Paarung von IT und Fertigung mischt Karten auf beiden Feldern neu

Chancen und Risiken mit Industrie 4.0

Deutschland ist eine Industrie-Nation mit einem weltberühmten Ruf für die Fähigkeiten seiner Ingenieure. Für die Fähigkeiten und Ideen im Bereich der IT und IT-Sicherheit sind eher andere Nationen bekannt. Aber mit Industrie 4.0 bietet sich für Deutschland die Möglichkeit, auch in diesem Bereich international Fuß zu fassen: Das Land ist gerade dabei, als Vorreiter aus der Atomenergie auszusteigen und auf alternative Energien umzusteigen. Dafür sind intelligente Stromnetze erforderlich, die an das Internet angeschlossen sind. Das heißt, alle bekanntgewordenen Angriffe im Internet sind auch auf die Stromversorgung anwendbar. Die Elektromobilität mit all ihren Vorteilen macht auch Fahrzeuge und Verkehrsinfrastrukturen angreifbar, weil diese miteinander und im Internet verbunden sind. Industrie 4.0 bedeutet für die deutsche Industrie viele positive Perspektiven, aber auch neue IT-Sicherheitsrisiken, denen angemessen entgegenzuwirken ist. Die zukünftigen Angriffe werden die damit verbundenen Schäden von heute noch deutlich überschreiten!

Hinter dem Begriff Industrie 4.0 verbirgt sich die vierte Stufe der industriellen Revolution. Die erste Stufe begann am Ende des 18. Jahrhunderts mit der Erfindung der Dampfmaschinen und bezeichnet die mechanische Fertigung. Stufe zwei bezieht sich auf die Nutzung elektrischer Energie zur Massenproduktion zu Beginn des 20. Jahrhunderts. Mit Hilfe von Elektronik und Informationstechnologie entstanden speicherprogrammierbare Steuerungen (kurz SPS), welche die weitere Automatisierung der Produktion vorantrieben. Ab Mitte der 70ger Jahre des 20. Jahrhunderts war diese dritte Stufe erreicht. Heute bildet das Internet der Dinge und Dienste mit der Vernetzung von allem und jedem den Grundstein für die Gesellschaft und die Industrie von morgen. Die Einführung von „Cyber-Physischen Systemen" (kurz CPS) bildet für die industrielle Produktion die Schnittstelle zum globalen Netzwerk und damit die vierte Stufe.

Warum diese neue Stufe im Prozess der automatisierten Produktion eine große Chance für Deutschland als Standort bildet, lässt sich wie folgt am besten verdeutlichen. „Deutschland ist Export-Weltmeister" – Diese Aussage ist weit verbreitet und die Tatsache, dass Deutschland eine der führenden Exportnationen weltweit ist, führte auch schon zu Bedenken der Europäischen Kommission (1). Schaut man auf die Zahlen des Statistischen Bundesamtes, sieht es für Deutschland in der Tat sehr gut aus: Im Jahr 2012 landet Deutschland auf Platz drei der Top-20-Exportländer der Welt, mit einem Volumen von 1.407,10 Milliarden US-Dollar. Das ist knapp hinter den USA (1.547,28 Milliarden US-Dollar) auf Platz zwei, aber schon deutlich vor Japan auf Platz vier mit 798,57 Milliarden US-Dollar. Wird dieses Volumen nun nach den Güterabteilungen aufgeschlüsselt, zeigt sich direkt, warum eine neue Stufe in der industriellen Produktion einen großen Teil deutscher Industrie betrifft. Platz eins belegen Kraftwagen und Kraftwagenteile mit einem Volumen von 189,98 Milliarden Euro, gefolgt von Maschinen auf Platz zwei mit 163,59 Milliarden Euro. Im internationalen Vergleich liegt Deutschland mit einem Volumen von 250 Milliarden Euro im Jahr 2012 auf Platz vier für den Bereich Maschinenbau. Diese Zahlen zeigen anschaulich, warum Deutschland jede Entwicklung für den Bereich der industriellen Produktion nicht nur mitmachen, sondern am besten anführen sollte.

Um die Spitzenreiterrolle zu festigen, hat die Bundesregierung unter Federführung des BMBF und BMWi das Zukunftsprojekt Industrie 4.0 ins Leben gerufen. Nach Initiierung der Promotorengruppe KOMMUNIKATION durch die Forschungsunion (FU) Wirtschaft-Wissenschaft Ende 2011 wurde im Januar 2012 der Abschlussbericht des Arbeitskreises Industrie 4.0 vorgelegt. Dieser enthält weiterführende strategische Empfehlungen für die Umsetzung des Zukunftsprojekts. Darüber hinaus reklamiert er Handlungsbedarf für folgende Tätigkeitsfelder: Standardisierung und Referenzarchitektur, Beherrschung komplexer Systeme, flächendeckende Breitbandinfrastruktur für die Industrie, Sicherheit, Arbeitsorganisation und -gestaltung, Aus- und Weiterbildung, rechtliche Rahmenbedingungen und Ressourceneffizienz. Der Bereich Sicherheit umfasst sowohl Sicherheit für die Menschen, welche die Maschinen bedienen, als auch Schutz der Produkte und Maschinen selbst vor unbefugtem Zugriff durch eindeutigen Identitätsnachweis. Für die IT-Sicherheitsindustrie in Deutschland ist vor allem Letzteres von großer Bedeu-

