Die Rüstungsindustrie – jetzt auch im Fokus des IT-SiG 2.0

The world is how we shape it

sopra steria

Das IT-Sicherheitsgesetz 2.0 – Herausforderungen und Konsequenzen

Digitale Transformation, Internet of Things (IoT) und Industrie 4.0 sind für die Zukunft der wehrtechnischen Industrien von zentraler Bedeutung. Mit zunehmender Vernetzung der Informations- und Kommunikationssysteme steigen jedoch auch die Angriffsmöglichkeiten – Digitalisierung ohne eine angemessene Informations- und Cybersicherheit ist schier unmöglich.

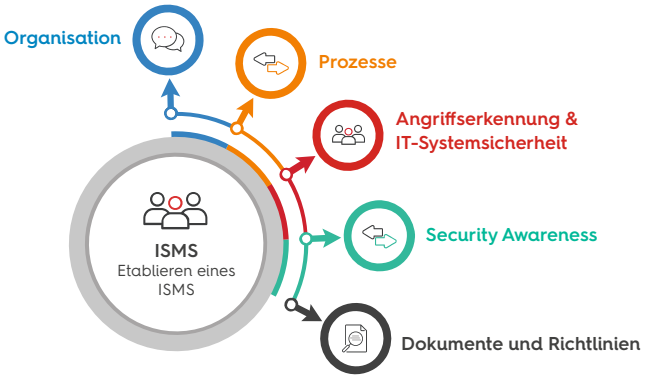
Mit dem „Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme", kurz IT-Sicherheitsgesetz (IT-SiG), hat die Bundesregierung 2015 Anforderungen definiert und Maßnahmen festgelegt, die dem Schutz der Gesellschaft, der Wirtschaft und des Staates dienen. Bislang standen Kritische Infrastrukturen im Fokus des Gesetzgebers. Mit der Version 2.0 des IT-SiG sind auch Infrastrukturen im besonderen öffentlichen Interesse zur Umsetzung der Vorgaben verpflichtet – darunter auch die Rüstungsindustrien.

Im Vordergrund stehen die Umsetzung und der Nachweis angemessener Sicherheitsmaßnahmen zum Schutz informationstechnischer Systeme, Komponenten und Prozesse nach dem „Stand der Technik". Für die Umsetzung haben die Unternehmen zwei Jahre nach Inkrafttreten Zeit. Weitere Anforderungen sind der Einsatz von Systemen zur Angriffserkennung, das Einrichten einer dauerhaft erreichbaren Kontaktstelle und die unverzügliche Meldung von IT-Störungen. Bei Verstößen drohen Geldbußen von bis zu 20 Millionen Euro.

Umsetzung des IT-SiG 2.0 – was auf Unternehmen zukommt

Um die Gesetzesanforderungen erfolgreich umzusetzen, benötigen die betroffenen Unternehmen ein **Informationssicherheitsmanagementsystem (ISMS) nach ISO/IEC 27001**. Sie führen entweder ein ISMS neu ein oder passen ein vorhandenes an die neuen Anforderungen an. Dazu ist es unter anderem notwendig, eine Informationssicherheitsorganisation aufzubauen, die notwendigen Rollen und Verantwortlichkeiten festzulegen sowie ein System zur Erkennung von Cyberangriffen einzuführen.

Von zentraler Bedeutung ist der Auf- und Ausbau der richtigen Prozesse, z. B. für das Risikomanagement, Notfallmanagement, Berichtswesen, für Audits sowie den Umgang mit Sicherheitsvorfällen. Alle technischen und organisatorischen Maßnahmen müssen dabei stets dem „Stand der Technik" entsprechen. Das bedeutet, sie müssen von führenden Fachleuten anerkannt sein und sich in der Praxis bewährt haben.



IT-SiG 2.0 @ Sopra Steria – so unterstützen wir Sie

Sopra Steria begleitet Sie in allen Phasen. Sie bestimmen anhand Ihres Bedarfs die passende Unterstützung.

Analyse und Pre-Check
Wir analysieren, ob Ihr ISMS die Anforderungen des IT-Sicherheitsgesetzes 2.0 erfüllt, ermitteln den konkreten Handlungsbedarf, identifizieren Quick Wins und erstellen eine Budgetplanung für weitere Maßnahmen.

ISMS-Implementierung
Wir begleiten Sie bei der Planung, Einführung und Weiterentwicklung Ihres ISMS bis zur Konformität mit dem IT-Sicherheitsgesetz 2.0, inklusive Tool-Auswahl und -Integration.

Post-Services
Wir stellen Ihnen zielgerichtete Services bereit, die Sie dabei unterstützen, das festgelegtes Sicherheitslevel Ihres ISMS praktisch zu erreichen, z. B. Security Awareness as a Service, Audits gem. IT-SiG, Coaching, Erstellung von IT-Sicherheitskonzepten und Richtlinien.

Unsere Leistungsbausteine – an Ihre individuelle Lage anpassbar.

IT-Sicherheitsexpertise – so profitieren unsere Kunden

Sopra Steria bietet fachliches und technologisches Know-how. Sie erhalten messbare Mehrwerte für Ihr IT-SiG-2.0-Projekt.

Unsere Fachkompetenz und Erfahrung:

- Für alle gängigen Managementsysteme (z. B. nach ISO/IEC 27001, ISO 22301, ISO 9001) zertifizierte Auditoren
- Nach BSI-Gesetz/IT-Sicherheitsgesetz (Prüfverfahrenskompetenz § 8a IT-SiG) zertifizierte Prüfer
- Langjährige Berufserfahrung in der Implementierung von Informationssicherheitsmanagementsystemen
- Umfassende Branchenkenntnis der wehrtechnischen Industrien und der Bundeswehr

Messbare Vorteile für unsere Kunden:

- Kosteneinsparung, Kostenvermeidung und Reduktion von Risiken
- Entlastung Ihrer eigenen Mitarbeiter und Einsparung interner Ressourcen
- Detaillierter Überblick über Ihr IT-Sicherheitsniveau und Ihren Handlungsbedarf
- Verbesserung des Unternehmensimage
- Erkennen und Verhindern von potenziellen Angriffen und damit Verhinderung von Betriebsunterbrechungen und -schäden
- Nachhaltige Verhaltensänderung und Sensibilisierung Ihrer Mitarbeiter

Über Sopra Steria

Als ein führender europäischer Management- und Technologieberater unterstützt Sopra Steria mit 46.000 Mitarbeiterinnen und Mitarbeitern in 25 Ländern seine Kunden dabei, die digitale Transformation voranzutreiben und konkrete und nachhaltige Ergebnisse zu erzielen. Sopra Steria bietet mit Beratung, Digitalisierung und Softwareentwicklung umfassende End-to-End-Lösungen, die große Unternehmen und Behörden wettbewerbs- und leistungsfähiger machen – und zwar auf Grundlage tiefgehender Branchenexpertise, innovativer Technologien und eines kollaborativen Ansatzes. Das Unternehmen stellt die Menschen in den Mittelpunkt seines Handelns mit dem Ziel, digitale Technologien optimal zu nutzen und eine positive Zukunft für seine Kunden zu gestalten.

The world is how we shape it

10127

Sopra Steria SE
Hans-Henny-Jahnn-Weg 29
22085 Hamburg
it-security.defence@soprasteria.com
www.soprasteria.de

sopra steria