industrie-wegweiser

Vernetzte Systeme | Chancen und Risiken anhand von Projektbeispielen

Lösungen, Tipps, Tools und Best Practice
für mehr Effizienz in der Produktion

- Industrie 4.0
- Industrial Security
- Fertigungsverfahren
- Automotive

industrie-wegweiser.de
Thomas W. Frick | Postfach 14 | 64853 Otzberg | Ust-Nr. DE 243367281
Tel: 06162-7203-382 | Fax 06162-7203-389 | info@industrie-wegweiser.de | www.industrie-wegweiser.de

Vernetzte Systeme | Chancen und Risiken anhand von Projektbeispielen

http://industrie-wegweiser.de/vernetzte-systeme/

Vernetzte Systeme in der Automobilindustrien

Die Vision der Autoindustrie ist deutlich: Autos sollen miteinander kommunizieren. Viele Autohersteller bieten vernetzte Systeme für ihre Autos an. Die unterschiedlichen Systeme der Hersteller bieten viele Möglichkeiten an. Das Übersenden des Standortes soll vor Staus warnen, bei einem Autounfall soll das Auto automatisch eine Datenverbindung zur Notrufzentrale herstellen oder die Vertragswerkstatt wird automatisch informiert wenn ein Service oder eine Reparatur fällig ist. Dies sind nur einige wenige Beispiele, welche die Hersteller mit ihren Systemen anbieten.

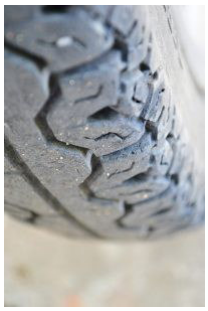
Vernetzte Systeme schaffen automatisierte Transparenz

Auf den ersten Blick wirkt das Vernetzungsangebot sehr nützlich. Doch mit dem vernetzten Fahren entstehen auch viele Gefahren. Eine Gefahr ist beispielsweise der gläserne Fahrer. Ein Beispiel dass die gläserne Transparenz nicht immer von Nachteil sein muss, zeigt folgender Fall vor dem Landgericht Köln:

Das Landgericht überführte einen Nutzer von BMW's Carsharing-Dienst DriveNow, der einen Radfahrer angefahren und tödlich verletzt hatte. Die nötigen Informationen lieferte sein Auto. Wodurch festgestellt werden konnte, dass der Fahrer zur fraglichen Zeit am fraglichen Ort war.

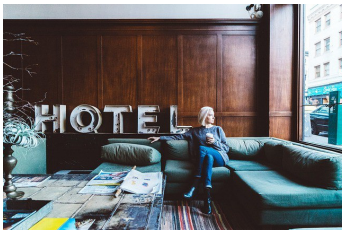
Auch wenn in diesem Beispiel das Recht dank vernetzter Systeme gewonnen hat, ist vieles, was technisch möglich ist, rechtlich noch nicht ganz geklärt. Es fehlt noch eine gesetzliche Norm, die den Schutz von PKW-Daten regelt und festlegt, welche Informationen gespeichert werden dürfen und welche nicht. Zudem könnten Kriminelle etwa mit bekannten Methoden wie Phishing, Keylogging und Social Engineering die Zugangsdaten zur Webseite des Autoherstellers stehlen und damit unautorisiert auf Anwenderinformationen zugreifen. Allgemein birgt die fortschreitende Vernetzung von Hacker-Angriffen Gefahren, ebenso bieten vernetzte Systeme viele Vorteile. also müssen die Anbieter und Autohersteller auch entsprechenden Schutz anbieten.

Beispielszenaria für die Reifenherstellung



Ein Beispielszenario aus der Industrie wäre ein Reifenhersteller. Dieser lässt die Innenschicht aus einer genau abgestimmten Gummimischung produzieren. Was wäre wenn ein Hacker über das Internet Zugriff auf die Steuerungsanlage erhält und somit die Zusammensetzung der Mischung verändern könnte? Niemand würde bemerken dass die Reifen die hergestellt werden, mit einer falschen Gummimischung ausgeliefert und an Autos montiert würden. Bei Autobahnfahrten würde sich die Gummimischung jedoch so stark erhitzen, dass die Reifen Luft verlieren. Es würde zu schweren Unfällen kommen. Nun müsste der Reifenhersteller Schadensersatz bezahlen und das Image es Herstellers wäre ruiniert.

