White Paper

Paradigmen für resiliente Digitalisierung

10/2020

DETECON
CONSULTING

Table of Contents

Die zunehmende Vernetzung von Technologien erfordert heute ein hohes Maß an Innovation und Verständnis für die spezifischen Bedürfnisse dieser neuen Ökosysteme. Neue Datenquellen und Technologien ermöglichen neue Geschäftsmodelle und das Potenzial für digitale Wertschöpfung. In diesem Papier wird beschrieben, wie Sicherheitsbedenken berücksichtigt und die neue Wertschöpfung abgesichert werden kann, wenn sich bestehende Umgebungen digital weiterentwickeln, sei es durch Fernarbeit oder durch neue IoT-Produkte und -Paradigmen.

Kritische Schwachstellen kritischer Infrastrukturen

Industrielle Steuerungssysteme (ICS), Industrielle Automatisierungs- und Steuerungssysteme (IACS) oder allgemeiner Operational Technology (OT) sind Systeme, die zur Steuerung und Überwachung von Funktionen verwendet werden, die für den kontinuierlichen Betrieb von Produktionsanlagen sowie für kritische Infrastrukturen wie Wasserreinigungs-, Energieerzeugungs- und Transportsysteme (KRITIS)[1] entscheidend sind. Für die meiste Zeit, in der diese Systeme bis jetzt im Einsatz waren, wäre es unmöglich gewesen, aus der Ferne auf sie zuzugreifen. Um eine Fabrik oder ein Kernkraftwerk zu überwachen und zu kontrollieren, musste sich eine Person physisch im gesicherten und abgeschotteten Kontrollraum aufhalten, der durch verschiedene Zugangskontrollen physisch geschützt ist. Das ist zunehmend nicht mehr der Fall - industrielle Steuerungssysteme sind mehr denn je miteinander verbunden und angreifbarer als je zuvor.

Informationstechnologie (IT) und Betriebstechnik (OT) waren traditionell getrennte Bereiche innerhalb der Unternehmen und funktionierten völlig unabhängig voneinander. Diese bezieht sich sowohl auf die Aufgabendefinition als auch auf die Systemarchitektur, die Organisationsstruktur und das Führungsmodell. IT-Systeme nutzen Computer, Speicher- und Netzwerkgeräte zur Verarbeitung und Speicherung von Daten. Sie basieren in der Regel auf einer offenen, standardisierten Architektur. Am anderen Ende des Spektrums befinden sich OT-Systeme, die in der Regel geschlossene Systeme sind und auf proprietäre Protokolle und speicherprogrammierbare Steuerung (SPS) angewiesen sind. Die Konvergenz von IT- und OT-Systemen wird schon seit geraumer Zeit diskutiert, aber die aktuellen Umstände und Trends beschleunigen die Konvergenz zunehmend.

Industrieunternehmen stehen heute vor der Herausforderung, agil und kurzfristig auf rasante Marktveränderungen und volatile globale Wirtschaftsbedingungen reagieren zu müssen. Kürzere Entwicklungs- und Produktionszyklen, steigende Kundenanforderungen und Qualitätsansprüche sowie die andauernde COVID-19-Pandemie haben zur Notwendigkeit beigetragen, die Digitalisierung innerhalb der Ökosysteme der Industrie und der kritischen Infrastrukturen voranzutreiben. Angesichts dieser erheblichen Veränderungen und um im Wettbewerb mithalten zu können, führen Unternehmen rasch Digitalisierungsmaßnahmen ein, die die Sicherheit kritischer Systeme in ihrer IT/OT-Umgebung möglicherweise nicht berücksichtigen. Die Bedeutung der Resilienz der Industrie ist heute deutlicher denn je. Industrielle Systeme müssen in der Lage sein, aufkommende Störungen zu bewältigen und den normalen Betrieb innerhalb kürzester Zeit und zu minimalen Kosten zu gewährleisten, um Verluste und Verschwendung so gering wie möglich zu halten.

[1] Kritische Infrastruktursektoren werden von jedem EU-Staat festgelegt. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32008L0114&from=EN

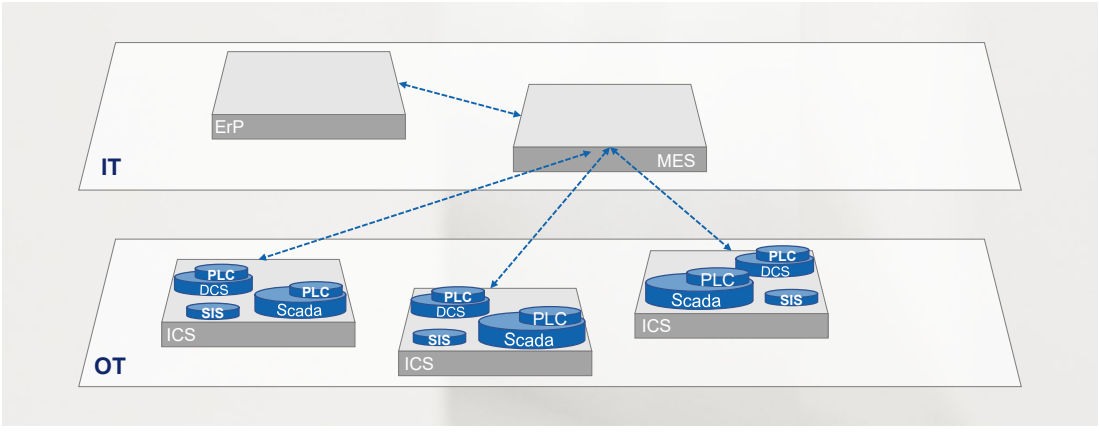
Die ICS-Security und die Cybersecurity im Allgemeinen rücken für nationale und internationale Behörden immer mehr in den Vordergrund und daher ist die Absicherung vernetzter physischer Anlagen nicht nur zur Vermeidung von Schadensereignissen, sondern auch zur Einhaltung von Vorschriften und Kundenanforderungen von entscheidender Bedeutung. Im Jahr 2016 veröffentlichte die EU die NIS-Richtlinie, die die EU-Mitgliedstaaten dazu verpflichtet, die Anforderungen in nationales Recht umzusetzen.[2] In Deutschland hat die IT-Sicherheitsverordnung (§ 8a Absatz 5 BSIG innerhalb des BSI-Gesetzes)[3] einen hohen Standard für Betreiber kritischer Infrastrukturen für das Risiko- und Sicherheitsmanagement im gesamten Unternehmens-Ökosystem festgelegt. Sie wurde durch die KRITIS-Bestimmung ergänzt, die festlegt, welche Anbieter kritischer Infrastrukturen zur Umsetzung der IT-Sicherheitsverordnung verpflichtet sind. Ein Leitfaden zur konkreten Umsetzung der Verordnung wurde im März 2020 veröffentlicht.[4]

