„FÜR DIE ETABLIERUNG EINER FUNKTIONIERENDEN IT-SICHERHEIT BEDARF ES ZUNÄCHST EINHEITLICHER VORGABEN FÜR DIE NUTZUNG VON IT-KOMPONENTEN SOWIE DIE ETABLIERUNG VON FEST DEFINIERTEN PROZESSEN FÜR DIE VERWALTUNG DIESER KOMPONENTEN."

Foto und Grafiken: accessec GmbH

„Die Potenziale bei der digitalen Transformation im Mittelstand sind riesig."

Sebastian Rohr ist Geschäftsführer und Mitbegründer der accessec GmbH, Groß-Bieberau. Die accessec GmbH berät Unternehmen bei der Planung, Umsetzung und dem Betrieb von Sicherheitskonzepten.

Wie ist der Status quo bzgl. Digitalisierung und IT-Sicherheit?
Leider muss ich sagen, dass dieser im internationalen Vergleich unterdurchschnittlich ist. Wissen Sie, das Problem ist, dass die deutsche Wirtschaft und insbesondere der Mittelstand im Bereich der produzierenden Industrie in den letzten Jahren den Fokus eher auf die weitergehende Optimierung bestehender Fertigungsprozesse und interner Abläufe gelegt haben. Das ist auch gut und wichtig. Die Digitalisierung ist dabei allerdings weitestgehend auf der Strecke geblieben. Fortschritte gibt es lediglich hinsichtlich einzelner Prozessschritte. Dem Anspruch einer digitalen Transformation mit ihren destruktiven Anteilen wird dies aber nicht gerecht.

Etwas anders verhält es sich mit der IT-Sicherheit. Hier deutet alles darauf hin, dass die deutsche Industrie die Zeichen der Zeit erkannt hat. Das zeigt nicht nur eine tatsächliche Belebung des Umsatzes, der mit grundlegenden Sicherheitslösungen erzielt wird, sondern auch die vermehrte Arbeit an der Etablierung von nachhaltigen Sicherheitsmanagementsystemen für die langfristige Reduzierung der IT-Risiken. Allerdings sprechen wir hier zunächst nur von einem Nachholbedarf. Von Investitionen als Enabler für die digitale Transformation kann auch hier nicht die Rede sein.

Beide Erkenntnisse in Kombination zeichnen aus meiner Sicht – und damit bin ich nicht allein – ein weiterhin eher erschreckendes Bild zur Gesamtlage des deutschen industriellen Mittelstandes hinsichtlich seiner Positionierung für die anstehenden Aufgaben der digitalen Transformation. Dabei darf man nicht vergessen, dass es um die fortschreitende Globalisierung der Märkte eben dieser Unternehmen geht. Für mich bleibt nach wie vor fraglich, ob der Mittelstand trotz seiner technologischen Marktführerschaft für Produktionsverfahren Gefahr läuft, den internationalen Anschluss zu verlieren, da Absatzwege und neue Möglichkeiten zur Kundenbindung schlicht nicht genutzt werden.

Was gibt es bisher an Sicherheitskonzepten?
Hier besteht durchaus ein starker Gegensatz zur allgemeinen Wahrnehmung. Tatsächlich gibt es nämlich bereits etliche Ansatzpunkte um maßgeschneiderte Sicherheitskonzepte mit angemessenem Aufwand zu erzeugen. Lassen Sie mich ein paar Beispiele nennen: Neben der bereits seit längerem bestehenden Richtlinien VDI/VDE 2182 und der vormaligen ISA 99, die sich in der IEC 62443 spiegelt, haben diverse deutsche Verbände wie der VDMA oder der ZVEI eigene Ratgeber, Leitlinien und Orientierungshilfen erstellt. Oder denken Sie an die Plattform Industrie 4.0, die eine Reihe von Dokumenten zur besseren Absicherung von Anlagen und Maschinen durch deren Hersteller sowie Leitlinien und Vorgaben für den sicheren Betrieb solcher Maschinen bei den mittelständischen Produktionsunternehmen veröffentlicht hat. Richtet man den Blick auf die deutsche Wirtschaft und Forschung, so finden sich insbesondere im Leuchtturmprojekt des Bundesministeriums für Bildung und Forschung die Ergebnisse des IUNO-Forschungsprojektes. In enger Zusammenarbeit zwischen angewandter und universitärer Forschung, Partnern der Großindustrie sowie mittelständischen

