# Industrie 4.0 – mehrere Wege, ein Ziel

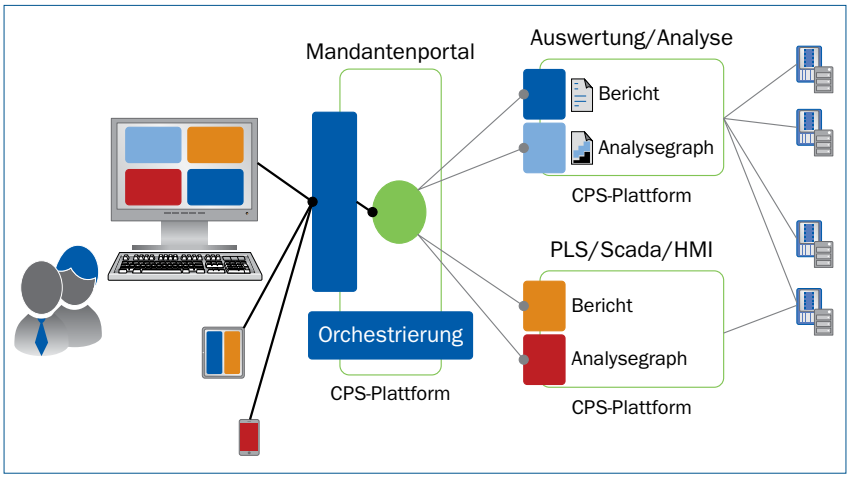
Die produzierenden Unternehmen stehen an der Schwelle zu Industrie 4.0, um Kosteneffizienz, Qualität und Flexibilität deutlich zu erhöhen. Wichtige Stichpunkte hierbei sind Big Data, Datentransparenz, Konnektivität und IT-Sicherheit. Das Unternehmen Videc stellt dafür passende Lösungen zur Verfügung, über die openautomation mit Geschäftsführer Dieter Barelmann sprach.

Ronald Heinze

Die Hightech-Strategie 2020 der Bundesregierung hat das Ziel, die bisherige Wettbewerbsstellung Deutschlands durch technische Innovation zu sichern. Hier gab es bereits eine Rüge seitens der Regierung: Von dem Gesamtkonzept Industrie 4.0 wurde noch nicht viel umgesetzt. Die Plattform Industrie 4.0 (plattform-i40.de) hat bereits konkrete Konzepte veröffentlicht. Diverse Arbeitskreise stellen ihre Ergebnisse zur Verfügung. „Was jetzt noch fehlt, ist die Umsetzung von Industrie 4.0“, betont D. Barelmann. „Da dies größere Investitionen nach sich zieht, müssen die Unternehmen eindeutige Vorteile daraus ziehen können, die sich auch in Zahlen widerspiegeln – in sinkenden Produktionskosten oder im gesteigerten Gewinn bei gleichem Umsatz.“

Vieles wird aber heute nur unter dem Deckmantel des Begriffes I40 gestellt; optimiert wird höchstens im herkömmlichen Sinne. Dagegen steht die Aussage in den Referenzarchitekturmodellen von Industrie 4.0 und Industrial Internet Consortium, die zukünftig kompatibel gemacht werden. „Wer behauptet, dass die bisherigen Softwarekonzepte in der ‚good old factory‘ für Industrie 4.0 geeignet sind, sollte in den nächsten Jahren gut aufpassen, sonst findet er sich im Abseits wieder“, warnt der Videc-Geschäftsführer. „Es gewinnt nicht immer die beste Lösung, der Markt

Dieter Barelmann ist Geschäftsführer der Videc GmbH in Bremen




Alle Freiheiten beim Zusammenstellen von bedarfsgerechten Oberflächen je nach Benutzerprofil, Know-how und Aufgabenbereich: Applikationen orchestrieren

bis zum Endverbraucher wird es bestimmen“, setzt er fort. „Internet, Smartphones in der Industrie? Das war vor einigen Jahren noch nicht möglich, heute gehört es zum Standard.“

Das Unternehmen Videc hat bereits vor über fünf Jahren mit einer Umstrukturierung des Produktportfolios begonnen, um sich den neuen Anforderungen an die digitale Transformation zu stellen. „Unser Angebotsspektrum umfasst Scada, Historian-Systeme, Berichtswesen, Analyse sowie die Alarmierung“, erklärt der Geschäftsführer. „Bei allen Systemen haben wir die Kommunikation in Richtung OPC UA vorangetrieben, die Front-Ends der Produkte in Richtung ‚Pure Web‘ fokussiert.“

