Pressekontakt:
Kora Alice Lejko
Tel.: + 49 151 40251 298
E-Mail: kora-alice.lejko@capgemini.com
www.twitter.com/CapgeminiDE

Jedes zweite Fertigungsunternehmen rechnet mit Zunahme von Cyberangriffen – bei weiterhin lückenhafter Cybersicherheit

Berlin, 11. Juli 2022 – Die Hälfte der Industrieunternehmen (51 Prozent) geht davon aus, dass die Zahl der Cyberangriffe auf Smart Factories[1] in den nächsten 12 Monaten steigen wird. Dennoch sagt ebenfalls fast jeder zweite Hersteller (47 Prozent), dass die Cybersicherheit der eigenen intelligenten Fabriken nicht im Fokus der höchsten Managementebene steht. Erst wenige Hersteller verfügen über ausgereifte Strukturen in allen kritischen Bereichen der Cybersicherheit. Die mit dem Industrial Internet of Things (IIOT) geschaffene Konnektivität der Smart Factories erhöht die Gefahr durch Cyberangriffe in der intelligenten Industrie exponentiell. Zu diesen Ergebnissen kommt das Capgemini Research Institute in seiner neuen Studie Smart & Secure: Why smart factories need to prioritize cybersecurity.

Rund 53 Prozent der Unternehmen – sowohl weltweit als auch in Deutschland – denken, dass Smart Factories in Zukunft Hauptziele von Cyberangriffen sein werden. In der Schwerindustrie gehen davon sogar 60 Prozent aus, im Pharma- und Life-Sciences-Sektor 56 Prozent. Ein ausgeprägtes Gefahrenbewusstsein führt jedoch nicht automatisch dazu, dass Unternehmen entsprechend vorbereitet sind. Unzureichende Aufmerksamkeit des obersten Managements, knappe Budgets und menschliche Faktoren werden als die größten Hürden für Cybersicherheit genannt, die sie zu überwinden haben.

„Hersteller kennen die Vorteile der digitalen Transformation und investieren entsprechend massiv in Smart Factories – ein riskanter Schritt, wenn Cybersicherheit nicht von Beginn an integriert ist. Die wachsende Angriffsfläche, Vernetzung und die Menge an Betriebstechnologie sowie IIOT-Geräten machen Smart Factories zu einem leichten Ziel für Cyberkriminelle", sagt Torsten Jüngling, Head of Cybersecurity bei Capgemini in Deutschland. *„Solange dies keine Priorität des Vorstands ist, wird es Unternehmen schwerfallen, der Gefahr effektiv zu begegnen, ihre Mitarbeitenden und Zulieferer fortzubilden sowie die Kommunikation zwischen den Cybersecurity-Teams und der C-Suite verbessern."*

Hürden für sichere Smart Factories: Fehlende Tools und nicht-standardkonforme Prozesse
Die Studie zeigt, dass Cybersicherheit für viele Unternehmen kein Grundstein ihrer Strategie ist; nur 51 Prozent integrieren standardmäßig Cybersicherheitspraktiken in ihre Smart Factories. Anders als bei IT-Plattformen sind möglicherweise nicht alle Unternehmen in der Lage, die Maschinen in einer Smart Factory im laufenden Betrieb zu überprüfen.

Die Sichtbarkeit von Betriebstechnologie (OT) und IIOT-Geräten auf Systemebene ist notwendig, um zu erkennen, sobald sie kompromittiert wurden. 77 Prozent der Unternehmen sind besorgt darüber, dass zur Reparatur oder Aktualisierung von OT-/IIOT-Systemen regulär nicht-standardkonforme Prozesse angewandt werden. Diese Problematik ist zum Teil auf die geringe Verfügbarkeit der richtigen Tools und Prozesse

[1] Smart Factories setzen digitale Plattformen und Technologien ein, um Produktivität, Qualität, Flexibilität und Service deutlich zu verbessern. Sie basieren auf drei digitalen Schlüsseltechnologien: Konnektivität (Nutzung des industriellen Internets der Dinge zur Erfassung von Sensordaten), intelligenter Automatisierung (z. B. fortschrittliche Robotik, maschinelles Sehen, Distributed Control, Drohnen usw.) sowie Cloud-basierter Datenverwaltung und -analyse.

zurückzuführen. Allerdings denkt die Hälfte der Unternehmen in Deutschland und weltweit, dass Cyberrisiken für Smart Factories in erster Linie von den Netzwerken ihrer Partner und Zulieferer ausgehen. 28 Prozent haben zudem beobachtet, dass die Zahl der Mitarbeiter oder Zulieferer, die infizierte Geräte wie Laptops und Mobilgeräte zur Installation oder zum Patchen von Smart-Factory-Anlagen mitbringen, seit 2019 um 20 Prozent gestiegen ist.

Menschen – nicht Technologien – bleiben die größte Gefahr für die Cybersicherheit
Nur wenige der befragten Unternehmen gaben an, dass ihre Cybersicherheitsteams über die erforderlichen Kenntnisse und Fähigkeiten verfügen, um bei Vorfällen dringende Sicherheits-Patches ohne externe Unterstützung durchzuführen. Eine häufige Ursache für diese verbreitete Schwachstelle besteht darin, dass Cybersecurity Manager fehlen, um die erforderlichen Weiterbildungsprogramme einzuführen.

