FÖRDERTATBESTAND 10

Sicherheit für IT-Systeme **und Datenbestände**

Die Cybersicherheit ist in Krankenhäusern von essentieller Bedeutung. Es betrifft alle IT-Systeme von der Gebäudetechnik bis hin zu Internettechnologien. Um die Gesundheitsversorgung zu gewährleisten müssen die richtigen IT-Anbieter ausgewählt, Systeme konfiguriert und regulatorischen Anforderungen erfüllt werden. Zusätzlich ist der Aufbau eines fortschrittlichen und flexiblen IT-Managements ebenso unabdingbar, wie die Integration von Informationssicherheitsanforderungen in IT-Systeme und -prozesse.

siemens.de/khzg

SIEMENS

Governance
- Gesetze & Standards
- Rahmenwerke & Richtlinien
- Rollen und Verantwortlichkeiten
- Risikomanagement

Asset-Management
- IT-Anlagenverwaltung
- Software-Asset-Verwaltung
- Daten-Inventarisierung

Datenhandhabung
- Klassifizierung von Daten
- Aufbewahrung und Löschung
- Handhabung von Backups
- Schutz der Daten

Netzwerksicherheit
- Netzwerkdesign
- Netzwerkkontrollen
- Schnittstellen & Systemintegration

Sicherheitsoperationen
- Patch- und Konfigurationsmanagement
- Hardening
- Schwachstellen-Management
- Monitoring der Sicherheit

Identitäts- & Zugriffsmanagement
- Benutzer- und Zugriffskontrollen
- Autorisierungsmechanismen
- Handhabung von privilegierten Rollen
- Kryptographie & PKI

Assessment der Sicherheit
- Audit & Reifegradbewertung
- Penetrationstests
- Digitale Forensik
- Managementberichterstattung

Inzidenthandhabung
- Betriebliches Kontinuitätsmanagement
- IT-Notfallplanung
- IT-Störungsmanagement
- Verfügbarkeit

Die **Informationssicherheit** basiert auf vielen Einzelmaßnahmen. Durch die aufeinander aufbauende Absicherung entsteht eine Defense-in-Depth Ansatz. Dies schließt sowohl die Prävention und Detektion von Cyberaktivitäten als auch die Mitigation im Ernstfall ein. Begleitet wird dies durch Lernkonzepte und -inhalte für Awareness und Training für alle sicherheitsrelevante Themen. Wir helfen Ihnen maßgeschneiderte Ansätze zu finden.

HR
- Onboarding und Offboarding
- Training
- Awareness
- Bedrohungen durch Insider

Physische Sicherheit
- Sicherheit der Anlage
- Sicherheit des IT-Equipments

Gebündelte Kompetenzen für mehr Sicherheit

Gemeinsam mit Ihnen können wir Lösungen für Netzwerkgestaltung, Komponentenauswahl- und Konfiguration sowie Schnittstellen, Verschlüsselungs- und Schutzkonzepten entsprechend den Kernkompetenzen Ihrer Organisation bündeln.

Passend zu Ihren Anforderungen kümmern wir uns um den Aufbau eines Security Operation Center und verknüpfen KI-Lösungen mit dem Security Event Management, dem Inzident- oder dem Vulnerabilitätsmanagement.

Wir entwickeln ebenfalls physische und logische Backup-Lösungen und binden diese in administrative, physische und technische Kontrollmechanismen ein.

Mit einer Gap-Analyse in der Gebäudetechnik sowie einer Reifegradmessung und einem Benchmarking der IT- und Cybersicherheit können wir die Potenziale und Entwicklungsschritte Ihres Objekts fundiert bewerten.

Wir übernehmen für Sie den Aufbau sicherer Cloud-Architekturen und die Anbindung von Systemen – ohne dass Systembrüche beim Datenfluss entstehen. Bei der Erstellung und Umsetzung von Schnittstellen setzten wir bewusst auf Multifaktorenauthentifizierung.

Für sämtliche unserer Lösungen übernehmen wir die Gewährleistung der rechtlichen Konformität und stellen sicher, dass die Anforderungen der DSGVO erfüllt sind.

Herausgeber
Siemens Deutschland AG

Siemens AG
Smart Infrastructure
Lyoner Straße 27
60528 Frankfurt am Main
Deutschland
Tel. +49 69 6682 6660

Stand: 03/2021