Die Herausforderung besteht darin, die Vorteile der Digitalisierung mit dem Bedarf an einer robusten, widerstandsfähigen und sicheren IT/OT-Infrastruktur zu verbinden. In diesem Papier werden die Trends innerhalb der industriellen IT/OT-Konvergenz untersucht und ein Weg zur Sicherung von neuen und bestehenden Systemen und funktionierende Modelle aufgezeigt.

Die Welt der Betriebstechnik

Bevor man die Sicherheitsbedürfnisse der IT/OT-Infrastruktur versteht, ist es zunächst unerlässlich, die Begriffe zu verstehen, die zur Beschreibung dieser Technologien verwendet werden und wie sie sich in einen breiteren IoT-Kontext einfügen.

Während sich der Begriff IT auf Unternehmensgeräte, Netzwerke und Systeme bezieht, umfasst der Begriff OT die gesamte Hard- und Software, die zur Überwachung und Steuerung physischer Prozesse, Geräte und Infrastruktur eingesetzt wird. Ein wesentlicher Teil der Betriebstechnik sind die industriellen Steuerungssysteme (ICS) oder auch Industrial Automation and Control Systems (IACS).



Diese Systeme werden zur Steuerung und Überwachung von Funktionen verwendet, die für den kontinuierlichen Betrieb von Produktionsanlagen sowie von kritischen Infrastrukturen wie Wasserreinigungs-, Energieerzeugungs- und Transportsystemen (KRITIS)[1] entscheidend

[2] https://www.enisa.europa.eu/topics/nis-directive
[3] https://www.gesetze-im-internet.de/bsig_2009/__8a.html
[4] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/IT_SiG/Konkretisierung_Anforderungen_Massnahmen_KRITIS.html

sind. Gemäß der Definition der Automatisierungsnorm IEC 62443 umfasst ein ICS/IACS verschiedene Arten von Geräten, Systemen, Controllern und Netzwerken, die eine Vielzahl von industriellen Prozessen steuern.

Am gebräuchlichsten sind SCADA-Systeme (Supervisory Control and Data Acquisition) zur Datenerfassung, Überwachung und Steuerung sowie DCS-Systeme (Distributed Control Systems). DCS- und SCADA-Systeme steuern mehrere speicherprogrammierbare Steuerungen (SPS). Diese werden zur Ausführung von Automatisierungsaufgaben eingesetzt und übernehmen so einen Großteil der Arbeit, die zur Aufrechterhaltung der umfangreichen Funktionalität erforderlich ist. Der Unterschied zwischen SCADA und DCS besteht darin, dass SCADA-Systeme PLCs über ein großes geografisches Gebiet (mehrere Standorte) steuern können, während DCS-Systeme in der Regel auf eine Anlage oder einen Industriestandort konzentriert sind.

Safety Instrumented Systems (SIS) sind besonders wichtig für industrielle Systeme, die in Einrichtungen mit Gefahrenstoffen eingesetzt werden, da sie dafür ausgelegt sind, potenziell unsichere Arbeitsumgebungen zu erkennen und Warn- oder Abschaltbefehle zu senden. Diese Kontrollsysteme halten eine Verbindung zu den wichtigen Sensoren und Systemen aufrecht, sind aber ganz bewusst von anderen Kontrollsystemen getrennt, um zu verhindern, dass eine Fehlfunktion in einem anderen System die Sicherheit der Mitarbeiter beeinträchtigt.

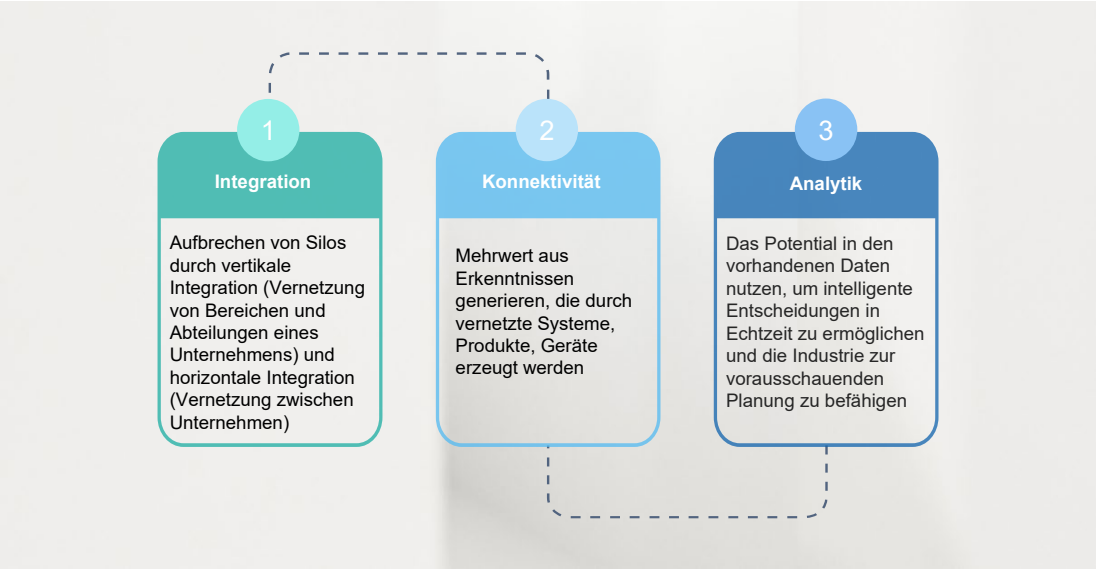
Im Vergleich zur IT wird OT oft als Nische betrachtet und übersehen. Ein differenziertes Verständnis der Funktion und des Aufbaus von OT-Systemen wird zu einer nahtloseren und sichereren Integration der IT beitragen, damit Unternehmen in die Lage versetzt werden, Remote-Arbeit zu ermöglichen, die Effizienz zu steigern, die Kosten zu senken und die allgemeine Betriebssteuerung zu verbessern.

