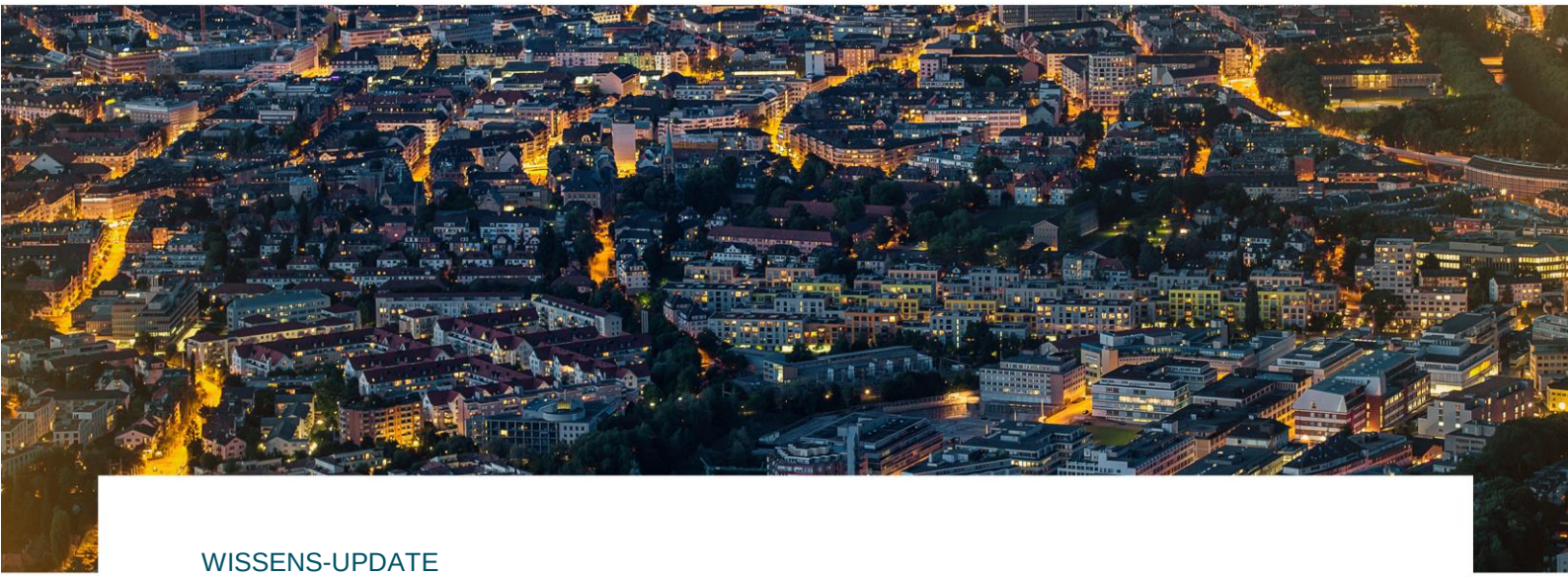
CyOne Security AG
Hinterbergstrasse 18
6312 Steinhausen

Telefon +41 41 748 85 00
info@cyone.ch
cyone.ch



WISSENS-UPDATE

OT – vom isolierten System zur potenziellen Sicherheitslücke

Reto Amstad | Senior Security Consultant | Steinhausen, 14. Mai 2019

In der IT etabliert sich langsam ein vertieftes Bewusstsein für Cyber-Security-Fragen. In der Operational Technology (OT) von Industrieunternehmen ist das noch nicht der Fall. Dabei können gerade vernetzte Anlagen und Geräte als Einfallstor für Hacker und Industriespione dienen. Damit es nicht so weit kommt, braucht es bereichsübergreifende Cyber-Risikoanalysen und individuelle auf die neu auftretenden Risiken abgestimmte Massnahmenpakete.

