VDMA

Software und Digitalisierung

Management Summary

Nach 2013 und 2019 hat der VDMA mit Unterstützung des Fraunhofer AISEC in 2025 eine erneute Befragung zur Industrial Security des Maschinen- und Anlagenbaus durchgeführt, deren Ergebnisse in der vorliegenden Studie veröffentlicht sind. Dabei geht es vorrangig um die Fragen, welche Kompetenzen die Unternehmen diesbezüglich aufgebaut haben, welche Standards und Maßnahmen zum Einsatz kommen, welche Bedrohungen aus aktueller Sicht das größte Risiko darstellen und welche Auswirkungen Security-Vorfälle verursacht haben.

Die wichtigsten Ergebnisse im Überblick.

- Rund 54 Prozent der Unternehmen rechnen für die kommenden Jahre mit einer Steigerung der Security-Vorfälle im eigenen Unternehmen.

- Von Security-Vorfällen betroffene Unternehmen verzeichnen zumeist Kapitalschäden (32 Prozent) und Produktionsausfälle (29 Prozent). Safety-relevante Auswirkungen (Gefährdung von Mensch oder Umwelt) sind in den vergangen zwei Jahren erfreulicherweise nicht registriert worden. Der Anteil der betroffenen Unternehmen mit Produktionsausfällen unterstreicht die Notwenigkeit von Industrial Security neben der „klassischen“ IT-Security in den Unternehmen.

- Obwohl die Zahl der Cybersecurity-Vorfälle im Vergleich zur VDMA Studie Industrial Security von 2019 gestiegen ist, haben diese weniger Auswirkungen bei den betroffenen Unternehmen gezeigt, als im Jahr 2019. Dies spricht für eine wachsende Cyberresilienz der Unternehmen.

- Zu den Bedrohungen mit der höchsten Risikoeinschätzung gehören erstmalig „Social Engineering und Phishing“ (Platz 1) sowie „Menschliches Fehlverhalten und Sabotage“ (Platz 2). Neu hinzugekommen in die Liste der Top 10 Bedrohungen ist die Thematik „Soft- und Hardwareschwachstellen in der Lieferkette“ auf Platz 3. Dass der Faktor Mensch Platz 1 und 2 belegt, spricht für ein Vertrauen in technische Securitymaßnahmen und unterstreicht den Nutzen von Cybersecurity Awareness Trainings in der Produktion.

- Mittlerweile kennen 93 Prozent der Unternehmen einen der gängigen Security-Standards und knapp die Hälfte (52 Prozent) wendet diese auch an. Insbesondere mangelndes Know-how ist jedoch noch ein Hindernis für den Einsatz, vornehmlich bei kleineren und mittelständischen Unternehmen (bis 250 Mitarbeitende) wird dieser Umstand deutlich. Gerade kleine und mittelständische Unternehmen müssen unterstützt werden, um ihr Security Know-how weiter auszubauen.

- Bei der Etablierung eines Risikomanagements im Produktionsumfeld gibt es noch Handlungsbedarf. Erst 61 Prozent haben ein solches eingeführt. Das Risikomanagement bietet die Grundlage für die effektive wirtschaftliche Implementierung von Cybersecuritymaßnahmen. Eine gezielte Abschätzung von Ausfallkosten bei Security-Vorfällen spielt nach wie vor für rund drei Viertel der Unternehmen keine Rolle.

- Vom Cyber Resilience Act (CRA) und der Netzwerk- und Informationssicherheitsdirektive 2 (NIS2) sind die befragten Unternehmen vielfach direkt betroffen. Rund zwei Drittel (68 Prozent) werden aufgrund der Tätigkeit als Servicedienstleister, Komponentenlieferant oder Integrator davon berührt.

- Nur 8 Prozent der Unternehmen können sich bisher ein Security-Gütesiegel als „generell verpflichtendes Entscheidungskriterium“ für den Produkteinkauf vorstellen. Security ist jedoch ein Lifecycle-Thema: Schwachstellen können auch während der Verwendung eines Produktes identifiziert werden. Ein beim Verkauf angebrachtes Gütesiegel könnte so also gegebenenfalls rasch seine Bedeutung verlieren.

Die nachfolgenden Seiten vermitteln einen detaillierten Einblick in die Ergebnisse der Befragung.