

Bestandsaufnahme: Cybersecurity in der Industrie

Mehr Sicherheit trotz zunehmender Unsicherheiten

Cyberattacken auf Industrieanlagen sind kein wirklich neues Phänomen. Bereits 2010 meldete Siemens einen Hackerangriff auf gleich mehrere Industrieanlagen. Ziel waren bestimmte Modelle von Siemens-Steuereinheiten, die etwa in vielen Industrieanlagen, Klimasteuerungen und Pipeline-Kontrollsystemen eingesetzt werden. Dahinter steckte Stuxnet – eine Schadsoftware, die so speziell und komplex konstruiert war, dass Experten sehr bald von einem gezielten Angriff eines Geheimdienstes ausgingen. Es blieb nicht der einzige Vorfall dieser Art.

In dem Bericht „Die Lage der IT-Sicherheit in Deutschland 2014“ des BSI (Bundesamt für Sicherheit in der Informationstechnik) ist ein weiterer bemerkenswerter Fall enthalten. Demnach sind Hacker in das Netzwerk eines Stahlwerks eingedrungen, haben die Steuerung des Hochofens übernommen und die Anlage massiv beschädigt. Die Angreifer haben sich zunächst durch Phishing-E-Mails, die auf Mitarbeiter zugeschnitten waren, Zugriff auf das Office-Netzwerk der Anlage verschafft und sich von dort aus bis in die Produktionsnetze vorgearbeitet. Das BSI hat den Namen des betroffenen Unternehmens nicht genannt. Nicht immer sind bei scheinbar ähnlich strukturierten Attacken die Industrieanlagen selbst das Ziel. Ein auf den ersten Blick ähnlicher Angriff auf Thyssen-Krupp im Jahr 2016 diente – ausweislich der Erkenntnisse des betroffenen Unternehmens – zur Industriespionage und verschonte die Industrieanlagen selbst [1].

Sicherheit vernetzter Anlagen

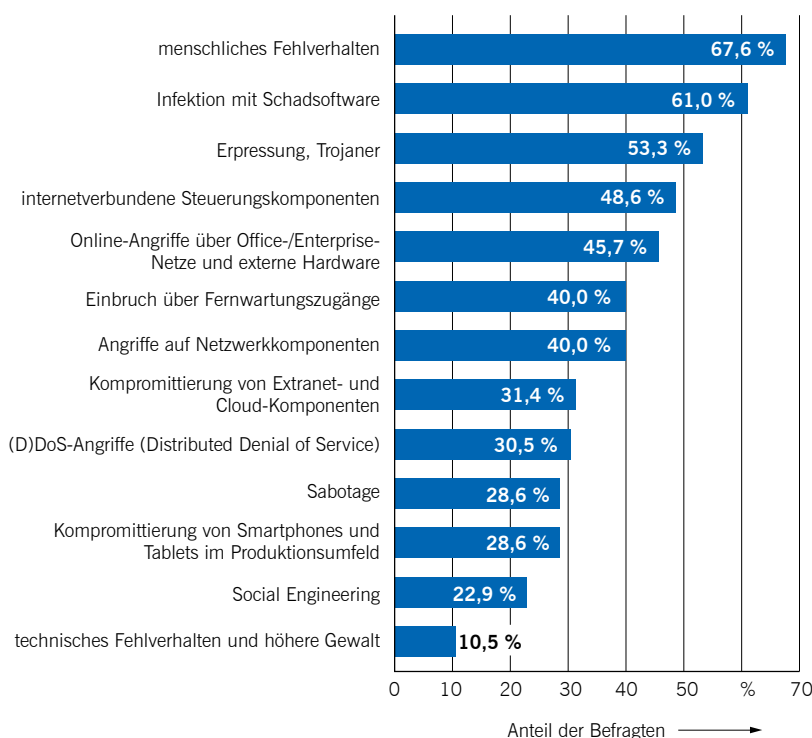
Das eigentliche Problem der Unsicherheit einzelner Steuerungssysteme existiert schon länger, gerät aber erst in letzter Zeit in den Fokus der Betrachtungen. Durch die zuneh-

mende Vernetzung der Anlagen und – wie im Beispiel beschrieben – vor allen Dingen auch durch die Verbindung der bis dato weitgehend getrennten Netze auf Fabrikebene (sogenannte Operational Technology – OT) mit dem, was als IT (Informationstechnologie) des Betriebes bekannt ist. Ein ganz ähnliches Problem gibt es übrigens in Krankenhäusern bei Medizintechnikgeräten, bei denen die

