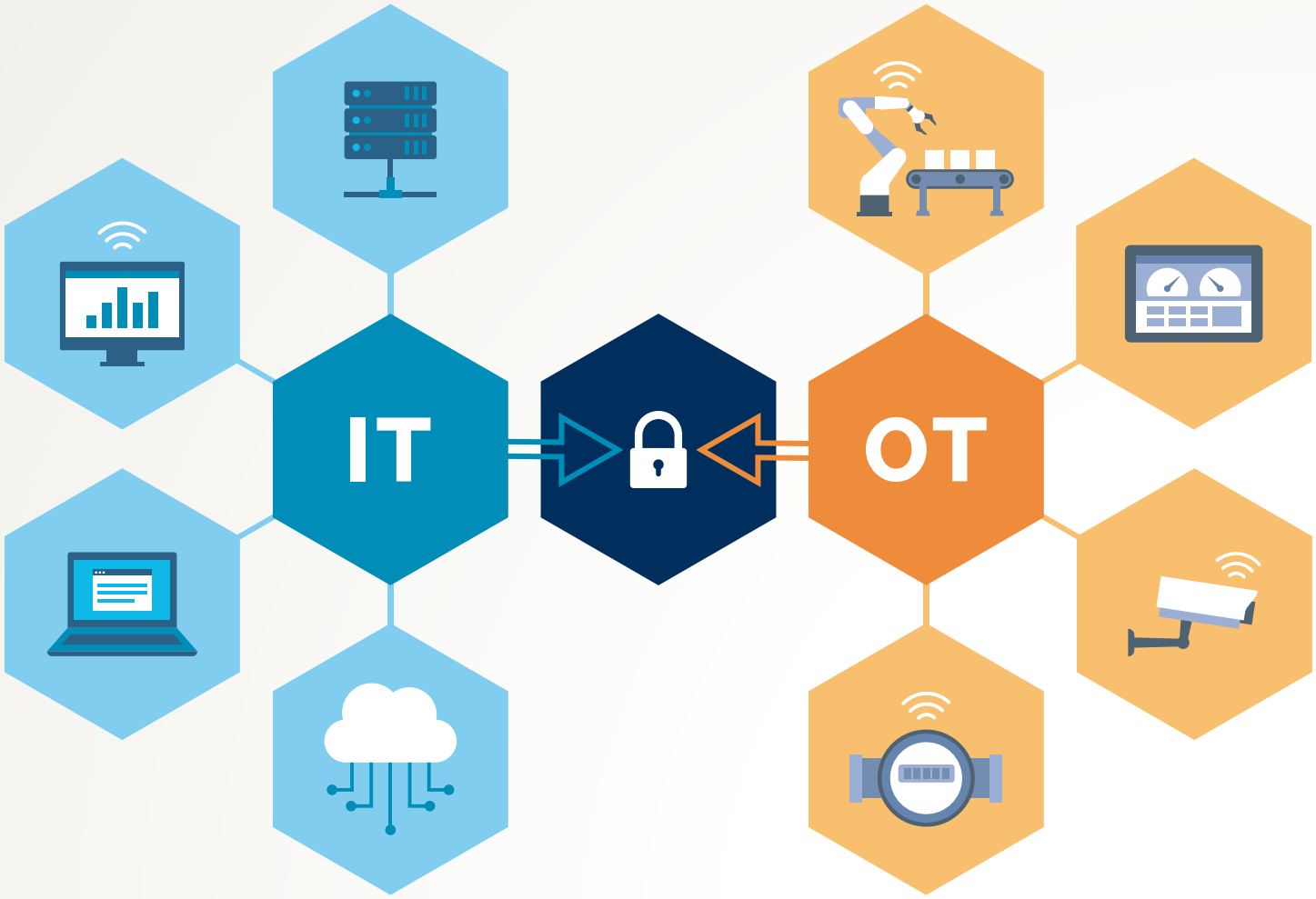

Unterschiedliche Schutzziele unter einem Dach

WARUM AUF LANGE SICHT IT DIE OT MANAGEN MUSS

Die ehemals vom Grundsatz her separierten Welten der Information Technology (IT) und Operational Technology (OT) wachsen im Zuge der Digitalisierung vermehrt zusammen. Doch was ist dabei aus Sicht der IT/IT-Sicherheit zu berücksichtigen und wem kann oder muss die letztendliche Verantwortung für eine durchgängige IT-Sicherheit des Unternehmens obliegen? Eine nicht ganz leicht zu klärende Aufgabenstellung – insbesondere mit Blick auf den Aspekt, dass die Schutzziele der beiden Unternehmensbereiche nicht einheitlich sind.