Bei den Anwendungen geht es um die technische und branchentypische Umsetzung. Zuerst muss überprüft werden, ob die Anforderungen in den Produkten umsetzbar sind. Dieser Punkt ist in der Regel am einfachsten umzusetzen. „Kommt der Interessent mit seinen Geschäftsmodellen zu uns und sucht nach einer Lösung, wird es neben den anwendungsspezifischen Anforderungen unterschiedliche Ansätze der Umsetzung geben müssen“, berichtet D. Barelmann. „Unsere Aufgabe ist es dann, nach der besten Lösung zu suchen.“

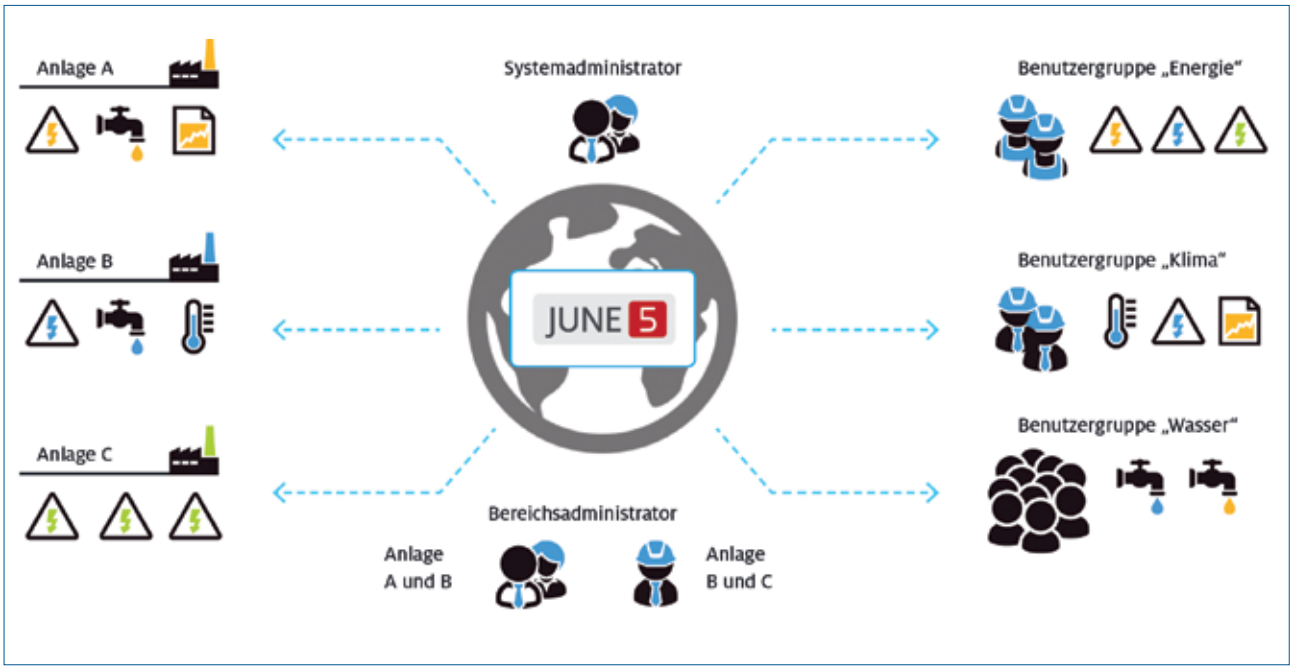
## Aus der Datenflut Wissen extrahieren

Eine immer öfter auftauchende Aufgabe ist es, aus der Datenflut im Unternehmen Wissen zu extrahieren. „Wissen ist Produktivität – bei der zu erwartenden Datenflut mehr denn je“, ist der Geschäftsführer überzeugt. Als probate Mittel für das „Wie“ gelten Cloud-basierte Portale – vorausgesetzt, sie sind ausbaufähig und flexibel anpassbar, auch hinsichtlich der Analyse-Algorithmen und Darstellungsoptionen. „Dass dies möglich ist, zeigen wir bei der zweiten Generation der Portal-Lösung ‚June5‘ anhand umfangreicher Analysen mithilfe von Ad-hoc-Diagrammen, konfigurierbaren Templates sowie einer API-Server-Schnittstelle für externe Anwendungen.“ Dadurch lassen sich Altkonzepte (Industrie 3.0) mit Lösungen der neuen Generationen schrittweise verbinden.

