IT-Sicherheit in der Produktion

Auf einen Blick

- ☑ Bedrohung durch cyber-physikalische Angriffe auf Werkzeugmaschinen
- ☑ IFW untersucht Auswirkungen möglicher Angriffsszenarien
- ☑ Wissenschaftler bewerten Risiken und erarbeiten Schutzmöglichkeiten
- ☑ Live-Demonstrationen zur IT-Sicherheit am IFW geplant

07. 2019

IFW | Mit zunehmender Digitalisierung steigt die Gefahr, dass produzierende Unternehmen Opfer von Cyberkriminalität werden. Welche Ursachen und Auswirkungen cyber-physikalische Angriffe auf Produktionsanlagen haben und wie sich Unternehmen schützen können, erforscht das IFW.

Für produzierende Unternehmen ist die Digitalisierung Fluch und Segen zugleich. Vernetzte Maschinen ermöglichen höhere Produktivität, verbesserte Qualität und individualisierte Produkte. Gleichzeitig stellen sie die IT-Sicherheit vor neue Herausforderungen.

Kriminelle Angriffe über das Internet betreffen längst nicht mehr nur PCs an Büroarbeitsplätzen. Auch Maschinen und Anlagen stehen durch den steigenden Vernetzungsgrad immer häufiger im Visier. Cyber-physikalische Angriffe – das sind digitale Angriffe aus dem Netz, die an einer Maschine tatsächlichen Schaden anrichten können – erreichen mittlerweile Unternehmen aller Branchen. Doch zu wenige schützen sich: Eine Studie der ZVEI zeigt, dass nur 36 % der Unternehmen Richtlinien zur Umsetzung von IT-Sicherheitsmaßnahmen wie beispielsweise die IEC 62443 heranziehen.

Die Risiken unterschiedlicher Angriffsszenarien zu bewerten und passende Schutzmaßnahmen zu identifizieren ist das Ziel des Forschungsprojekts "IT-Sicherheit in der Produktion". Das Institut für Fertigungstechnik und Werkzeugmaschinen (IFW) arbeitet im Rahmen des Production Innovations Network (PIN) mit den Unternehmen Tomorrow Labs und Kaspersky Lab zusammen. Gemeinsam wollen sie verschiedene Szenarien von cyber-physikalischen Angriffen testen und analysieren. Dazu haben sie ein abgeschlossenes Netzwerk aufgebaut, das aus Maschinensteuerung, virtueller Prozesssimulation sowie Netzwerküberwachung besteht.

Angreifer können die Produktion manipulieren

Vom Totalausfall einer Maschine über verminderte Produktivität und Qualität bis hin zum Datendiebstahl: Cyber-physikalische Angriffe können ganz unterschiedliche Auswirkungen haben. Das IFW hat im Rahmen des Forschungsprojekts potentielle Angriffsszenarien erarbeitet und entsprechend ihrer Auswirkungen kategorisiert.

Dazu zählen als erstes Angriffe, die zu einem Totalausfall der Maschine führen und damit erhebliche Auswirkungen auf die Produktion haben. Ein Totalausfall kann beispielsweise durch einen Spindelcrash verursacht werden, der durch Manipulation der Achsbewegungen realisiert wird. Zudem können sicherheitsrelevante Steuerungsfunktionen wie das Schließen der Maschinentür manipuliert werden oder Maschinenstopps im NC-Code eingebaut werden – beides führt zu einem temporären Ausfall der Maschine.

Auch die Produktivität der Fertigungsanlage kann durch cyber-physische Angriffe reduziert werden. Dies kann zum Beispiel durch Reduzierung des Vorschubs, Minderung der Eilganggeschwindigkeit oder Verlängerung der Verfahrwege innerhalb der Maschinensteuerung erreicht werden. Besonders unangenehm sind dabei minimale Parametermanipulationen, die im Produktionsalltag nicht sofort entdeckt werden, die Produktivität jedoch langfristig senken.