Während es bei der Sicherheit der IT in erster Linie um den Schutz der Daten beziehungsweise der digitalen Werte eines Unternehmens geht, steht im Kontext der OT zur Erhaltung der Betriebskontinuität eine Systemverfügbarkeit 24/7 an vorderster Stelle. Aufgrund der hohen Anzahl von Ransomware-Angriffen auf Fertigungsunternehmen – deren Schadensausmaß im vergangenen Jahr 22 Milliarden Euro betrug – ist es somit an der Zeit, die genannte Fragestellung genauer zu beleuchten.

Ein Ansatzpunkt hierfür ist, detailliert zu betrachten, wem im Rahmen der Digitalisierung welche Aufgabenstellung zuteilwird. Grundsätzlich ist die Kernaufgabe der IT Agilität und Geschwindigkeit im Sinne der Geschäftsentwicklung durch Flexibilität, Kostensenkung, Geschäftseinblick sowie IT-Sicherheit zu gewährleisten. Im Gegensatz dazu liegt bei der OT traditionell der Schwerpunkt auf Effizienz, Konsistenz, Kontinuität und (mittlerweile auch) IT-Sicherheit. Gemäß der Definition, dass „OT die produktionsnahe Steuerung aller operativen Abläufe von CPS (Cyber Physical Systems) in der smarten Fabrik umfasst", müsste die notwendige Verantwortlichkeit dafür insgesamt – also auch der Schutz der OT – in den entsprechenden Fachbereichen Produktionsplanung und -steuerung angesiedelt sein.

Faktisch sind jedoch im Rahmen der Digitalisierung die Zuständigkeiten von IT und OT nicht mehr genau zu definieren, und dementsprechend ist die ehemals klare Aufteilung nicht mehr evident. Das lässt sich anhand eines typischen Beispiels gut nachvollziehen: Maschinen und Anlagen sind sowohl zunehmend vernetzt als auch mit IT ausgestattet – etwa Sensoren, die permanent Produktionsdaten liefern. Diese sind nicht nur notwendig im Sinne der Prozessoptimierung, sondern liefern gleichzeitig auch Anhaltspunkte für neue und lohnende Geschäftsmodelle wie etwa die Bereitstellung von Services hinsichtlich einer optimierten Instandhaltung via Fernwartung. Von daher hat die Konnektivität zwischen IT und OT eine hohe Bedeutung. Deren Sicherstellung fällt teilweise in die Zuständigkeit der IT-Abteilung. Ebenfalls zu deren Aufgabenbereich gehört das Sammeln sowie die Analyse und Auswertung der relevanten Daten, die am Rand der Produktionsnetzwerke – Stichwort Edge Computing – zusammengetragen werden, da für die adäquate Nutzung der Produktionsdaten zunehmend künstliche Intelligenz (KI) zum Einsatz kommt und hierfür ausreichend leistungsstarke IT-Systeme zur Verfügung stehen müssen.

HERAUSFORDERUNGEN BEZÜGLICH IT-SICHERHEIT BEI OT UND IT

Die Herausforderungen in puncto IT/IT-Sicherheit im Rahmen der OT unterscheiden sich gravierend von denen der IT. Die IT wandelt sich in zunehmend kürzeren Zyklen – diese liegen momentan bei durchschnittlich drei Jahren – wodurch es möglich ist, die IT-Sicherheitsmaßnahmen dynamisch anzupassen. Bei der OT ist eine solche Vorgehensweise nicht möglich. Denn Fakt ist hier, dass die IT-Sicherheit der Systeme in der Produktion originär bei der Entwicklung nicht im Vordergrund stand. Dadurch und bedingt durch die Tatsache, dass es in der Produktion Systeme mit einem extrem langen Lebenszyklus gibt – teilweise bis zu 25 Jahre – sowie der Tatsache, dass in Produktionsstraßen Maschinen von verschiedenen Herstellern zum Einsatz kommen und der Anlagenbestand unterschiedlich veraltet ist, muss aufgrund der zunehmenden Vernetzung in der Produktionsumgebung ein Umdenken erfolgen. Denn die Verbindung der IT mit der OT führte dazu, dass die ehemals isolierten Maschinen übergangslos angreifbar geworden sind.

