INDUSTRIEUNTERNEHMEN BEHANDELN DAS THEMA „INFORMATIONSSICHERHEIT“ ALLZU SORGLOS. DIE FORTSCHREITENDE DIGITALISIERUNG UND VERNETZUNG VERLANGT NACH EINER ANPASSUNG DER BISHERIGEN SICHERHEITSSTRATEGIE

ANGEMESSENES SICHERHEITSNIVEAU AUCH IN DER DIGITALEN WELT GEWÄHRLEISTEN

VON SEBASTIAN ROHR, ACCESSEC GMBH

Je weiter die Digitalisierung voranschreitet und je mehr sich ein Unternehmen intern sowie mit Kunden, Lieferanten und anderen Geschäftspartnern vernetzt, umso größer wird das Risiko, Opfer von Spionen, Saboteuren oder Datendieben zu werden. Analysen und Statistiken belegen: die Angriffe nehmen weltweit zu und werden immer zielgerichteter ausgeführt. In den Sicherheitsmaßnahmen von Industrieunternehmen wird der zugespitzten Bedrohungslage bislang allerdings nur unzureichend Rechnung getragen. Die große Mehrheit behandelt das Sicherheitsthema nach wie vor eher stiefmütterlich: Man beschränkt sich auf technische Fragen der IT-Sicherheit – und unterschätzt weitgehend, dass die größte Gefahr erwiesenermaßen vom eigenen Mitarbeiter ausgeht. Umfassende Sicherheit in einer zunehmend digitalisierten (Geschäfts-)Welt zu gewährleisten, verlangt, über die reine technische IT-Sicherheit hinaus auch Prozesse und Mitarbeiter in ein ganzheitliches Schutz- und Sicherheitskonzept einzubinden. Für die Mehrzahl der Unternehmen bedeutet dies, dass sie ihre bisherige Sicherheits-Policy grundlegend überdenken und sich – sicherheitsstrategisch – weitgehend neu ausrichten müssen.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) erstellt turnusmäßig einmal im Jahr seinen Lagebericht zur IT-Sicherheit in Deutschland. Die Fakten sind eindeutig, die verschärfte Gefährdungslage sollte jedem Unternehmen zu denken geben: „Zunehmende Digitalisierung und Vernetzung bieten Cyber-Angreifern fast täglich neue Angriffsflächen und weitreichende Möglichkeiten, Informationen auszuspähen, Geschäfts- und Verwaltungsprozesse zu sabotieren oder sich anderweitig auf Kosten Dritter kriminell zu bereichern.“[1] Nach den Erkenntnissen des BSI verfügen die Angreifer über enorm leistungsfähige und flexibel einsetzbare Angriffsmittel und -methoden. Die Angriffe können jederzeit und aus allen möglichen Richtungen kommen. Die bisherigen klassischen Abwehrmaßnahmen verlieren dadurch weiter an Wirksamkeit.

In konkreten Zahlen bedeutet dies, dass in den vergangenen 24 Monaten bereits mehr als die Hälfte der Unternehmen in Deutschland (53 Prozent) angegriffen und Opfer von Wirtschaftsspionage, Sabotage oder Datendiebstahl geworden ist.[2] Die Zahl der kompromittierten Unternehmen dürfte noch um einiges höher liegen, denn in vielen Fällen versuchen die Verantwortlichen, erfolgte Cyber-Angriffe nicht publik werden zu lassen – vor allem, weil sie negative wirtschaftliche Konsequenzen befürchten und/oder den „guten Ruf“ des Unternehmens nicht beschädigt sehen möchten.

