

INFORMATIONSSICHERHEITS- STATUS-ANALYSE (ISSA)

↳ FÜR UNTERNEHMEN IM GESUNDHEITSWESEN:
CYBERRISIKEN ERKENNEN. SICHERHEIT GEZIELT STÄRKEN.

Die Anforderungen an die Informationssicherheit im Gesundheitswesen steigen stetig. Regulatorische Vorgaben wie NIS2, die EU-DSGVO und die BSI-Kritisverordnung sowie branchenspezifische Standards wie der B3S Krankenhaus erfordern eine umfassende und nachweisbare Absicherung der IT von Krankenhäusern und anderen Gesundheitseinrichtungen.

Gleichzeitig gefährden Cyberangriffe, kompromittierte Benutzerkonten und Schwachstellen medizinische Prozesse und die Sicherheit sensibler Gesundheitsdaten. Umso wichtiger ist es, Risiken frühzeitig zu erkennen, Sicherheitsmaßnahmen wirksam umzusetzen und die eigene Compliance jederzeit belegen zu können. Informationssicherheit ist heute eine Voraussetzung für eine sichere und zuverlässige Patientenversorgung.

Informationssicherheit als Basis für eine sichere Patientenversorgung

Krankenhäuser und andere Einrichtungen des Gesundheitswesens sind in hohem Maße von verfügbaren und verlässlichen IT-Systemen abhängig. Neben dem Schutz sensibler Patienteninformationen stehen daher die Aufrechterhaltung der Versorgung, die Integrität medizinischer Daten und die sichere Fortführung kritischer Prozesse im Mittelpunkt.

Deshalb gilt es zu prüfen, ob die getroffenen Sicherheitsmaßnahmen wirksam sind, dem aktuellen Stand der Technik entsprechen, wirtschaftlich angemessen und ordnungsgemäß umgesetzt sind. So lässt sich sicherstellen, dass sie den individuellen Anforderungen an die Cybersicherheit gerecht werden. Neben technischen und organisatorischen Maßnahmen spielen auch das Sicherheitsbewusstsein und die gelebte Sicherheitsstrategie eine entscheidende Rolle.

Proaktiv werden mit der ISSA

Die Informations-Sicherheits-Status-Analyse (ISSA) liefert die entscheidenden Antworten, indem sie relevante Aspekte der Informationssicherheit und des Datenschutzes erfasst und mögliche Defizite im bestehenden IT-Sicherheitskonzept aufdeckt. Praxisgerechte Empfehlungen unterstützen dabei, erkannte Schwachstellen in der IT-Sicherheit zu beheben. Zudem werden konkrete Kontrollmaßnahmen vorgeschlagen, um ein angemessenes Sicherheitsniveau zu gewährleisten. Die dokumentierten Ergebnisse und der daraus abgeleitete Maßnahmenkatalog können zudem als fundierte Grundlage für die Vorbereitung und Begründung von Förderanträgen dienen – etwa im Rahmen des geplanten Sofortprogramms Cybersicherheit des Bundesministeriums für Gesundheit (BMG) oder, sofern das jeweilige Vorhaben die Fördervoraussetzungen erfüllt, des Krankenhaustransformationsfonds (KHTF).

WIE KANN SVA SIE UNTERSTÜTZEN?



Im Rahmen einer **Informations-Sicherheits-Status-Analyse (ISSA)** werden dokumentierte und praktizierte Prozesse analysiert. Diese umfassen technische und organisatorische Maßnahmen in Bezug auf IT-Sicherheit, IT-Betrieb, Datenschutz und IT-Compliance. Besonderes Augenmerk gilt den für die Patientenversorgung und den Geschäftsbetrieb kritischen Systemen und Prozessen. Dazu können beispielsweise Krankenhausinformationssysteme, medizinische Subsysteme, vernetzte Medizinprodukte, Cloud-Dienste, Fernwartungszugänge, Identitäts- und Berechtigungsmanagement sowie Schnittstellen zu Partnern und IT-Dienstleistern gehören. Bei Begehungen vor Ort werden physische Aspekte der Informationssicherheit stichprobenartig erfasst. Neben den bestehenden Anforderungen an Informationssicherheit und Datenschutz betrachten unsere Security Consultants auch gegenwärtige sowie zukünftige Entwicklungen im Bereich der Bedrohungsabwehr und -erkennung.