Da jedoch hinsichtlich der Schutzmaßnahmen keine Veränderung stattgefunden hat, ist der hierfür jetzt notwendige Aufwand zur Absicherung aus verschiedenen Gründen komplex. Die hohe Komplexität resultiert unter anderem daraus, dass die Software der einzelnen Komponenten zumeist proprietär ist. Dies stellt, ebenso wie die fehlende Interoperabilität im Hinblick auf den uneinheitlichen Anlagenbestand, ein nicht zu unterschätzendes Sicherheitsrisiko dar. Doch auch wenn Hersteller Software-Updates zur Verfügung stellen, so ist es nicht einfach möglich, den Vorgang automatisiert in den vorgegebenen Intervallen durchzuführen, denn dies erfordert eine Stilllegung der gesamten Produktionsanlage oder zumindest Teilen davon – was sich zumeist nicht ohne Weiteres realisieren lässt, da die Produktionszyklen in der Regel auf einen Betrieb 24/7 an 365 Tagen ausgelegt sind. Von daher sind hier Konzepte erforderlich, mittels derer diesen Schwachpunkten entgegengewirkt werden kann.

Bei der IT hingegen werden in der Regel weder Produkte oder Lösungen von unterschiedlichen Herstellern eingesetzt – bevorzugt die in ihrem Sektor führenden Unternehmen. Hier ist eher das Problem, dass die genutzten IT-Systeme und -Infrastrukturen nicht sicher genug konzipiert, aufgebaut, konfiguriert und upgedatet sind, um den Angriffen intelligenter Hacker erfolgreich entgegenzuwirken. Ein Beleg dafür, dass die Softwarequalität noch nicht den Anforderungen genügt, wurde im aktuellen „Bericht zur Lage der IT-Sicherheit in Deutschland 2022" vom Bundesamt für Sicherheit in der Informationstechnik (BSI) aufgezeigt: Die bekannten Schwachstellen sind um zehn Prozent gestiegen. Doch auch der immer höhere Komplexitätsgrad der IT-Systeme und -Infrastrukturen sorgt für größere Angriffsflächen. Konträr dazu konzipieren Cyberkriminelle zunehmend ausgefeilte Methoden, organisieren sich in Ökosystemen und investieren einen Teil ihrer Gewinne in neue, immer intelligentere und automatisierte Angriffstools. Daraus resultiert nicht nur ein hohes Gefährdungspotenzial mit Blick auf die Büro-IT, sondern auch für die Produktionsumgebung, da Angreifer zumeist die IT als Einfallstor nutzen.

PROBLEM ERKANNT: BASIS FÜR EINE GUTE VORGEHENSWEISE

Bevor die Befugnisse und Aufgaben für die Verantwortlichen im Bereich IT und OT bezüglich der IT-Sicherheit festgelegt werden können, muss als wichtigste Maßnahme die gesamte Angriffsfläche – sowohl physisch als auch virtuell – des Unternehmens eruiert werden. In diesem Rahmen gilt es, die bestehenden Prozesse sowie die zu deren Schutz eingesetzten Maßnahmen zu beleuchten. Dazu gehört auch ein Asset-Management zu etablieren, in dem die Komponenten der Netzwerk-Topologie inklusive aller installierten Hard-/Software- und Firmware-Versionen enthalten sind. Zur Erstellung dieses Profils ist es zudem notwendig, die Informationen bezüglich der Kommunikationsflüsse zu erheben. Als weiterer wichtiger Punkt muss das Daten-Management auf der Agenda stehen: Die Kategorisierung aller Daten im Unternehmen – also auch jener in der Produktion – ermöglicht, die sensiblen und unternehmenskritischen herauszufiltern. Da diese besonders schützenswert sind, ist es erforderlich, dass die Verantwortlichen genaue Kenntnisse darüber haben.

Basierend darauf gilt es, strategisch alle Schwachstellen zu betrachten, um entsprechende IT-Sicherheitsmaßnahmen dagegen zu entwickeln. Zum Beispiel, um möglichen Angriffen entgegenzuwirken: Einige neuralgische Punkte sind vom Ansatz her sowohl bei der IT als auch bei der OT gleich – etwa im Hinblick auf die Authentifizierung oder die Gewährung von Zugriffsrechten. Natürlich ist die Organisation der Zugriffsrechte für viele Unternehmen eine große Herausforderung, da jedem Mitarbeiter der Zugriff auf genau die Informationen und Systeme zur Verfügung gestellt werden muss, die er für seine Arbeit benötigt. Dies stellt insbesondere in der Produktion ein Problem dar, weil dort oftmals keine Benutzerzuordnung vorgesehen ist – allein aus dem Grund, dass die Funktionalität höchste Priorität hat. Von daher werden entweder aufgrund der Komplexität, oder der Bequemlichkeit sehr oft vielen Mitarbeitern in OT und IT zu umfangreiche Zugriffsrechte eingeräumt.