Digitale Technologien sind im Herzen von Industrieunternehmen angekommen. Sie stecken nicht mehr nur in der IT, sondern auch in der Produktionssteuerung oder der Gebäudetechnik. Diese Technologien, die für den geregelten Ablauf von Betriebsprozessen nötig sind, nennt man Operational Technology (OT). In der Vergangenheit waren OT und IT klar voneinander getrennt: Während sich die OT in einem meist geschlossenen, proprietären System darum kümmerte, die Verfügbarkeit der Anlagen zu gewährleisten, konzentrierte sich die IT auf die Datenverarbeitung.

Diese strikte Trennung löst sich im Zeitalter von Industrie 4.0 auf, die technologischen Grenzen verschwimmen: Heute übernehmen industrielle Steuerungen Hardware-Elemente und Protokolle aus der Welt der IT. Plötzlich halten IP-Protokolle mit VNC, aber auch Hardware-Elemente wie Prozessoren von Intel in der OT Einzug. Die Automatisierung von Prozessen mit Hilfe des Internets der Dinge (IoT) schafft so vernetzte Systeme. Sensoren und Software kommunizieren untereinander und generieren durch die Aggregation der Daten in einer IT-Umgebung einen Mehrwert – ein IoT-Ökosystem entsteht.

Optimierungspotenzial, aber auch neue Gefahren

Für Anwender aus der Industrie bietet die Vernetzung grundsätzlich grosse Vorteile: Komplexe Produktionsprozesse können sich automatisiert abstimmen. Supply-Chain-Prozesse werden zeit- und bedarfsgerecht ausgeführt. Die Daten, die über einzelne Anlagen gesammelt werden, zeigen dem Hersteller Optimierungspotenzial auf – nicht nur der Anlagenbetrieb selbst, sondern auch die Wartung kann optimiert werden; sie muss nur noch dann erfolgen, wenn sie auch wirklich nötig ist. Das spart auf der einen Seite unnötige Serviceleistungen ein und verhindert auf der anderen Seite kostspielige Ausfälle. Für Hersteller ergibt sich dadurch die Möglichkeit für ein Businessmodell mit Wartung per Remote-Zugriff oder Servicefunktionen via Smartphone-App.

Allerdings entstehen auch neue Gefahren: Die Verwendung von IT-Komponenten im OT-Umfeld bedeutet auch die Übernahme der entsprechenden Cyber-Risiken. Durch die Vernetzung sind einerseits die Elemente der OT verwundbar, wenn sich Unbefugte über eine ungenügend geschützte IT-Umgebung Zugang dazu verschaffen. Andererseits öffnet der Datenaustausch von OT- auf IT-Umgebungen, aktuellen und vergangenen Schwachstellen, welche in der IT-Landschaft schon gepatcht wurde. Infolge des oft ungenügenden Cyber-Schutzes in der OT-Umgebung erhöht sich das Risiko für aktuelle und neue Cyber-Bedrohungen.

Fehlendes Bewusstsein für Cyber-Risiken

Oftmals ist OT ein einfaches Einfallstor für Industriespione oder Hacker: Sie können beispielsweise betriebsrelevante Prozessinformation stehlen, ganze Produktionsprozesse manipulieren oder unterbrechen, durch die Chiffrierung von Daten Geld erpressen oder das Netzwerk eines Unternehmens für illegale oder unerwünschte Aktivitäten nutzen (z. B. Bitcoin-Mining) – gerade Letzteres kann behördliche Untersuchungen auslösen, die den Betrieb lahmlegen, und massive finanzielle Folgen haben. Diese Gefahren sind ernst zu nehmen: Eine Studie von IBM zeigt, dass sich Angriffe auf industrielle Kontrollsysteme in den vergangenen zwei Jahren mehr als verdoppelt haben.

