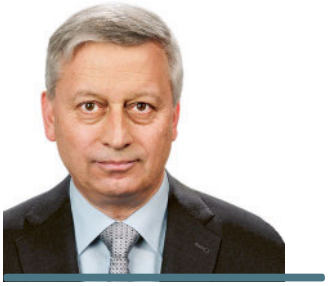
Industrie 4.0:
IT Security first

Max Felser
Professor für industrielle Netzwerke, Leiter Studiengang Elektrotechnik und Informationstechnologie, BFH

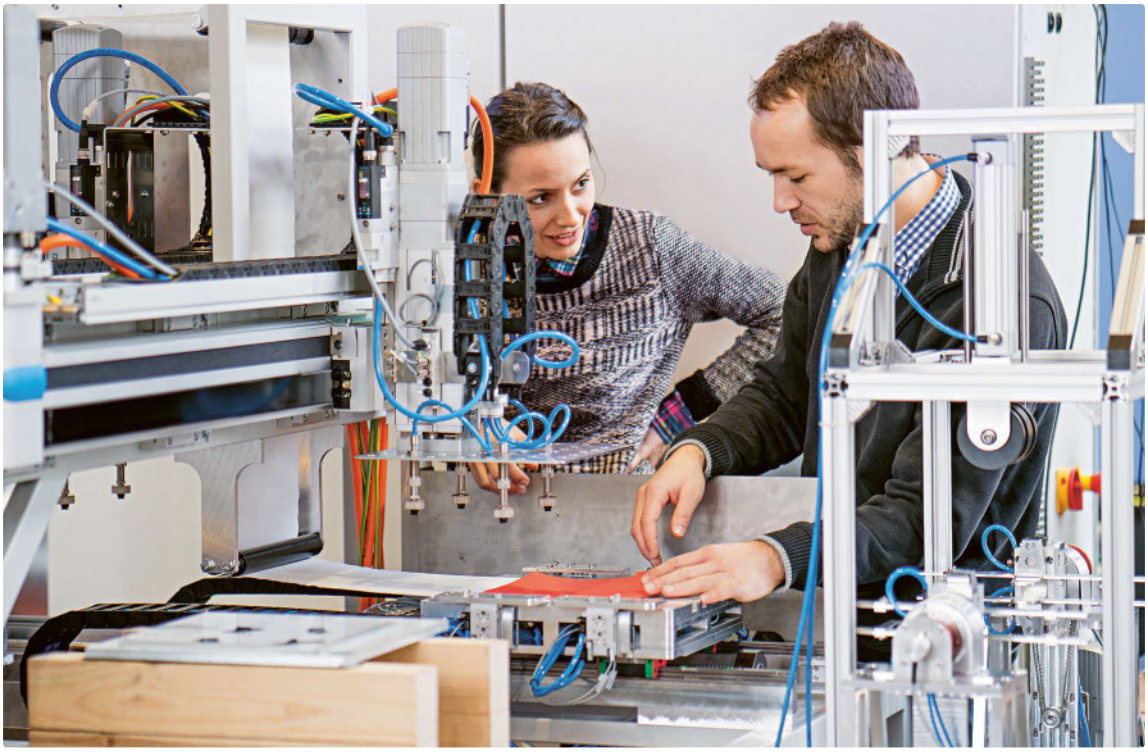


Rolf Lanz
Professor für sichere Kommunikationssysteme, BFH

Industrie 4.0 ist in aller Munde: Die Vernetzung der industriellen Produktion mit moderner Informationstechnik schafft viele neue Möglichkeiten. Sie sorgt aber auch für grosse Risiken und gefährdet das Vertrauen der Konsumenten und Unternehmer. «Wenn wir so weiterfahren wie heute, machen wir uns sehr angreifbar», sagen die Professoren Max Felser und Rolf Lanz von der Berner Fachhochschule.

Viele Unternehmer sehen in der Industrie 4.0 das Heil der Zukunft: Der Begriff steht für die vierte industrielle Revolution, die nach Ansicht von Experten erst begonnen hat. Dank der Digitalisierung lässt sich die industrielle Produktion komplett mit neuer Informationstechnologie verzahnen. Die Vernetzung sämtlicher am Produktions- und Geschäftsprozess beteiligten Mittel und Parteien soll letztlich zu einer Verbesserung der Prozesse und zu einer Steigerung der Produktion führen.

«Die Automatisierung, die man heute oft auch als Operation Technology (OT) bezeichnet, wird in der Industrie 4.0 mit Informationstechnologie (IT) verbunden», sagt Max Felser, Professor für Elektrotechnik und Informationstechnologie an der BFH. Diese Vernetzung berge aber auch Gefahren. «Bei der OT gibt es traditionell ein grosses Vertrauen in die Integrität der eingesetzten Komponenten. Diese werden zuerst ausführlich geprüft und sollen danach in einem autonomen System möglichst lange unverändert funktionieren.» Für die Trennung von der IT sorgte bislang Feldbus-Technik. Doch mit der Vernetzung und den neuen Möglichkeiten der Digitalisierung ist das Automatisierungsmotto «Never change a running system» überholt. «In der Industrie 4.0 muss sich auch die OT den Gefahren stellen, die in der Welt der IT lauern», betont Felser und spricht dabei insbesondere böswillige Attacken an. «Malware



Nur unter Beachtung der IT-Security ist das gewünschte Vertrauen in Industrie 4.0 zu erreichen.

kann Rechner und ganze Netzwerke in ihrer Funktionalität beeinflussen oder lahmlegen. Solche Schadprogramme werden ganz bewusst zu diesem Zweck hergestellt.»

