SocietyByte
Wissenschaftsmagazin des BFH-Zentrums Digital Society
https://www.societybyte.swiss

Unternehmen müssen auch Roboter vor Cyberattacken schützen

Autor : Roman Haltinner

Datum : 4. September 2019

Roboter sind die Schnittstelle, durch welche IT-Systeme ganz konkret auf die reale Welt einwirken. Gefahren für Mensch und Umwelt wurden bislang durch strikte Abgrenzung minimiert. Mit zunehmender Vernetzung, neuen Technologien und Formen der Zusammenarbeit wird diese Isolation aufgebrochen. Das stellt neue Anforderungen an die Cybersicherheit.

Noch bis vor wenigen Jahren standen Roboter in der Industrie fast ausschliesslich hinter trennenden Schutzeinrichtungen im Einsatz. Die Arbeitsbereiche von Mensch und Roboter waren strikt voneinander isoliert. Diese starre Trennung wird durch neue intelligente Robotertechnik aufgehoben: Sogenannte sensitive Roboter, die in der Lage sind, ihre Umgebung wahrzunehmen und mithilfe regelungstechnischer Methoden darauf zu reagieren, sind der Schlüssel für eine Zusammenarbeit zwischen Mensch und Maschine.

Wie Mensch und Maschine zusammenarbeiten

Es gibt drei Formen der Zusammenarbeit: Wenn eine Aufgabe nur durch Mensch und Roboter gemeinsam erledigt werden kann, also jeder seine speziellen Fähigkeiten einbringen muss, spricht man von Kollaboration. Ein Beispiel wäre das Platzieren eines sehr schweren oder heissen Objekts an einem Gegenstück, das sich aufgrund hoher Fertigungstoleranzen nicht immer an der gleichen Stelle be?ndet. Der Roboter bringt die nötige Leistung und Robustheit mit, der Mensch nutzt seine visuellen Fähigkeiten, um den Roboter zur richtigen Position zu führen. Echte Kollaboration ist in der Industrie bis dato selten anzutreffen, denn in Arbeitsschritten, die dafür in Frage kämen, ist eine Vollautomatisierung oft einfacher und günstiger.

Bei den Formen der Zusammenarbeit, die derzeit entwickelt werden oder bereits in Fertigungsprozesse integriert sind, handelt es sich in der Regel um Kooperation oder Koexistenz von Mensch und Roboter. Bei einer Kooperation teilen sie sich zwar einen Arbeitsplatz, arbeiten aber nie zeitgleich am selben Ort und an derselben Aufgabe. Vielmehr gibt es Schnittstellen zwischen sequenziellen Arbeitsprozessen; die Schritte ergänzen sich. Von einer Koexistenz wiederum spricht man, wenn lediglich die trennende Schutzeinrichtung wegfällt, die Arbeitsprozesse von Mensch und Roboter sich aber nicht überschneiden.

Neue Technologie, neue Risiken

Die Automatisierung von Geschäftsprozessen führt zu neuen Risiken. Das Thema Robotiksicherheit steht bei vielen Unternehmen bereits auf der digitalen Agenda. Alle Beteiligten – der Verwaltungsrat, die AktionärInnen und die KundInnen – erwarten, dass Unternehmen dieser Herausforderung genügend Aufmerksamkeit schenken. Das betrifft einerseits die physische Sicherheit – im Englischen "safety" – sowie andererseits die als "security" bezeichnete informationstechnische Cybersicherheit. Dabei müssen Unternehmen berücksichtigen, dass Security und Safety oft unterschiedliche Ziele verfolgen: Steht bei Safety zum Beispiel die Sicherung des Arbeiters vor den Bewegungen eines Roboterarmes im Vordergrund, so ist Security notwendig, um das Robotersystem vor einem unerlaubten Eingriff des Menschen zu schützen.