Angreifer ebenfalls immer wieder technische Schwächen, die entdeckt werden, ausnutzen können. Solange die Geräte für sich im „Stand Alone-Betrieb“ arbeiten, ist dies kein Problem. Mit zunehmender Vernetzung entstehen dann jedoch unter Umständen Gefahren für die Anlagen selbst, aber eben auch für die Nutzer und – im Falle von Krankenhäusern – Patienten. Traurige Berühmtheit erreichte etwas 2019 eine Meldung von GE (General Electric) über eine technische Schwachstelle in Betäubungsgeräten, die in der Empfehlung gipfelte, man sollte die Geräte vom Datennetz trennen. Hacker hätten – zumindest theoretisch – die Dosis von verabreichten Betäubungsmitteln unbemerkt verändern können [2].

Auch eher triviale und altbekannte Sicherheitsprobleme wie Ransomware-Attacken können Industrieanlagen und Logistikkontrollsysteme lahmlegen, wenn die Netze zwischen Officebetrieb und Steuerungstechnik bzw. Waren- und Lagerwirtschaft nicht hinreichend getrennt sind. Beispiele von Maersk (2017), Norsk Hydro (2019), Garmin (2020), Palfinger (2021) und tegut (2021) zeigen deutlich die Problematik.

IT-Sicherheit und Industrie 4.0: Wo sehen Sie aktuell die größten Bedrohungen?



Weitere Informationen:

Deutschland, 105 Befragte; VDE-Mitgliedsunternehmen und Hochschulen der Elektro- und Informationstechnik; Online-Umfrage

Umfrage zu den Bedrohungen in der IT-Sicherheit und in der Industrie 4.0 in Deutschland, 2019

Quelle: VDE/Statista 2020

Autor

Thomas R. Köhler ist Experte und Buchautor im Themenfeld Cybersicherheit, Holzkirchen. Er ist Gründer der Technologieberatung CE21. Seit 2019 ist er Research Professor am Institute for International Innovation der Hankou University in Wuhan, China. Veröffentlichungen: u. a. „Chefsache Cybersicherheit“ (Campus Verlag) www.ce21.de

„Altes“ Sicherheitsmodell funktioniert nicht mehr

Wie oben bereits kurz ausgeführt, sind Sicherheitslücken in einzelnen Steuerungssystemen des IIoT (Industrial IoT) kein Problem, solange diese Systeme keine Verbindung nach außen besitzen. Mit einiger Verzögerung wiederholt sich im OT-Bereich nun jedoch eine Entwicklung, die aus dem Bereich der Office-IT bekannt ist: Es geht nicht mehr ohne Verbindungen nach außen. Damit ist alles außerhalb des Produktionsnetzes gemeint, also etwa Übergänge zu IT-Systemen des Unternehmens selbst oder auch Übergänge zu anderen Unternehmen (Abnehmern wie Lieferanten), mit denen man im Bereich von vernetzten Lieferketten zusammenarbeitet (gern auch unter dem Schlagwort „Industrie 4.0“ zusammengefasst) sowie Fernzugänge für einzelne Anlagen, die typischerweise durch Lieferanten zu Wartungszwecken genutzt werden.

All diese Zugangsmodelle sorgen dafür, dass die alte Vorstellung einer Burgmauer, die den Bereich Industrieanlagen abschottet, überdacht werden muss. In Fachkreisen spricht man auch von „Perimeter Security“. Anders gesagt, es kann in vielen Fällen nicht mehr ausgeschlossen werden, dass in komplexen Installationen „alles dicht“ gemacht wird. Damit richtet sich die Aufmerksamkeit notwendigerweise auf die Sicherung von einzelnen Systemen. Diese stehen in der Praxis oft mehr oder weniger ungesichert im Netz. Die Suchmaschine „Shodan“ – eine Suchmaschine für das Internet der Dinge – liefert immer wieder spannende Steuerungs- und Überwachungstechnik zur unbefugten Übernahme frei Haus. Mit etwas krimineller Energie und Kenntnissen lassen sich anderswo vorhandene Hürden vielfach ebenfalls relativ einfach überwinden. Einen interessanten Blick auf die wichtigsten Angriffsvektoren liefert eine BSI-Studie aus dem Jahr 2019. Zu den wesentlichen 10 Cyberrisiken für Industrieanlagen nach BSI gehören demnach:

- Einschleusen von Schadsoftware über Wechseldatenträger und externe Hardware (Tendenz steigend)
- Infektion mit Schadsoftware über Internet/Intranet (Tendenz steigend)
- Menschliches Fehlverhalten und Sabotage (Tendenz stark steigend)
- Kompromittierung von Extranet- und Cloud (Tendenz stark steigend)
- Social Engineering und Phishing (Tendenz rückläufig)
- (D)DOS-Angriffe (Tendenz stark steigend)
- Internet-verbundene Steuerungskomponenten (gleichbleibend)



Strom im Haus Wandlertechnik

Überall dort, wo ein hoher Strom sicher und nachhaltig gemessen werden muss, kommt die Wandlertechnik zum Einsatz. Egal ob es sich um einen Zweckbau, Ladepunkte für die Elektromobilität oder die Einspeisung einer PV-Anlage handelt – eine Wandlermessung, auf die man sich verlassen kann, benötigt jeder. Mit den Wandleranlagen bieten wir hier die perfekte Ergänzung zu den direkt messenden Zählerplätzen im System Prisma XS.



Geprüftes Wandler-system nach DIN VDE 0603-2-2.

Geprüfte Qualität, auf die man sich verlassen kann.



Der Wandlerkomplett-schrank ist VNB-konform vormontiert. Damit kommen Sie einfach und schnell zum passenden Schrank.



Eine große Anzahl an Wandler-, Mess- und Verteilerfeldern bietet unzählige Möglichkeiten. Stellen Sie die Anlagen einfach VNB-konform zusammen.

- Einbruch über Fernwartung (gleichbleibend)
- „Technisches Fehlverhalten“ und höhere Gewalt (Tendenz rückläufig)
- Kompromittierung von Smartphones im Produktionsumfeld (gleichbleibend)

Insecure by Design: Probleme für Industrieanlagen

Es sei an dieser Stelle ausdrücklich darauf hingewiesen: Cybersicherheit ist – gerade bei Industrieanlagen – vielfach nicht nur ein technisches Problem, sondern auch ein Problem der Verantwortung. Für IoT-Geräte im Haushalt scheuen viele Hersteller Sicherheitsupdates, da diese in der Regel dann anfallen, wenn das Produkt längst auf dem Markt bzw. häufig bereits abverkauft und das Ganze nur noch ein Kostenfaktor ist. Diese gefährliche Denkweise gibt es manchmal auch im Bereich von Steuerungssystemen und Komponenten für Industrieanlagen. Vom chinesischen Hersteller für Kamerasysteme Xiongmai, der Komponenten liefert, die wiederum in Maschinen weltweit eingebaut werden, ist bekannt, dass er auf eine Sicherheitslücke (ausweislich auf der Unternehmenswebsite) mit folgender Stellungnahme geantwortet hat: „Security issues are a problem facing all mankind. Since industry giants have experienced them, Xiongmai is not afraid to experience them once, too.“ Auf Deutsch: Sicherheitsfragen sind ein Problem der gesamten Menschheit. Da Branchenriesen sie erlebt haben, hat Xiongmai keine Angst, sie auch einmal zu erleben. Dies zeugt nicht gerade von Verantwortungsbewusstsein und setzt alle, die Abnehmer dieser Module sind, potentiell hohen Risiken aus.

Risiko „Supply Chain Security“

Das Risiko um was es hier geht, nennt man „Supply-Chain-Risiko“. Damit ist – anders als vielleicht erwartet – nicht gemeint, dass Komponenten nicht geliefert werden können und die Lieferkette reißt, sondern dass, Risiken über Zulieferkomponenten, wie eben die gerade genannten Kamerasysteme, in Endprodukte wie etwa Maschinen wandern, ohne dass dem Maschinenhersteller gewahr ist, dass er diese Risiken mit sich herumschleppt. Hier gibt es vielfältige Fallbeispiele. Wegen der enormen Tragweite soll hier nur ein Fall: „Ripple 20“ näher betrachtet werden. Demnach hat im Jahr 2020 die Cybersicherheitsfirma JSOF ein und dieselbe Lücke u. a. in Geräten von ABB, Cisco, Dell, Miele, Mitsubishi Electric, Ricoh, Schneider Electric,

Xerox – um nur die bekanntesten Namen zu nennen – festgestellt. Betroffen von der gemeinsamen Lücke waren so unterschiedliche Geräte wie Drucker, USV-Stromversorgungen, Kraftwerkssteuerungen, Medizintechnik- und Laborreinigungsgeräte und natürlich Industriesteuerungsanlagen. Schuld an dem Dilemma war ein kleines Stück Software für die Netzwerkkommunikation, das in den Grundsätzen auf eine Entwicklung in den späten 1990er Jahren zurückgeht und von einer Firma stammt, die es längst nicht mehr gibt. Was nun? Die meisten der genannten Anbieter haben vorbildlich reagiert und nach einem Sicherheitshinweis durch die Firma JSOF Updates für ihre Systeme auf den Markt gebracht.

