HEALTHCARE

KRITIS im Gesundheitswesen

Delivering Transformation. Together.

sopra steria CONSULTING

HERAUSFORDERUNGEN DURCH DAS IT-SICHERHEITSGESETZ

Wohlstand, Fortschritt und Gesundheit: Die Digitalisierung leistet dazu einen wesentlichen Beitrag – aber sie macht unsere Gesellschaft auch anfällig für immer komplexere Cyber-Gefahren. Seit Juli 2015 verpflichtet das IT-Sicherheitsgesetz Unternehmen mit besonderer Bedeutung für die Funktionstüchtigkeit des staatlichen Gemeinwesens – sogenannte Kritische Infrastrukturen (KRITIS) – geeignete Maßnahmen zu ergreifen, um die Funktionstüchtigkeit ihrer informationstechnischen Systeme auch in Ausnahmesituationen gewährleisten zu können. Im Gesundheitssektor fallen neben der Arzneimittelindustrie und medizinischen Laboren auch Krankenhäuser und Kliniken in den Geltungsbereich des IT-Sicherheitsgesetzes. Am 29.07.2017 hat das BSI dann die konkreten Vorgaben für die betroffenen Unternehmen des Gesundheitssektors veröffentlicht. Damit beginnt nun auch für diese die Umsetzungsfrist von 2 Jahren. Zu den Mindestanforderungen gehört die Einrichtung eines sogenannten Information Security Management Systems (ISMS), sowie die Absicherung der gesamten IT nach dem „aktuellen Stand der Technik". Darüber hinaus haben medizinische Einrichtungen auch ein erhebliches Eigeninteresse an der Sicherung ihrer IT-Landschaft durch diese Maßnahmen. Denn nur durch einen nachweislichen Schutz ihrer kritischen IT-Systeme können sie beispielsweise Schadensersatzforderungen und Patientenschäden vermeiden sowie die digitale und auch reale Patientensicherheit deutlich erhöhen.

WAS IST ZU TUN

Das IT-Sicherheitsgesetz und die fachlichen Vorgaben des BSI haben insbesondere für solche Gesundheitsunternehmen weitreichende Konsequenzen, die bisher weder ein ISMS noch ISMS-ähnliche Strukturen implementiert haben.
Was ist zu tun?

- Schaffung einer Informationssicherheits-Organisation gemäß ISO/IEC 27001: Rollen, Verantwortlichkeiten & Gremien
- Umfangreiche Sicherheitsmaßnahmen: physische Sicherheit, Netze, Organisation, Schulungen & IT-Systeme
- Aufbau entsprechender Prozesse: Berichtswesen, Qualitätsmanagement, Audits, Notfallmanagement, Meldewege, Compliance, Einkauf, Entwicklung, Umgang mit Sicherheitsvorfällen & Risikomanagement
- IT-Systemsicherheit: Zugang, Zutritt, Berechtigungen & Verantwortlichkeiten
- Netzwerksicherheit: Protokollierung, Zugriff & Trennung
- Anwendungssicherheit: Entwicklung, Aktualisierung & Betrieb
- Schulung und Sensibilisierung, zum Beispiel durch Awareness-Kampagnen
- Dokumente: Leitlinien, Richtlinien, Konzepte, Arbeitsanweisungen & Dokumentation

ISO/IEC 27001:2013 - ISMS

Weitere Herausforderungen rund um Ihr ISMS:

- Etablieren eines ISMS, bestehend aus Organisation, Prozessen & Dokumentation inklusive eines kontinuierlichen Verbesserungsprozesses
- Definition des Informationsverbundes (Anwendungsbereich des ISMS)
- Soll-Ist-Analyse des Informationsverbundes
- ISMS-Assessment anhand ISO 27001, 27002 und weiterer relevanter Standards
- Risikomanagement
- Ableitung und Definition notwendiger Maßnahmen zur Erreichung eines angemessenen Sicherheitsniveaus
- Priorisierung, Planung und Umsetzung dieser Maßnahmen

