CYBERSICHERHEIT IST CHEFSACHE!

Im Herbst wird die NIS2 in Österreich zu nationalem Recht. Das bedeutet: Unternehmen aus kritischen oder wesentlichen Branchen sind gefordert, sich um die Cybersicherheit zu kümmern. Die Geschäftsführung ist auch persönlich haftbar.

Am 18. Oktober 2024 wird in Österreich der bisherige Anwendungsbereich der NIS-Richtlinie (Cybersicherheit für Netz- und Informationssysteme) durch die NIS2 auf einen wesentlich größeren Teil der europäischen Wirtschaft ausgeweitet. Unter der NIS-2-Richtlinie müssen betroffene Unternehmen, darunter solche aus kritischen Infrastrukturen, Finanzwesen, digitalen Diensten sowie Branchen wie Logistik, Chemie und Fertigung, ein entsprechendes Cybersicherheits-Risikomanagement betreiben und Vorfälle schnell melden. Auch kleinere Zulieferer oder Dienstleister dieser Sektoren sind betroffen, besonders bei EU-weitem Handel. Die NIS2 beinhaltet auch eine neue, persönliche Haftung von Führungskräften. So werden Geschäftsführer verpflichtet, die Einhaltung der Maßnahmen im Bereich der Cybersicherheit zu ermöglichen und ihre Umsetzung zu überwachen. Eine Übertragung dieser Verpflichtungen auf Dritte ist nicht zulässig. Die Geschäftsführung und die Mitarbeiter:innen müssen regelmäßig an Schulungen teilnehmen, um Risiken sowie Risikomanagementpraktiken zu erkennen und zu bewerten.

SAFTIGE STRAFEN DROHEN

Für kritische Unternehmen ist der Bußgeldrahmen auf mindestens zehn Millionen Euro oder zwei Prozent des weltweiten Jahresumsatzes festgelegt, je nachdem, welcher Wert höher ist. Bei wichtigen Einrichtungen beträgt der maximale Bußgeldbetrag mindestens sieben Millionen Euro oder 1,4 % des weltweiten Jahresumsatzes.

Fotos: Industrial Automation GmbH

Industrial-Automation-GmbH-Geschäftsführer Klaus Lussnig

IRMA – automatisierter, ganzheitlicher Schutz vor Cyberangriffen in Infrastruktur-, Fertigungs- und Produktionsanlagen inkl. Risikomanagement

Die Vernetzung mit Lieferanten und Dienstleistern birgt hohe Sicherheitsrisiken. Laut NIS2 müssen diese Verbindungen gesichert und im Risikomanagement überwacht werden, um Cyberangriffe zu verhindern. Es gilt, spezifische Schwachstellen, die Produktqualität und die Cybersicherheitspraktiken, einschließlich der Sicherheit der Entwicklungsprozesse, zu bewerten und entsprechende Maßnahmen zu ergreifen. Zertifizierungen und Audits dienen als Nachweis für die Einhaltung der Sicherheitsanforderungen.

IRMA – GANZHEITLICHER SCHUTZ VON INFRASTRUKTUR- UND PRODUKTIONSANLAGEN

„Mit der NIS2-Richtlinie wird der Einsatz einer Angriffserkennung absolut erforderlich. IRMA (Industrie Risiko Management Automatisierung) entspricht der NIS2-Anforderung und ermöglicht die organisatorische Einbindung zur Erkennung von Angriffen auf informationstechnische Systeme“, erklärt Industrial-Automation-GmbH-Geschäftsführer Klaus Lussnig. Bei IRMA handelt es sich um ein leistungsfähiges Industrie-Computersystem, das ohne jegliche Aktivitäten im IT/OT-Netz kontinuierlich Infrastruktur- und Produktionsanlagen überwacht, Informationen zu Cyberangriffen liefert und die risikobasierte Analyse sowie die intelligente Alarmierung mittels einer übersichtlichen Managementkonsole ermöglicht. So können Risiken frühzeitig bewertet und Aktionen verzögerungsfrei gestartet werden, um einen Angriff zu stoppen oder seine Folgen wirkungsvoll zu entschärfen.