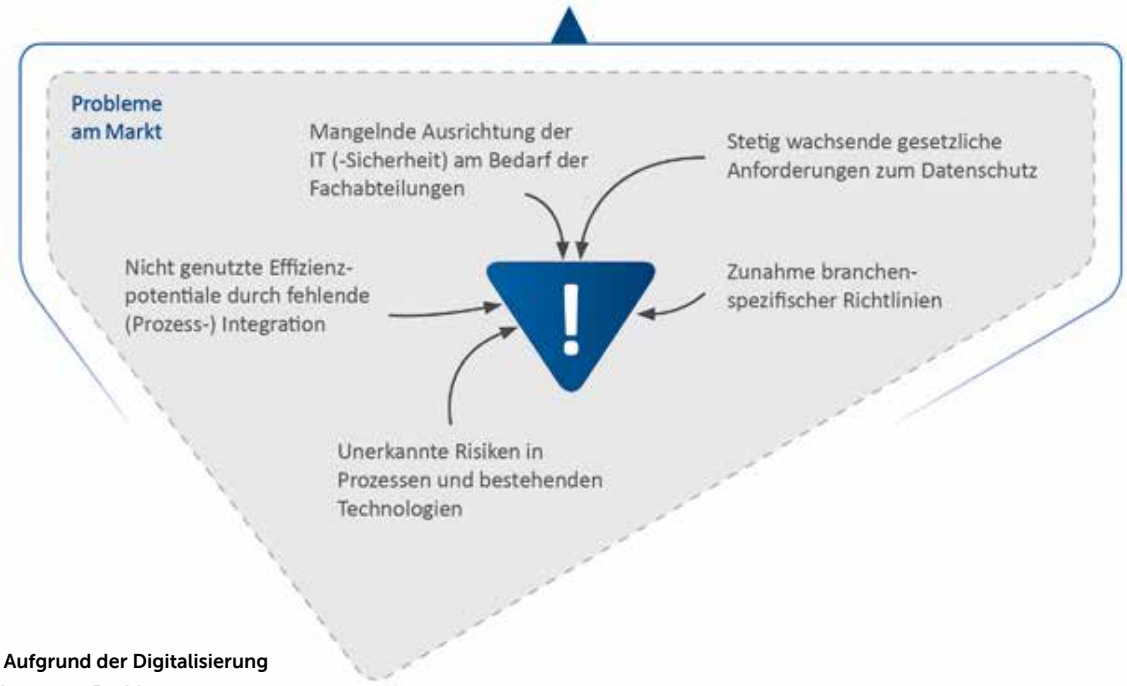

Bild 1: **Aufgrund der Digitalisierung entstehen neue Probleme.**

Unternehmen wie der accessec GmbH konnten im Verlauf der letzten 24 Monate erste Demonstratoren für neue, sichere Geschäftsmodelle auf Basis von I-4.0-Technologien entwickelt werden und neue Sicherheitsmodelle sowie mögliche Sicherheitsinfrastrukturen im Rahmen der Demonstration gezeigt werden.

Auch auf europäischer Ebene finden sich eine ganze Reihe interessanter und vor allem gut anwendbarer Hinweise. Ich möchte insbesondere auf die hervorragende Arbeit der ENISA (Europäische Agentur für Netz- und Informationssicherheit) als europäisches Pendant zum deutschen BSI hinweisen. Unter der Ägide des ehemaligen BSI-Präsidenten Udo Helmbrecht hat sich ENISA zu einer wertvollen Organisation auf europäischer Ebene entwickelt.

Funktioniert das Zusammenspiel der verschiedenen Lösungen?

Nein. Nicht mit dem derzeitigen Stand der Technik und Dokumentation. Hierfür bedarf es zunächst der Etablierung neuer Methoden für die Verwaltung der Bestandssysteme. Zudem entpuppt sich auch die stark vernachlässigte Qualifikation der Mitarbeiter der Instandhaltung in der Produktion als zentraler Stolperstein. In der Mehrheit der Fälle, die wir beobachten, kennen sich die Instandhalter hervorragend mit der klassischen Automatisierung und den elektrischen und elektronischen Komponenten der Fertigung aus. Die über die letzten zwei Dekaden eher schleichend in die Produktion Einzug gehaltene IT wurde bei der Ausbildungsplanung bzw. Fortbildung dieses bereits hoch qualifizierten Personals zumeist vergessen. Hin und wieder erleben wir auch, dass hier schlicht angenommen wurde, dass „das kleine bisschen PC-Technik" doch durch die allgemeine Verfügbarkeit solcher Technologien im beruflichen und privaten Umfeld mit abgedeckt sein müsste. Wohin es mit der Produktions-IT gehen kann, zeigt sich hingegen in den Laboren und auf futuristischen Bildern von vollautomatisierten Produktionsanlagen, die über moderne, mobile Endgeräte mit Touch-Oberflächen bedient werden. Möglich ist hier also einiges.