MANGELNDE SENSITIVITÄT AUF DER OBERSTEN FÜHRUNGSEBENE

In vielen Unternehmen sind sich die Verantwortlichen der enorm verschärften Gefährdungslage überhaupt nicht bewusst. Manche – darunter auch erfolgreiche mittelständische Unternehmen des produzierenden Gewerbes – beginnen sogar erst langsam zu realisieren, wie sehr sie bereits jetzt von den über die Jahre implementierten IT-Systemen und deren reibungsfreiem Funktionieren abhängig sind. Mittlerweile kann es sich kaum noch ein Industrieunternehmen leisten, seine IT über einen längeren Zeitraum nicht verfügbar zu haben. Bei Ausfällen von drei, vier Schichten kann die Situation durchaus schon brenzlig werden. Dazu ist nicht einmal ein Komplettausfall der Systeme nötig. Es reicht, wenn bestimmte Anwendungen wie der elektronische Datenaustausch mit den Kunden nicht funktioniert. Bei JIT-/JIS-Lieferverträgen kann das wegen entsprechender Konventionalstrafen sehr schnell extrem teuer und äußerst unangenehm werden.

In den Sicherheitsmaßnahmen der Unternehmen spiegelt sich diese weitreichende System-Abhängigkeit allerdings nur unzureichend wider. Was wir stattdessen in der Praxis immer wieder feststellen können: viel zu viele Unternehmen begnügen sich in Sicherheitsfragen mit den standardmäßigen technischen Schutzmaßnahmen. Dass heute überall mit Passwörtern, Antivirus-Programmen und Firewalls gearbeitet wird, bedarf eigentlich keiner besonderen Erwähnung. Intrusion-Detection-Systeme, die es ermöglichen, Angriffe auf Computersysteme und Netzwerke zu erkennen und anzuzeigen, findet man hingegen nur selten. Doch auch mit diesen oder ähnlichen anspruchsvolleren Maßnahmen wird man den gewachsenen Sicherheitsanforderungen von heute noch lange nicht gerecht. Ausschließlich auf technische Schutzmaßnahmen zur IT-Sicherheit zu setzen, wie dies die meisten Unternehmen handhaben, greift viel zu kurz. Oder – um es einmal plakativ auszudrücken: in weiten Teilen des industriellen Mittelstandes ist das Sicherheitsniveau allenfalls drittklassig.

Manchmal ist es für uns geradezu schockierend, zu sehen, wie fahrlässig und gedankenlos Unternehmensverantwortliche das Thema IT-Sicherheit behandeln und wie sie mit diesem Verhalten im Prinzip die gesamte Organisation gefährden. Ein gutes Niveau an Sicherheit ist nur zu erreichen, wenn neben der technischen Seite auch die Prozesse und die Mitarbeiter in eine unternehmensindividuell zu konzipierende Security-Strategie eingebunden werden. Der Mensch ist nun mal das größte Sicherheitsrisiko – und es ist vollkommen egal, ob man das Topmanagement betrachtet, das mittlere Management, Sachbearbeiter, den Werker auf dem Shopfloor oder die Mitarbeiter am Empfang: jeder kann eine Schwachstelle sein und ist daher als mögliches „Einfallstor“ gefährdet. Bei den besag-

[1] Die Lage der IT-Sicherheit in Deutschland 2017, BSI – https://www.bsi.bund.de/DE/Publikationen/Lageberichte/lageberichte_node.html
[2] Bitkom-Studie 2017: Spionage, Sabotage und Datendiebstahl – Wirtschaftsschutz in der Industrie

ten Unternehmen, die in den vergangenen zwei Jahren Opfer von Cyber-Angriffen geworden sind, stammten zwei von drei Tätern (62 Prozent) aus dem Kreis aktueller und ehemaliger Mitarbeiter.

Auf welche Art und Weise Angreifer in ein Netzwerk eindringen, ist ihnen in aller Regel egal. Sind sie erst einmal „drin", besteht für sie immer die Möglichkeit, sich von diesem Punkt aus lateral durch die Organisation zu bewegen, um ihre Ziele zu erreichen. Dass dieses Vorgehen funktioniert, zeigt uns die Praxis Tag für Tag. Geradezu exemplarisch hierfür ist der vom BSI publik gemachte Fall, in dem es Angreifern gelang, bei einem deutschen Stahlkonzern die Steuerung eines Hochofens zu übernehmen.

