Was Hersteller und Betreiber vernetzter Maschinen und Anlagen beachten sollten

Hausaufgaben für Industrial Cybersecurity

Die Verknüpfung von IT und OT zum IIoT macht in Industrieunternehmen eine umfassende Cybersecurity-Strategie immer dringlicher. Doch was ist dabei zu beachten? Und was sind die größten Cyberbedrohungen, gegen die es sich zu wappnen gilt?

VON STEPHAN STROHMEIER,
BEREICHSLEITER SAFETY &
SECURITY SOLUTIONS BEI NEWTEC

Wegen des russischen Angriffs auf die Ukraine rief das Bundesamt für Sicherheit in der Informationstechnik (BSI) am 12. Mai 2022 die deutschen Unternehmen auf, ihre IT-Sicherheitsmaßnahmen zu erhöhen: »Bleiben Sie wachsam und machen Sie Ihre digitalen Hausaufgaben!«

Laut oberster Cybersecurity-Behörde hieße das: Notfallpläne aktualisieren, regelmäßig Backups machen und Systeme aktuell halten. Das Problem: In Zeiten zunehmender Vernetzung von Information Technology (IT), Operational Technology (OT) und Internet of Things (IoT) ist es damit nicht getan. Alle, die am Produktlebenszyklus vernetzter Komponenten beteiligt sind, müssen ihre Hausaufgaben machen, nicht nur die Betreiber, sondern auch die Hersteller. Für industrielle Umgebungen gilt das in besonderem Maße.

Gesamte Lieferkette gefährdet

Der Anfang Juni 2022 veröffentlichten Studie »The State of Industrial Cybersecurity« des Sicherheitsunternehmens Trend Micro zufolge erlebten 90 Prozent der befragten deutschen Unternehmen (aus den Bereichen Fertigung sowie Strom-, Öl- und Gasversorgung) in den letzten zwölf Monaten Cyberangriffe auf industrielle Systeme, 75 Prozent sogar mindestens sechsmal. Die Angriffe verursachten finanzielle Schäden von durchschnittlich etwa 2,9 Millionen Euro.

Knapp 90 Prozent der Befragten berichteten zusätzlich zum Kernbetrieb von Beeinträchtigungen der Lieferkette. Das musste vor Kurzem auch Toyota erfahren: Als ein Ransomware-Angriff am 28. Februar einen wichtigen Zulie-

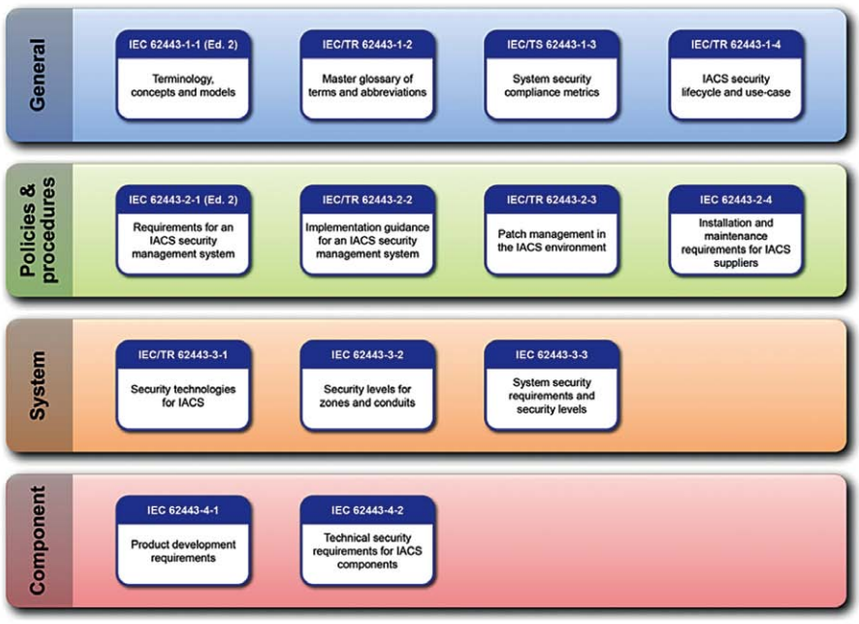

Bild: DKE

Struktur der Normenreihe IEC 62443

ferer traf, musste der weltgrößte Autobauer seine Produktion in 14 Fabriken und 28 Produktionslinien stoppen, denn Tier-1-Zulieferer sind direkt in Toyotas Just-in-Time-Produktionssteuerung eingebunden.