Mit der Trenddarstellung der Daten im „June5“-Portal wurden schnell neue Kundenwünsche deutlich. Insbesondere Anwender aus dem Energiesektor hatten die Anforderung, die Daten in den typischen Diagrammtypen Sankey und Carpet darzustellen. „Mit der neuen ‚June5‘-Version 2.3 tragen wir dieser Anforderung Rechnung“, erläutert D. Barelmann. „Diese ergänzen dann die bereits in der Version 2.0 enthaltenen Diagramme, wie diverse Kurvendarstellungen, Balken- und Tortendiagramme. Die neue Version ist darüber hinaus auf Cloud-Lösungen und Multi-Mandanten-Lösungen mit Dashboard-Funktionen fokussiert. Neben dem hauseigenen Historian-System Acron werden weitere Datenbanken als Informationsquellen eingebunden, zum Beispiel OSI PI und GE Historian. Zusätzlich werden weitere Schnittstellen implementiert, die Anbindung an OPC UA HA ist bereits vorhanden.

Durch die zentrale Erfassung von Prozessdaten zu Industrial Big Data und rollenspezifische Sichten auf die Daten und den daraus resultierenden Informationen entsteht der Bedarf, diese Informationen übergreifend darzustellen. Somit ist die Platzierung der Daten in einer Cloud-Umgebung ebenso sinnvoll, wie ein übersichtliches Einstiegsportal für Anwender. Funktional kann „June5“ genauso in einer Public-Cloud-Infrastruktur implementiert werden, wie auch in der häufiger verwendeten „Private Cloud“. „Aus heutiger Sicht der Datensicherheit ist die Private Cloud vorzuziehen“, betont D. Barelmann.

„Eine Trennung von Daten und Sichten auf die Werte ist nicht nur organisatorisch sinnvoll, sondern auch hinsichtlich Sicherheit unbedingt erforderlich“, setzt er fort. In der Datenbank Acron beispielsweise werden die Daten von unterschiedlichen Quellen sicher, dokumentenecht und echtzeitfähig in einer skalierbaren Softwarearchitektur über lange Zeitspannen gespeichert. Um die Auswertungsergebnisse, Berichte und Kennzahlenberechnungen auf den unterschiedlichen Organisationsebenen zu präsentieren, ist ein betriebssystemunabhängiger Ansatz zwingend erforderlich. Moderne Web-




Die Portal-Lösung „June5“ ermöglicht umfangreiche Analysen mithilfe von Ad-hoc-Diagrammen, konfigurierbaren Templates sowie einer API-Server-Schnittstelle für externe Anwendungen

technologie, das heißt keine Verwendung von Plug-ins, ist hier der passende Informationsträger für solche Anwendungen und deshalb vollständig im Systemansatz des Webportals implementiert.

Die Portal-Architektur bietet weitere Vorteile: Beispielsweise lässt sich die Lösung zu einer Multi-Mandanten-Plattform erweitern. Damit eröffnet sich für Unternehmen die Möglichkeit zu unterschiedlichen Geschäftsmodellen. Der Kunde wird eingebunden und kann seine eigenen Zugriffe selbst organisieren.

Die Daten können dabei aus unterschiedlichen Organisationseinheiten in getrennten Acron-Archiven – auch örtlich getrennt – abgelegt werden. Das „June5“-Portal bindet diese verschiedenen Datenquellen mit ihren dedizierten Berichten und Kennzahlen an und stellt diese den jeweiligen Organisationseinheiten zur Verfügung. Den unterschiedlichen Mandanten ist jeweils ein Bereichsadministrator zugewiesen, der die Voreinstellungen für Templates und Berichte individuell definieren oder aus Vorlagen wählen kann. Jeder Benutzer einer Organisationseinheit kann wiederum eigene Sichten, bezogen auf die benötigten Daten, erhalten.

