Industrie 4.0 in Gefahr: Cyberrisiken bedrohen unsere Betriebe!

Entdecken Sie die Herausforderungen und Lösungen in der Cybersicherheit für industrielle Systeme, die IT und OT vereinen.

Nicht spezifiziert, Land - In der heutigen zunehmend vernetzten Welt ist die Sicherung industrieller Systeme ein heißes Thema geworden. Vor dem Hintergrund wachsender Cyber-Bedrohungen wie Ransomware und Insider-Angriffen müssen Unternehmen innovative Ansätze entwickeln, um ihre Operational Technology (OT) zu schützen. Ein reifes OT-Cybersecurity-Programm muss sich auf tiefgehende Sichtbarkeit, kontinuierliche Risikobewertung und eine starke Governance konzentrieren, die speziell auf OT-Umgebungen zugeschnitten ist. Laut industrialcyber.co bleibt vielen industriellen Unternehmen der Übergang zu modernen Sicherheitsstrategien jedoch schwerfallen.

Ein oft vernachlässigter Aspekt sind die Herausforderungen, die mit der Verschmelzung von IT- und OT-Sicherheit einhergehen. Diese beiden Bereiche weisen nicht nur unterschiedliche Ziele, sondern auch Ausrichtungen und Technologien auf. Die IT konzentriert sich auf Datenmanagement und Informationsfluss, während OT sich auf die Steuerung physischer Prozesse in der Industrie fokussiert. Diese unterschiedlichen Prioritäten erfordern eine sensible Herangehensweise bei der Integration beider Disziplinen. IBM hebt hervor, dass die kulturellen Spannungen zwischen IT-Sicherheitsexperten und OT-Teams eine bedeutende Hürde darstellen, die es zu überwinden gilt, um effektive Sicherheitsmaßnahmen zu implementieren.

Risikobewertung als Schlüsselkomponente

Ein zentraler Bestandteil eines effektiven OT-Cybersecurity-Programms ist die Risikobewertung. Unternehmen müssen die Infrastruktur ihrer Industrial Automation and Control Systems (IACS) genau verstehen, einschließlich der Datenflüsse und möglichen Schwachstellen. Hier kommt die Methodik von methodcysec.com ins Spiel, die empfiehlt, für jede Zone Risikoprofile zu entwickeln und das Kritikalitätsniveau basierend auf möglichen Konsequenzen im Falle einer Kompromittierung festzulegen. Worst-Case-Szenarien müssen klar definiert werden, um die Risiken effektiv zu managen.

Forschung hat gezeigt, dass viele Unternehmen immer noch auf veraltete Risikomodelle setzen, die für moderne Bedrohungen nicht geeignet sind. Unternehmen ohne einen klaren regulatorischen Rahmen, wie etwa dem COMAH, sollten alternative Risikokennzahlen in Betracht ziehen, die unter anderem die Geschäftskontinuität und Reputation berücksichtigen. Die Einbeziehung verschiedener Fachbereiche ج von IACS-Verantwortlichen bis hin zu Prozessingenieuren ج ist entscheidend für eine umfassende Risikobewertung.

Der Wandel der Verantwortung

Ein weiterer bedeutender Trend im Bereich OT-Cybersecurity ist der Wandel der Verantwortlichkeiten. Während bisher häufig Plant Engineers oder Manager für die Sicherheit zuständig waren, verschiebt sich die Verantwortung zunehmend hin zu Chief Information Security Officers (CISOs) und zentralen Sicherheitsteams. Dies kann herausfordernd sein, besonders in Umgebungen, in denen Ausfallzeiten nicht toleriert werden. Viele CISOs sind nicht ausreichend auf die technischen und kulturellen Herausforderungen von OT-Cybersecurity vorbereitet.

Die effektive Sicherung von OT-Systemen erfordert nicht nur eine technische Strategie, sondern auch ein gutes Händchen für kulturelle Veränderungen, um die Kluft zwischen den Betriebsabläufen und der Cybersicherheit zu überbrücken. Engagierte Zusammenarbeit mit OEMs und Systemintegratoren spielt hierbei eine wesentliche Rolle und die Kommunikation der Cyberstrategie an die Lieferanten ist unerlässlich für eine erfolgreiche Implementierung.

Es ist offensichtlich, dass Organisationen, die in der OT-Sicherheit erfolgreich sein wollen, in eine reife Cybersecurity-Strategie investieren müssen, die sowohl technische als auch kulturelle Aspekte berücksichtigt. Der Einsatz von Sicherheitsrahmen wie NIST oder IEC 62443 kann den Unternehmen helfen, ihre OT-Sicherheitsstrategie wirklich zu verbessern und sich gegen moderne Bedrohungen zu wappnen.

Insgesamt ist die koloniale Herausforderung, die zwischen IT- und OT-Sicherheitskulturen besteht, nicht zu übersehen. Die Bereitschaft, über den Tellerrand hinauszublicken, kann entlang dieser Schnittstelle nicht nur Sicherheitslücken schließen, sondern auch die Effizienz und Zuverlässigkeit industrieller Prozesse steigern. In einer Zeit, in der Cyberangriffe die Schlagzeilen bestimmen, ist dies nicht nur eine Notwendigkeit, sondern eine unternehmerische Verantwortung.

Details	
Ort	Nicht spezifiziert, Land
Quellen	• industrialcyber.co • www.methodcysec.com • www.ibm.com