Ein Problem liegt darin, dass in vielen Unternehmen in der Vergangenheit unterschiedliche Abteilungen für IT beziehungsweise OT zuständig gewesen sind, was zu unterschiedlichen Kulturen, Prioritäten und Wissensständen geführt hat. So treffen wir in vielen Unternehmen auf der einen Seite IT-Spezialisten an, welche zwar mit Fragen der Cyber Security vertraut sind, aber die OT-Landschaften und die damit verbundenen Betriebsprobleme ungenügend verstehen. Auf der anderen Seite sind die OT-Verantwortlichen, welchen wiederum ein vertieftes Bewusstsein für IT-Betriebs- und Sicherheitsfragen sowie das Verständnis für Cyber-Risiken fehlt. Mit Blick auf die Vergangenheit ist dieser Umstand verständlich, waren doch im OT-Umfeld stabile Prozesse und die damit verbundenen Ausfallsicherheiten prioritär. Aufgrund der isolierten Stellung benötigte die OT zudem nicht das gleiche Mass an Überwachung, Schutz und Aufsicht. Auch wurde die Datensicherheit in Bezug auf Unveränderbarkeit und Nachvollziehbarkeit vernachlässigt. Mit dem Sicherheitsblick auf die vernetzte Zukunft ist dieser Zwei-Welten-Zustand kaum mehr haltbar.

Nun ist es an den Chief Information Security Officers (CISO), die zwingend beide Welten kennen, ihre diesbezüglichen Hausaufgaben zu erledigen. Das heisst zum einen, ein gemeinsames, für IT und OT gleichermassen geltendes Verständnis für Cyber-Sicherheit zu schaffen; und zum anderen, Risiken für das gesamte System zu minimieren und Angriffe zu verhindern – oder schnell zu erkennen, sollten sie trotzdem passieren.

Fundierte Cyber-Risikoanalyse und individuelle Massnahmenpakete

Auf eine standardisierte Cyber-Security-Lösung kann ein CISO dabei nur bedingt zurückgreifen. Denn wie die Prozesse und Anlagen sind auch die Sicherheitsrisiken und die Strategien zu deren Minimierung von Unternehmen zu Unternehmen, von Branche zu Branche verschieden. In einer heutigen Industrieumgebung können zudem Anlagen und Geräte unterschiedlichster Hersteller aufeinandertreffen. Darum muss ein erster Schritt darin bestehen, die betriebseigene OT eingehend zu analysieren. Erst wenn ein CISO genau weiss, wie die OT im Betrieb genutzt wird und welchen Zwecken sie dient, kann er geeignete Massnahmenpakete zusammenstellen. Als oberste Schutzziele gelten dabei Vertraulichkeit, Datenintegrität, Authentizität und Verfügbarkeit. Dies bedeutet:

- **Vertraulichkeit**
  Nur Maschinen, Prozesse oder Personen, welche die Daten auch einsehen dürfen, sollen Zugang erhalten. Dabei sollen die Kunden der Hersteller, welche oftmals im selben Marktsegment agieren, von Verbesserungen profitieren, ohne die KPIs und Fabrikationsgeheimnisse preisgeben zu müssen.

- **Datenintegrität**
  Es muss sichergestellt werden, dass die Daten nicht modifiziert oder gelöscht und keine neuen Daten unbemerkt hinzugefügt werden können. Das gilt für Daten, die gerade verarbeitet werden, ebenso wie für solche, die im System gespeichert sind.

- **Authentizität**
  Die Vertrauenswürdigkeit und Echtheit der Knotenpunkte, die Daten senden und empfangen können, müssen jederzeit belegt werden können.

- **Verfügbarkeit**
  Korrekte, prozessrelevante Daten sind im richtigen Moment verfügbar.

Breite Cyber-Security-Strategie für sichere OT-Umgebung

Als zweiter Schritt steht eine individuelle, aber umfassende Cyber-Sicherheitsbedrohungs- und Risikobewertung an. Dabei wird analysiert, welchen grundsätzlichen Sicherheitsrisiken sich ein Unternehmen aussetzt, wenn ein OT-System an eine IT-Unternehmensinfrastruktur angeschlossen wird. Die Risikobewertung blickt dabei vom besser geschützten auf das weniger gut geschützte Umsystem, also in den meisten Fällen von der IT-Umgebung auf das OT-System. Typischerweise liegt ein besonderes Augenmerk auf Übergängen und Schnittstellen von OT und IT – also dort, wo Produktionsdaten zurück in Planungssysteme, ERP und Auftragsmanagement fliessen.