Industrie 4.0 – Steigerung von Sichtbarkeit, Effizienz und Kontrolle

Das betriebliche Umfeld, in dem IT und OT zusammenwachsen, ist geprägt von rasanter Entwicklung, Digitalisierung und Integration. Diese Trends sind ein wichtiger Aspekt, weshalb die Cybersicherheit heute mehr denn je bei der gesamten Entwicklung von IT/OT-Infrastrukturen berücksichtigt werden muss.

Industrieunternehmen müssen heute die herkömmlichen Kriterien (Zuverlässigkeit, Qualität und Preis) erfüllen, gleichzeitig aber auch dem Wunsch nach Flexibilität und zunehmender Individualisierung der Produkte Rechnung tragen. Aus diesen Gründen müssen die klassische Business-IT und die Prozess-/Produktions-IT (OT) sowohl technisch als auch organisatorisch enger zusammenwachsen. Es besteht ein großer Bedarf, Daten aus allen Teilen des Unternehmens zu integrieren, um eine ganzheitlichere Übersicht und Kontrolle zu schaffen. Das Ziel ist ein belastbarer, ständig optimierter Betrieb, mit hoher Effizienz bei Ressourcen, Kosten und Produktivität sowie stärkere Kundenorientierung und reduzierte Systemkomplexität.

Im Bereich der Industrie 4.0 gibt es drei Hauptaktivitäten, die versuchen, diese Ziele zu erreichen: Integration, Konnektivität und Analytik.



Integration:

Bei dem Begriff Integration geht es im Wesentlichen darum, die einzelnen Datensilos aufzubrechen und die Daten so zu integrieren, dass am Ende ein Datenfluss entsteht, der alle Systeme zur richtigen Zeit mit den richtigen Informationen versorgt.

Der Begriff **vertikale Integration** kann synonym für die IT/OT-Konvergenz verwendet werden und beschreibt die durchgängige Vernetzung der einzelnen Hierarchieebenen der Produktionssysteme (von der Unternehmensleitebene bis zum Sensor). Die Prozesse sollten transparenter und flexibler werden, um die Produktionsaufgaben an die sich ändernden Kundenanforderungen anzupassen. Andererseits ermöglichen die Daten aus den Produktionsanlagen eine bessere Steuerung und Kontrolle des gesamten Prozesses.

Bei der **horizontalen Integration** geht es um die durchgängige, digitale Verbindung entlang der Liefer- und Wertschöpfungskette, mit der Absicht, mehr Transparenz zu erreichen und die Flexibilität in Produktion und Service zu erhöhen.

Die Bedeutung der **Produktionsresilienz** wird in Zukunft deutlich zunehmen, wobei der Fokus auf dem Wertschöpfungsnetzwerk liegt. Covid-19 hat veranschaulicht, wie anfällig einige Lieferketten sind, und wird Unternehmen dazu ermutigen, ihre derzeitige Strategie zu überdenken. **Ökosysteme** und **Plattformen** werden eine besonders wichtige Rolle bei der Vermeidung künftiger Engpässe spielen und eine rasche Anpassung an sich verändernde Marktsituationen ermöglichen. Die lineare Lieferkette wird allmählich durch Ökosysteme ersetzt.

Konnektivität & Kommunikation:

Konnektivität ist der Eckpfeiler des digitalen Wandels in der Industrie und eines der wichtigsten Themen, wenn es um die Realisierung von Industry 4.0-Use-Cases geht.

Das **(industrielle) Internet der Dinge (IoT)** spielt eine entscheidende Rolle bei der Vernetzung von Betriebstechnik und IT. Im Allgemeinen ist IoT die Technologie, die es ermöglicht, alle Arten von Geräten und Maschinen über das Internet zu verbinden und Daten zu nutzen, die vorher nicht zugänglich waren. Das Zusammenspiel zwischen IoT und Cyber-physischen Systemen ermöglicht es den Geräten, miteinander zu interagieren und zu kooperieren.

Ein **Cyber-Physikalisches System** ist die Kombination aus physikalischen (z.B. mechanische Maschine) und informationstechnischen Komponenten (z.B. eingebettetem System). Die eingebetteten Systeme sammeln über Sensoren Daten aus der physischen Welt und steuern und regulieren sie über Aktoren.

Das cyber-physikalische System entfaltet in Kombination mit einem **digitalen Zwilling** sein volles Potenzial und ermöglicht Szenarien bis hin zu einem selbstregulierenden System.