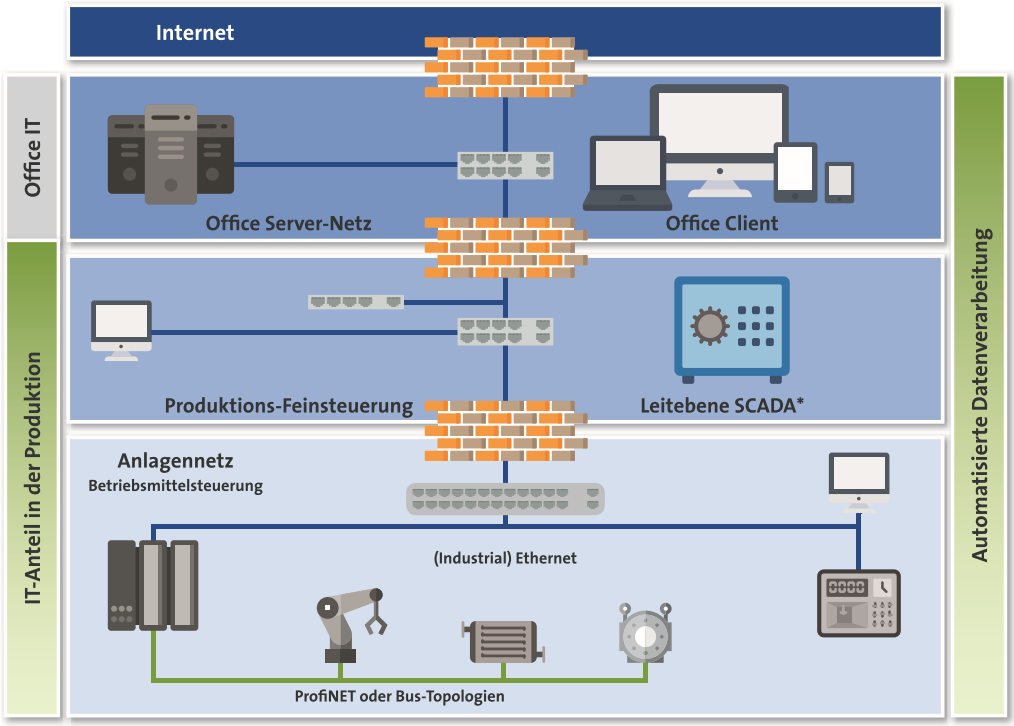
Dem BSI-Bericht zufolge haben sich die Angreifer zunächst durch sogenanntes Spear-Phishing, also mit gezielt auf spezielle Mitarbeiter zugeschnittenen falschen E-Mails, Zugang zum Büro-Netzwerk der Anlage verschafft. Von dort aus arbeiteten sie sich Stück für Stück bis in die Produktionsnetze vor. Die Kompromittierung erstreckte sich letztlich auf eine Vielzahl unterschiedlicher interner Systeme bis hin zu industriellen Komponenten. Der Zugriff auf das Produktionsnetz ermöglichte es den Angreifern, die Steuerkomponente des Stahlwerkes zu manipulieren. Konsequenz war: Die Ausfälle einzelner Steuerungskomponenten oder ganzer Anlagen häuften sich. Die Probleme spitzten sich schließlich derart zu, dass ein Hochofen nicht mehr geregelt heruntergefahren werden konnte und sich – wie das BSI es formulierte – „in einem undefinierten Zustand" befand. Man könnte auch sagen: Den Angreifern war es gelungen, diesen Hochofen lahmzulegen.