Für Industrie 4.0 gibt es die Notwendigkeit, eine verteilte dienstorientierte Architektur als Basistechnologie zu verwirklichen (Serviceorientierte Architektur, SOA), für kooperierende und dezentrale Fertigungseinrichtungen in einem CPPS. Doch der Ansatz muss weitergehen: Auch die herkömmlichen Systeme müssen in smarte Dienste integriert werden. Grundlage dafür sind verteilte Dienste, eine fast beliebige logische Vernetzung und bedarfsgerechtes Abonnieren oder Verwenden von benötigten Diensten. „Um das komplexe System an der Oberfläche einfach wirken zu lassen, sind dem Kunden in diesem Bereich entsprechende Werkzeuge bereitzustellen“, weiß D. Barelmann. „Es sind sämtliche Freiheiten beim Zusammenstellen von bedarfsgerechten Oberflächen je nach Benutzerprofil, Know-how und Aufgabenbereich zu geben.“ Entsprechende Mechanismen ermöglichen es, einzelne vom Softwareprodukt bereitgestellte UI-Dienste zu kombinieren. Industrie 4.0 spricht vom „Orchestrieren“ – egal, ob eine Kombination von Diensten mit Daten oder die CPS-Plattform für eine Benutzeroberfläche gemeint ist.

„Auf Basis dieser Betrachtung werden die bisherigen monolithischen Softwaresysteme in einem Produktionsunternehmen gänzlich zur Disposition stehen“, ist sich der Geschäftsführer sicher. „Die bisherigen Systementscheidungen wird ein Anwender nicht unmittelbar revidieren. Die aufgebrochenen Systemfunktionen erhalten erst nach und nach Einzug in die produzierenden Unternehmen.“ Es wird also in einer längeren Periode einen Mischbetrieb geben, bei dem die historisierten Daten und Information sowie Funktionen aus Altsystemen in eine neue Plattform übernommen werden müssen. Videc hat für diese Anwendungen in „June5“ die Portal- und die Dashboard-Funktionalitäten implementiert. Die Integration von Alt- und Neudaten kann in einer gemischten Form stattfinden. „Aus Daten werden damit Informationen“, schließt er an. „Und zwar übergreifend und auch für zukünftige Anwendungen.“

Die Spezialität, Werte und Berichte darzustellen, ist um eine Kommunikationsanbindung an OPC UA HA (Part 11: Historical Access) erweitert worden. Darüber lassen

sich historisierte Werte aus Datenquellen nutzen, die diesen OPC-UA-Standard unterstützen. „Diese Schnittstelle wird zurzeit auch von einigen SPS-Anbietern direkt auf der SPS implementiert, da nicht alle Daten über längere Zeiträume archiviert werden müssen“, erläutert der Diplomingenieur dazu. „Die Firma Beckhoff Automation hat diese Schnittstelle bereits implementiert, andere sind mit diesen Schnittstellen in der Entwicklung.“ Somit ist die Darstellung von Daten aus der SPS heraus zusammen mit den historisierten, archivierten Daten in Trendverläufen und grafischen Auswertefunktionen möglich. Bestimmte Funktionen können in die untere Automatisierungsebene verlegt werden. Der Zugriff bleibt ohne eine weitere Zwischenebene erhalten. Hier entsteht eine Flexibilisierung der Datenhaltung. Doppelte Datenhaltungen werden reduziert.

Darüber hinaus ist eine leistungs- und webfähige Visualisierung in einer Smart Factory wichtig. „Wir haben vor sechs Jahren das Produkt Atvise Web Scada in das Portfolio übernommen“, berichtet D. Barelmann. „Mittlerweile wird die Version 3.0 ausgeliefert – bezeichnend auch hier die Durchgängigkeit von OPC UA.“ Die Web-Front-Ends laufen ohne Plug-ins – unter sicherheitstechnischen Gesichtspunkten ein wichtiger Aspekt.

Mit der integrierten Java Script Engine lassen sich neben den normalen Visualisierungsfunktionen auch individuelle Lösungen gestalten. Diese Funktion findet starken Anklang im Serienanlagenbau, bei dem die individualisierte Applikation frei bestimmt werden kann. „Sämtliche Board-Werkzeuge lassen sich grafisch anpassen und verleihen dem Anwender größtmögliche Freiheiten bei der Umsetzung“, so der Videc-Chef. Atvise ist das erste Pure-Web-Scada-System mit einer Hot-Stand-by-Redundanz.