Wie weitreichend die Folgen von böswilligen Angriffen sein können, zeigte im Oktober 2016 das Botnetz «Mi-rai». Eine riesige Anzahl schlecht geschützter Geräte wurde gehackt und für einen massiven DDoS-Angriff (Distributed Denial of Service) auf den Infrastrukturanbieter «Dyn» genutzt. Das Versagen von dessen DNS-Services führte zum Ausfall von zahlreichen Internetdiensten wie Amazon, Spotify und Netflix sowie von Cloud-Anbietern. Da fortschrittliche Firmen über eine Datenanbindung an die Cloud verfügen, kann ein solcher Angriff zum Stillstand der Produktion führen.

Rolf Lanz fordert generelles Umdenken

Weil die Feldbusse in der industriellen Produktion im Rahmen der Digitalisierung durch Netzwerke ergänzt oder ersetzt wurden, ist unter Umständen die ganze Produktion gefährdet. «Wenn wir weiterhin so verfahren wie jetzt, machen wir uns sehr angreifbar», warnt Rolf Lanz, Professor für sichere Kommunikationssysteme an der BFH, und fordert ein Umdenken. Bei der Automatisierung werde kaum oder erst zu spät an die IT-Sicherheit gedacht. «Dabei ist dies bei komplett vernetzten Systemen, die auf dem Internet basieren, elementar.» Heute hinke deshalb die IT Security hinterher und müsse fast jeden Tag neue Sicherheits-Updates liefern. «Dabei ist es eigentlich fast gar nicht mehr möglich, nachträglich für Sicherheit zu sorgen, wenn nicht von Anfang an daran gedacht wurde.»

An der BFH gibt es seit fast 20 Jahren Weiterbildungskurse für IT-Sicherheit. Sicherheit ist auch fixer Bestandteil der Studien in Informatik und Elektrotechnik. «Unsere Studierenden sind für diese Themen sensibilisiert, werden dann aber in der Wirtschaft schnell mit der Realität konfrontiert», sagt Lanz. «Dort kommen Sicherheitsaspekte durch sportliche Zeitpläne und knappe Budgets schnell unter Druck.» Dabei sei es heute entscheidend, dass IT-Sicherheit ein Bestandteil des Gesamtsystems werde, betont Lanz. «Die Sicherheit müsste sogar die Basisfunktionalität jedes Programms sein, noch bevor die gewünschten spezifischen Anforderungen hinzugefügt werden.» An seinen Kursen an der BFH zeige er deshalb auf, wie angreifbar vernetzte Systeme seien. «Ich zeige aber auch, wie leicht man die Sicherheit verbessern kann und wie viel sicherer die Systeme durch bezahlbaren Aufwand werden.»

Firewalls, Sniffer & Co.

Während Sicherheitsspezialist Rolf Lanz ein generelles Umdenken in der Branche fordert, zählt Max Felser weitere Lösungsansätze auf. «Die OT muss lernen, dass es nach der Vernetzung mit der IT keine absolute Sicherheit mehr gibt. Schutzmassnahmen, welche die Automatisierung verteuern, müssen geplant und umgesetzt werden.» Zum einen greifen Massnahmen, die sich in der IT bewährt haben, auch hier: die Verschlüsselung von Meldungen, die Identifizierung mit Benutzernamen, Passwörtern und zusätzlichen Schlüsseln oder die Abgrenzung von Systemen mit Firewalls und «demilitarisierten Zonen» (DMZ). In geschützten Zonen könnten zudem «Sniffer» eingesetzt werden: Programme, die den Datenverkehr überwachen und bei Auffälligkeiten Alarm schlagen. Das helfe bei der Vorbereitung auf zukünftige Schädlinge, sagt Felser.

Die Bedeutung von Edge-Gateways steigt

Wichtig sei aber auch, dass in der Industrie 4.0 Informationen in «wichtig» und «weniger wichtig» aufgeteilt würden. «So kann man entscheiden, welche Teile der OT man ganz bewusst nicht mit der IT verbindet, auch wenn dies der Philosophie der Industrie 4.0 zuwiderläuft.» In diesem Bereich kommt der Edge-Gateway ins Spiel: Dieses Gerät koppelt Automatisierungsnetzwerke sicher an eine Cloud oder eine Applikation für das Internet of Things (IoT). «Es sammelt als Stellvertreter der IT-Welt die Informationen in der OT ein und sendet diese, ergänzt mit den notwendigen Sicherheitsmassnahmen, an vertrauenswürdige Cloud-Anwendungen», erklärt Felser. «Es ist die einzige Schnittstelle, die Befehle von der IT an die OT weiterreicht. Ganz nach dem Motto ‹Vertrauen ist gut, Kontrolle ist besser›.»

Das Konzept der Edge-Gateways und weitere Massnahmen werden an der BFH in den Kursen zu Industrial Internet of Things (IIoT) erläutert und in praktischen Vorführungen präsentiert.

Kontakt
- max.felser@bfh.ch
- rolf.lanz@bfh.ch

Infos
- i3s.bfh.ch
- smartfactory.ch
- ti.bfh.ch/informatik
- ti.bfh.ch/elektro
- ti.bfh.ch/weiterbildung

Video zu Industrie 4-0 auf
spirit.bfh.ch › IT Security first

Swiss Smart Factory und Industrie 4.0

Die Swiss Smart Factory (SSF) in Ipsach will der Schweizer Wirtschaft die Industrie 4.0 näherbringen. SSF ist Teil des Switzerland Innovation Parks Biel/Bienne. Das Unternehmen forscht, entwickelt, betreibt industrielle Demonstrationsanlagen und will den Wissensaustausch zwischen Forschung und Wirtschaft fördern. Mehrere Hochschulen, darunter auch die BFH, und über zehn Industriepartner haben sich der SSF bisher angeschlossen.