Vernetzte Systeme in der Hotelindustrie



Der Fall eines österreichischen Hotels zeigt deutlich das Risiko vernetzter Systeme. Bei dem Hotel wurde das elektronische Schlüsselsystem von Ransomware verschlüsselt. Die Folge war, dass keine neuen Schlüssel ausgestellt werden konnten und anreisende Gäste nicht in ihre Zimmer konnten. Ein weiterer Fall spielte sich in Washington D. C. ab. Netzwerkvideorekorder wurden dort durch Ransomware angegriffen. Dadurch konnten knapp zwei Drittel der Überwachungskameras drei Tage lang keine Aufnahmen speichern.

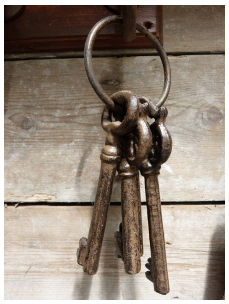
Branchenübergreifende Vernetzung der Systeme

Der Trend zur Digitalisierung fördert vernetzte Systeme. Alles wird vernetzt, egal ob Schloss, Kamera, ein internes Verwaltungssystem und die Vernetzung nach Außen z. B. über die Internetseite oder ein Kundenportal. Dadurch soll die Verwaltung, der Zugriff oder die Weiterbearbeitung der Daten vereinfacht werden. Es werden unterschiedliche Anbindungen für die Vernetzung der Systeme genutzt. Es beginnt beim internen Netzwerk, geht über eine externe Internet-Anbindung und endet bei der Anbindung in die "Cloud". Da immer mehr Produktlösungen beworben werden stellt sich nun die Frage, ob die Vernetzung der Systeme auch wirklich Vorteile bringt. Aus der Sicht des Datenschutzes und der IT-Sicherheit hinterfragt man die Sinnhaftigkeit vernetzter Systeme und glaubt, dass dadurch eher Gefahren und Risiken entstehen.

Angriffe auf vernetzte Systeme auch von innen

Die eben genannten Beispiele demonstrieren einen möglichen Angriffsweg und zwar der von außerhalb, also hauptsächlich über das Internet. Die Gefahr eines Angriffs von innen ist aber mindestens genau so groß. So können einerseits die eigenen Mitarbeiter aus dem Internet unbeabsichtigt Schadprogramme auf die zentralen IT-Systeme übertragen, die sich von dort auf die Steuerungssysteme ausbreiten. Andererseits stellen auch die Techniker oder Partner eine Gefahr dar, wenn sie über mobile Geräte auf die Systeme im Haus zugreifen können oder Dateien schicken, die Viren enthalten.
Bestes Beispiel hierfür war der Computerwurm Stuxnet. Der Wurm verbreitete sich über USB-Sticks an Notebooks, die zur Programmierung und Wartung von Anlagen angeschlossen worden waren. Die wohl bekannteste Auswirkung erreichte Stuxnet in iranischen Anlagen zur Urananreicherung. Dort manipulierte der Wurm die Drehzahl der Zentrifugen und schädigte so die Uranproduktion.

Wie sinnvoll sind vernetzte Systeme überhaupt?



Warum konnte das elektronische Schlüsselsystem überhaupt von Ransomware befallen werden?

Diese Frage stellt sich als Erstes im Fall des Hotels. Denn eigentlich sollte so ein System in einem segmentieren Netz betrieben werden können, auf das nur das elektronische Schlüsselsystem Zugriff haben. Für die Hauptaufgabe, also dem Schließen und Öffnen der Türen, wäre eine Vernetzung zu anderen Systemen eigentlich nicht notwendig.

Natürlich unterstützt die Vernetzung der Systeme die Arbeitsabläufe im Hotel wie beispielsweise bei den Buchungs- und Reservierungssystemen, wodurch direkt aus dem Buchungssystem die Schlüssel des Raumes erstellt werden können. Dadurch erhöht sich allerdings auch das Risiko, da das Reservierungssystem wahrscheinlich mit dem Internet verbunden ist. Deswegen sollten durch die Vernetzung mit dem Buchungs- und Reservierungssystemen für das elektronische Schlüsselsystem weitere Sicherheitsmaßnahmen wie regelmäßige Updates umgesetzt werden. Allerdings erhöhen zusätzliche Maßnahmen auch die Komplexität und den Wartungsaufwand der betriebenen IT-Infrastruktur. Deswegen stellt sich hier folgende Frage: Ist die Vernetzung mit den dadurch notwendigen Sicherheitsmaßnahmen wirklich sinnvoll oder ist es nicht einfacher die Verwaltung der Buchung und das Erzeugen von Schlüsseln in separaten Systemen vorzunehmen.