## Industrie 4.0 und IT-Security – eine Symbiose

Wer mit Software und Konnektivität zu tun hat, kommt nicht an der IT-Sicherheit vorbei. Videc beschäftigt sich bereits seit drei Jahren intensiv mit dieser Thematik. „Zu der Zeit war es ein noch wenig beachtetes Thema im Bereich Automatisierung“, weiß der Geschäftsführer. „Erst mit dem IT-Sicherheitsgesetz und den stark ansteigenden Angriffen auf die deutsche Industrielandschaft bekommt IT-Sicherheit entsprechend mehr Raum.“ Er setzt fort: „Das Know-how aus diesem Segment haben wir in die Sicherheitskonzepte aller unserer Produkte einfließen lassen. Externe Sicherheitstests gehören seitdem zu unserem Standard.“

Über das Industrial Ethernet erhalten Automatisierungsanlagen schon heute eine direkte Internet-Konnektivität. Jedoch sind klassische IT-Security-Konzepte – insbesondere aus der Bürokommunikation – nicht mehr ausreichend, da diese bei restriktivem Einsatz häufig die Anlagen-Verfügbarkeit gefährden und auch einen hohen Betriebsaufwand erzeugen. „Es sind Lösungen gefordert, die weitgehend automatisiert Cyberangriffe ohne direkten Eingriff in den Produktionsprozess erkennen“, betont D. Barelmann. „Der Anlagenbetreiber ist damit in der Lage, sein IT-Netz mit voller Transparenz sicherheitstechnisch zu managen.“

Die aktuelle Entwicklung zielt auf die flexible Integration von Maschinen- und Unternehmensdaten sowohl standort- und als auch unternehmensübergreifend ab. Maschinen kommunizieren mit Maschinen. Werkstücke und Maschinen steuern selbstständig in Echtzeit die Produktion. Daraus resultiert ein erhöhtes Risiko: Anlagen und Produkte, aber auch Daten und Know-how müssen verlässlich vor Manipulation und Informationsabfluss geschützt werden. Festzustellen ist: Das am schwächsten geschützte Unternehmen wird als erstes betroffen.

„Grundlegend ist immer ein durchgängiges Sicherheitsniveau in allen Schichten für die einzelnen Schutzzonen zu definieren“, so D. Barelmann. „Ein übergreifendes, standardbasiertes Informationssicherheitsmanagement legt Maßnahmen fest und überprüft kontinuierlich deren Wirksamkeit.“ Der Mensch befindet such auch bei Industrie 4.0 immer noch im Zentrum vieler Prozesse und damit möglicher Cyberangriffe. Deshalb ist trotz Einsatz von Sicherheitstechnik die Sensibilisierung aller Beteiligter zum sicheren Umgang mit Systemen, Anwendungen und Daten von höchster Bedeutung.

Im Gegensatz zur Büro-IT steht bei Automatisierungen nicht die Vertraulichkeit der Daten im Vordergrund, sondern die Verfügbarkeit der unverfälschten Daten und der nicht-kompromittierten Systeme. Ein uneingeschränkter Zugriff auf Steuerungs- und Produktionsdaten ist jederzeit und in Echtzeit zu gewährleisten.

Daraus ergeben sich bereits die ersten Anforderungen an zukünftige Sicherheitslösungen: Selbsttäti-

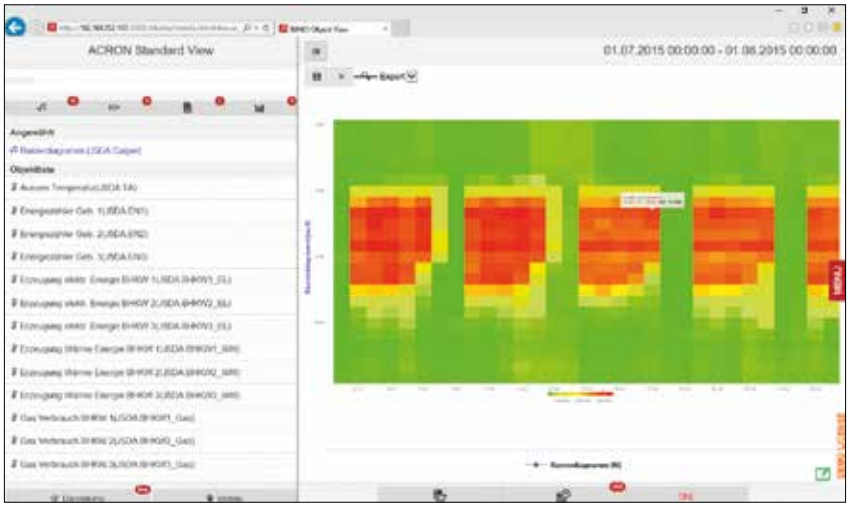
### Kernbereiche in der mobilen Webanwendung von „June5“