Was sind die wichtigsten Punkte für eine funktionierende IT-Sicherheit?

Ein Punkt betrifft die erwähnte Heterogenität der IT-Komponenten in der Produktion, ein weiterer den ebenso genannten deutlichen Nachholbedarf bei der Qualifikation und Weiterbildung des Personals. Für die Etablierung einer funktionierenden IT-Sicherheit bedarf es also zunächst einheitlicher Vorgaben für die Nutzung von IT-Komponenten sowie die Etablierung von fest definierten Prozessen für die Verwaltung dieser Komponenten. Und natürlich setzt ein gutes Management der IT-Sicherheit eine vollständige Kenntnis der schützenswerten Assets in der Produktion voraus. Hieran mangelt es jedoch. Dabei würde alleine eine umfassende Kenntnis über alle in einem Produktionsnetzwerk oder in einer abgeschotteten Anlage vorhandenen IT-Komponenten – dazu zählt die Hardware, das Betriebssystem, Anwendungssoftware, Spezialsoftware, verwendete Protokolle, Benutzerkonten/Passworte sowie möglicherweise bereits implementierte Sicherheitsmaßnahmen – den Stand der IT-Sicherheit in den meisten Unternehmen deutlich verbessern. Die Inventarisierung der in der Produktion vorhandenen netzwerktechnisch verbundenen Komponenten stellt wirklich eine große Herausforderung für viele Betriebe dar. Denn in den letzten Jahren wurde vornehmlich „ein Stück Produktionsanlage" geliefert und in Betrieb genommen und