In Verbindung mit dem Fachkräftemangel wird dies zu einer Herausforderung: 57 Prozent der Unternehmen halten den Mangel an Fachkräften für die Cybersicherheit von Smart Factories für weitaus akuter als für den Bereich der IT-Sicherheit. Viele Unternehmen berichten, dass ihre Cybersicherheitsanalysten überlastet sind von der Vielzahl an OT- und IIOT-Geräten, die sie überwachen müssen, um Angriffe zu erkennen und zu verhindern. Darüber hinaus sehen sich 43 Prozent der Cybersicherheitsmanager in Deutschland und weltweit nicht in der Lage, auf Angriffe in ihren Smart Factories und Produktionsstandorten zu reagieren.

Zu wenig Zusammenarbeit zwischen den Leitern von Smart Factories und dem Chief Security Officer ist für über die Hälfte der Befragten – 53 Prozent weltweit, 58 Prozent in Deutschland – ebenfalls ein bedenklicher Umstand. Diese Kommunikationslücke beeinträchtigt die Fähigkeit von Unternehmen, Cyberangriffe frühzeitig zu erkennen, was zu einem größeren Ausmaß der Schäden führen kann. Mehr als die Hälfte (55 Prozent) der deutschen Unternehmen gab an, dass Verluste in der Vergangenheit hauptsächlich durch Verzögerungen bis zur Entdeckung von Cyberangriffen entstehen konnten.

Cybersecurity-Vorreiter sichern sich Wettbewerbsvorteile
Es gibt Vorreiter unter den Herstellern – 6 Prozent, in der Studie als „Cybersecurity Leaders" bezeichnet –, die in ihren Smart Factories schon ausgereifte Konzepte für die entscheidenden Dimensionen der Cybersicherheit umsetzen: Sensibilisierung, Reaktionsfähigkeit und Implementierung. Aus der Studie geht hervor, dass sie ihren Wettbewerbern dadurch in mehreren Aspekten überlegen sind: 72 Prozent können sich gegen Cyberangriffe schützen und deren Auswirkungen minimieren, und 74 Prozent sind in der Lage, bekannte Angriffsmuster frühzeitig zu erkennen. Dies ist nur bei 41 bzw. 46 Prozent der anderen Unternehmen der Fall.

Basierend auf der Auswertung und den Erfahrungen der ermittelten „Cybersecurity Leaders" empfehlen die Studienautoren einen sechsstufigen Ansatz für die Ausarbeitung einer effektiven Cybersicherheitsstrategie für Smart Factories:

- Durchführung eines umfassenden Cybersecurity Assessments
- Sensibilisierung des gesamten Unternehmens für Cybergefahren für Smart Factories
- Definition der Verantwortlichkeiten für die Risiken von Cyberangriffen
- Einführung von Frameworks für Cybersicherheit in Smart Factories
- Entwickeln von auf Smart Factories zugeschnittenen Cybersicherheitspraktiken
- Aufbau einer Governance-Struktur und eines Frameworks zur Kommunikation mit der Unternehmens-IT

Die vollständige Studie, eine Infografik sowie ein Portraitbild des Zitatgebers Torsten Jüngling stehen hier zum Download für Sie bereit.

Methodik der Studie
Das Capgemini Research Institute hat 950 Unternehmen befragt und Tiefeninterviews mit Führungskräften aus verschiedenen Unternehmen geführt. Die Umfrage fand im Oktober und November 2021 statt – mit Befragungen in Australien, Italien, UK, den USA, Frankreich, Deutschland, Spanien, Skandinavien, Indien, China und den Niederlanden. Zu den untersuchten Sektoren gehören die Konsumgüter- und Schwerindustrie, Pharma und Life Sciences, Chemie, Automobil, Luft- und Raumfahrt, Verteidigung sowie Hightech.

Über Capgemini
Capgemini ist einer der weltweit führenden Partner für Unternehmen bei der Steuerung und Transformation ihres Geschäfts durch den Einsatz von Technologie. Die Gruppe ist jeden Tag durch ihren Purpose angetrieben, die Entfaltung des menschlichen Potenzials durch Technologie zu fördern – für eine integrative und nachhaltige Zukunft. Capgemini ist eine verantwortungsbewusste und diverse Organisation mit einem Team von über 340.000 Mitarbeiterinnen und Mitarbeitern in mehr als 50 Ländern. Eine 55-jährige Unternehmensgeschichte und tiefgehendes Branchen-Know-how sind ausschlaggebend dafür, dass Kunden Capgemini das gesamte Spektrum ihrer Geschäftsanforderungen anvertrauen – von Strategie und Design bis hin zum Geschäftsbetrieb. Dabei setzt das Unternehmen auf die sich schnell weiterentwickelnden Innovationen in den Bereichen Cloud, Data, KI, Konnektivität, Software, Digital Engineering und Plattformen. Der Umsatz der Gruppe lag im Jahr 2021 bei 18 Milliarden Euro.
Get The Future You Want | www.capgemini.com/de

Über das Capgemini Research Institute
Das Capgemini Research Institute ist Capgeminis hauseigener Think-Tank in digitalen Angelegenheiten. Das Institut veröffentlicht Forschungsarbeiten über den Einfluss digitaler Technologien auf große Unternehmen. Das Team greift dabei auf das weltweite Netzwerk von Capgemini-Experten zurück und arbeitet eng mit akademischen und technologischen Partnern zusammen. Das Institut hat Forschungszentren in Indien, Singapur, Großbritannien, und den USA.
Besuchen Sie uns auf www.capgemini.com/researchinstitute