- Analyse in Ad-hoc-Diagrammen und Speicherung konfigurierbarer Diagramme jedes Teilnehmers
- Auswertung durch PDF-Berichtswesen
- Handwerterfassung (Offline/Online)
- Anbindung weiterer Historiensysteme (OSI PI, GE Historian, …)
- Web API-Server-Schnittstelle für externe Anwendungen
- Add In (Werteexport) zu Microsoft Excel
- Implementierung von Web Scada oder webfähiger Messgräte
- Carpet- und Sankey-Diagramme
- Jahresganglinien/Summenhäufigkeit

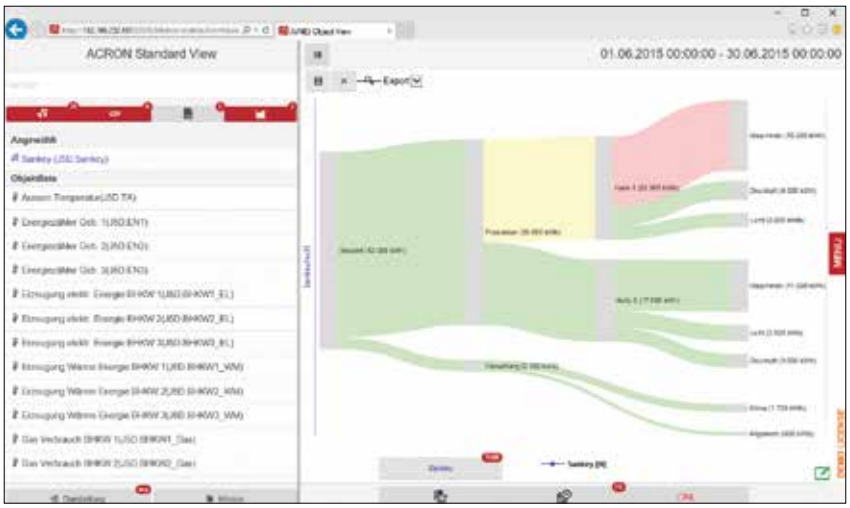
ge Schutzmechanismen gefährden die uneingeschränkte Verfügbarkeit aller Komponenten und Systeme und damit den gesamten Produktionsablauf. Fehlende oder unvollständige Datenübertragung oder -verarbeitung führt in den allermeisten Fällen zu einem kritischen Zustand einer Produktionsanlage. Das notwendige Update- und Patchmanagement der eingesetzten Software und Betriebssysteme sowie die unmittelbare Aktualisierung von Virensignaturen sind im Produktionsbetrieb nicht umsetzbar. In der Regel lassen sich anstehende Aktualisierungen einerseits nur nach Freigabe der Hersteller der Automatisierungs- und Prozessleitsysteme und andererseits nur in definierten Wartungszeitfenstern durchführen.

## Industrie 4.0 sicherheitstechnisch am Anfang

„Grundsätzlich genügt es bei Industrie 4.0 nicht, nachträglich Security-Funktionen in den Komponenten zu ergänzen“, weiß D. Barelmann. „Hier besteht schon seit Langem die Anforderung nach ‚Security by Design‘. Das bedeutet, dass bereits in der Produkt- oder Anlagenplanungsphase an die Implementierung notwendiger IT-Sicherheitsfunktionen gedacht wird.“




Vielfältige Darstellungsmöglichkeiten der Daten mit der Portal-Lösung „June5“: Trenddarstellung mit Diagrammtyp Carpet




Anwender aus dem Energiesektor haben oft die Anforderung, die Daten im Diagrammtyp Sankey abzubilden

Die neu eingesetzten Systeme und Komponenten müssen immer Security-Funktionen nach dem Stand der Technik implementiert haben. Diese Forderung ergibt sich auch aus dem IT-Sicherheitsgesetz, das zukünftig durchaus auch eine Ausstrahlungswirkung auf Nicht-Kritis-Unternehmen haben dürfte.

