

## **Cyber-Resilienz für die Industrie: das 6-Schritte-Programm gegen Cyberangriffe**

Industrieunternehmen sind ein interessantes Ziel für Cyberattacken, die Schäden sind enorm. Wie kann sich die Industrie wehren?

Cybersicherheits-Experte Thomas Doms vom TÜV AUSTRIA empfiehlt ein 6-Schritte-Programm als Vorgehensmodell. Das Modell basiert auf den Grundlagen der international anerkannten Sicherheitsnorm IEC 62443, die wirksame Schutzmaßnahmen und Prozesse für die Industrie 4.0 definiert und beschreibt. Dieses stellte er in seinem Vortrag am TÜV AUSTRIA Symposium IT- und Datensicherheit Anfang April vor.

### **Die häufigsten Angriffsvektoren**

Hacker nutzen beispielsweise spezielle Malware, um die Produktionsumgebung – also dort, wo Programme und Produkte für den Endbenutzer in Echtzeit zur Verfügung stehen – mit Schadsoftware zu „infizieren“. Die häufigsten Ziele heutiger Angreifer sind Daten-Leaks und Lösegelderpressungen. Abhilfe schaffen die aus der IEC 62443 abgeleiteten Vorgehensweisen: Sie ermöglichen eine signifikante Erhöhung des Schutzniveaus und infolgedessen die Abwehr von Angriffen auf Unternehmen.

### **Cyberabwehr in 6 Schritten**

Der erste wichtige Baustein zur Implementierung angemessener Schutzmaßnahmen ist die Durchführung einer IST-Analyse mittels Erstellung eines Systeminventars über die derzeit verwendeten Produktionssysteme, Protokollsprachen und Patch-Stände. Schritt zwei betrifft die Durchführung einer umfassenden Gap-Analyse, Schritt drei integrierte Risikobewertungen mittels „Threat Models“, um potenzielle Angriffsvektoren und deren Auswirkungen zu identifizieren. Die gemeinsame Betrachtung von Funktionaler Sicherheit und Cybersecurity als Schritt vier hilft, produktions- und sicherheitskritische Komponenten und Systeme in eigenen definierten Sicherheitszonen zusätzlich abzusichern. Im nächsten Schritt können die derzeitigen Sicherheitsmaßnahmen je nach Anforderung und Security Level verbessert werden. Der letzte wichtige Baustein, Schritt 6, betrifft die Definition von konkreten Sicherheitsvorgaben für Lieferanten und Integratoren für zukünftige Beschaffungen, um die Voraussetzungen für die wirksame Implementierung von notwendigen Schutzmaßnahmen zu gewährleisten.

Außerdem gab Thomas Doms einen interessanten Einblick in die Arbeit des TÜV AUSTRIA „#SafeSecLab - Research Lab for Safety & Security in Industry“, einer interdisziplinären gemeinsamen Fakultät der TU Wien und des TÜV AUSTRIA zur Entwicklung neuer innovativer Verfahren und Sicherheitslösungen für Produktionsumgebungen.

Weiters am Programm standen Neuerungen im Datenschutz, rechtliche Anforderungen bei digitaler Barrierefreiheit, Datenschutzmanagementsysteme nach ISO 27701, Neuerungen zur ISO 27002, die Behebung des IT-Fachkräftemangels durch moderne Weiterbildungsmethoden sowie die sinnvolle Nutzung von Daten. Eine Live-Vorführung über die Einsatzmöglichkeiten von Virtual Reality erhöhte den Spannungsfaktor.

### **Rückfragehinweis:**

Stefan Grüneis, Programmverantwortlicher für die Bereiche IT & Datensicherheit, TÜV AUSTRIA Akademie, [stefan.grueneis@tuv.at](mailto:stefan.grueneis@tuv.at), Tel.: +43 (0)5 0454-8172

Bildcredit: @Daniel Mikkelsen