„Ein digitaler Zwilling ist die virtuelle Darstellung eines physischen Objektes, wobei operative Daten und andere Datenquellen verwendet werden, um die Überwachung und dynamische Kontrolle des Objektes zu ermöglichen. Dies deckt den gesamten Bereich angefangen von einer Lebenszyklusphase bis hin zum gesamten Produktlebenszyklus ab. Die Reife eines digitalen Zwillings wird abhängig von der Ebene der Kommunikation und dem Grad der Standardisierung definiert. Der Grad der Kommunikation beschreibt dabei die Verbindung zwischen dem digitalen Zwilling und dem physischen Objekt. Der Grad der Standardisierung spiegelt dabei die Modellierung der Daten- und Datenquellen wider. “

(Source: Detecon Study: Digital Twins)

Um sicherzustellen, dass neue Geräte schnell integriert werden können und Anwendungen skalierbar sind, spielt die **Interoperabilität** eine wichtige Rolle. Der offene Schnittstellenstandard **OPC Unified Architecture (OPC UA)** setzt sich zu diesem Zweck zunehmend durch und ist auf dem Weg, zum Industriestandard zu werden. OPC UA ist ein offener Schnittstellenstandard für die industrielle Kommunikation, der den plattformunabhängigen Austausch von Daten sicherstellen soll.

Analytik:

Mit dem raschen Wachstum internetfähiger Geräte nimmt auch die Menge der Daten zu, die auf automatisierte und strukturierte Weise erzeugt werden - das Aufkommen großer Datenmengen (**Big Data**) bietet das Potenzial für detailliertere Insights. Die Verwaltung und Analyse dieser Daten zur Schaffung von Erkenntnissen ist der wahre Wert, den die IT/OT-Konvergenz bieten kann. Daten innerhalb des Unternehmens und aus Produkten werden zu einem Asset und müssen als solches behandelt werden.

Damit Produkte, Maschinen, Anwendungen und die entsprechenden digitalen Zwillinge intelligente Entscheidungen treffen können, muss das Unternehmen über das entsprechende Know-how im Umgang mit den Daten verfügen.

Verschiedene **KI** und **Machine Learning** Methoden ermöglichen es, diese Daten zielgerichtet zu analysieren, um Produkte zu optimieren, den Produktionsprozess besser zu verstehen und zu steuern, vorausschauende Wartung zu realisieren und damit Ausfallzeiten zu minimieren oder das Energiemanagement zu optimieren.

Der Trend zur Konvergenz von IT und OT bietet viele Vorteile für Unternehmen auf der ganzen Welt. Diese Vorteile, die im Folgenden zusammengefasst werden, treiben Innovation und Fortschritt in fast allen Branchen an. Leider ist eine höhere Effizienz und Benutzerfreundlichkeit auch mit Kosten verbunden. Die IT/OT-Konvergenz hat auch zu mehr Interdependenzen geführt, die von böswilligen Akteuren oder sogar ahnungslosen Insidern negativ verwendet werden können.

Vorteile:

- Ganzheitliche Nutzung aller im Unternehmen vorhandenen Daten
- Verbesserte Kontrolle und automatisierte Steuerung von Prozessen
- Bessere Vorhersagen und Systeme mit besseren Reaktionen auf Ereignisse
- Verbesserte Automatisierung durch Kombination der Informationsbeschaffung aus Unternehmen und Produktion
- Verbesserte Entscheidungsfindung auf der Grundlage genauerer und zeitnaher Informationen.
- die richtigen Informationen zur richtigen Zeit dort bereitzustellen, wo sie benötigt werden
- Bessere Kundenerfahrung durch proaktive Dienstleistungen (Wartung, Beratung, Optimierung, Entwicklung)

Bedrohung der Cybersecurity in Industrieumgebungen – Gefahren der Konnektivität

Viele cyber-physikalische Systeme sind für die Ausführung kritischer Funktionen wie Energieerzeugung, Fertigung oder dem öffentlichen Verkehr zuständig. Die im vorigen Abschnitt hervorgehobenen Trends - verstärkte Fernüberwachung und -konfiguration sowie die Einführung neuer, relativ unerprobter Technologien - bedeuten für viele Unternehmen zwar eine erhebliche Steigerung der Effizienz und des Entwicklungsstands, stellen aber auch eine Bedrohung für die Gesamtsicherheit dieser Systeme dar. Die Risiken eines Cyber-Angriffs speziell gegen physische Systeme können schwerwiegende Folgen für die Gesellschaft im Allgemeinen sowie für Unternehmen im Hinblick auf die allgemeine Geschäftskontinuität und die Gewinne haben.

Die Gefahr solcher Angriffe ist nicht länger spekulativ oder hypothetisch; Cyber-Angriffe auf physische Systeme finden immer häufiger statt, seit der Stuxnet-Wurm 2009 iranische Urananreicherungszentrifugen infiltriert hat, um Fortschritte auf dem Weg zu einer Atomwaffenfähigkeit zu verzögern.[5] Es wird vermutet, dass Stuxnet, ein Regierungsprojekt, das aus einer Zusammenarbeit zwischen den Vereinigten Staaten und Israel hervorgegangen ist, über einen infizierten USB-Stick in das Netzwerk eingedrungen ist. Von dort aus änderte das bösartige Programm die Geschwindigkeiten der Zentrifugen, um gängige Betriebsausfälle nachzuahmen. Die Stuxnet-Malware hat Schätzungen zufolge das iranische Atomprogramm um zwei Jahre zurückgeworfen.[6]

[5] https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/
[6] https://ccdcoe.org/uploads/2018/10/Falco2012_StuxnetFactsReport.pdf; Eine Einschätzung von Ralph Langer, einem der Sicherheitsexperten, der an der Analyse des Stuxnet-Wurms beteiligt waren.