MIT DER VERNETZUNG WACHSENDE SICHERHEITSRISIKEN ERFORDERN NEUE SICHERHEITSLÖSUNGEN

Leider sind gezielte Angriffe auf Fertigungs- und Industriesteuerungssysteme hierzulande längst Realität. Fakt ist auch, dass die Angreifer immer professioneller werden und immer zielgerichteter vorgehen. Was Unternehmensverantwortlichen darüber hinaus zu denken geben sollte, ist die Tatsache, dass wir uns erst am Anfang einer Entwicklung befinden, in deren Verlauf sich immer mehr Industrieunternehmen vernetzen und mit Kunden, Lieferanten, Dienstleistern und weiteren Stakeholdern Daten austauschen werden.

Mit der zunehmenden Vernetzung wachsen also auch die Sicherheitsrisiken enorm an. Denn Maschinen und Anlagen stehen dann eben nicht mehr „abgeschottet" in einer Fabrikhalle. Stattdessen werden sie zu Bestandteilen eines unternehmensübergreifenden Netzwerkes, über das – unter Einschluss des World Wide Web – ständig Daten hin und her transferiert werden. Eigentlich liegt es auf der Hand, dass in diesen Szenarien die klassischen Sicherheitsmaßnahmen einfach nicht mehr ausreichen, um ein ordentliches Sicherheitsniveau zu gewährleisten. In dieser neuen (Geschäfts)-Welt braucht es allerdings nicht nur neue Sicherheitslösungen, sondern zunächst einmal die Erkenntnis, dass man in der „schönen neuen Industrie 4.0-Welt" als Unternehmen noch einmal deutlich gefährdeter ist als ohnehin schon.

In der Vergangenheit war der Produktionsbereich informationstechnisch in gewisser Weise abgeschottet, weil die Maschinen grundsätzlich über eine eigene Sprache und eigene Netze miteinander kommuniziert haben. Über die Jahre wurden dann auch in den Werkshallen immer mehr Windows-Rechner bzw. Standard-Office-Technologie eingesetzt, um bestimmte Aufgaben der Produktion zu übernehmen. Die Unternehmen haben zudem in Computer Aided Manufacturing und Fertigungs-Informationssysteme investiert, die eine übergreifende Vernetzung erforderten. Zusammen mit der fortschreitenden Standardisierung in der Automatisierungs- und Leittechnik hat dies dazu geführt, dass von einem Büro-Arbeitsplatz in der Verwaltung bis hin zu einem Steuergerät in der Produktion eine offene Kommunikation möglich wurde. Über die Implikationen für die Informationssicherheit



*SCADA = Supervisory Control and Data Acquisition (Konzept zur Überwachung und Steuerung techn. Prozesse)

↘
Abbildung 1:
Wie sich industrielle Netze von der Office-IT abgrenzen sollten

hat sich dabei niemand Gedanken gemacht. Inzwischen können manche Maschinen und Anlagen über ihre Einbindung ins Internet genauso angesprochen werden, wie handelsübliche Bürocomputer – ein kurzer Blick in spezialisierte Suchmaschinen wie „Shodan.io“ bringt erschreckende Erkenntnisse zu Tage: ganze Steuerungsanlagen von der Glockenturmsteuerung bis hin zu Klärwerksteuerungen sind aus dem Internet frei zu erreichen. Im Umkehrschluss bedeutet dies: Die bestehenden Sicherheitslücken und Schwachstellen im Windows-Betriebssystem werden nun auf einen hochsensiblen Bereich, die Produktion, übertragen und sind gegebenenfalls von außen leicht zu erreichen.