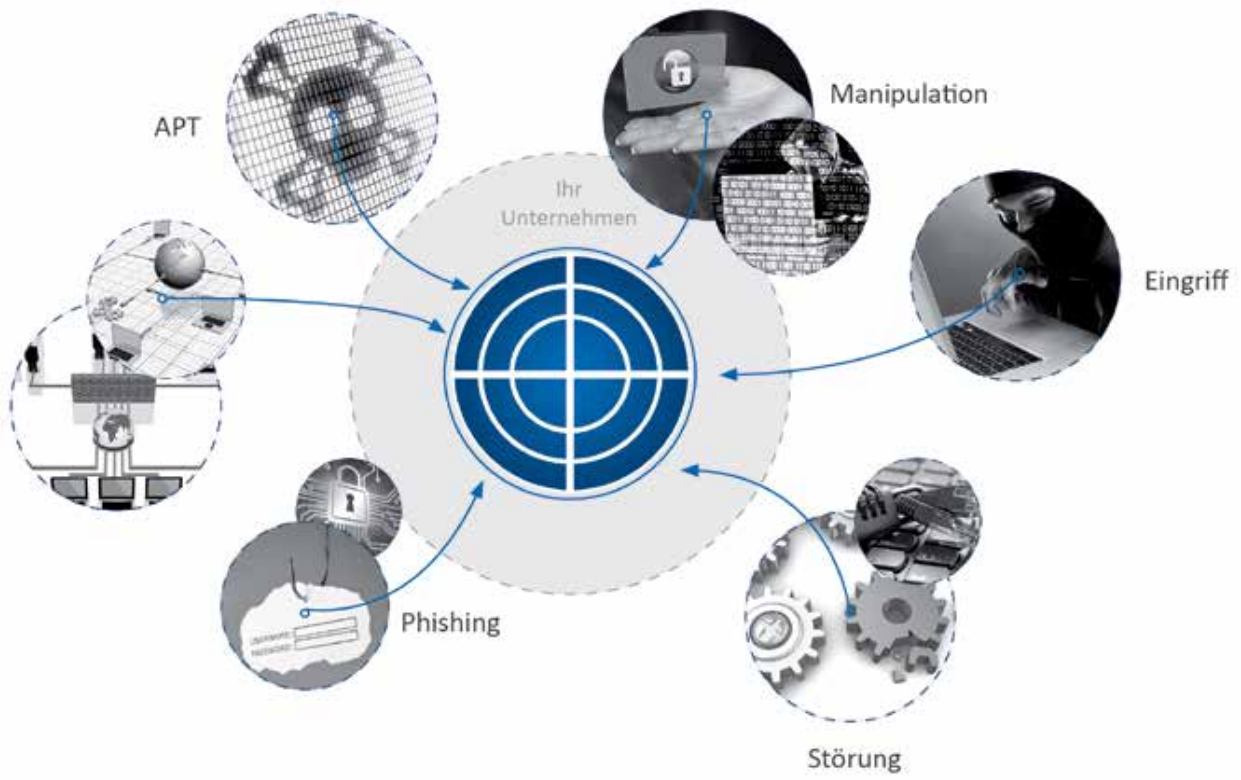

Bild 2: **Durch die Digitalisierung mögliche Angriffe auf Unternehmen.**

hat in eben dieser Art auch Einzug in die Dokumentation bzw. die Bücher gehalten.

Um noch einmal zum Personal zurückzukommen: Der Fokus muss hier in naher Zukunft nicht unbedingt auf dem Erlernen neuer Sicherheitstechnologien oder Lösungen liegen, sondern sollte sich eher an der Vermittlung bzw. Vertiefung der Kenntnisse über Standard-IT und Netzwerkkomponenten sowie Protokolle konzentrieren.

Wo besteht der dringendste Handlungsbedarf für Industrieunternehmen wie Gießereien?

Notwendiger Schritt Nummer eins ist die angesprochene Inventarisierung der Assets bzw. Produktions- und Anlagenkomponenten sowie deren detaillierte Abbildung in einer entsprechenden Inventardatenbank (in der Office-IT CMDB genannt: Configuration Management Database). In einem nächsten Schritt muss eine Bewertung der Kritikalität der gefundenen Assets erfolgen und die daraus abzuleitenden Risiken für eine Beeinträchtigung der IT-Sicherheit dokumentiert werden. Hier fehlt es nahezu flächendeckend an einem Verständnis für die Abhängigkeiten zwischen den einzelnen Komponenten und den daraus resultierenden Risiken für die Verfügbarkeit der gesamten Produktion. Es ist zwingend erforderlich, dass die Geschäftsleitungen der Unternehmen sich intensiv in kompetenzübergreifenden Teams zusammenfinden, um gemeinsam mit den Verantwortlichen aus den Bereichen Instandhaltung, IT, Produktion und IT-Sicherheit die kritischen Schwachstellen zu finden und einen strategischen Plan für die nachhaltige Senkung des Risikoniveaus zu entwickeln.

Aus der Erfahrung der letzten Jahre stehen hier zunächst fast ausschließlich Maßnahmen der Netzwerktrennung, der Aufarbeitung fehlender Dokumentation sowie der Beurteilung von notwendigen und nicht notwendigen Kommunikationsbeziehungen im Vordergrund. Eine Investition in teure Sicherheitslösungen – insbesondere solche mit hohem Konfigurationsaufwand und Betriebskosten – verbieten sich nahezu automatisch, wenn der durchschnittliche niedrige Reifegrad des IT-Managements und der Dokumentation der IT in der Produktion betrachtet wird. Erst wenn die grundlegenden Bedürfnisse für ein einheitliches Management der heterogenen IT in der Produktion geschaffen sind, kann ernsthaft über die Sinnhaftigkeit einer Investition in neue Sicherheitstechnologien nachgedacht werden.

Wie sieht eine von Ihnen angebotene Risiko-Analyse konkret aus und welche Art von Maßnahmen ergeben sich daraus?