Hersteller und Lieferanten müssen Security-Patche und Support auch für ältere Software- und Firmwarestände zur Verfügung stellen. Die Behebung von Schwachstellen muss getrennt von funktionalen Erweiterungen möglich sein. Kunden dürfen nicht gedrängt werden, aktuelle Software- und Firmwarestände zu nutzen, weil ein einzelnes herstellerspezifisches Update durchaus weitergehende Securityrelevante Auswirkungen auf die Gesamtanlage haben kann.

„Für den Aufbau einer unternehmensübergreifenden Kommunikationsinfrastruktur in Industrie 4.0 ist Vertrauen eine Grundlage für diesen Austausch“, weiß D. Barelmann. „Es muss zwingend eine Authentifizierung sowohl von Mensch und Maschine als auch von Maschine zu Maschine über sichere Identitäten erfolgen.“ Die organisationsübergreifende Identitätsverwaltung stellt Unternehmen aktuell noch vor eine ungelöste Aufgabe.

Die Lieferung „robuster“ internetfähiger Systeme und Komponenten ist von elementarer Bedeutung. Wichtig ist eine durchgehend verschlüsselte Kommunikation auf Netzwerkebene oder – wenn möglich – eine Ende-zu-Ende-Verschlüsselung auf Komponentenebene. Zukünftige Industrie-4.0-Komponenten müssen die hierfür notwendigen krypthografischen Grundfunktionen bereits „im Bauch“ implementiert und bereits im Auslieferungszustand aktiviert haben.

Die genannten Anforderungen sind für zukünftige Industrie-4.0-Anlagen grundlegend zu realisieren. Der begonnene Standardisierungsprozess, u. a. festgelegt in den branchenspezifischen IT-Sicherheitskatalogen oder der IEC 62443, wird Vorgaben in den nächsten Jahren hierzu formulie-

ren. Aber was kann heute schon umgesetzt werden?

## Verheiratung von Industrie 3.0 mit Industrie 4.0

Es wird laut D. Barelmann noch zehn bis 20 Jahre dauern, bis die Industrie-4.0-Infrastruktur durchgehend aufgebaut ist. Aktuell und in den nächsten Jahren werden Industrie-3.0-Komponenten mit Industrie-4.0-Technologie funktional „ergänzt". „Hier entstehen möglicherweise beträchtliche Lücken, da alle Systeme, Geräte und Komponenten am Industrial Ethernet angeschlossen sind, jedoch nur die Industrie-4.0-Komponenten und deren Datenaustausch nach dem Stand der Technik geschützt werden", betont er.

Was ist zu beachten für die Industrie-3.0-Systeme? „Zunächst steht die konsequente Aktivierung und Nutzung vorhandener Security-Funktionen in den bestehenden Anlagen, wie die personalisierte Systemanmeldung und die Trennung von Netzen mit unterschiedlichem Sicherheitsniveau an vorderster Stelle", erläutert der Geschäftsführer.

„Die komplexen Angriffsmethoden von Stuxnet und Co. sind durch eine hohe Flexibilität und Dynamik gekennzeichnet", setzt er fort. „Die Erkennung solcher Cyberangriffe ist nur durch ein automatisiertes Monitoring des Datenverkehrs möglich. Nur durch die kontinuierliche Beobachtung werden diese Anomalien erkannt." Eine umgehende Alarmierung bei einem Sicherheitsvorfall stärkt die Reaktionsfähigkeit im Unternehmen. Mittels dieser Fähigkeiten lassen sich Risiken frühzeitig und gezielt bewerten und angemessene Maßnahmen festlegen.