Angriffstypen und -vektoren

Wer sich wirksam vor Cyberangriffen schützen will, muss wissen, wie professionelle Hacker vorgehen. Wichtig: Unternehmen sind heutzutage zunehmend gezielten und sorgfältig vorbereiteten Angriffen ausgesetzt, sogenannten Advanced Persistent Threats (APT). Dem neuesten X-Force Threat Intelligence Index Report von IBM zufolge war 2021 die Fertigungsindustrie der am häufigsten angegriffene Sektor. Angriffe nutzten hier vor allem Sicherheitslücken von Systemen aus (47 Prozent) oder nutzten Phishing Mails (40 Prozent); über alle Sektoren gerechnet ist Phishing der wichtigste Angriffsvektor.

Dabei reagieren Cyberkriminelle flexibel auf veränderte Rahmenbedingungen. Vier der fünf am häufigsten ausgenutzten Sicherheitslücken im Jahr 2021 waren neu (v. a. Log4j); zudem stieg die Zahl der entdeckten Schwachstellen im Zusammenhang mit IoT-Geräten (+16 Prozent) und industriellen Steuerungssystemen (+50 Prozent). Ausspähungsaktivitäten gegen industrielle Netzwerke nehmen zu, etwa gegen das häufig von SCADA-Systemen genutzte Modbus-Protokoll auf TCP-Port 502 (hier gab es in neun Monaten einen Anstieg von 2200 Prozent). Wahrscheinlich um Cloud-Umgebungen bedrohen zu können, setzen Angreifer auch verstärkt auf Malware für Linux (neue Linux-Ransomware wuchs um 146 Prozent) und auch speziell für Docker und andere Container (z. B. XorDDoS, Groundhog, Siloscape).

Der wichtigste Angriffstyp ist nach wie vor Erpressung per Ransomware. Aber auch hier gibt es Weiterentwicklungen: Der Trend geht in Richtung »Triple Extortion«: Angreifer verschlüsseln Daten nicht nur, sondern stehlen sie auch und drohen mit ihrer Veröffentlichung sowie zusätzlich mit DDoS-Attacken (Distributed Denial of Service), um mehr Druck aufzubauen.

Gestaffelte Verteidigung für die OT-Sicherheit

Angreifer können unterschiedlichste Wege in ein Netzwerk finden, etwa über Schwachstellen in Servern, schlecht gesicherte Wartungszugänge von Anlagen, kompromittierte