Basierend darauf kann der CISO in einem dritten Schritt damit beginnen, Massnahmen zu treffen. Dabei sollte er eine breit angelegte Cyber-Security-Strategie verfolgen, um langfristig eine funktionstüchtige, sichere und widerstandsfähige OT-Umgebung aufrechtzuerhalten. Grundsätzlich empfiehlt es sich, der Cyber-Sicherheit bereits bei der Auswahl eines neuen Geräts oder Steuersystems Beachtung zu schenken. Hersteller, die auf Security-by-Design setzen, sind zu bevorzugen. Weiter braucht es technische und organisatorische Massnahmen, um die Sicherheitsziele Vertraulichkeit, Datenintegrität, Authentizität und Verfügbarkeit zu gewährleisten. Hinzu kommen Werkzeuge, die dazu dienen, Angriffe zu erkennen und schnell darauf zu reagieren. Soll-Bruchstellen stellen definierte Übergänge zwischen IT und OT dar, welche während eines Vorfalls getrennt werden können, wobei trotzdem ein definierter Notbetrieb aufrechterhalten werden kann. Und schliesslich braucht es Mittel, um die Folgen eines erfolgreichen Cyber-Angriffs zu minimieren und sicherzustellen, dass der

Produktionsbetrieb schnell wieder aufgenommen werden kann. Diese Massnahmen und Prozesse müssen kontinuierlich überprüft und gegebenenfalls optimiert werden.

Zusammenarbeit über Bereichsgrenzen hinweg

Den Mitarbeitenden kommt im gesamten Prozess eine wichtige Rolle zu. Wichtig ist primär, dass Führungskräfte klar kommunizieren und unterstützen. Weiter ist die Zusammenarbeit über Bereichsgrenzen von IT und OT hinweg unerlässlich, wenn Massnahmen aus dem Gebiet der Cyber Security erfolgreich umgesetzt werden sollen. Und schliesslich braucht es gerade in der OT, einem Umfeld, das bislang wenig mit Cyber Security zu tun hatte, Programme, um Mitarbeitende für Fragen der Informations- und Datensicherheit zu sensibilisieren.

CyOne Security ist der kompetente Partner für die Umsetzung von OT-Schutzzielen

Informations- und Datensicherheit muss ein substanzieller Bestandteil in der Entwicklung und der Implementierung von OT sein. Da in OT-Systemen nicht nur Security (Sicherheit), sondern auch Safety (Schutz) eine entscheidende Rolle spielt, sollte zwingend sichergestellt werden, dass selbst bei einem Cyber-Vorfall keine Gefahr für Menschen und Umgebung besteht.

Um die vernetzten Geräte und Systeme vor den Bedrohungen aus dem Cyberspace zu schützen, bringt die CyOne Security jahrzehntelange Erfahrung und vertieftes Expertenwissen auf dem Gebiet der Cyber Security in die Sicherheitskonzepte und -lösungen ein.

Unternehmen profitieren von einer ganzheitlichen Betrachtungsweise und einer fundierten Analyse für Schnittstellen und Übergänge aus Datensicht. CyOne Security unterstützt Industriebetriebe bei der Umsetzung ihrer Schutzziele im OT-Umfeld und setzt dabei auf die 360°-Sicherheitskompetenz von Product Security, System Security und Operational Security.

Beginnen Sie heute und schützen Sie Ihre Operational Technology vor Cyber-Risiken.

Machen Sie den ersten Schritt: Analysieren Sie gemeinsam mit unseren Experten Ihre aktuellen und zukünftigen Sicherheitsbedürfnisse Ihrer Operational Technology, damit wir mit Ihnen über zielgerichtete Sicherheitslösungen diskutieren können.

Kontaktieren Sie uns für ein kostenloses Expertengespräch.