tung, bietet dieses Feld doch den ansässigen Unternehmen neue Möglichkeiten der Kooperation sowie des Aus- und Aufbaus von Kompetenzen für den Bereich CPS.

Das derzeit größte Projekt im Zukunftsfeld Industrie 4.0 ist der „it's OWL"-Spitzencluster (2) und umfasst 45 Forschungsprojekte von 174 Unternehmen, Hochschulen und weiteren Partnern. Die Forschungsprojekte gliedern sich wie folgt: In Innovationsprojekten werden neue Produkte und Anwendungen zur Marktreife gebracht. Bei Querschnittsprojekten werden neue Technologien und Methoden für intelligente technische System entwickelt. Die Nachhaltigkeitsmaßnahmen sichern die Entwicklungsdynamik und stärken die Wettbewerbsfähigkeit der Unternehmen. Anhand dieser Projekte ist gut ersichtlich, dass die ersten Schritte getan wurden, und je tiefer man in die Materie einsteigt, desto mehr Handlungsfelder und Potenzial erkennt man.

Industrie 4.0 in der Praxis

Wie verändert Industrie 4.0 die Produktion in Deutschland? Welche Auswirkungen hat die Art und Weise, wie wir arbeiten? Um diese und andere Fragen zu beantworten, wird an dieser Stelle ein Beispiel für Industrie 4.0 eingeführt.

Die Firma PlastikPop ist auf die Herstellung von Plastikprodukten für die Lebensmittel- und Kosmetikindustrie spezialisiert und bietet dank Industrie 4.0 eine große Auswahl an individualisierbaren Produkten an. Das Unternehmen Pepper möchte für das zehnjährige Jubiläum seiner Linie Peppers Popcorn eine Jubiläumsverpackung herausbringen. Auf der Webseite von PlastikPop werden die gewünschte Form und Farbe ausgewählt und die Vorlagen für den Aufdruck eingestellt und abgeschickt. Nachdem der Auftrag für die Produktion von 10.000 Stück Plastikeimern für Popcorn eingegangen ist, erhält der Schichtleiter eine Mitteilung auf seinem Tablet und einen Vorschlag, wie die geänderte Auftragslage am besten in die momentane Situation eingearbeitet werden kann. Er begutachtet den Vorschlag und bestätigt ihn. Bei der produzierenden Maschine müssen das Werkzeug ausgetauscht und die Zusammensetzung des Plastiks geändert werden. Ein Werkzeugmechaniker des Betriebs erhält auf seinem Tablet eine Nachricht mit dem Arbeitsauftrag zum Wechseln des Werkzeugs. Der Maschinenführer erhält die Nachricht über den neuen Auftrag und auf seiner Zugangskarte die Berechtigung für den Zutritt zum Lager. Hier kann er das gerade fertig gemixte Granulat für die Eimer abholen. Das Gemisch wurde automatisch fertig gestellt, nachdem der Schichtleiter die Produktion abgesegnet hatte. Die Etiketten zur Bedruckung der Eimer werden parallel erzeugt und für die Produktionsstraße bereitgestellt. Nach Fertigstellung der Eimer und Qualitätsprüfung werden diese per Express an den Lebensmittelhersteller versendet. Der Auftrag hierfür wurde automatisch vom System generiert, nachdem berechnet wurde, wann die Produktion abgeschlossen sein würde.

Anhand dieses Beispiels lassen sich sehr wichtige Fragestellungen verdeutlichen, die vor der Nutzung von Industrie 4.0 geklärt werden müssen. Einer der Vorteile von Industrie 4.0 soll es sein, dass Menschen die Maschinen in ihrer Umgebung besser steuern können. Informationen über Status und Zustand der Maschinen und Produkte sollen direkt abrufbar sein. Aus diesem Grund ist die erste wichtige Frage:

Wie erkenne ich Dinge, die steuerbar beziehungsweise über die Informationen abrufbar sind?