Vielen mittelständischen Unternehmen scheint diese Problematik noch nicht so recht bewusst zu sein – zumindest nicht in ihrer ganzen Dimension. Die Erfahrung unzähliger Gespräche auf C-Level-Ebene hat gezeigt, dass das Thema „Informationssicherheit“ und dessen Bedeutung im Zeitalter von Digitalisierung und Vernetzung noch nicht vollständig erfasst und vor allem nicht ausreichend bewertet ist. So trifft ein extrem gewachsener Sicherheitsbedarf hier noch immer auf ein unzureichend ausgeprägtes Sicherheitsbewusstsein. Dies muss sich dringend ändern! Denn: Wer die Sicherheitsproblematik nicht in den Griff bekommt, wird auch seine digitale Transformation nicht erfolgreich gestalten können. Ohne ein sicheres Fundament stehen jegliche Bestrebungen der Industrie 4.0 oder der Digitalisierung sprichwörtlich auf tönernen Füßen. Aus unserer Sicht ist es daher unerlässlich, die eigene Informationssicherheits-Strategie – sofern es sie denn überhaupt schon gibt – zu überarbeiten und der verschärften Gefährdungslage anzupassen.

DIGITALISIERUNG ALS CHANCE ZUR OPTIMIERUNG DES SICHERHEITSNIVEAUS NUTZEN

Einen hundertprozentigen Schutz vor Spionage, Sabotage und Datendiebstahl kann und wird es nie geben. Mit einem ganzheitlichen Ansatz zur „Informationssicherheit“ lässt sich jedoch das immanente Risiko, Opfer eines Cyber-Angriffes zu werden, auf ein Minimum reduzieren. Schafft man es, Informationssicherheit umfassend und von Grund auf im Unternehmen zu verankern und „Security by Design“ quasi in die DNA des Unternehmens einzubauen, werden klassische Maßnahmen der

IT-Sicherheit schnell sekundäre Schauplätze. Neben der eher technischen Seite müssen vor allem die Informationsflüsse im Unternehmen und über dessen Grenzen hinaus betrachtet werden. Und zwar sowohl die „realen“ – von Mensch zu Mensch im Prozess – als auch die digitalen zwischen den Systemen. Es gilt die Fragen zu beantworten:

- Wo könnte jemand Drittes negativ Einfluss nehmen, indem er Informationen abzieht, auf die er keinen Zugriff haben dürfte?
- Wo könnte jemand Informationen fälschen und dadurch Abläufe verändern?
- Wie verläuft die Kommunikation zwischen der Produktion und der Office-IT und wie lassen sich kritische Produktionsanlagen vom restlichen Netzwerk „abschotten“?
- In welchen Wertschöpfungsprozessen sind die ökonomischen Verluste durch Cyber-Angriffe besonders gravierend und wieviel Risiko lässt sich durch geeignete Gegenmaßnahmen reduzieren?

Letztlich geht es darum, ein unternehmensspezifisches Gefahren- und Sicherheitsprofil zu erstellen und zu erkennen, wo man besonders gefährdet ist bzw. wo ein Angriff besonders schwerwiegende Folgen haben könnte. Der Spezialist spricht in diesem Zusammenhang von einer Business-Impact-Analyse, oder „BIA“. Informationssicherheit hat also auch einen deutlichen Bezug zum Risikomanagement eines Unternehmens. Nachhaltige Informationssicherheit zu erreichen ist demnach kein „einmaliger Akt“, sondern eine stetige Aufgabe, die ebenso steter Aufmerksamkeit bedarf. Operativ wird Informationssicherheit deshalb als Prozess-Zyklus praktiziert und muss sich wiederkehrend einer Selbst- und Fremdprüfung (etwa durch Audits) unterziehen. Nur wer im eigenen Unternehmen immer „auf der Hut“ ist, kann Cyberangriffen kompetent entgegenwirken und die Auswirkung erfolgreicher Angriffe minimieren. Management und Geschäftsführung sind zur Wahrnehmung dieser Aufgaben übrigens durch die Sorgfaltspflicht nicht delegierbar verpflichtet. Es ist und bleibt in der Verantwortung von Vorstand und Geschäftsführung, das Unternehmen bedrohende Risiken zu erkennen, zu erfassen, zu bewerten und notwendige Gegenmaßnahmen zu ergreifen!