Um die Bauteilqualität zu vermindern, könnten Angreifer den Werkzeug-Durchmesser in der Werkzeugliste oder die Nullpunkt¬verschiebung manipulieren. Auch durch Änderungen des Werkzeugwegs oder die Auswahl ungeeigneter Vorschub- sowie Schnittgeschwindigkeiten kann dies geschehen.

Ferner können cyber-kriminelle Angriffe auf Produktionsanlagen genutzt werden, um Industriespionage zu betreiben. Angreifer könnten beispielsweise den NC-Code auf der Steuerung auslesen, Fertigungsprogramme identifizieren und Produktivitäts-Kennzahlen stehlen.

Wissenschaftler nutzen virtuelle Maschine für Test-Angriffe

Während in produzierenden Unternehmen echte Werkzeugmaschinen als potentielle Angriffsziele bereitstehen, wird im Forschungsprojekt eine zum Teil virtuelle Maschine genutzt. Die genutzte Nachbildung einer Werkzeugmaschine besteht aus einer Siemenssteuerung vom Typ 840D sl, wie sie in vielen Werkzeugmaschinen verbaut ist (siehe Bild 3). Diese Steuerung ist nach entsprechender Konfiguration in der Lage, NC-Codes identisch zu einer realen Maschine abzuarbeiten und somit die Bewegungen der Achsen vorzugeben.

Die Vorgaben für die Achsbewegungen nutzt das IFW für eine Materialabtragssimulation in der hauseigenen Software IFW CutS (siehe Bild 4). In der Simulation können Werkzeug und Werkstück entsprechend dem Vorbild eines realen Prozesses definiert werden. Während die Steuerung ein

NC-Programm abarbeitet, werden auf Basis der Achsdaten virtuelle Achsen verfahren, wodurch ein virtuelles Werkstück bearbeitet wird.

Durch die Kopplung einer realen Steuerung mit einer virtuellen Prozesssimulation schaffen die Wissenschaftler ein Umfeld, in dem Auswirkungen von Manipulationen gefahrlos erfasst und analysiert werden können.

Wie lassen sich Werkzeugmaschinen vor Cyberkriminalität schützen?

Um die wirtschaftlichen Auswirkungen von Cyber-Angriffen darzustellen, verwenden die Wissenschaftler die Software TomorrowConnect, die vom Projektpartner Tomorrow Labs zur Verfügung gestellt wird. Die Software liest Daten aus der Steuerung über eine OPC-UA Verbindung aus und aggregiert diese zu Kennzahlen, wie beispielsweise der mittleren Bearbeitungszeit pro Bauteil. Die Kennzahlen werden von den Auswirkungen der Cyber-Angriffe beeinflusst, sodass insbesondere Produktivitätseinbußen visualisiert werden können. Sobald der Soll-Zustand des produzierenden Systems erfasst ist, können Abweichungen dargestellt werden.

Zeitgleich überwacht die Software Kaspersky Industrial CyberSecurity (KICS) des Projektpartners Kaspersky Lab den gesamten Netzwerkverkehr mit dem Ziel, Anomalien zu erkennen. Bei Cyber-Angriffen werden zum Beispiel zusätzliche Datenpakete im Netzwerk versandt. Wird eine solche Anomalie erkannt, wird diese anschließend gemeldet.

Nachdem die Wissenschaftler ihre Test-Angriffe durchgeführt und ausgewertet haben, werden sie die Ergebnisse nutzen, um Schutzmaßnahmen für Werkzeugmaschinen zu erarbeiten. Die Testumgebung werden sie am Ende verwenden, um interessierte Personen aus Industrie und Forschung für IT-Sicherheit zu sensibilisieren: In Live-Demonstrationen wird das IFW sowohl die Auswirkungen erfolgreicher Cyber-Angriffe als auch die entsprechenden Schutzmechanismen zeigen.

Förderhinweis

Das Forschungsprojekt "IT-Sicherheit in der Produktion" wurde durch den Arbeitskreis Digitale Fertigung innerhalb des Produktion Innovation Network (PIN) initiiert und wird durch diesen unterstützt.

von Sven Friebe und Julia Huuk

E-Mail: friebe@ifw.uni-hannover.de
Tel.: (0511) 762-18074
Webseite: www.ifw.uni-hannover.de