Daneben ist es auch bei der Authentifizierung angebracht, über neue Konzepte nachzudenken, denn in beiden Unternehmensbereichen sind vorwiegend schlecht gehandhabte Passwörter im Einsatz. Überall wird dieser Schwachpunkt noch zu selten berücksichtigt. Mit Blick auf die Gegebenheiten in der Produktionsumgebung ist dies jedoch nachvollziehbar: Da es für die OT weder eine vollumfängliche Nutzerverwaltung gibt, noch ein übergreifendes Tool zum Managen der Passwörter – aufgrund der Vielzahl an proprietären Systemen – werden oftmals die vorkonfigurierten Standard-Passwörter einfach übernommen.

FAZIT

Bei der Entscheidung bezüglich der Verantwortlichkeiten für die durchgängige IT/IT-Sicherheit sind einige Punkte bedenkenswert. Zum Beispiel der Aspekt, ob in IT-Abteilungen ein entsprechendes Know-how bezüglich der Produkte, etwa spezielle Firewalls, zur Absicherung von Produktions-Netzwerken und deren Eignung für den jeweiligen Einsatz des angefragten Anwendungszwecks tatsächlich vorhanden sein kann. Auch die Beschränkung der Zugriffsrechte gemäß dem Minimal-Prinzip – das bedeutet, den Zugriff auf Bediensysteme nur Mitarbeitern zu gewähren, die tatsächlich fachlich/disziplinarisch eine Berechtigung haben – ist nicht trivial und setzt entsprechende Kenntnisse voraus, da bestimmte Einschränkungen den Ablauf in der Produktion beeinträchtigen können.

Des Weiteren sollte dem Umstand Rechnung getragen werden, dass eine Netzwerksegmentierung – die klassische Maßnahme mit unmittelbar großer Auswirkung auf die IT und IT-Sicherheit – grundsätzlich auch von einem versierten OT-Spezialisten vorgenommen werden kann. Das ist allein schon unter dem Aspekt sinnvoll, dass dieser gleich die Implementierung der Produkte, die dezidiert zur Absicherung der Maschinen notwendig sind, initiieren kann.

Um jedoch die hohen Anforderungen, die mittlerweile an die Absicherung von Unternehmen gestellt werden, zu meistern, müssen IT und OT unbedingt an einem Strang ziehen, Stärken aber auch Schwächen der jeweils anderen Abteilung kennen und permanent im Austausch bleiben, um gut operativ zusammenarbeiten zu können. Dies erfordert, dass der jeweilige Verantwortungsbereich bezüglich der IT/IT-Sicherheit klar definiert sowie die Zuständigkeiten eindeutig zugeordnet werden. Die Aufgaben der IT sind dabei grundsätzlich: zum einen alle Maßnahmen zu ergreifen, um Angriffsmöglichkeiten aus dem Internet zu minimieren, sowie die Konnektivität zur OT auf das notwendige Minimum zu beschränken. Hierfür ist eine Abstimmung zwischen IT und OT unbedingt erforderlich, da nur dann die Initialisierung und Durchführung von Prozessen zur Absicherung der Produktionsnetzwerke reibungslos verläuft und Einigkeit über die Priorisierung von notwendigen Projekten hergestellt werden kann.

Um zu vermeiden, dass insgesamt divergente Konzepte entstehen, die keinesfalls umfassend genug sind, um das erforderliche Schutzniveau zu gewährleisten, muss strategisch gesehen eine Instanz vorhanden sein, die alle Anforderungen aus der IT und OT zusammenführt, sowie entsprechend überwacht. ■

SIEGFRIED MÜLLER
ist VP Advanced Technologies bei der MB Connect Line GmbH, die in den Bereichen Fernwartung, Datenerfassung und Industrial Security aktiv ist, und hat in einem internen Forschungsprojekt des Instituts für Internet-Sicherheit mitgewirkt.

NORBERT POHLMANN
ist Professor für Cybersicherheit und Leiter des Instituts für Internet-Sicherheit – if(is) an der Westfälischen Hochschule in Gelsenkirchen sowie Vorstandsvorsitzender des Bundesverbands IT-Sicherheit – TeleTrusT und im Vorstand des Internetverbandes – eco.