Robin Data

Cyber-Attacken betreffen zunehmend Krankenhäuser

Cyber-Attacken haben sich in den letzten Jahren stark professionalisiert und sorgen allein in Deutschland für bis zu 220 Milliarden Euro Schaden pro Jahr. Laut einer Bitkom-Studie hat sich die Schadenssumme seit 2018 verdoppelt. Cyber-Attacken verursachen den Ausfall von Informations- und Produktionssystemen oder die Störung von internen Abläufen, oftmals durch den Einsatz von Ransomware über Phishing-Angriffe.

Insbesondere im Fokus solcher Angriffe stehen Organisationen mit **kritischer Infrastruktur (KRITIS)**, denn hier drohen neben Versorgungsengpässen in der Folge eines Angriffs erhebliche Störungen der öffentlichen Sicherheit und Versorgung. Laut der Bundesregierung wurden im Zeitraum von Januar bis Anfang November 2020 171 erfolgreiche Hackerangriffe auf Einrichtungen der Kritischen Infrastruktur gezählt, 2019 waren es noch 62, das ergibt einen Anstieg um 175 Prozent. In den letzten Jahren sind **Kritische Infrastrukturen des Sektors "Gesundheit"** immer häufiger durch Cyber-Attacken angegriffen wurden.

Cyber-Angriffe auf Krankenhäuser und Kliniken in 2021

Juli	September	September	Oktober	Dezember
Cyber-Atacke Klinikum Wolfenbüttel	Cyber-Attacke Krankenhaus Friedrichsroda	Cyber-Attacke SRH-Stiftung und zugehörige Kliniken	Cyber-Attacke Klinikum Dessau	Cyber-Attacke Klinikum Braunschweig

Unsere moderne Gesellschaft ist in hohem Maße von einer funktionierenden Gesundheitsversorgung abhängig. Gesundheitsdaten gehören zu besonders schützenswerten personenbezogenen Daten.

Betreiber von Krankenhäusern unterliegen daher einer großen Verantwortung, Investieren Sie jetzt in das Management Ihrer Informationssicherheit und Ihres Datenschutzes und sichern Sie diese Daten nachhaltig vor Cyber-Attacken.

Wir unterstützen Sie dabei pragmatisch und zielorientiert!

Prof. Dr. Andre Döring, CEO der Robin Data GmbH
Ihr Experte für Datenschutz und Informationssicherheit

Robin Data GmbH | sales@robin-data.io | +49 (0) 3461 4798960 | www.robin-data.io

Robin Data

Branchenspezifischer Sicherheitsstandard (B3S) und gesetzliche Vorgaben für den Gesundheitssektor

- Krankenhäuser müssen die **Anforderungen des BSI-Gesetzes** umsetzen
  - Der B3S dient der Etablierung eines angemessenen Sicherheitsniveaus i.S.v. § 8a (1) BSIG bei gleichzeitiger Wahrung des üblichen Versorgungsniveaus der Patientenversorgung und der Verhältnismäßigkeit der umzusetzenden Maßnahmen.
  - Weist der Betreiber kritischer Infrastrukturen die Umsetzung eines durch das BSI als „geeignet zur Umsetzung der Anforderungen nach § 8a Abs. 1 BSI-Gesetz" anerkannten B3S nach, wird von der Einhaltung der gesetzlich vorgeschriebenen Maßnahmen ausgegangen
- Krankenhäuser müssen gemäß §75c SGB V **seit 01.01.2022 ein Informationssicherheits-Management-System** betreiben:

(1) Ab dem 1. Januar 2022 sind Krankenhäuser verpflichtet, nach dem Stand der Technik angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität und Vertraulichkeit sowie der weiteren Sicherheitsziele ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit des jeweiligen Krankenhauses und die Sicherheit der verarbeiteten Patienteninformationen maßgeblich sind. Organisatorische und technische Vorkehrungen sind angemessen, wenn der dafür erforderliche Aufwand nicht außer Verhältnis zu den Folgen eines Ausfalls oder einer Beeinträchtigung des Krankenhauses oder der Sicherheit der verarbeiteten Patienteninformationen steht. Die informationstechnischen Systeme sind spätestens alle zwei Jahre an den aktuellen Stand der Technik anzupassen.

Schritte zu Umsetzung des B3S und Einhaltung des §75c SGB V zur IT-Sicherheit in Krankenhäusern

Nr.	Schritt und Ziel	Tätigkeit
1	**Kontext des ISMS definieren**	Geltungsbereich des ISMS und strategische Ziele der Informationssicherheit definieren
2	**Managementstruktur für ISMS definieren**	Entwicklung und Inkraftsetzung von Richtlinien / Standards
3	**Grundsätzliche Maßnahmen umsetzen**	Implementierung der Sicherheitsorganisation, Entwicklung und in Kraft-Setzung von Verfahren
4	**Bestandsaufnahme, Risikoeinschätzung und Konzeption**	Identifikation von Schwachstellen, Bewertung aktueller TOMs, Risikoanalyse
5	**Umsetzung der Maßnahmen (von detailliertem Plan zur Risikobehandlung)**	Umsetzung der Maßnahmen gemäß definierter Richtlinien, Prozesse und Verfahren.
6	**Projektbegleitende Trainings, Ausbildung und Awareness**	Schulungsbedarf ermitteln, Zeitplan zu Umsetzung definieren, Durchführung von Schulungen und Sensibilisierungen
7	**Evaluierung der Effektivität des ISMS**	Monitoring & Überwachung, Planung und Durchführung interner Audits

Robin Data

Audits gemäß B3S und §75c SGB V für Krankenhäuser

Professionelles Audit durch zertifizierte Experten in ganz Deutschland. Profitieren Sie von der langjährigen Erfahrung durch kompetente und praktische Beratung.

