 Segmente/48 Ports oder 48 Segmente/96 Ports) zentral bereitstellen.

Auf der Endpoint-Seite bieten sich dort, wo man keine „normale" Office-IT-Sicherheitslösung ausbringen kann, Application-Safelisting-Lösungen an. Diese stellen eine gangbare und ressourcenschonende Alternative dar. Anstatt Dateien oder Netzzugriffe jedes Mal in Echtzeit zu untersuchen, wird beim Einrichten definiert, dass bestimmte (bereits installierte) Software zur Ausführung kommen darf. Danach wird das System quasi „abgeschlossen" und jegliche später aufgebrachte Software (eben auch Schadsoftware) schlichtweg an der Ausführung gehindert.

Zusammenfassung

IT-Security ist ein Thema, mit dem die Produktion sich zwangsläufig beschäftigen muss. Das bedeutet aber nicht, die erstbeste technische Lösung planlos auszurollen. Der Risikobewertungsprozess steht an erster Stelle. Daraus ableitend können verschiedene Maßnahmen zum Einsatz kommen, von denen einige technischen Lösungen entsprechen. Denn letztendlich ist die IT-Security nur ein Aspekt der Produktion. Daher empfiehlt es sich, bei der Einführung von Security sehr genau darauf zu achten, was nicht- oder minimal-invasiv eingeführt werden kann (insbesondere bei bestehenden Umgebungen) und wo IT-Security von Anfang an (invasiv) im Design berücksichtigt werden muss.

Trend Micro bietet mit der TXOne-Produktfamilie technische Lösungen an, die speziell für den OT-Security-Bereich entwickelt wurden. Neben transparenten Netzwerklösungen jeder Größe (von kleinen IPS-Lösungen für ein Segment über Firewalls bis hin zu IPS-Arrays mit hoher Portdichte) gehören dazu auch verschiedene Endpunkt-Lösungen, die installationsloses Scannen, Application Safelisting und industrietauglichen Malwareschutz ermöglichen.

Udo Schneider, Trend Micro