DGQ Expertenwissen

Mythen der Cyber-Sicherheit

DGQ
Deutsche Gesellschaft
für Qualität

Mythen der Cyber-Sicherheit

Die Art und Weise, wie wir in Zukunft arbeiten werden, hat sich durch die Digitalisierung grundlegend verändert. Das gilt auch für die industrielle Produktion. Intelligente und vernetzte Produktionsanlagen und Systeme bilden die Grundlagen für die Industrie 4.0. Diese Vernetzung bietet Unternehmen vielfältige Möglichkeiten. Gleichzeitig entstehen durch die eigenständige Kommunikation der Anlagen neue Sicherheitsrisiken.

In den Medien sind Berichte von Datenpannen, Cyber-Angriffen und Sicherheitslücken allgegenwärtig und die Folgen für die Unternehmen oft weitreichend. So wurden laut der Cyber-Sicherheits-Umfrage des Bundesamts für Sicherheitstechnik und Informationstechnik (BSI) aus dem Jahr 2017 rund 70 Prozent der Befragten Opfer von Cyber-Angriffen.

Diese Attacken hatten zum Teil erhebliche Konsequenzen für die Betriebe. Jeder zweite Betroffene gab an, dass es 2016/2017 zu Produktions-bzw. Betriebsausfällen kam. Darüber hinaus entstanden bei knapp 23 Prozent der Befragten Kosten für die Aufklärung der Vorfälle und die Wiederherstellung der IT-Systeme. Bei rund 16,5 Prozent der Befragten waren Reputationsschäden die Folge. Auch wenn das Gefahrenbewusstsein für Cyber-Angriffe in Unternehmen inzwischen sehr hoch ist und vielfältige Gegenmaßnahmen getroffen werden, beziehen sich diese nicht speziell auf die vernetzte Produktion. Zudem kursieren immer noch diverse Mythen über Cyber-Sicherheit. Diejenigen, die das Büro- oder Verwaltungsnetzwerk in Unternehmen betreffen, sind uns geläufig. Zum Beispiel, dass eine gute Verschlüsselung von E-Mails zu aufwendig und teuer sei oder dass eine Sicherheitssoftware ein Unternehmen hinreichend vor Angriffen schützt. Das Gleiche gilt für eine vernetzte Produktionsanlage. Auch hier ist es wichtig, über die verbreitetsten Mythen aufzuklären und Unternehmen optimal auf die Anforderungen der Industrie 4.0 vorzubereiten. Die DGQ hat Dr. Christian Haas, Experte des Fraunhofer IOSB, gefragt, um welche Mythen es sich konkret handelt, und was Unternehmen tun können, um sich zu schützen.

Mythos 1: Unsere Systeme sind nicht über das Internet erreichbar

Dieser Mythos ist bei Unternehmen in der industriellen Produktion weit verbreitet. Tatsächlich sind durch die zunehmende Digitalisierung Vernetzungen zwischen Fertigungs- oder Produktionsnetzwerk und dem Büro- oder Verwaltungsnetzwerk noch ausgeprägter. Zudem sind verschiedene Komponenten der industriellen Produktionsanlagen direkt mit dem Internet verbunden. Produktionsanlagen kommunizieren nicht mehr nur miteinander, sondern auch mit ihrem Hersteller außerhalb des Unternehmens. Hinzu kommen drahtlose Komponenten und Daten-und Service-Clouds. Hier liegen nicht nur Potenziale, sondern auch mögliche Angriffspunkte für Cyber-Angriffe auf Produktionsnetze. Diese können enorme Auswirkungen bis hin zu kompletten Ausfällen oder im Extremfall sogar die physische Zerstörung der Anlage haben. Können sich Geräte mit dem Internet vernetzen, können sie auch gefunden und theoretisch angegriffen werden. Eine Methode, internetfähige Geräte oder auch Komponenten von Produktionsanlagen zu finden, ist die Suchmaschine „Shodan“. Mit ihr lassen sich Geräte finden, die mit dem Internet gekoppelt sind – auch wenn den Betreibern die Verbindung zum Internet nicht unbedingt bewusst ist. Hierzu zählen Webcams, Router, Server, Netzwerkdrucker aber auch industrielle Steuerungsanlagen. Sind diese nicht ausreichend geschützt, ergeben sich erhebliche Sicherheitslücken.

