

Cyber Resilience Act Release Pentest

Beschreibung

Um die im CRA festgelegten Sicherheitsanforderungen zu erfüllen, ist ein umfassender Penetrationstest vor der Auslieferung unverzichtbar. Der Test überprüft sowohl IT- wie OT-Schnittstellen, identifiziert Fehlkonfigurationen, Schwachstellen in Firmware und Netzwerkkommunikation und bewertet die Wirksamkeit von Segmentierung, Authentifizierung und Monitoring. Auf diese Weise können Maschinenhersteller vor der Auslieferung sicherstellen, dass ihre Produkte den technischen Anforderungen erfüllen.

Vorteile

- Nachweis der technischen Sicherheit der Maschine durch strukturierte Prüfung
- Dokumentierter Beleg der CRA-Konformität zum Zeitpunkt der Auslieferung
- Bereitstellung einer normgerechten Dokumentation gemäß CRA-Anforderungen
- Trägt zur Erfüllung der CRA Compliance bei

Methodik

- Berichtserstellung nach CRA-Anforderungen für die Maschinendokumentation
- Dokumentation bestandener Testfälle zur Nachweisführung
- Erfassung identifizierter Schwachstellen (Findings) inklusive konkreter Handlungsempfehlungen zur sicheren Umsetzung
- Durchführung von Penetrationstests an Maschinenkomponenten sowie an Netzwerkübergängen zwischen IT- und OT-Systemen



Schnell und richtig reagieren

Sorgfältig ausgearbeitete Notfallpläne und ein Business Continuity Management sind eine sichere Grundlage. Im Notfall unterstützen Sie die Incident Response Teams der @-yet IIS, damit Sie schnell wieder arbeitsfähig werden.



Fachübergreifender Ansatz

Die @-yet IIS betrachtet klassische IT-Security und die Sicherheit in der Automatisierung als einheitlichen Prozess. Alle wichtigen Bereiche der Cybersicherheit von Industrieunternehmen werden so abgedeckt.



Umfassende Prävention

Die @-yet IIS sorgt mit fundierten Schulungsprogrammen für aufmerksame Mitarbeitende, damit der Ernstfall erst gar nicht eintritt. Diese Awareness wird durch professionelle technische Maßnahmen unterstützt.