Typen von Angriffen auf OT 2021

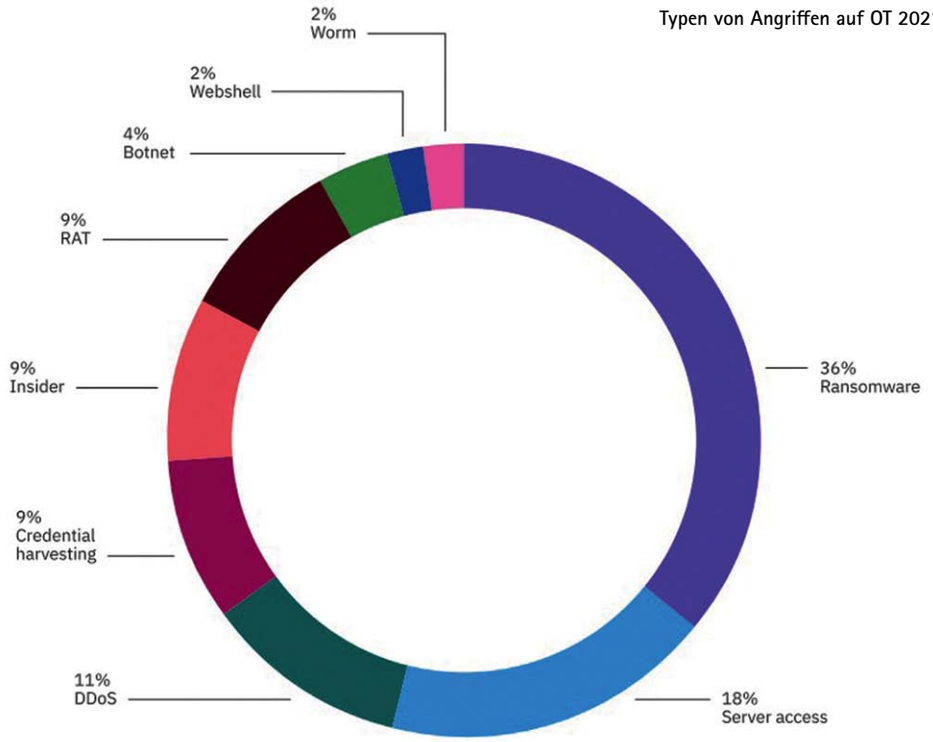

Bild: IBM X-Force Threat Intelligence Index Report 2022

Smartphones oder gutgläubige Mitarbeiter. Eine einzige »offene Tür« kann ausreichen, damit Angreifer in ganze Produktionslinien eindringen können. Denn die Produktion ist zunehmend bis hinunter auf die Feldebene vernetzt und beispielsweise mit IoT-Geräten, MES- und ERP-Systemen oder für Wartungsaufgaben oder Updates direkt mit dem Internet verbunden. Wegen dieser Komplexität empfiehlt sich gerade bei der Absicherung industrieller IT/OT-Umgebungen ein systematisches und strukturiertes Vorgehen. Dabei hilft die einschlägige Normenreihe ISO/IEC 62443, die Maßnahmen für die Netzwerk- und Systemsicherheit in industriellen Kommunikationsnetzen beschreibt.

Eine zentrale Forderung der Norm ist es, Sicherheit stets mit Blick auf das Gesamtsystem zu betrachten. Dafür verfolgt ISO/IEC 62443 einen »Defense-in-Depth«-Ansatz: Auf Basis einer detaillierten Bedrohungs- und Schwachstellenanalyse wird das Gesamtnetz in verschiedene Sicherheitszonen (Zones) segmentiert. Diese Zonen sowie die Übergänge bzw. Kommunikationskanäle (Conduits) zwischen ihnen werden separat abgesichert, um das Vordringen eines eingedrungenen Angreifers

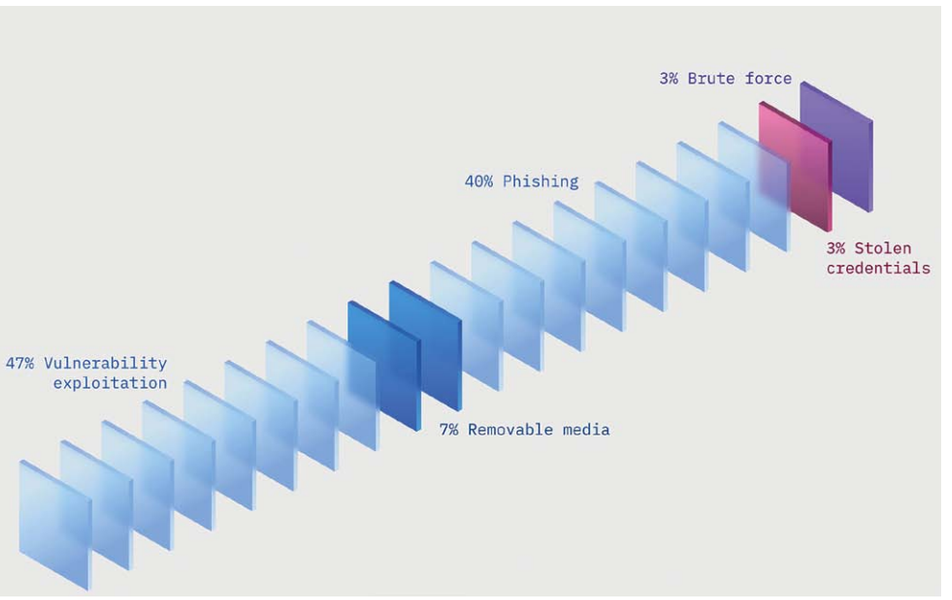

Bild: IBM X-Force Threat Intelligence Index Report 2022

Die wichtigsten Angriffsvektoren in der Fertigung

in weitere Bereiche (Network Propagation) zu verhindern. Dafür werden den Zones und Conduits in Abhängigkeit von Schutzwürdigkeit und aktueller Bedrohungslage individuelle Security Levels (SL) zugewiesen.

Hersteller in der Pflicht

ISO/IEC 62443 fordert, bei der Absicherung den gesamten Lebenszyklus eingesetzter Produkte und Systeme in den Blick zu nehmen. Hier sind besonders auch die Hersteller vernetzter Komponenten gefordert. Die Norm unterscheidet drei grundlegende Rollen – Hersteller, Systemintegratoren und Anlagenbetreiber – mit jeweils spezifischen Security-Anforderungen.