Stellen wir uns den Arbeitsablauf des Werkzeugmechanikers aus dem Beispiel vor. Er erhält einen Auftrag zum Wechseln eines Werkzeugs. Woran kann er nun steuerbare Dinge in seinem Arbeitsumfeld erkennen? Eine Möglichkeit wäre, dass er automatisch zu seinem Auftrag eine Anleitung mit Arbeitsanweisungen, vielleicht sogar mit Bildern, erhält. Wenn er vor Ort aber feststellt, das es nötig ist auch weitere Geräte zu steuern, wie kann er diese nun identifizieren? Gibt es einen Lageplan der Produktionshalle, welchen er abrufen kann, um dann anhand seines Standorts die nächsten Geräte angezeigt zu bekommen? Die sich aus dieser Situation weiter ergebende Frage lautet zwangsläufig:

Wie erhalte ich die Berechtigung zum Steuern/Informationsabruf?

Hat der Mechaniker die Geräte identifiziert, welche er steuern muss beziehungsweise über welche er Informationen abrufen möchte, wie kann er sich nun gegenüber der Maschine als berechtigte Person ausweisen? Woher weiß die Maschine, dass eine neue Person unter Umständen temporäre oder persistente Berechtigungen hat? Ein Weg führt über den Informationsaustausch durch den neuen Auftrag: Das System identifiziert alle nötigen Geräte und erteilt den Personen automatisch die Berechtigungen. Die Maschinen selber erhalten die Nachrichten automatisch per Push-Nachricht oder rufen diese im Falle einer Anmeldung von der zentralen Stelle ab. Für fest installierte Geräte ist dieser Weg bestimmt der zielführendste. Wie sich diese Problematik jedoch bei mobilen Dingen wie zum Beispiel fertigen Produkten verhält, ist eine wichtige weitere Frage die geklärt werden muss. Ist der Mechaniker nun berechtigt, seine Umgebung zu steuern, ist die nächste Frage:

Wie steuere ich Geräte unterschiedlicher Hersteller?

Gerade in Deutschland existiert für verschiedene Bereiche eine Fülle von Anbietern mit guten Produkten. In Unternehmen werden viele Maschinen unterschiedlicher Hersteller eingesetzt. Diese Diversität führt unter dem Aspekt Industrie 4.0 zu der Frage, wie diese Geräte und Systeme miteinander kommunizieren und agieren können. Der Lösungsweg führt hier über neue Standards. Diese müssen sowohl für die Kommunikationsprotokolle als auch für standardisierte Sicherheitsmodule wie etwa TPM (Trusted Platform Module) neu entwickelt oder angepasst werden. Unter dem Gesichtspunkt der Sicherheit sollten die neuen Entwicklungen natürlich von vornherein aktuelle Konzepte und Implementierungen der IT-Sicherheit mit beinhalten. Hierbei stellt sich zwangsläufig die Frage:

Bedeutet mehr Integration und mehr Interaktion mit anderen Komponenten weniger Sicherheit?

Die Ursache liegt hier in einer einfachen Tatsache: Je mehr unterschiedliche Techniken und Protokolle unterstützt werden, desto größer ist die Angriffsfläche des Gerätes. Das Einbinden von Schnittstellen, die man unter Umständen nicht selbst bereitgestellt hat, führt dazu, dass man sich auf andere verlassen muss. Das beste Beispiel hierfür ist Microsoft mit seinem Betriebs-

system Windows: Es unterstützt viele weitere Programme wie zum Beispiel die Produkte von Adobe, aber wenn in diesen Sicherheitslücken vorkommen, ist meist auch das Betriebssystem selbst in Gefahr. Für den Mechaniker in der Fabrik der Zukunft sähe das Szenario wie folgt aus: Sein Tablet zur Steuerung und für den Informationsabruf muss nicht nur die gängigen Anwendungen für die innerbetriebliche Kommunikation unterstützen, sondern auch die Steuerungen für Maschinen unterschiedlicher Hersteller. An dieser Stelle kommt die neue Herausforderung und Chance für die deutsche IT-Sicherheitsbranche ins Spiel. Denn mehr Integration und mehr Interaktion mit anderen Komponenten bedeutet nicht zwangsläufig weniger Sicherheit! Wenn die Partner eng zusammen an Sicherheitslösungen arbeiten, kann das Maß an Sicherheit der Komponenten und deren Zusammenspiel wesentlich erhöht werden.

Hierfür bietet Deutschland im Gegensatz zu anderen Märkten wie zum Beispiel den Vereinigten Staaten die besten Voraussetzungen. Deutschland hat sehr viele mittelständische Unternehmen mit einem hohen Maß an Innovation in den wichtigen Bereichen für das Projekt Industrie 4.0. Die Probleme der Integration und verschiedener Techniken müssen hierzulande gelöst werden. Gelingt das, ist dies der Erfolgsgarant für die Marktführung in diesem Bereich. Deutschland ist aufgrund der industriellen Struktur mit einem breit gefächerten Mittelstand und seiner Einstellung gegenüber Dingen wie Standards und Zertifizierungen wie geschaffen dafür, diese Probleme zu lösen.