An einem kalten Dezemberabend, im Jahr 2015, gab es bei den Strombetreiber in der Ukraine ein Blackout. Die Angreifer befanden sich seit Monaten im System des Stromkonzerns; sie verschafften sich zunächst Zugang, indem sie infizierte Microsoft Word-Dokumente an Ziele innerhalb des Unternehmens schickten. Von dort aus erhielten sie Zugang zu den ICS/SCADA-Stromversorgungssystemen, die sich hinter einer Firewall befanden. Der Angriff bestand aus: Deaktivierung der unterbrechungsfreien Stromversorgungssysteme (USV), Aktualisierung der Seriell-zu-Ethernet-Konverter mit erweiterter Firmware und schließlich Überflutung der Telefonleitungen des Kundendienstes mit betrügerischen Anrufen, um zu verhindern, dass von dem Angriff betroffene Kunden den Vorfall melden. Die Manipulation der USV bedeutete, dass selbst die Betreiber im Dunkeln arbeiteten, als der Befehl zum Abschalten des Systems gegeben wurde. Die erweiterten Seriell-zu-Ethernet-Konverter waren dann nicht mehr in der Lage, Befehle von einem größeren Leitsystem zu den Unterstationen zu übertragen. Die Angreifer befanden sich zudem bereits im Netzwerk, so dass die Befehle, die sie erteilten, um die Stromversorgung für einen bedeutenden Teil der Ukraine abzuschalten, von innerhalb des Netzwerks kamen und nicht als anomal gekennzeichnet wurden. Die Nichtverfügbarkeit der Telefonleitungen verzögerte die Reaktionszeit, die Informationsbeschaffung und förderte eine allgemeine Unsicherheit für alle Beteiligten. Nach dem Angriff dauerte es etwa sechs Stunden, bis die Verbraucher wieder mit Strom versorgt wurden. Es ist offensichtlich, dass ein solcher Angriff fatale Auswirkungen auf die Bevölkerung haben kann.[7]

Ein weiterer Vorfall mit gezielter ICS-Malware ereignete sich 2017 in einer saudi-arabischen petrochemischen Anlage. Die Malware wurde nach einer vermutlich versehentlichen Abschaltung des Werksbetriebs identifiziert; Fireeye, ein in den USA ansässiges Cyber-Sicherheitsunternehmen, hat postuliert, dass die Absicht des Angreifers darin bestand, die Safety Instrumentation Systems (SIS) im Werk zu verändern, was katastrophale Folgen hätte haben können. Ein solcher Angriff würde theoretisch darauf abzielen, einen Chemieunfall oder eine Fehlfunktion in der Anlage zu verursachen, die dann durch die Manipulation des SIS unbemerkt bleiben würde. Die Beschäftigten einer solchen Anlage wären am meisten gefährdet, aber die Auswirkungen könnten sich auf die gesamte Umgebung der Anlage erstrecken. Malware, die auf SIS abzielt, ist besonders hervorzuheben, weil SIS zum Schutz der Mitarbeiter eingesetzt werden und daher jede Manipulation solcher Systeme darauf abzielt, Menschen persönlichen Schaden zuzufügen, was oft als nicht vorstellbar für Cyber-Angriffe angesehen wird.[8]

Grundprinzipien für die Sicherung industrieller IT/OT-Umgebungen

Die wichtigsten Ziele für die Sicherheit innerhalb einer IT-Umgebung sind Vertraulichkeit, Integrität und Verfügbarkeit, in der Regel in dieser Reihenfolge. In einem industriellen Umfeld ist die Verfügbarkeit das wichtigste, zu schützende Ziel (wobei die Integrität an zweiter Stelle steht). Vorrangig muss sichergestellt werden, dass die Systeme weiterhin funktionieren und die Produktion nicht beeinträchtigt wird, was zu Verzögerungen und finanziellen Verlusten, aber auch zum Ausfall integrierter Systeme mit noch schlimmeren Folgen führen kann. Die Integrität muss ebenfalls geschützt werden, um sicherzustellen, dass die Systembefehle nicht verändert und die Systemprozesse gestört oder zerstört werden.

[7] https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/
[8] https://www.fireeye.com/blog/threat-research/2017/12/attackers-deploy-new-ics-attack-framework-triton.html; https://www.darkreading.com/vulnerabilities---threats/triton-trisis-attacks-another-victim/d/d-id/1334388

Detecon hat mit vielen Kunden zusammengearbeitet, um mehr Konnektivität, Transparenz und Effizienz in ihren industriellen Umgebungen einzuführen. Zu den Themen, die das Team von Detecon derzeit untersucht, gehören:

- Sichere Vernetzung von Maschinen und Anlagen
- Erfassen von Maschinendaten
- Integration von Shopfloor Technologien in bestehende und neue IT-Architekturen

Durch die Schaffung eines Ökosystems aus miteinander verbundenen Geräten ist klar, dass ein erhebliches Risiko für die zugrunde liegenden Systeme besteht. Eine Schwachstelle in einem System ist eine Schwachstelle der gesamten Plattform, einschließlich einzelner Eingabesysteme. Um die oben erwähnten Sicherheitsziele zu schützen, erfordert eine solche Plattform strenge Sicherheitsstandards, Tests und Strategien.

Die in diesem Abschnitt beschriebenen Prinzipien sind die Kernaktivitäten, die zur Aufrechterhaltung der operativen Systeme und Geschäfte unternommen werden müssen, wenn auf immer mehr kritische Funktionen über das Internet zugegriffen wird.

Dabei handelt es sich um allgemeine Prinzipien, die in einer cyber-physikalischen oder IoT-Systemkonstellation einen Unterschied machen können. Der Standard ISA/IEC 62443[9] bietet jedoch einen umfassenden Überblick sowohl über organisatorische als auch technische Sicherheitsmaßnahmen zur Absicherung von ICS-Umgebungen. Dieses Dokument definiert weitere, detailliertere Maßnahmen, die zur Gewährleistung der Systemsicherheit ergriffen werden können - zum Beispiel die Einführung einer Multi-Faktor-Authentifizierung, einer physischen Zugangskontrolle oder die Änderung von Standardpasswörtern.