Mythos 2: Unsere Systeme sind sicher, sie sind hinter einer Firewall

Auch diese Aussage kennt man vom heimischen PC und dem Büronetzwerk. Sie lässt sich aber ebenso auf vernetzte Industrieanlagen übertragen. Eine Firewall ist ein wichtiger Aspekt von Cyber-Sicherheit im Industrieumfeld. Allerdings ist jede Firewall nur so sicher, wie ihre Konfiguration. Eine Auswertung von Fehlern in Firewall-Konfigurationen zeigte beispielsweise, dass in mehr als der Hälfte der Fälle neun der 12 klassifizierten Fehler auftraten. Auch wenn dieses Beispiel aus dem IT-Umfeld stammt, ist in der vernetzten Produktion von ähnlichen Zahlen auszugehen. Dass eine Firewall vorhanden ist, ist also allein kein ausreichender Schutz gegen Cyber-Attacken auf Produktionsanlagen.

Mythos 3: Wir wurden noch nie angegriffen, wir sind kein Ziel

Auch diese Aussage gehört zu den Mythen der Cyber-Sicherheit. Sowohl im privaten Alltag, als auch bei Unternehmen ist die Meinung weit verbreitet, man sei für Cyberangriffe zu uninteressant oder zu unbedeutend. Im Privaten kommt oft noch die Aussage hinzu, man habe ja nichts zu verbergen und müsse sich deswegen auch keine Sorgen um Datenmissbrauch machen. Das ist in Unternehmen natürlich ganz anders gelagert. Hier können Hacker auf zahlreiche sensible und wertvolle Daten zugreifen. Jüngstes Beispiel ist der Datendiebstahl bei British Airways bei der ca. 380.000 Bank- und Kreditkarten betroffen waren. Bei produzierenden Unternehmen kommt neben dem Diebstahl von Informationen zum Betriebsablauf, den Produktionssystemen und Informationen aus Forschung und Entwicklung sowie Patente auch die digitale Sabotage von Produktionsanlagen als Risikofaktor hinzu. Unternehmen können auch dann angegriffen werden, wenn Sie nicht das primäre Ziel eines Hackerangriffs sind. Ein Beispiel ist hier Ransomware, die Computer von Industrieunternehmen lahmlegte, ohne dass diese das eigentliche Ziel waren. Jedes Unternehmen wird erpressbar, wenn erst mal die Produktion gestört ist oder zum Erliegen kommt. Zudem liegt die Dauer zwischen dem Angriff und der Entdeckung im Schnitt bei drei bis fünf Monaten. Es ist also fraglich, ob jedes Unternehmen weiß, ob und wie oft es bereits Ziel von Hackerangriffen war.

Sicherheit zur Chefsache machen

Damit Sicherheit, und insbesondere Cyber-Sicherheit in der vernetzten Produktion zur Chefsache wird, muss die Geschäftsführung und Führungskräfte für dieses Thema sensibilisiert werden. Diese und die folgenden Empfehlungen haben Bitkom und Bundesverfassungsschutz für mehr Sicherheit in Unternehmen veröffentlicht*. Ebenso lassen sich diese auch auf die vernetzte Produktion anwenden. Auf Leitungsebene müssen die geeigneten Schutzmaßnahmen initiiert werden – sowohl für das Verwaltungs- als auch für das Fertigungsnetzwerk.

Führungskräfte sollten sich vor der Einführung adäquater Schutzmaßnahmen über die Risiken von Cyberangriffen auf Ihre Produktionsanlagen informieren. Die DGQ bietet hierzu in Kooperation mit dem Fraunhofer IOSB das Seminar Management Know-how Cyber-Sicherheit für Fach- und Führungskräfte an. In nur zwei Tagen verschaffen sich Teilnehmer in diesem Training einen umfassenden Überblick über die wichtigsten Sicherheitsfragen in der digitalen Transformation und Industrie 4.0. Sie erkennen und verstehen die sicherheitstechnischen Herausforderungen und Risiken der stetig zunehmenden Vernetzung.