Im Gegensatz hierzu sind amerikanische Unternehmen eher monopolistisch ausgelegt und kaufen sich Innovation von außen ein, um diese in ihre Systeme zu integrieren. Die wenigen großen Global Player wollen alles aus einer Hand anbieten und richten ihre Strategie hierauf aus. Dies bietet natürlich auch viele Vorteile für das Unternehmen, weil die Technik den eigenen Bedürfnissen an Integration angepasst werden kann. Der Vorteil für das Unternehmen ist aber in vielen Fällen der Nachteil für die Kunden, wenn es um Interoperabilität geht. Als Beispiel: Apple implementiert in seinen iPhones keinen Datenaustausch per Bluetooth mit Handys anderer Hersteller.

Wenn es ums Thema Sicherheit geht, geht es auch immer um Vertrauen und Verantwortung. Im Zuge einer Umstellung auf Industrie 4.0 und des Ausbaus des Internets der Dinge und Dienste ist zu klären, welche Institutionen hier die Federführung übernehmen. Wer die Verantwortung für eine gemeinsame und vor allem notwendige IT-Sicherheitsinfrastruktur für bestehende und zukünftige PKIs, die Namensgebung in den neu erschlossenen Bereichen sowie die Personalisierung von Sicherheitsmodulen für die jeweiligen Produkte übernimmt, ist von zentraler Bedeutung.

Denn bei allen Vorteilen von Industrie 4.0 ist nicht außer Acht zu lassen, dass mit der vollständigen Verzahnung der Industrie mit dem Internet auch viele neue Angriffsmöglichkeiten entstehen. Hierbei sind nicht mehr nur die Webseiten der Unternehmen das Ziel von DDoS-Angriffen aus dem Internet, sondern vielleicht direkt die Produktion oder ähnlich kritische IT-Systeme wie der Warenversand. Hier gilt es durch die konsequente Anwendung von bewährten und neuen Strategien und Techniken die IT-Sicherheit der Unternehmensnetzwerke sicherzustellen. Gerade wenn die großen Militärnationen der Welt immer mehr Geld in den Aufbau von digitalen Streitkräften investieren und auch schon erfolgreich Feldzüge durchführen (China, USA), sollte beim Thema Industrie 4.0 auch an den Schutz der heimischen Industrie gedacht werden. Die USA haben schon im letzten Jahr begonnen, ihr Personal für den Krieg im Internet um das Fünffache aufzustocken (3) und binden die großen IT-Unternehmen in ihre Spionagetätigkeiten mit ein. Dass es für diese neue Art der Kriegsführung oder Informationsbeschaffung auf den ersten Blick keine Grenzen gibt, zeigte dann auch spätestens der NSA-Skandal. Spionage und der digitale Krieg im Internet verschwimmen hier zu einer neuen, bisher unbekannten Form des Angriffs auf Werte.

Setzen sich auch unter diesem Gesichtspunkt IT-Sicherheitstechniken und -Produkte aus Deutschland durch, gibt dies der Aussage „IT-Security made in Germany" eine ganz neue Dimension und eine gute Position auf dem globalen Markt. Damit wäre „Made in Germany" nicht nur ein Zeichen für Qualität, sondern auch ein Zeichen für Vertrauen und Sicherheit.

Gerade Deutschland hat kulturell und gesetzlich, aber auch in der IT-Sicherheitsforschung und in der IT-Sicherheitsindustrie die idealen Voraussetzungen, einen wichtigen Beitrag zu einer sicheren und vertrauenswürdigen Industrie 4.0 zu leisten. Die schon vorhandenen innovativen und wirkungsvollen IT-Sicherheitsmechanismen aus Deutschland müssen konsequent eingesetzt werden. Anreize für die Wirtschaft müssen geschaffen und die IT-Sicherheitsforschung muss noch stärker gefördert werden. Nur so lassen sich die vielen positiven Möglichkeiten in Zukunft vertrauenswürdig nutzen und nur so lässt sich ein wirksamer Schutz vor neuen Angriffen aufbauen. ■

CHRISTIAN NORDLOHNE,
wissenschaftlicher Mitarbeiter am Institut für Internet-Sicherheit der Westfälischen Hochschule Gelsenkirchen und Projektleiter für den Bereich Botnetze.

NORBERT POHLMANN,
Informatikprofessor für Verteilte Systeme und Informationssicherheit sowie geschäftsführender Direktor des Instituts für Internet-Sicherheit – if(is) an der Westfälischen Hochschule Gelsenkirchen

1) *http://www.focus.de/finanzen/news/eu-untersuchung-deutschland-droht-wegen-exportstaerke-milliardenstrafe-der-eu_aid_1157270.html*
2) *http://www.its-owl.de/home/*
3) *http://www.spiegel.de/netzwelt/netzpolitik/us-cyber-command-aufruestung-um-das-fuenffache-a-879990.html*