Das von uns in Zusammenarbeit mit Kundenunternehmen entwickelte Paket zur Standortbestimmung in der IT-Sicherheit (ICS-SCI: Industrial Control System-Security Capability Index) hilft uns dabei, den Reifegrad der IT-Sicherheit in einem Unternehmen mit automatisierten Produktionsabläufen standardisiert zu bestimmen. Wir haben uns bei der Entwicklung dieses Werkzeugs darauf konzentriert, einen möglichst brei-

ten Abdeckungsgrad für die verschiedenen Aspekte der Informationssicherheit zu erreichen, ohne den besonderen Fokus auf die Anforderungen der Produktion zu verlieren. Durch die Beantwortung gezielter Fragestellungen aus von uns definierten sieben Dimensionen lassen sich erste Anhaltspunkte über den erreichten Reifegrad der jeweiligen Dimension ableiten. So sind wir in relativ kurzer Zeit von 10-15 Tagen in der Lage, der Produktionsleitung sowie der Geschäftsführung ein leicht verständliches Bild der eigenen Sicherheitssituation zu skizzieren. Die Erfahrung aus unzähligen Analysen und Ergebnispräsentationen hat dazu geführt, dass wir nicht nur im Vorhinein ein Zielniveau für das Unternehmen definieren, das sich an der Größe des Unternehmens, der konkreten Branche sowie weiteren Kennzahlen orientiert, sondern darüber hinaus – je nach Verfügbarkeit von Referenzdaten – auch eine entsprechende Benchmark-Linie in unserer Auswertung einziehen. Anhand der Darstellung in einem Spinnennetzdiagramm können das Topmanagement und die Produktionsleitung sehr schnell und gut nachvollziehbar eine Priorisierung der anstehenden Handlungsfelder ablesen. Dort, wo der eigene Wert am stärksten vom Benchmark bzw. dem anzustrebenden Zielwert abweicht, sind konsequenterweise auch die am höchsten zu priorisierenden Maßnahmen zu definieren. Im Nachgang fordern wir üblicherweise dazu auf, einen konkreten Maßnahmenplan für die Umsetzung zu definieren. Die weitere Vorgehensweise hängt dann stark von der Art und den Kernthemen der anstehenden Aufgaben und Teilprojekte ab und natürlich von der Art und Intensität unserer weiteren Einbindung.

Wohin geht die zukünftige Entwicklung bezüglich Angriffen bzw. Verteidigungsstrategien?

Leider kann ich hier sagen, dass ein Trend über die letzten zwei Dekaden meiner Karriere in der IT-Sicherheit hinweg eindeutig und jederzeit spürbar war: Und das ist die zunehmende Professionalisierung der dunklen Seite der IT! Wo früher die größte Menge an Sicherheitsvorfällen eher vernachlässigbar war, weil wenig professionelle Angriffe von sogenannten „Skript Kiddies" produziert wurden, finden sich heute vermehrt hoch professionelle Angreifer, die eindeutig dem Milieu der organisierten Kriminalität zuzuordnen sind und sich in internationaler Kooperation arbeitsteilig um die Ausbeutung von Schwachstellen in den IT-Systemen der Unternehmen kümmern. Allein die erschreckend hohe Anzahl an erfolgreichen Angriffen mit sogenannten Krypto-Trojanern, die unfassbar schnell die wichtigen Dateien auf betroffenen Rechnern verschlüsseln und dann Lösegeld für die Bereitstellung des notwendigen Schlüsselmaterials erpressen, zeigt, dass IT-Sicherheit nicht mehr ein Spielfeld für gelangweilte Jugendliche ist, sondern ein ertragreicher Markt für professionelle Missetäter.

Zudem hat sich neben diesen sehr offen und sichtbar ausgeführten Ransomware-Angriffen eine zweite Klasse der Angriffe „unter dem Radar" etabliert – die sogenannten Advanced Persistant Threats oder kurz APTs. Zu unserem Unbehagen und vor allem zum Schrecken unserer Kunden finden wir häufiger als uns lieb ist Anzeichen dafür, dass sich bereits professionelle Angreifer auf sehr leisen Sohlen in die Netzwerke unserer Kunden eingeschlichen haben, um unbemerkt die digitalen Goldstücke aus dem Unternehmensnetzwerk zu extrahieren und sie auf dem Schwarzmarkt meistbietend zu verkaufen. Lassen Sie mich hier noch schnell ein glimpflich ausgegangenes Beispiel erzählen: In einem vertraulichen Anruf wurde einer unserer Kunden vom Wettbewerber in Kenntnis gesetzt, dass ihm soeben die Konstruktionszeichnung für ein noch nicht auf dem Markt befindliches neues Produkt angeboten wurde. Sie können sich vorstellen, welchen Schock diese Nachricht bei unserem Kunden erzeugt hat!

Mit Sebastian Rohr sprach Berit Franz