Um dieser permanenten Aufgabe mit der gebotenen Ernsthaftigkeit nachzukommen, ist es zwingend erforderlich, in den Unternehmen eine voll verantwortliche Person für diesen Themenbereich zu benennen und zu etablieren. In größeren Unternehmen sollte diese Aufgabe von einem speziell ernannten Chief Security Officer (CSO) wahrgenommen werden, der organisatorisch direkt unterhalb der Geschäftsleitungsebene angesiedelt ist und idealerweise an den CFO berichtet. Dies ist erforderlich, um die Governance-Aufgaben der Position gegenüber der internen IT, etwa dem CIO, mit dem nötigen Nachdruck wahrnehmen zu können. In mittelständischen Unternehmen muss dies keine Vollzeitstelle sein. Benötigt wird ein verantwortlicher „Kümmerer“ mit professioneller Aufstellung aber auch dort. Wichtig ist, dass diese Person möglichst weisungsfrei agieren kann und die volle Unterstützung der obersten Führungsebene besitzt.

Eine solche Funktion zu etablieren, reicht natürlich nicht aus. Der oder die Betreffende muss auch über die Autorität und die Machtposition verfügen, verbindliche Sicherheits-Policies erstellen und verabschieden zu dürfen. Zu seinen Aufgaben gehört ferner, die bereits erwähnte Risikoanalyse zu erstellen und darauf zugeschnittene Policy-konforme Sicherheitsmaßnahmen abzuleiten. Um diese Aufgabe schnell und effizient anzugehen und sich nicht in der Komplexität der Sicherheitsthematik zu verlieren, sollten erfahrene Sicherheitsexperten eingebunden werden, die mit vergleichbaren Aufgaben bereits in anderen Unternehmen betraut waren.

Diese Experten haben die notwendige Erfahrung, Sicherheitsprobleme und Risiken korrekt einzuschätzen und Maßnahmen sinnvoll und nachhaltig zu planen. Zudem können externe Spezialisten mögliche Fallstricke bei der Umsetzung von Maßnahmen frühzeitig identifizieren und Aussagen treffen, was in der betreffenden Branche vor dem Hintergrund der fortschreitenden Digitalisierung

und Vernetzung „State of the Art“ in Sachen Informationssicherheit ist. Wichtige Erkenntnis ist: Man muss nicht alle Fehler selber begehen, sondern lernt im Optimalfall aus den Fehlern Anderer. Ein erfahrener Externer kann hier wertvolle Hinweise liefern und hilft dabei, übereilte punktuelle Investitionen gegen strategisch wertvolle, nachhaltige Maßnahmen zu tauschen.

Bewährt hat sich die Einbindung eines externen Sicherheitsexperten zudem als Initiator und Moderator eines Jour-Fixes, bei dem alle relevanten Stakeholder aus der Produktion, der Instandhaltung, der Werks-IT und der zentralen IT in regelmäßigen Abständen zusammenkommen und sich gegenseitig auf den neuesten Stand bringen.

Eine regelmäßige Zusammenkunft dieser Stakeholder ist ungemein wichtig, weil dort aufs Tapet kommt, welche Auswirkungen – aus dem Blickwinkel der Informationssicherheit – bestimmte neue Vorhaben für die jeweils anderen Bereiche mit sich bringen. Dabei entsteht fast beiläufig die gegenseitige Erkenntnis, dass die IT eine vollautomatisierte Produktionsanlage nicht so ohne Weiteres ins Netzwerk einbinden kann, während die IT ihrerseits – moderiert durch den „Neutralen“ – der Produktion erläutern kann, warum bei einer neu zu beschaffenden Produktionsanlage tunlichst bestimmte IT-Sicherheitsanforderungen berücksichtigt werden sollten. Anforderungen, die idealerweise dann auch Eingang in die Einkaufsleitfäden und in die Verhandlungen mit Lieferanten finden. Am Ende des Tages geht es bei diesen regelmäßig durchzuführenden interdisziplinären Zusammenkünften darum, gegenseitiges Vertrauen aufzubauen, einen Blick für die Herausforderungen der jeweils anderen zu bekommen und diese Erkenntnisse in zielführende Sicherheitsmaßnahmen einfließen zu lassen.