Ablauf des Informationssicherheits-Audits

In einem 1-tägigen Workshop führt ein Informationssicherheit-Experte der Robin Data GmbH ein Audit bei Ihnen vor Ort durch. In dem Audit wird der aktuelle Reifegrad des Managementsystems für Informationssicherheit (ISMS) gegen den B3S für die medizinische Versorgung begutachtet. Ergänzend wird auch der aktuelle Reifegrad des Datenschutz-Managementsystems betrachtet.

1

Vorbereitung und Angebot
In einem kostenfreien Erstgespräch mit Robin Data beraten wir Sie unverbindlich zum Thema ISMS-Audit und den Umfang Ihrer Anforderungen. Zur Vorbereitung auf das Audit werden auf Basis einer Anforderungsliste des Kunden die vorhandene Dokumentation und verwendete Richtlinien des ISMS abgefragt.

2

Durchführung des Informationssicherheits-Audits
Während des ISMS-Audits werden interne und externe Sicherheitsvorgaben (Kontrollen, Security Policy und Guidelines), Prozesse und relevante Dokumente überprüft. Offene Maßnahmen dokumentiert und am Ende des Audits priorisiert. Auf dieser Basis werden sicherheitsrelevante Abweichungen von den Standards direkt angegangen.

3

Ergebnis-Gutachten und Maßnahmenkatalog
Anschließend erfolgt die Bewertung unserer Experten über den Zustand des etablierten Informationssicherheits-Managementsystems. Sie erhalten 5-10 Werktage nach Abschluss des ISMS Audits ein zusammenfassendes Gutachten und eine Übersicht der Ergebnisse des Audits. Dieses enthält die Abweichungen zu den Norm-Kontrollen und die priorisierte Maßnahmenliste. Ein Gespräch schließt das Audit ab.

4

Maßnahmenkatalog
Ergebnis der Analyse sind konkrete Handlungsempfehlungen, um die Defizite zwischen “Ist” und “Soll” zu beheben. Die definierten Maßnahmen können bspw. die Erstellung von Richtlinien, die Überprüfung einzelner Sicherheitskonzepte, die Etablierung eines Löschkonzeptes oder die Umsetzung genereller technisch-organisatorischer Maßnahmen sein. Sei erhalten diese Analyse in Form einer Dokumentation und in Zusammenfassung als Auditbericht.

Umfassende Informationssicherheits-Audits gemäß B3S und §75c SGB V für die medizinische Versorgung

Jetzt Angebot anfordern

Robin Data GmbH | sales@robin-data.io | +49 (0) 3461 4798960 | www.robin-data.io

Robin Data

ISO-zertifizierte Lösungen für Informationssicherheit und Datenschutz für die medizinische Versorgung

Über 50 TÜV / DEKRA zertifizierte Experten

Beratung regional oder digital

Digitales Datenschutz-Management-System

Das sagen Kunden von Robin Data

„In dem Audit unseres Informationssicherheits-Management-Systems durch die Robin Data GmbH, wurde der aktuelle Reifegrad unseres ISMS gegen den Standard des IT-Grundschutzes auditiert. Interne und externer Prozesse und Dokumente wurden überprüft und offene Maßnahmen dokumentiert. Durch die Beratung und klare Verteilung von Verantwortlichkeiten kennen wir eventuelle Schwachstellen und können diese nun aktiv angehen.

Marco Voigt, Leiter IT in der Stadtverwaltung Merseburg

IHK Industrie- und Handelskammer Halle-Dessau

„Herr Professor Döring wurde von uns mit der Durchführung eines Datenschutz- und Informationssicherheitsaudits im Jahre 2021 beauftragt. Wir wollten uns Aufschluss über die Angemessenheit und Wirksamkeit bereits ergriffener Maßnahmen und über etwaige Verbesserungsmöglichkeiten verschaffen. Die Zusammenarbeit mit Herrn Professor Döring gestaltete sich sowohl fachlich als auch menschlich sehr erfreulich. Das Audit wurde termingerecht und zügig durchgeführt; die Ergebnisse unverzüglich und verständlich dargelegt. Vor dem Hintergrund dieser positiven Erfahrungen haben wir nunmehr die Robin Data GmbH zum externen Datenschutz- und Informationssicherheitsbeauftragten bestellt.

Dr. Markus Reinhardt, Geschäftsführer Zentrale Dienste der Industrie- und Handelskammer Halle-Dessau

Westpfalz-Klinikum GmbH

„Wir wollten eine moderne und digitale Umsetzung unseres Datenschutz-Management-Systems. Robin Data hat uns durch die Funktionen, die vielen Vorlagen, die Automatisierungsmöglichkeiten und den sehr kompetenten und freundlichen Service sowie die Zusammenarbeit mit einem Partner in der Nähe überzeugt.

Myriam Marley, Datenschutzbeauftragte Westpfalz-Klinikum GmbH

Die einfache und gesetzeskonforme Umsetzung von Informationssicherheit und Datenschutz

Erstberatungsgespräch buchen

Jetzt Angebot anfordern

Robin Data GmbH | sales@robin-data.io | +49 (0) 3461 4798960 | www.robin-data.io