Was Sie bei vernetzten Systemen beachten sollten

In dem zweiten genannten Fall, bei dem es um Überwachungskameras in Washington ging, sieht es schon ein wenig anders. Dabei mussten die Videokameras mit den Videorekordern vernetzt werden, damit die Aufnahmen für die spätere Auswertung aufbewahrt werden können. Es geht hierbei mehr darum, wie die Anbindung und Absicherung der Überwachungskamera am besten umgesetzt werden kann. Eine Option wäre die Anbindung der Kameras über ein dediziertes Netzwerk, so dass die Kameras nicht aus dem Internet erreichbar wären. Allerdings scheint diese Maßnahme für die Umsetzung zu teuer zu sein, da überall in der Stadt Kameras montiert sind.

Eine andere wichtige Sicherheitsmaßnahme ist das regelmäßige aktualisieren der Software um Sicherheitslücken rechtzeitig zu schließen. Eine weitere Möglichkeit wäre die Anbindung zwischen den Systemen über VPN-Strecken zu realisieren und dadurch nicht die Überwachungskamera und Videorekorder Systeme direkt aus dem Internet erreichbar zu haben, sondern nur die genutzten VPN-Gateways.

ÜBER UNS

industrie-wegweiser.de ist eine herstellerunabhängige Informationsplattform, mit einem über 14.000-köpfigen Forum. Die Redaktion sammelt mit kritischer Brille Projektbeispiele, Tipps und Erfahrungen aus der Praxis für die Produktion, mit dem Schwerpunkt Industrie 4.0, Industrie-Anwendungen und innovative Fertigungsverfahren. Unser Ziel ist es die Angebote des Marktes herauszufiltern, die echte Mehrwerte liefern für mehr Effizienz in der Produktion.

Machen Sie mit!

Tauschen Sie sich gezielt zu Ihren aktuellen Themen rund um Industrie, Produktion und Fertigung mit unseren Mitgliedern und Experten in unserem Fachforum aus und teilen Sie uns mit, über welche Themenschwerpunkte Sie mehr erfahren möchten.

Herzlicher Handschlag, ergänzend zum Mausklick!

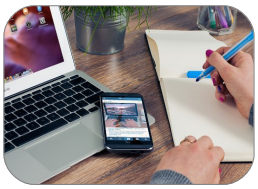
Wir sind mehr als ein Online Portal, lernen Sie uns auch außerhalb der virtuellen Welt kennen und besuchen Sie eine unserer nächsten Veranstaltungen. Bei Interesse organisieren wir mit Ihnen ein gemeinsames Event z.B. mit einer Betriebsbesichtigung oder einem Fachvortrag in Ihrem Haus.

Greifen Sie auf unser Expertennetzwerk zurück!

Sie möchten sich eine neutrale zweite Meinung bei Ihren geplanten Investitionen einholen oder haben fachliche Fragen zu neuen Technologien oder Ihrer Ihrer Produktionsoptimierung? Unser Experten-Team steht Ihnen jederzeit für Ihr individuelles Anliegen zur Verfügung, rufen Sie uns einfach an!

Bleiben Sie auf dem Laufenden!

Um keine Veranstaltung, Projektbeispiele und Expertentipps zu verpassen, sende Sie uns eine E-Mail mit dem Betreff „



Nutzen Sie unseren netzwerkinternen Stellenmarkt!

Aufgrund des über 10-jährigen Vertrauens gegenüber unseren Mitgliedern erreichen uns sowohl von Arbeitgeber- als auch Arbeitnehmerseite Informationen hinsichtlich Wechselbereitschaft und Stellenbedarf. Unser Konzept ist mehr als eine klassische Personalvermittlung, sprechen Sie uns bei Bedarf an.

Teilen Sie mit uns Ihre Best Practice!

Sie haben selbst ein spannendes Projekt oder Ideen zu einem speziellen Thema?
Dann lassen Sie uns prüfen, über welche Projekte aus Ihrem Haus wir gemeinsam berichten können.

Sie erreichen uns über den Live-Chat auf unserem Portal oder:

Tel:. +49 (6162) 7203-382 I Fax: +49 (6162) 7203-389
Email: info@industrie-wegweiser.de
direkt über unser Kontaktformular

Vernetzen Sie sich mit uns

Klicken Sie hierfür auf das jeweilige Symbol