Der Bereich Security wird im Rahmen der Prozessautomatisierung mithilfe von Robotern (RPA, siehe Kasten) vor neue Herausforderungen gestellt. Zurecht fragen sich Unternehmen, welche Cyberrisiken mit dem Einsatz von Automatisierungstechnologien verbunden sind. Mit RPA stehen Hackern nämlich neue Angriffspunkte zur Verfügung, um sensible Daten oder sensible Informationen offenzulegen, zu stehlen, zu ändern oder zu zerstören. Zudem könnten Unbefugte auf nicht autorisierte Anwendungen und Systeme zugreifen und Schwachstellen ausnutzen, um weiteren Zugriff auf die Daten des Unternehmens zu erhalten. Und schliesslich besteht die Gefahr, dass ein "Denial of Service"-Angriff die Systeme eines Unternehmens mit so vielen Informationen bombardiert, dass die Produktion zum Erliegen kommt. (Vergleiche Abbildung 1 anhand von Bots)

Abbildung 1

Was Unternehmen tun können

Angesichts dieser Risiken ist es wichtig, dass die Geschäftsleitung das Thema Cybersicherheit im Zusammenhang mit dem Einsatz von Robotern ernst nimmt. Abbildung 2 zeigt Cyberdomänen, die in der Robotiksicherheit zentral sind. So kann eine ausreichende Priorisierung der Thematik in der gesamten Unternehmung erreicht und auf bestehenden Sicherheitsmassnahmen aufgebaut werden. Cybersicherheit muss als Bestandteil aller Betriebs- und Produktionsprozesse und somit als Längsschnittthema verstanden werden. Alle Mitarbeitenden – insbesondere diejenigen, die Teil der Betriebsprozesse sind – sollten sich der bestehenden Bedrohungen bewusst sein und ein entsprechendes Verhalten verinnerlichen.

Abbildung 2

Bereits die Auswahl der Hard- und Software stellt die Weichen für eine sichere Anwendung von Robotik im Unternehmen. Je weiter die Digitalisierung und Vernetzung voranschreitet, desto stärker wird bereits bei der Entwicklung von Hard- wie Software darauf geachtet, die Systeme so frei von Schwachstellen und so resistent gegen Cyberangriffe wie möglich zu konzipieren. In diesem Fall spricht man von "security by design". Das ist gerade bei komplexen Systemen und Anwendungen zentral: Bereits während der Konzeption einer Roboteranwendung müssen potenzielle Schwachstellen des Systems durch eine strukturierte Analyse identi?ziert werden.

Starkes Design, aber schwache Implementierung

Viele Schwachstellen, die bei Cyberangriffen ausgenützt werden, sind allerdings keine Designfehler, sondern entstehen während der Implementierung im Unternehmen. Ein erster Schritt zur Vermeidung von Sicherheitslücken liegt in der Analyse der Computercodes, die im Roboternetzwerk zum Einsatz kommen. Dazu stehen Unternehmen zahlreiche Werkzeuge zur Verfügung, die im Rahmen der statischen Codeanalyse automatisiert angewendet werden können.

Da viele Anwendungen zwangsweise verteilt in einem Netzwerk arbeiten, müssen die internen Kommunikationskanäle genauso gesichert werden wie eine Datenübertragung in externe Systeme. Dass Roboter und Sensoren zwar in einem komplexen Netzwerk physisch miteinander verbunden sind, aber dank maschinellem Lernen auch einen hohen Grad an Autonomie haben, macht diese Aufgabe besonders komplex: Eine Middleware-Schicht sorgt dafür, dass zum Beispiel Sensoren und Roboterarme ihre Funktionen unabhängig voneinander weiterentwickeln können. Diese Entkopplung bringt grosse Sicherheitsrisiken mit sich, da in diesem dynamischen Umfeld nicht mehr kontrolliert werden kann, wer Daten produziert

beziehungsweise konsumiert. Somit kann auch eine Manipulation des Daten?usses nicht erkannt werden.

Eine solche Middleware ist das Robot Operating System (ROS); sie findet sich mittlerweile immer häufiger auch in industriellen Anwendungen und Robotikprodukten. ROS sieht allerdings derzeit keine Mechanismen für Authenti?zierung, Autorisierung oder Sicherstellung der Datenintegrität vor – das müssen sich Anwender bewusst sein. Somit sind Roboter, die auf ROS basieren, inhärent anfällig für Cyberangriffe und Manipulationen. Allerdings werden derzeit Ansätze entwickelt, um ROS-Anwendungen besser vor Angreifern zu schützen. Es wird damit künftig möglich sein, für einzelne Elemente im Netzwerk Zerti?kate auszustellen, die deren Authentizität beweisen und auch ihre Berechtigung zum Senden und Empfangen von Daten regeln.