Klar ist also: Es braucht vor allem eine gemeinsame, von allen Stakeholdern getragene Antwort auf die verschärfte Bedrohungslage.

Fakt ist vielmehr, dass wir mit der digitalen Transformation und dem Wandel zu Industrie 4.0 plötzlich eine Branche ins Internet-Zeitalter katapultieren, die oft noch mit Windows 95, Windows 2000 & Co. arbeitet. Von Windows XP ganz zu schweigen. Auf sichere Kommunikation, Verschlüsselung und Authentisierung wurde nie besonderes Augenmerk gelegt. Auf einmal möchte man diese nur unzureichend geschützten IT-Systeme sensorgestützt als Datensammler „missbrauchen“, um neue digitale Geschäftsmodelle aufzubauen. Das kann nicht funktionieren.

Bei der digitalen Transformation handelt es sich um eine disruptive Änderung. Als Unternehmen sollte man sich daher jetzt die Frage stellen: Kann mein bestehendes Sicherheitsregelwerk die neuen Anforderungen überhaupt abdecken? Die meisten Unternehmen werden dies verneinen müssen. Wir können Unternehmensverantwortliche daher nur ermutigen, diese neue Situation als große Chance zu sehen. So können überkommene Zöpfe abgeschnitten und bestehende Regelungen gründlich überdacht werden. Ein gründliches Aufräumen und Ausmisten birgt letztlich die Chance, sich sicherheitsstrategisch so aufzustellen, dass auch die digitalen Geschäftsmodelle durch eine neue Sicherheits-Policy abgedeckt werden.

Bei neu zu entwickelnden digitalen Geschäftsmodellen halten wir es für ungemein wichtig, einen „Security and Privacy by Design“-Ansatz zu fahren. Wer also in Zukunft zusätzliche Daten generieren, aufbereiten, in einer Cloud bereitstellen und daraus Mehrwert ziehen möchte, sollte nicht nur über das Wie nachdenken. Genauso wichtig ist vielmehr die Frage, wie dies technologisch gelingt, ohne die Sicherheit des Unternehmens zu gefährden. Wenn die Sicherheit schon von Anfang an in ein Produkt oder Geschäftsmodell hinein modelliert wird, dann erleichtert dies die Umsetzung ungemein. Hinzu kommt: Die Kosten für Informationssicherheit werden hier als Investitionskosten in den „Business Case“ mit eingeplant. Wenn die Geschäftsidee sich dadurch nicht rechnet, sollte man sie lieber fallen lassen. Dann reicht der Reifegrad in der IT, in der Produktions-IT und generell in der Informationssicherheit eben nicht aus, um schon jetzt in die Industrie-4.0-Welt einzusteigen.

So wichtig die in diesem Beitrag bereits vorgestellten Maßnahmen und Empfehlungen sind: Eine der größten Herausforderungen wurde noch nicht adressiert – der eigene Mitarbeiter. Mitarbeiter müssen in Sicherheitsfragen professionell geschult und für das Thema Informationssicherheit sensibilisiert werden. Aus unserer Sicht besteht auf diesem Themenfeld ein gehöriger Nachholbedarf.