Man kann jedoch nur schützen, was man kennt. Nur sofern ein aktueller Netzstrukturplan vorhanden ist, lassen sich die Bedrohungen und daraus resultierenden Risiken analysieren und geeignete Maßnahmen umsetzen. Hierbei sind internationale Standards wie die ISO- 2700x-Familie hilfreich. Das bewusste und kontrollierte Eingehen von Restrisiken ist dann – ähnlich wie bei der Maschinensicherheit (Safety) – ein normaler und beherrschbarer Vorgang. „Es ist zu beachten, dass die Bediener einer Produktionsanlage keine Security-Spezialisten sind und auch aufgrund des Tagesgeschäfts nicht werden können", betont D. Barelmann. „Deshalb müssen sämtliche beschriebenen Präventions-, Detektions- und Reaktionsfähigkeiten weitgehend automatisiert durchführbar und einfach zu administrieren sein."

## Cyber Security funktioniert nur kontinuierlich und mit IT-Transparenz

Was ist zu beachten? Alle Sicherheitsfunktionen, die Geräte- und Systemanbieter bereitstellen, sind möglichst maximal einzuschalten und zu nutzen. Alle Schnittstellen und Datenverbindungen müssen strikt und kontinuierlich überwacht werden. Das Alarmieren von erkannten oder vermuteten Anomalien im IT-Netz erfolgt automatisch.

Die Security- und Risiko-Managementprozesse sind einfach und nachvollziehbar gestaltet. Hierbei hilft eine möglichst weitgehende Automatisierung dieser Prozesse. „Sicherer wird es nur, wenn es einfach ist", unterstreicht D. Barelmann. „Die Bedienung muss auch für Nicht-IT-Security-Fachleute möglich sein und sich in die Betriebsprozesse integrieren." Alle Mitarbeiter, vom Anlagenbediener bis zum Betriebsleiter, müssen die notwendigen Security-Anforderungen in ihrem Verantwortungsbereich bewerten, die bestehenden Risiken behandeln und daraus resultierende Maßnahmen managen können.

„Wir sind nicht aktiv in der Abwehr der Angriffe. Dafür gibt es bereits eine Vielzahl unterschiedlicher Produkte", sagt der Geschäftsführer. „Der passive Ansatz beim Abfragen der Netzwerkteilnehmer ist das Grundprinzip. Wir monitoren, validieren und überwachen das Netzwerk und die Assets sowie Automatisierungskomponenten." Erst wenn es Unregelmäßigkeiten gibt, wird alarmiert. Damit stehen drei wichtige Punkte im Vordergrund, die häufig vergessen oder ignoriert werden:

Was passiert, wenn ein Angriff erfolgreich war? Wie kann ein Betreiber merken, dass er eine befallene Anlage hat? In der Regel ist die Dauer nach einer Infektion bis zum Anlagenstillstand immer mehr als eine Woche. Wenn man aber den Befall erkennt, kann sofort reagiert und die notwendigen Maßnahmen eingeleitet werden, um die Anlage zu schützen.

Kaum eine Schutzmaßnahme wirkt gegen den inneren Angriff – also durch Mitarbeiter. Auch hier kann auf jede Unregelmäßigkeit sofort reagiert werden. Das Videc-Produkt Irma logged den gesamten Datenverkehr und kann auch im Nachhinein die notwendigen Informationen für eine Aufklärung liefern.

Servicezugänge oder nicht einsehbare Zugänge können Einfalltore für jeden Angreifer sein. Diese sind jedoch bei den herkömmlichen Maßnahmen kaum herauszufinden. Das kann man nur, wenn man eine kontinuierliche Sicht auf die Anlage hat. Das macht Irma mittels eines passiven Scannings. „Wir greifen nie aktiv in die Kommunikation ein", betont D. Barelmann. „Das aktive Abfragen der gesamten Teilnehmer im Bereich der Automatisierung ist nicht gerade förderlich für die Anlagensicherheit. Auch ein punktuelles Abfragen einiger Komponenten im Netzwerk hat immer noch große Lücken in einem Security-Konzept." Irma hat zusätzlich ein integriertes Risikomanagement, um die Anforderungen der neuen ISO 9001-2015 gerecht zu werden. Dadurch erhält die Geschäftsleitung bewertbare Kennzahlen.

Mit diesem Angebot kann Videc die digitale Transformation in den Unternehmen vorantreiben und die Voraussetzung für den Übergang zu Industrie 4.0 schaffen. Kernpunkte bleiben dabei maximale Transparenz, hohe Konnektivität und eine bestmögliche Datensicherheit.

www.videc.info