Daneben müssen Unternehmen auch darauf achten, dass die Speicherung von Daten und der Zugriff auf das System mit entsprechenden Massnahmen abgesichert sind. Dazu gehören Aspekte wie Schlüssel- und Zerti?katsspeicherung sowie geeignete Work?ows für die Wartung. Werden Zerti?kate nicht sicher aufbewahrt, ist auch eine Sicherung der Kommunikation zwecklos. Genauso wichtig ist es, dass nicht einfach Änderungen am System vorgenommen werden dürfen, daher muss während der Wartung, die oft nicht vor Ort sondern über einen Zugriff von aussen stattfindet, auch das Personal gegenüber dem Netzwerk des Unternehmens beziehungsweise der Maschine authenti?ziert werden. Erst danach darf über einen gesicherten Kanal eine Wartung vorgenommen werden. Hierbei empfiehlt es sich zudem, alle Aktionen während der Wartung unveränderbar zu protokollieren, damit sie später nachvollziehbar sind.

Widerstandsfähigkeit gegen Cyberangriffe ist das Ziel

Alle diese proaktiven Massnahmen dienen dazu, Angriffe zu erkennen und schnell darauf reagieren zu können. Es braucht aber auch organisatorische und technische Mittel, um die Folgen eines erfolgreichen Cyberangriffs zu minimieren und sicherzustellen, dass der Produktionsbetrieb schnell wieder aufgenommen werden kann. Die Sicherheit des Gesamtsystems steht somit im Mittelpunkt und muss als gemeinsames Schutzziel definiert werden. Hierfür wird auch neues Know-how für Mitarbeitende in vernetzten Produktionen nötig sein, das weit über die klassische IT-Sicherheit hinausgeht.

Es sind grosse Herausforderungen, die auf Unternehmen zukommen. Die Erkenntnis, jederzeit selbst Opfer von Cyberangriffen werden zu können, ist ein erster wichtiger Schritt. Um erfolgreich und verantwortungsvoll in der Industrie 4.0 tätig zu sein, ist es aber unerlässlich, zusammen mit kompetenten Partnern die richtigen Sicherheitstechnologien auszuwählen und zu implementieren.

Wie Unternehmen Robotersysteme nutzen

Unternehmen nutzen die Fähigkeit von Robotikplattformen, um Arbeitsabläufe zu automatisieren, zu koordinieren und kognitive Lernfunktionen auszuführen. Es herrscht oft Verwirrung darüber, was jeweils gemeint ist, wenn von Robotik die Rede ist. Im Allgemeinen

werden die folgenden drei Formen der Robotik angewendet:

- **Robotic Process Automation (RPA)** wird eingesetzt, um manuelle Aufgaben über verschiedene Geschäftsprozesse und Systeme hinweg bearbeiten zu können. Zu den typischen Aktivitäten gehören Dateneingabe, Datenmigration über mehrere Systeme, Datenbearbeitung, Datenabgleich und regelbasierte Entscheidungsfindung in Geschäftsprozessen.
- **Orchestration (OR)** konzentriert sich auf die Koordination von Automatisierungsaktionen. Ein Anwendungsbeispiel wäre die Abstimmung zwischen verschiedenen Bewegungssensoren und einem Roboterarm, dessen Bewegungen durch die Daten dieser Sensoren begrenzt werden.
- **Kognitives Lernen (CL)** geht über die regelbasierte Entscheidungsfindung hinaus und zielt darauf ab, komplexe Aufgaben ohne menschliche Interaktion zu erfüllen. Grundlage dafür sind selbstlernende Algorithmen. Ziel einer Anwendung könnte beispielsweise sein, dass Roboterarme durch Sensordaten lernen, wie gross ihr Bewegungsradius ist – bis zu dem Punkt, wo Sensoren letztlich überflüssig wären.