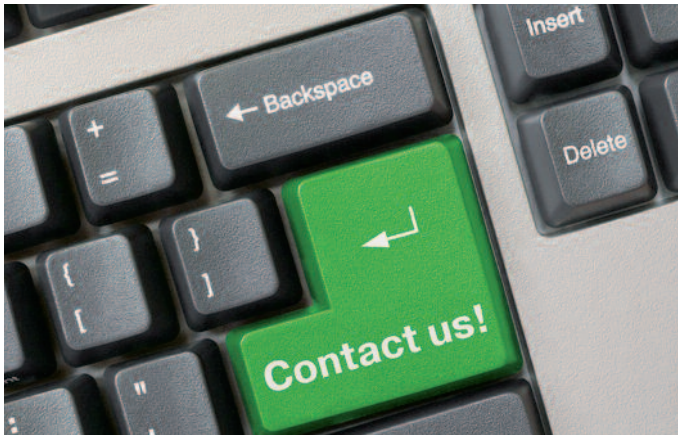
Fazit/Empfehlungen

„Industrie 4.0“ erfordert auch zusätzliche Sicherheitsmaßnahmen. Seien Sie sich der spezifischen Anforderung dieser Thematik bewusst.

- Beachten Sie dies bereits beim Entwurf Ihrer Sicherheitsarchitektur (Security by Design)
- Identifizieren Sie angreifbare Prozess-Elemente und schützen Sie diese im Einzelnen
- Passen Sie die technischen und organisatorischen Maßnahmen Ihres Sicherheitskonzeptes an die Veränderungen durch „Industrie 4.0“ an
- Achten Sie bei der Vertragsgestaltung im Zusammenhang mit „Industrie 4.0“ auf verbindliche Sicherheitsregularien
- Sensibilisieren und schulen Sie Ihre Mitarbeiter

Sprechen Sie uns an und vereinbaren Sie einen Termin für ein vertrauliches Sensibilisierungsgespräch



Ihre Ansprechpartner im Wirtschaftsschutz

initiative wirtschaftsschutz

Gemeinsam. Werte. Schützen.

Dort finden Sie weitere Informationen sowie die Kontaktdaten Ihrer örtlichen Ansprechpartner.

www.wirtschaftsschutz.info

Impressum

Herausgeber: Bundesamt für Verfassungsschutz für den Verfassungsschutzverbund
wirtschaftsschutz@bfv.bund.de

Bilder: © fotohansel - Fotolia.com
© magele-picture - Fotolia.com
© Nikolai Sorokin - Fotolia.com

Stand: Januar 2017

Verfassungsschutz

Bund Länder

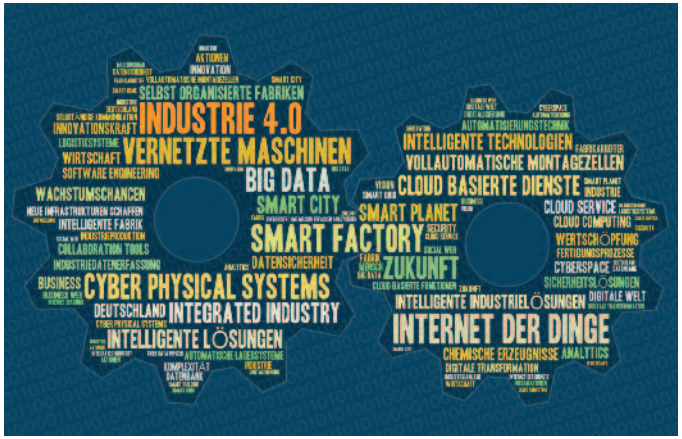
Wirtschaftsschutz

Herausforderungen neuer Technologien

Industrie 4.0

Was bedeutet „Industrie 4.0“?