1. Setzen Sie eine risikobasierte Strategie ein, die auf die kritischen Systeme abzielt.

Angesichts begrenzter Ressourcen ist es wichtig, die Dienstleistungen und Systeme zu bestimmen, die für das Unternehmen am wichtigsten sind, um so Prioritäten zu setzen. Sobald diese zentralen Dienste oder Systeme identifiziert sind, können Sie die Schlüsselfunktionen bestimmen, die bei einer Unterbrechung durch einen Cyberangriff die größten Auswirkungen auf das Geschäft haben würden. Bestimmen Sie von dort aus, welche dieser kritischen Systeme am anfälligsten für einen Angriff sind. Maßnahmen zur Sicherung dieser Komponenten würden daher zunächst im Rahmen einer priorisierten Sicherheitsstrategie implementiert, die die Bedürfnisse des Unternehmens und die Beiträge aller relevanten Interessengruppen einschließlich Management, IT und OT-Mitarbeiter berücksichtigt. Um beispielsweise eine für den Anlagenbetrieb kritische Funktion zu ändern, ist es sinnvoll, dass Vier-Augen-Prinzip einzuführen, bei dem zwei Personen die Änderung getrennt bestätigen müssen, damit sie im System implementiert werden kann. Dies würde sicherstellen, dass keine einzelne Person (ein böswilliger Insider oder ein ausgeklügelter Hacker) allein eine größere Abschaltung oder einen größeren Zwischenfall verursachen kann.

Der Nutzen von Sicherheitsmaßnahmen, vor allem bei Altsystemen, muss anhand einer Kosten-Nutzen-Analyse sorgfältig bewertet werden. In einigen Fällen ist die Absicht, das Gerät zu sichern, zwar gut gemeint, aber die Maßnahme selbst (z.B. durch Patches oder Fernüberwachung) kann sich nachteilig auf die Betriebssysteme auswirken und zu einer Unterbrechung des Betriebs oder zur Einführung einer zusätzlichen Schwachstelle führen. Bei OT-Systemen ist es weniger wahrscheinlich, dass sie über eine Testumgebung zum Testen

[9] https://www.isa.org/intech/201810standards/

neuer Konfigurationen oder Patches verfügen. Während man bei traditionellen IT-Systemen damit rechnen kann, dass ein System während des Patch- und Update-Prozesses für einige Stunden offline ist, gilt das Gleiche nicht für OT-Systeme. Dies kann zu einem schwerwiegenderen Problem führen als das, welches durch den Patch behoben werden soll.

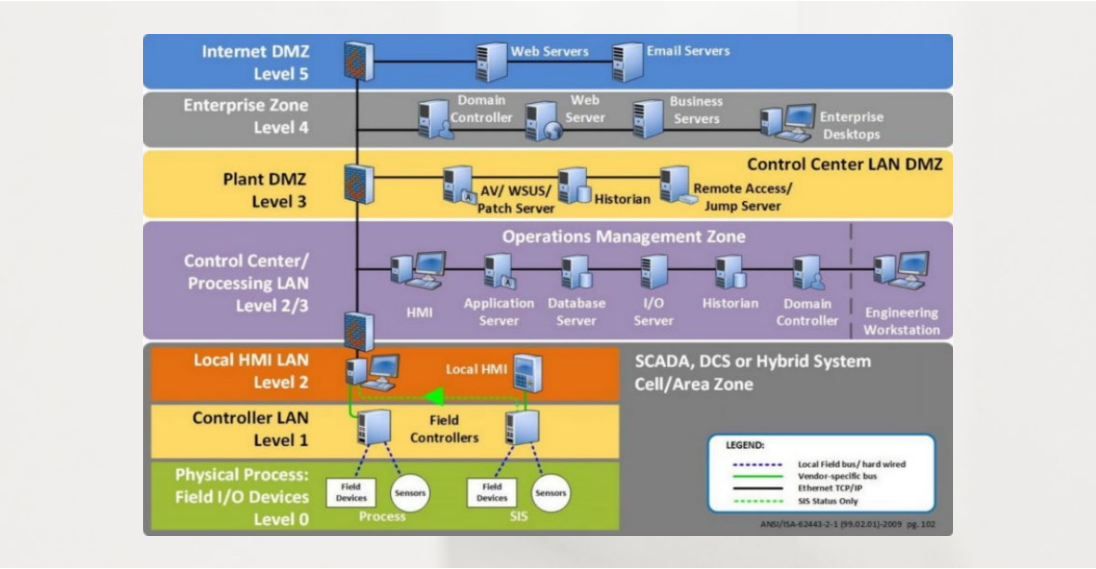
Daher sollte es, wie bei vielen Sicherheitsmaßnahmen, ein konsistentes und dokumentiertes Verfahren geben, um zu bestimmen, wann das "Risk of Doing Nothing" das Risiko der Durchführung von Sicherheitsmaßnahmen überwiegt.

2. Klare Definition und Schutz von Netzwerksegmenten, um laterale Bewegungen zu verhindern.

Unter Netzwerksegmentierung versteht man den Prozess der Begrenzung von Kommunikation zwischen definierten Zonen innerhalb eines Netzwerks, typischerweise durch den Einsatz von Firewalls, VLANs, VPNs und physischer Trennung von Netzwerkgeräten. Laut der Veröffentlichung des NIST zur Sicherheit industrieller Steuerungssysteme ist "Netzwerksegmentierung und -trennung eines der effektivsten Architekturkonzepte, dass eine Organisation zum Schutz ihres ICS implementieren kann".[10] Dahinter steht die Überlegung, dass ein System, selbst wenn es nicht direkt für Geschäftsfunktionen relevant ist, genutzt werden kann, um andere, kritischere Systeme innerhalb des Unternehmens zu erreichen. Historisch gesehen sind ICS-Umgebungen anfällig für die unbeabsichtigte oder schlecht konzipierte Integration von Geschäftsumgebung und der OT-Systeme. Beispielsweise verfügten in der Vergangenheit viele Energieeinrichtungen nicht über drahtlose Internetverbindungen. Während für das Kerngeschäft der Organisation kein drahtloses Interne nötig ist, wurden aus Komfortgründen, für die Mitarbeiter in einem Büroteil des Gebäudes, ein Router installiert und somit ein drahtloser Zugangspunkt kreiert. Leider öffnet die Hinzufügung dieses unsicheren Netzwerkgeräts die gesamte Einrichtung für böswillige Hacker.