Oft nutzen Angreifer die Hilfsbereitschaft und das Vertrauen von Mitarbeitern aus, um an wichtige Informationen zu kommen – über Zuständigkeiten im Unternehmen, zur Zusammensetzung von Abteilungen, zu internen Prozessen oder Organisationsstrukturen. Dieses sogenannte „Social Engineering" ist eine der kritischsten und am häufigsten verwendeten Angriffsmethoden. Laut einer aktuellen Umfrage des BSI[3] können Cyber-Angreifer mit den so gewonnenen Informationen erheblichen Schaden anrichten – etwa durch CEO-Fraud: mit fingierten E-Mails der Chefetage werden bei dieser „Masche" befugte Mitarbeiter angewiesen, hohe Geldsummen zu überweisen. Laut BSI geht es dabei um Millionensummen: Sobald Angreifer wissen, wen sie anschreiben müssen und wie die Prozesse im Unternehmen laufen, gelingt es ihnen sehr oft, großen psychischen Druck beim Angeschriebenen aufzubauen und auch erfahrene Mitarbeiter zur Überweisung hoher Beträge zu bewegen.

Die Sensibilisierung der Mitarbeiter für diese Art von Betrugsversuchen und Attacken sollte ein obligatorisches Element in jeder Schulungskonzeption sein. Nicht minder wichtig sind die fachliche Fortbildung der Mitarbeiter und der Aufbau spezieller Kompetenzen. In der Praxis erleben wir es zum Beispiel immer wieder als Problem, dass nur wenige Automatisierungs- und Anlagentechniker über tiefergreifende IT-Kenntnisse verfügen. Eine richtige Schulung haben nur die wenigsten bekommen. Genauso besitzen nur wenige IT-Mitarbeiter das Know-how, wie Anlagen- und Automatisierungstechnik funktioniert. In solchen Konstellationen macht es Sinn, zunächst eine gemeinsame Arbeitsgruppe zu bilden, damit die Betreffenden sich annähern und einfach mal in einen Diskurs kommen. Nicht selten entstehen Probleme ja bereits dadurch, dass die beteiligten Fachfunktionen unterschiedliche Sprachen sprechen. Im weiteren Verlauf sind dann die Produktionsleitung, die Standortleiter und die Team-Leads für Instandhaltung und -planung gefordert, in sehr enger Abstimmung mit der IT einen sinnvollen Aus- und Weiterbildungsplan für die Mitarbeiter am Standort zu entwickeln.

Sensibilisieren der Belegschaft einschließlich der obersten Führungsebene für die verschärfte Bedrohungslage, gezielte fachliche Aus- und Fortbildung der Mitarbeiter, Installieren einer Person, die sich hauptverantwortlich um das Thema „Informationssicherheit" kümmert, Überarbeiten der bestehenden Sicherheitsstrategie, Ausarbeiten und Umsetzen eines ordentlichen Policy Framework bzw. einer Sicherheitsstrategie, welche die Anforderungen der digitalen Welt mit berücksichtigt – dies alles lässt sich natürlich nicht von heute auf morgen realisieren. Und ohne Aufstocken der finanziellen und personellen Ressourcen in dieses Themenfeld kann es den gewünschten umfassenden Schutz ebenfalls nicht geben. Auf den ersten Blick mag es ein kostenträchtiges Unterfangen sein, ein hohes Niveau an Informationssicherheit zu gewährleisten. Wesentlich teurer wird es für Unternehmen in Zukunft allerdings, nicht oder nur unzureichend in dieses Themenfeld zu investieren. ↙

Sebastian Rohr ist Geschäftsführer (CTO) der accessec GmbH – ein Unternehmen, das sich auf Sicherheitsstrategien und ganzheitliche Sicherheitslösungen spezialisiert hat. Das Leistungsportfolio beinhaltet unter anderem die ganzheitliche Analyse kritischer Geschäftsprozesse, unternehmensindividueller Risikostrukturen und bereits etablierter Sicherheitsmaßnahmen.

accessec ist Kooperationspartner der TMG. TMG zieht die Expertise von accessec immer dann zurate, wenn es in Projekten zur digitalen Transformation von Industrieunternehmen um die Beantwortung sicherheitsrelevanter Fragestellungen geht.

[3] Pressemitteilung vom 26.07.2018 zur BSI-Umfrage – 06/2018