Dieser Begriff bezeichnet die intelligente Vernetzung von Produktentwicklung, Produktion, Logistik und Kunden. Treibende Kraft dieser Entwicklung ist die rasant zunehmende Digitalisierung von Wirtschaft und Gesellschaft. Sie verändert bereits heute nachhaltig die Art und Weise, wie Unternehmen arbeiten und handeln.



Ziele dieser Vernetzung sind die Optimierung von Unternehmensprozessen sowie die Entwicklung neuer Geschäftsmodelle im Hinblick auf eine gesteigerte Wertschöpfung. Gerade für kleine und mittlere Unternehmen eröffnen sich hier neue Perspektiven, die aber auch zusätzliche Herausforderungen mit sich bringen.

Neue Chancen

–

Neue Risiken

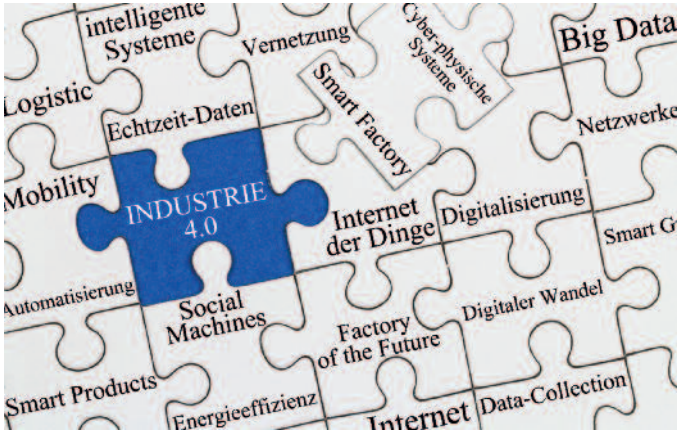
Risiken

Die zunehmende Digitalisierung und Vernetzung der Wirtschaft erhöht die Anzahl der Schnittstellen und Interaktionen zwischen verschiedenen Akteuren, die selten über einheitliche Sicherheitsstandards verfügen. Diese Entwicklung eröffnet völlig neue Angriffswege und potenziert darüber hinaus das bestehende Risiko von Cyberattacken.

Musste bisher nur ein zentrales Steuerungssystem (z. B. durch eine Firewall) abgesichert werden, erfordert „Industrie 4.0“ nun den Schutz jedes einzelnen, in der Anlage vernetzten intelligenten Elements und der damit zusammenhängenden Kommunikation. Diese sog. „Cyber-Physical-Systems“ (CPS) können eigenständig Informationen aufnehmen, Aktionen auslösen und sich wechselseitig steuern. Sie sollten jeweils wie ein eigenständiger Computer betrachtet und geschützt werden, um Sabotage und Spionage zu verhindern.

„Die Unternehmen müssen sich immer stärker dieser Vernetzung öffnen. Ein wesentlicher Aspekt dabei ist die Vertrauenswürdigkeit der eingesetzten Systeme. Hier ist ein wirksames und durchgehendes Security-Konzept zu erarbeiten.“

(Michael Ziesemer, Präsident Zentralverband Elektrotechnik- und Elektroindustrie, CompetenceBook, 2015)



Neuartige Bedrohungsszenarien

- Ausspähung der Produktionsdetails durch Auslesen von CPS-Parametern
- Sabotage durch Manipulation einzelner CPS bzw. der CPS-Kommunikation
- Beeinflussung bis hin zum Ausfall der Produktion durch DoS-Attacken auf CPS-Layer

Perspektive

„Industrie 4.0“ eröffnet einzelnen Unternehmen, aber auch der ganzen deutschen Volkswirtschaft beträchtliche Entwicklungspotentiale. Darüber hinaus wird die zunehmende Vernetzung (z. B. Smart-Cities, Internet of Things) vermehrt auch den Alltag bestimmen. Dieser Tatsache sollten sich alle Verantwortlichen in Wirtschaft und Gesellschaft bewusst sein und dies sowohl im beruflichen als auch privaten Umfeld entsprechend berücksichtigen.