Grundsätzlich müssen Hersteller vernetzter Maschinen, Anlagen oder Komponenten ihre Produkte über den gesamten Lebenszyklus hinweg sicher halten. Denn nur so ist in Zeiten von Industrie 4.0 ein bestimmungsmäßiger Gebrauch möglich. Dazu gehört beispielsweise schon bei der Entwicklung von Hard- und Software die Integration sicherer Verschlüsselungsmechanismen und Update-Wege. Ebenso müssen Hersteller über neu entdeckte oder entstandene Risiken informieren und gegebenenfalls Patches und Updates zur Verfügung stellen. Betreiber oder Integratoren müssen ihrerseits dafür sorgen, dass Firm- und Software aktuell sind, Herstellervorgaben eingehalten und zudem IT- und OT-Systeme regelmäßig auf mögliche Schwachstellen überprüft werden.

Hilfe bei der Umsetzung

Um die Anwendung der in ISO/IEC 62443 beschriebenen Methodik zu erleichtern, hat das BSI im Rahmen des sogenannten IT-Grundschutzes auch Anleitungen zur Absicherung von IIoT- und ICS-Komponenten veröffentlicht. Die speziellen Anforderungen von industrieller IT beschreiben die Grundschutz-Bausteine mit dem Kürzel IND (z. B. IND 2.2 »Speicherprogrammierbare Steuerung«, IND 2.3 »Sensoren und Aktoren«). Im ICS-Security-Kompendium des BSI bekommen Betreiber ebenfalls wertvolle Informationen. Auch die Richtlinie VDI/VDE 2182 zur »Informationssicherheit in der industriellen Automatisierung« beschreibt eine mit ISO/IEC 62443 kompatible Vorgehensweise zur Absicherung automatisierter Maschinen und Anlagen.

Weil aber auch mit den umfassendsten Security-Maßnahmen ein erfolgreicher Cyberangriff nie ganz auszuschließen ist, benötigen Unternehmen auch eine detaillierte Notfallplanung mit Zuständigkeiten und Sofortmaßnahmen, um die Schäden eines Angriffs zu minimieren und den Regelbetrieb schnell wieder aufzunehmen. Dabei unterstützt die internationale Norm ISO/IEC 27035 »Information Security Incident Management« mit Leitlinien zur Identifizierung, Bewertung und Behandlung von Sicherheitsvorfällen und Schwachstellen.

Bild: Grecaud Paul/stock.adobe.com

Security by Design und Zero Trust

Bei der Absicherung von OT und IT müssen Hersteller von Betreiber heute an einem Strang ziehen. Hersteller brauchen dafür Security by Design, denn nachträgliche Absicherungen sind teuer und wirken nur kurz. Und Betreiber müssen das Prinzip Zero Trust verinnerlichen, denn es gibt in komplex vernetzten Umgebungen kein sicheres Innen mit absolut vertrauenswürdigen Komponenten und Akteuren mehr.

Hersteller und Betreiber sollten also jetzt ihre digitalen Hausaufgaben machen. Dafür müssen sie entsprechendes Security-Know-how aufbauen oder externe Spezialisten einbinden. NewTec unterstützt Hersteller und Betreiber bei der Risikoabschätzung für konkrete Anwendungsfälle, prüft Geräte und Systeme auf Schwachstellen und bietet auch Hardware und Software für eine sichere Vernetzung und Cloud-Anbindung von IIoT-Geräten und Sensoren an. Für Hersteller hat NewTec einen strukturierten Security-Management-Prozess zur umfassenden Absicherung ihrer Produkte entwickelt. Die Besonderheit dabei ist ein integriertes Konzept von Sicherheit, das Security- und Safety-Aspekte, also funktionale Sicherheit, gleichermaßen berücksichtigt – denn: If it's not secure, it's not safe. (ak)

Safety und Security im IIoT

Kostenloses Whitepaper von NewTec

Zum Thema Cybersecurity im Industrial Internet of Things hat NewTec ein kostenloses Whitepaper veröffentlicht. Interessenten erfahren dort, was die Digitalisierung und Vernetzung für die Safety und Security von Industrieanlagen und Maschinen bedeutet und welche Herausforderungen und Lösungsansätze es gibt. Zur Verfügung steht das Whitepaper hier: https://heyflow.id/safety-and-security-whitepaper-de#whitepaper-nosafetywithoutsecurity. (ak)