Die Umsetzung der Netzsegmentierung ist komplex und zeitaufwendig; zudem muss sie genau auf jedes Unternehmen zugeschnitten sein. Um die logischen Netzwerksegmente zu identifizieren, sind mehrere Faktoren zu berücksichtigen, darunter Funktionalität, Managementzugang, Risiko, Volumen des Netzwerkverkehrs usw. In der Zwischenzeit ist es generell ratsam, sicherzustellen, dass keine Verbindungen bestehen, die unnötige Kommunikation ermöglichen (d.h. die Personalabteilung muss nicht auf die Managementkonsole eines OT-Systems zugreifen und daher sollte jede Verbindung vollständig deaktiviert werden). Jedes Segment sollte so organisiert sein, dass es mit Systemen innerhalb dieser Zone verbunden werden kann, wobei so wenig wie möglich zonenübergreifende Kommunikation stattfinden sollte. Zur Unterstützung dieser Struktur dient das weit verbreitete Purdue-Modell als Referenzmodell für große, nicht Cloud-basierte Umgebungen. Die Einführung von Cloud Computing und Speicherung in ICS-Umgebungen erfordert sehr differenzierte Überlegungen zur Zoneneinteilung.

[10] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf



(Quelle:[11])

Dieses Bild, das auf der Norm ANSI/ISA 62443 basiert, zeigt eine typische ICS-Netzwerksegmentierung, die durch die Funktion bestimmt wird.

3. Integration aller Beteiligten in den operativen Sicherheitsprozess und den allgemeinen Schutz kritischer Assets (IT/OT-Konvergenz)

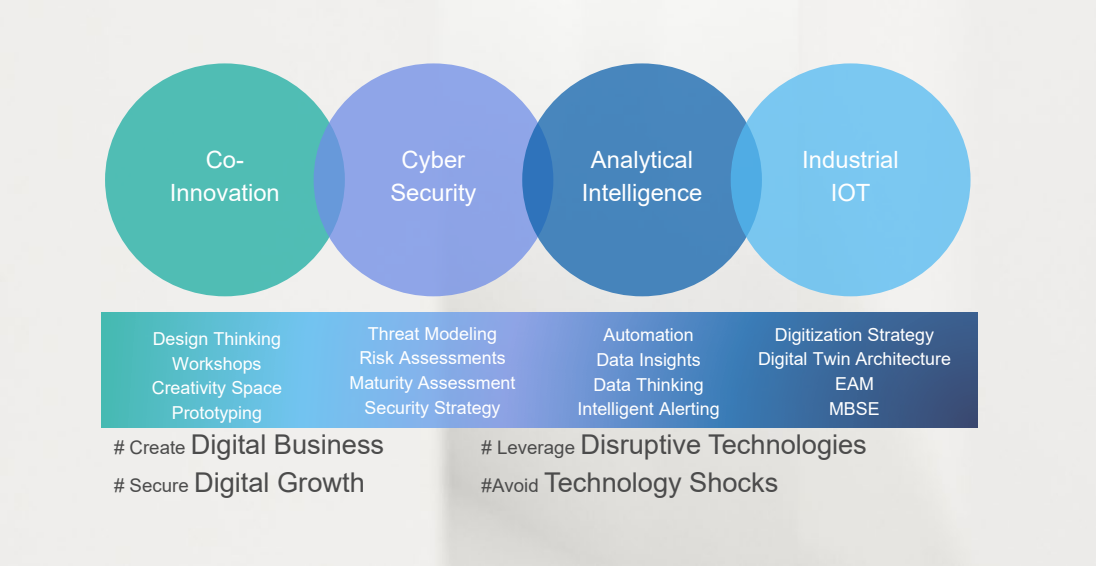
Die Fernverwaltung von OT-Systemen hat das Risikoprofil für physische Systeme mit Air Gap zweifellos verändert. Ein Gewinn für Komfort und schnelle Reaktionszeiten, aber durch die Verbindung mit der Außenwelt haben die Kontrollsysteme eine höhere Wahrscheinlichkeit ausgenutzt zu werden. Da das Prinzip der IT/OT-Konvergenz übergreifend Anwendung findet, muss es auch auf die Sicherheitsbemühungen um diese Systeme angewendet werden. Die für die IT-Sicherheit Verantwortlichen müssen die Vorgaben der OT-Betreiber und Experten einbeziehen, um sicherzustellen, dass die typischerweise angewandten IT-Sicherheitstechniken für IT/OT-Systeme angemessen und sinnvoll sind. Laut der Studie aus 2020 zum Stand der industriellen Sicherheit[12] sind 63% der Befragten der Meinung, dass das Risikomanagement für IT und OT nicht koordiniert ist.

Sicherheitsbemühungen für betriebskritische Systeme müssen auch strenge Anforderungen und Bewertungen an Drittanbietern beinhalten. Wie sich in den letzten Jahren vielfach gezeigt hat, sind Drittanbieter mit geringeren Sicherheitsstandards, aber hohen Zugriffszahlen innerhalb des Zielsystems oft der perfekte Einstiegspunkt für Angreifer. Beim Hack des großen Einzelhandelsunternehmens Target im Jahr 2013 verschafften sich die Angreifer über ein Unternehmen, das Heizungs-, Lüftungs- und Klimaanlagen installiert hatte, Zugang zum Netzwerk.[13] Aus diesem Grund müssen für jedes Unternehmen, das Zugang zu IT-Netzwerken erhält, Sicherheitsbewertungen, Risikobewertungen und adäquate SLAs vorhanden sein, um die Möglichkeit einer lateralen Bewegung innerhalb des Netzwerks zu begrenzen.