Bestehendes ISO-27001-Zertifikat

Sofern bereits ein ISO-27001-Zertifikat vorhanden ist, bleibt zu prüfen, ob der Informationsverbund alle notwendigen Systeme gemäß IT-Sicherheitsgesetz umfasst. Sämtliche Systeme mit unmittelbarem und mittelbarem Einfluss auf die Grundfunktionen des „kritischen" Unternehmens müssen vom ISMS explizit abgedeckt sein. In Kliniken betrifft das zum Beispiel auch wichtige medizintechnische Geräte zur Versorgung der Patienten, inklusive der zugehörigen Kommunikations- und IT-Systeme. Eine Zertifizierung des Rechenzentrums oder der Muttergesellschaft allein ist also nicht ausreichend.

IHR NUTZEN

Nutzen Sie unsere Erfahrung und Kompetenz zu Ihrem Vorteil:

- Zuverlässige Erfüllung aller Anforderungen des IT-Sicherheitsgesetzes und der spezifischen BSI-Fachvorgaben für den Gesundheitssektor
- Abfedern der Belastung Ihrer Mitarbeiter
- Angemessene, risikoorientierte Maßnahmen mit Augenmaß
- Kein Personalaufbau erforderlich
- Reduktion bestehender Risiken
- Erfahrene Projektleitung vermeidet Fehler, Misserfolge und Demotivation
- Wissenstransfer und Coaching reduziert Ihren Schulungsbedarf

UNSERE STÄRKEN

Wir sind Ihr idealer Partner, denn wir:

- verfügen über eine langjährige Erfahrung in der Implementierung und Weiterentwicklung von ISMS in den unterschiedlichen Branchen,
- unterstützen bereits mehrere KRITIS-Unternehmen, auch des Gesundheitssektors, bei der Erfüllung der neuen gesetzlichen Anforderungen,
- helfen Ihnen, die fachlichen Vorgaben effizient und pragmatisch umzusetzen,
- haben mehrere ISO 27001- sowie IT-Grundschutz-Auditoren (BSI),
- haben in Deutschland circa 35 und europaweit rund 650 ISMS-Experten,
- sind seit 2006 nach ISO 27001 zertifiziert,
- verfügen über ein integriertes Managementsystem gemäß ISO 27001, 14001, 9001 und 20000,
- bringen hochkarätiges Branchen-Know-how ebenso mit wie wertvolle Kontakte zu Kliniken, Gremien und Verbänden.

SIE ENTSCHEIDEN

- Pre-Check KRITIS als Vorprojekt: Standortbestimmung, Identifizierung des konkreten Handlungsbedarfs, Quick-Wins, Budgetplanung und Managementbericht
- Pre-Scan KRITIS als Vorprojekt: technische und faktenbasierte Bewertung des IT-Sicherheitsstatus in Ihrem Unternehmen
- ISMS-Implementierung als Hauptprojekt: Bedarfsgerechte Einführung oder Weiterentwicklung Ihres ISMS bis zur Konformität gemäß IT-Sicherheitsgesetz

SPRECHEN SIE UNS AN, WIR BERATEN SIE GERNE!

Über Sopra Steria Consulting

Sopra Steria Consulting zählt heute zu den Top Business Transformation Partnern in Deutschland. Als ein führender europäischer Anbieter für digitale Transformation bietet Sopra Steria mit mehr als 40.000 Mitarbeitern in über 20 Ländern eines der umfassendsten Angebotsportfolios für End-to-End-Services am Markt: Beratung, Systemintegration, Softwareentwicklung, Business Process Services. Unternehmen und Behörden vertrauen auf die Expertise von Sopra Steria, komplexe Transformationsvorhaben, die geschäftskritische Herausforderungen adressieren, erfolgreich umzusetzen.

Im Zusammenspiel von Qualität, Leistung, Mehrwert und Innovation befähigt Sopra Steria seine Kunden, Informationstechnologien optimal zu nutzen.

20009_IT_Sec_Kritis_DE

Hans-Henny-Jahnn-Weg 29
22085 Hamburg

www.soprasteria.de
info.de@soprasteria.com

sopra steria CONSULTING