Das Grundproblem der Komplexität bleibt und wird auch in anderen Fällen für Probleme sorgen.

ep TIPP

Seit 2007 sammelt CE21 Erfahrungen in Informationstechnologie und Telekommunikation aus Projekten für mittelständische und große Unternehmen der verschiedensten Branchen. Das Expertenteam widmet sich dabei folgenden Schwerpunkten: Datenschutz, Cybersicherheit, Digitalisierung und Beratung. Das Unternehmen liefert damit wichtige Bausteine für die Anforderungen der Zukunft.

www.ce21.de

Mehr Sicherheit ohne Quick-Fix

Wie erzeugt man Sicherheit in einer Welt voller – oft wenig bekannter – Unsicherheiten und vielfach nicht eindeutiger Abhängigkeiten und Beziehungen? Wie kann dies vor dem Hintergrund zunehmender externer Verbindungen und Verbindungen zwischen IT und OT, steigenden Notwendigkeiten für zwischenbetrieblichen Datenaustausch und Bereitstellung von Fernwartungsoptionen sowie bekannter aber vielfach nicht oder nur unvollständig gepatchter Schwachstellen in Anlagen und Komponenten erreicht werden?

Der wesentliche, erste Schritt lautet: Mehr Sichtbarkeit herstellen und folgende Fragen besonders berücksichtigen:

- Sind alle Geräte und Systeme auf Fabrikebene bekannt?
- Welche regulären Verbindungen haben diese Systeme/müssen diese Systeme ha-

ben, um funktionieren zu können (permanent wie auch temporär)?

- Welche Kommunikationsprotokolle sind mit welchen Komponenten etabliert?
- Wie sieht – in Konsequenz zu den obigen Fragen – der sogenannte „Baseline-Traffic“ aus (Verkehrsmuster im Tages- und Wochenverlauf)?
- Wie läuft das Zusammenspiel von IT- und OT-Sicherheit im Unternehmen?
- Sind die „Kronjuwelen“ (Systeme bei deren Ausfall nichts mehr geht) bekannt?

Ist diese Mindestsichtbarkeit hergestellt, ist der erste Schritt geschafft, um die Verteidigung auf eine gesunde Basis zu stellen, denn nun besteht ein Verständnis für die Systemumgebung und das Verhältnis zum Firmennetz. Falls noch nicht geschehen, sollte danach:

- ein dediziertes OT-Sicherheitsteam für die industriellen Anforderungen etabliert werden
- eine Möglichkeit geschaffen werden, um Hinweise auf aktuelle Bedrohungen systematisch entgegenzunehmen, auszuwerten und das Handeln darauf abzustimmen
- eine Risikobewertung vorgenommen werden (u. a. mit ehrlichen Kostenansätzen für Downtime und zerstörte Anlagen)
- ein OT-Überwachungssystem aufgesetzt werden
- besondere Maßnahmen zum Schutz der „Kronjuwelen“ getroffen werden
- ein Notfallplan erstellt und für den „attack day“ geübt werden
- neue Lieferanten auch unter Sicherheitsaspekten ausgewählt werden.

Falls man selbst Anbieter von Industrieanlagen oder -komponenten ist, sollte auch der Versicherungsschutz überprüft werden, d. h. es muss die Frage geklärt werden, ob die Produkthaftung auch auf die nicht endenden, informationstechnologisch bedingten Risiken eingestellt ist.

Es empfiehlt sich auf den „Rough Ride“ vorbereitet zu sein, denn die Sicherheitsproblematik in Industrieanlagen ist gerade dabei zum nächsten großen Schlachtfeld der Cybersicherheit zu werden.

Literatur

- [1] Webverweis: <https://www.thyssenkrupp.com/de/newsroom/datensicherheit>, Abruf: 02.05.2021
- [2] Webverweis: <https://www.zdnet.com/article/vulnerabilities-found-in-ge-anesthesia-machines/>, Abruf: 02.05.2021