[11] https://dale-peterson.com/2019/02/11/is-the-purdue-model-dead/
[12] https://img06.en25.com/Web/TUVRheinlandAG/%7Ba68a7b58-1215-4c4a-8c4f-f0bada2c4738%7D_DE20_I07_2000214_en_Whitepaper_OT_Survey_A4_Web_final.pdf
[13] https://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/

Die organisatorischen Aspekte der Sicherheit sind nicht zu unterschätzen. Durch die Implementierung klarer Prozesse, Richtlinien und Verfahren schränken Sie die Möglichkeiten für menschliches Versagen ein und stellen sicher, dass Risiken genau bewertet werden können. Um die wichtigsten Assets eines Unternehmens zu sichern, muss das gesamte Unternehmen ihre Rolle bei deren Sicherung verstehen. Dies beginnt mit einem starken Engagement des Managements, einer konsequenten und praktischen Anwenderschulung und einer Sicherheitskultur, die die Motivation der Mitarbeiter zur täglichen Anwendung sicherer Praktiken aufrechterhält.

Detecon's Digital Engineering Center konzentriert sich darauf, den neuen Digitalisierungstrends frühzeitig zu begegnen. Mit unseren vier Wissenszentren und Technologieexperten aus den Bereichen industrial IoT, Cyber Security (ICS-Sicherheit), Datenanalytik (KI) und Co-Innovation haben wir im Herzen Berlins eine praxisnahe Innovationshub geschaffen. Unser systematischer, kundenorientierter Ansatz kombiniert Beratung und Innovation mit Hightech-Know-How, um den Transfer vom innovativen Ökosystem in die reale Welt zu gewährleisten. Durch die Entwicklung und Bereitstellung von Prototypen und Proof-of-Concept bieten wir eine beschleunigte, risikoarme Umsetzung digitaler Strategien. Wir unterstützen das gesamte Spektrum von Organisationen und Unternehmen, die ihre Betriebsabläufe digitalisieren wollen, indem sie modernste Technologien mit erprobten Managementmethoden anwenden wollen. Nachstehend finden Sie eine Übersicht über einige der spezifischen Dienstleistungen, die wir anbieten:



Die Autoren

Eve Hunter ist Senior Consultant im Cybersecurity-Team des Detecon Digital Engineering Center. Ihr Schwerpunkt liegt im Bereich Cybersecurity Risikomanagement für kritische Infrastrukturindustrien, sie arbeitete jedoch zuvor im Bereich der nuklearen Sicherheitspolitik. Sie hat einen MSc in Cybersecurity von der Technischen Universität Tallinn und einen BA vom Smith College.

Sie ist zu erreichen unter: Eve.Hunter@detecon.com

Lino Lindner ist Business Analyst am Industrial IoT Center des Detecon Digital Engineering Center. Sein Beratungsschwerpunkt liegt auf IoT/Industry 4.0-Technologien für die Bereiche Maschinenbau, Produktion und Mobilität. Er unterstützt Kunden bei Konzepten des digitalen Zwillings sowie bei daten- und wissensgetriebenen Anwendungsfällen, die der digitale Zwilling in cyber-physikalischen Systemen ermöglicht. Lino Lindner studierte Verkehrswesen (B. Sc.) mit dem Schwerpunkt Luftfahrttechnik an der Technischen Universität Berlin und Maschinenbau (M. Eng.) mit dem Schwerpunkt Digital Engineering an der Fachhochschule Brandenburg.

Er ist zu erreichen unter: Lino.Lindner@detecon.com

Das Unternehmen

Detecon ist eine führende, weltweit agierende Management- und Technologieberatung mit Hauptsitz in Deutschland, die seit über 40 Jahren klassisches Management Consulting mit hoher Technologiekompetenz vereint. Ihr Leistungsschwerpunkt liegt im Bereich der digitalen Transformation: Detecon hilft Unternehmen aus allen Wirtschaftsbereichen, ihre Geschäftsmodelle und operativen Prozesse mit modernster Kommunikations- und Informationstechnologie an die Wettbewerbsbedingungen und Kundenanforderungen der digitalisierten, globalisierten Ökonomie anzupassen. Das Know-how der Detecon bündelt das Wissen aus erfolgreich abgeschlossenen Beratungsprojekten in über 160 Ländern.

Detecon ist ein Tochterunternehmen der T-Systems International, dem herstellerübergreifenden Digitaldienstleister der Deutschen Telekom. Gemeinsam mit der T-Systems Multimedia Solutions GmbH (MMS) und den digital ausgerichteten Bereichen der T-Systems Global Systems Integration (SI) bildet die Detecon International GmbH als Portfolio-Einheit „Digital Solutions“ einen der größten integrierten Digitalanbieter in Deutschland.

Mit dem neuen Bündnis forciert Detecon seinen Beratungsansatz „Beyond Consulting“, der klassische Beratungsmethoden deutlich weiterentwickelt und an heutige und künftige Digitalisierungsanforderungen anpasst. Dies beinhaltet etwa, dass Top-Beratung das Spektrum von Innovation zur Implementierung abdeckt. Zukunftsweisende Digitalberatung erfordert mehr und mehr Technologie-Expertise und ein hohes Maß an Agilität, das die flexible, aber passgenaue Vernetzung von Experten gerade für komplexe, digitale Ökosysteme miteinschließt. Gleichzeitig wird es in der digitalen Beratung zunehmend wichtiger, die Kunden von der Innovation über Prototyping bis hin zur Implementierung zu begleiten.

Daher gründete Detecon bereits 2017 in Berlin die Digital Engineering Center für Cyber Security, Analytical Intelligence, Co-Innovation und Industrial IoT, um die Wertschöpfungskette der Beratung zu erweitern und die Umsetzung von Digitalstrategien und -lösungen mittels Prototypen und Proof of Concepts zu beschleunigen.

Detecon International GmbH
Sternengasse 14 - 16
50676 Cologne
Phone: +49 221 9161 0
E-Mail: info@detecon.com
Internet: www.detecon.com

www.detecon.com