** Link zu den Empfehlungen: https://www.bitkom.org/Presse/Presseinformation/Spionage-Sabotage-Datendiebstahl-Deutscher-Wirtschaft-entsteht-jaehrlich-ein-Schaden-von-55-Milliarden-Euro.html*

Technische IT-Sicherheit steigern und organisatorische Sicherheit erhöhen

Neben einer verbesserten technischen Sicherheit sollte auch der Faktor Mensch nicht ignoriert und die organisatorische Sicherheit erhöht werden. Technische Sicherheit lässt sich u.a. durch angemessene Verschlüsselung, spezielle Angriffserkennung, Security by Design bei allen Schnittstellen und vernetzten Geräten verbessern. Für die organisatorische Sicherheit sollten Zugriffsrechte auf Daten und physische Zugangsrechte an eine vernetzte Produktion angepasst werden. Auch ein gut überlegtes Besuchermanagement und noch viel wichtiger ein wirkungsvolles Notfallmanagement wirken sich positiv auf die Sicherheit eines Unternehmens aus.

Neben Cyber-Sicherheit ist auch in einer vernetzten Produktion das Thema Datenschutz von Relevanz. Handelt es sich bei gestohlenen Daten um personenbezogene Daten, kommt die EU-Datenschutz-Grundverordnung zum Tragen. Die Risiken für personenbezogene Daten sollten auch in einer sogenannten Smart factory nicht unterschätzt werden.

Personelle Sicherheit verbessern

Um die personelle Sicherheit zu verbessern, sollten Unternehmen eine Sicherheitskultur im Unternehmen etablieren. Awareness-Schulungen und auch spezifische Schulungen am Arbeitsplatz sind hier ein geeignetes Mittel, um Mitarbeiter für Cyber-Sicherheit zu sensibilisieren. Vor allem Mitarbeiter der Produktion sollten die mit der zunehmenden Vernetzung entstehenden Risiken kennen und darauf reagieren können. Hier empfiehlt Bitkom ausdrücklich „IT-Experten mit Produktions-Know-how". Diese sollten möglichst zeitnah ausgebildet werden, um geeignetes Personal für die Umsetzung der genannten Empfehlungen für mehr Cyber-Sicherheit auszubilden. Auch hierzu bietet die DGQ zusammen mit dem Fraunhofer IOSB die passenden Trainings an. In der viertägigen Weiterbildung Cyber-Sicherheit in der vernetzten Produktion erwerben die Teilnehmer das erforderliche Wissen, um Gefahren durch Cyber-Angriffe zu erkennen, IT-Sicherheitslösungen umzusetzen und so die Produktion zu sichern. Im Lernlabor Cyber-Sicherheit erleben sie realitätsnahe Simulationen von Cyber-Angriffen auf Industrieanlagen, können die Folgen anhand des Modells einer Produktionsanlage unmittelbar nachvollziehen und ihr erlerntes Wissen direkt testen. Der DGQ-Spezialist für Cyber-Sicherheit in der vernetzten Produktion ist in der Lage, Gefahren zu erkennen, IT-Sicherheitslösungen umzusetzen und so die Produktion zu sichern. Die Schulung richtet sich an Fachkräfte und Mitarbeiter mit technischem Ausbildungshintergrund in der industriellen Produktion, Mitarbeiter der Qualitätssicherung oder IT-Mitarbeiter mit Interesse an Cyber-Sicherheit in der vernetzten Produktion.

Über die Autorin:
Christina Eibert ist studierte Sozialwissenschaftlerin und Produktmanagerin bei der DGQ. Sie verantwortet die Trainings in den Bereichen Compliance, Datenschutz, Statistik und Cyber-Sicherheit. Besonders wichtig ist es ihr, praxisnahe und zukunftsorientierte Weiterbildungen zu entwickeln, von denen Teilnehmer und Unternehmen gleichermaßen profitieren.

Ihr direkter Kontakt:
T 069 95424-189
christina.eibert@dgq.de