expertenReport

Quelle: DALL-E

Cyber-physische Systeme im Krisenmodus: Globale Spannungen erhöhen Sicherheitsrisiken

Michael Fiedler

Globale Lieferketten wanken, politische Spannungen nehmen zu – und mit ihnen die Risiken für vernetzte Industrie- und Infrastruktursysteme. Fast die Hälfte aller Sicherheitsverantwortlichen sieht ihre cyber-physischen Systeme inzwischen ernsthaft bedroht. Der neue Claroty-Report zeigt, warum gerade jetzt Fernzugriffe und Drittanbieter zu den größten Schwachstellen werden – und wie Unternehmen reagieren sollten.

Geopolitik und Lieferkettenverlagerung als Risikoquelle

Wirtschaftliche Unsicherheiten und geopolitische Spannungen setzen die Sicherheit cyber-physischer Systeme (CPS) zunehmend unter Druck. Das zeigt der aktuelle Report „The Global State of CPS Security 2025: Navigating Risk in an Uncertain Economic Landscape“ des Security-Spezialisten Claroty. Für die Studie wurden weltweit 1.100 Fachleute aus Informationssicherheit, OT-Engineering, Gesundheitswesen, Biotechnologie, Gebäudemanagement und industriellen Anlagen befragt. Das Ergebnis: 49 Prozent der Sicherheitsverantwortlichen sehen wachsende Risiken für CPS – vor allem durch Veränderungen in den Lieferketten.

67 Prozent der Befragten gaben an, ihre geografische Ausrichtung der Lieferketten neu zu bewerten, um geopolitische und wirtschaftliche Risiken zu minimieren. Gleichzeitig erklärten 45 Prozent, dass sie die Risiken ihrer eigenen Anlagen derzeit nicht effektiv einschätzen oder reduzieren können – ein gravierendes Problem für Unternehmen mit komplexen und vernetzten Produktionssystemen.

Schwachstelle Fernzugriff: Dritte als Einfallstor

Ein besonders kritischer Faktor ist der Fernzugriff durch externe Dienstleister. Durch die Integration neuer Anbieter und Tools entstehen in ohnehin sensiblen CPS-Umgebungen zusätzliche Angriffsflächen. 46 Prozent der Unternehmen berichteten, in den vergangenen zwölf Monaten Opfer eines Sicherheitsvorfalls durch den Zugriff Dritter geworden zu sein. Entsprechend überdenken 73 Prozent derzeit ihre Fernzugriffsstrategien.

Regulatorische Unsicherheiten verschärfen die Lage zusätzlich: Während in einigen Regionen Deregulierungstendenzen herrschen, verschärfen andere

Staaten die Vorgaben. 70 Prozent der Befragten sind überzeugt, dass ihre Programme heutigen Cybersicherheitsstandards wie dem NIST-Framework oder ENISA entsprechen – 76 Prozent befürchten jedoch, dass neue Vorschriften Anpassungen erzwingen und damit die Effizienz beeinträchtigen könnten.

„Instabilität als Einladung zum Angriff“

„Angreifer sehen Zeiten der Instabilität oft als Gelegenheit zum Zuschlagen. Gerade kritische Infrastrukturen sind ein attraktives Ziel, da ihre Störungen erhebliche Auswirkungen auf die wirtschaftliche Stabilität, die nationale und die öffentliche Sicherheit haben können“, erklärt Thorsten Eckert, Regional Vice President Sales Central bei Claroty. Er betont: „Die Ergebnisse unseres Reports zeigen, dass wirtschaftliche Unsicherheit und geopolitische Spannungen es Sicherheitsteams erschweren, kritische Systeme zu schützen. Schwachstellen in der Lieferkette bei Dritten und Partnern erhöhen die Risiken noch weiter.“

Prävention durch Impact-zentrierte Strategien

Um Risiken zu minimieren, setzen Sicherheitsverantwortliche laut Claroty-Report zunehmend auf regelmäßige Sicherheitsaudits (49 Prozent) und auf Prozessverbesserungen bei Genehmigungen von Änderungen (45 Prozent). Diese Maßnahmen stärken die Compliance und decken Schwachstellen auf – insbesondere dort, wo Drittanbieter im Spiel sind.

Claroty plädiert für einen Impact-zentrierten Ansatz, der regulatorische Anforderungen mit aktivem Exposure-Management kombiniert. Unternehmen, die ihre Sicherheitsarchitekturen vorausschauend modernisieren, könnten so nicht nur ihre Widerstandskraft erhöhen, sondern auch Wettbewerbsvorteile sichern.

Ausblick

Der vollständige Report „The Global State of CPS Security 2025: Navigating Risk in an Uncertain Economic Landscape“ bietet eine detaillierte Analyse und praxisorientierte Empfehlungen. Claroty präsentiert die Ergebnisse und Lösungen zur CPS-Sicherheit auch auf der it-sa 2025 vom 7. bis 9. Oktober in Nürnberg.

Versicherungs- und Finanznachrichten

expertenReport

https://www.experten.de/id/4946276/Cyber-physische-Systeme-im-Krisenmodus-Globale-Spannungen-erhoehen-Sicherheitsrisiken/