Sie decken konzeptionelle Schwachstellen in den getroffenen Maßnahmen auf und unterbreiten konkrete Lösungsvorschläge zur Schließung von Lücken. Gefundene Mängel und Schwachstellen werden bewertet, wobei eine qualitative Risikoabschätzung auf Grundlage unserer technischen Expertise erfolgt. Die Ergebnisse werden zusammen mit den Empfehlungen (Maßnahmen) in einem Risikoregister dokumentiert. Dieses Register ist so konzipiert, dass es als Maßnahmenkatalog verwendet und nahtlos in ein bestehendes Risikomanagement integriert werden kann. Die Resultate werden im Zuge eines Abschlussmeetings vor Ort präsentiert, in dem auch Raum für Diskussionen zu den empfohlenen Maßnahmen geboten wird.

Sie möchten gerne mehr erfahren?
Wir freuen uns auf Ihre Kontaktaufnahme!

UNSERE LEISTUNGEN

- **Analyse der Anforderungen** im Hinblick auf Informationssicherheit und Datenschutz basierend auf den individuellen Sicherheitsanforderungen Ihres Unternehmens
- **Ist-Aufnahme** der Kontrollmechanismen
- **Technische Einzelprüfungen** (Deep Dives) durch Sicht- oder Wirksamkeitsprüfung
- **Analyse der Bedrohungen** für die IT-Sicherheit durch interne und externe Täter sowie unbeabsichtigte Fehlhandlungen
- **Bewertung** nach dem Stand der Technik sowie qualitative Risikoabschätzung auf Grundlage relevanter und anerkannter Standards und Vorgaben, z. B. BSI-Gesetz, EU-DSGVO, ISO/IEC 27001, BSI IT-Grundschutz und B3S
- **Praxiserprobte Maßnahmenempfehlungen** zur Mängelbeseitigung
- **Umfassender Analysebericht** inkl. Management Summary
- **Ergebnisvorstellung** und Maßnahmenbesprechung

IHR MEHRWERT

Mit der ISSA bietet SVA eine maßgeschneiderte und kosteneffiziente Analyse, die auf die Anforderungen Ihrer Gesundheitsorganisation abgestimmt ist. Sie erhalten eine nachvollziehbare Bewertung des aktuellen Sicherheitsniveaus, der identifizierten Risiken sowie Erkenntnisse aus der stichprobenartigen Überprüfung der Wirksamkeit ausgewählter Maßnahmen.

Die ISSA schafft eine belastbare Entscheidungsgrundlage für Geschäftsleitung, IT-Verantwortliche, Informationssicherheitsbeauftragte und weitere relevante Funktionen. Sie zeigt auf, welche Risiken priorisiert behandelt werden sollten und in welchen Bereichen regulatorischer oder operativer Handlungsbedarf besteht.

ÜBER UNS

Die SVA System Vertrieb Alexander GmbH ist einer der führenden deutschen System-Integratoren und verknüpft hochwertige IT-Produkte mit Projekt-Know-how und Flexibilität zu optimalen Lösungen. Branchenunabhängige Kernthemen sind Datacenter, Business Continuity, Digital Process Solutions und SAP, ergänzt mit Expertise zu modernen Anforderungen wie Cloud, Cyber Security, Big Data & AI, Modern Workplace sowie Agile IT & Software Development.

KONTAKT

Mark Sobol
Fachbereichsleiter Cyber Security
security@sva.de

SVA System Vertrieb Alexander GmbH
Borsigstraße 26
65205 Wiesbaden
www.sva.de