Solidaris
Nutzen stiften – mit Freude für Menschen

MANDANTENINFORMATION

# IT-Governance

## Steuerung von IT-Risiken für Krankenhausverantwortliche

**Die Informationstechnik (IT) spielt in Unternehmen gleich welcher Größe, Rechtsform und Branche eine zentrale Rolle. Der zunehmende Kosten- und Effizienzdruck macht den Einsatz intelligenter, prozessunterstützender Systeme unabdingbar. Das Gesundheitswesen ist von dieser Entwicklung besonders betroffen. Doch der Einsatz von intelligenten IT-Systemen geht mit einer zunehmenden Komplexität und zudem mit erhöhten Sicherheitsrisiken einher. Auch technische Störungen und Fehlkonzeptionen der zu implementierenden Systeme wirken sich unmittelbar auf die Prozesseffizienz aus. Viele Aufsichtsgremien und Geschäftsführer befürchten zurecht finanzielle und imagebezogene Schäden sowie einen Vertrauensverlust in der Öffentlichkeit.**

Aus Sicht der Corporate Governance ist es daher essentiell, die Informationssicherheit im Unternehmen unter Berücksichtigung der damit einhergehenden rechtlichen Anforderungen zu gewährleisten. Vor diesem Hintergrund erweist sich die Konzeption einer hierzu notwendigen Informationssicherheitsstrategie innerhalb eines Unternehmens als unabdingbar. Diese setzt sich aus der Kombination verschiedener technischer und organisatorischer Maßnahmen zusammen und funktioniert ausschließlich als „Top-Down-Ansatz“, der aktiv die Steuerung durch die Unternehmensleitung voraussetzt.

Die Ereignisse des vergangenen Jahres zeigen deutlich, wie verwundbar Unternehmen im Gesundheitswesen bei IT-Vorfällen sind. Schon ungezielte Attacken, wie die immer noch anhaltenden Hackerangriffe mittels Verschlüsselungstrojanern, führen zu teils erheblichen Beeinträchtigungen der Geschäftsprozesse und gefährden den Unternehmenserfolg nachhaltig. Als Reaktion auf die steigende Bedrohung durch Cyber-Kriminalität versucht die Bundesregierung nun durch das IT-Sicherheitsgesetz, etablierte IT-Management-Standards wie die internationale Norm ISO 27001 oder den deutschen BSI IT-Grundschutz, verbindlich und zur direkten Aufgabe der Geschäftsleitung zu machen. Dabei stellen derartige Standards selbst versierte IT-Manager vor große Herausforderungen, so dass eine externe Unterstützung unentbehrlich erscheint. Insbesondere Fragestellungen rund um IT-Governance, Risk und Compliance, die aufgrund gebundener Personalressourcen i. d. R. nicht ausreichend Beachtung im Unternehmen finden, bereiten Aufsichtsgremien und Geschäftsleitungen Kopfschmerzen. Eine erste Abhilfe leisten die folgenden Ausführungen, die Krankenhausverantwortlichen zunächst einmal eine Orientierung im IT-Sicherheitsdschungel bieten.

Berlin
Erfurt
Freiburg
Hamburg
Köln
München
Münster
Wien (A)
Würzburg

1. **Implementierung eines Informationssicherheits-managements (ISMS)**

   Ein ISMS ist ein Rahmenwerk zur Gewährleistung der vorgeschriebenen Informationssicherheit im Krankenhaus. Die Einführung eines ISMS für Krankenhäuser, die gemäß IT-Sicherheitsgesetz zu den Betreibern kritischer Infrastrukturen (KRITIS) gehören (Entscheidung wird Ende 1. Quartal 2017 erwartet), wird voraussichtlich verbindlich sein. Dabei werden u. a. konkrete Leitlinien für das Sicherheitsmanagement festgelegt sowie klare Verantwortlichkeiten zugewiesen. Eine deutliche Positionierung der Geschäftsführung zur Informationssicherheit und somit die Übernahme einer Vorbildfunktion ist wesentlicher Bestandteil eines funktionierenden ISMS. Wir gehen davon aus, dass die Anforderungen des IT-Sicherheitsgesetzes sowie die erwartete Umsetzungsverordnung auch auf die Krankenhäuser mittelbar ausstrahlen, die zunächst nicht unter die Definition KRITIS fallen. Eine Zwei-Klassen-Gesellschaft von „sicheren Krankenhäusern" und „unsicheren Krankenhäusern" ist an dieser Stelle schwer denkbar, sodass auch diese Häuser gut beraten sind, frühzeitig mit der Implementierung eines ISMS zu beginnen.

2. **Software Asset Management (SAM)**

   Im Rahmen unserer Prüfungen stellen wir regelmäßig fest, dass historisch gewachsene IT-Infrastrukturen in Verbindung mit dem Einsatz neuer Technologien das Risiko von Falsch- oder Fehllizenzierungen erhöhen. Dabei ist es von grundlegender Bedeutung, Transparenz über die rechtliche und finanzielle Lizenzsituation herzustellen. Lizenzen stellen ein wichtiges Wirtschaftsgut dar, dessen korrekter Einsatz zu wesentlichen Kosteneinsparungen führen kann. Andererseits kann aber eine Falsch- oder Fehllizenzierung rechtliche Folgen haben und hohe Kosten verursachen. Immer häufiger machen Softwarehersteller wie Microsoft von ihrem Recht Gebrauch und überprüfen die lizenzvertragskonforme Nutzung der Software. Wird im Rahmen einer solchen Überprüfung festgestellt, dass die Software nicht lizenzkonform eingesetzt wird, müssen entsprechende Lizenzen nachträglich erworben werden. Und das wird häufig teuer. In der Praxis zeigt sich, dass ein konsequentes Lizenzmanagement über den gesamten Lebenszyklus der Software (SAM) eine notwendige Maßnahme zur Beherrschung der Risiken von Falsch- oder Fehllizenzierungen darstellt. SAM ist ein anerkanntes Verfahren zur Verwaltung und Optimierung der IT-Assets in einem Unternehmen. Mittels dieses Verfahrens werden regelmäßige Hard- und Softwareinventarisierungen anwendungsbasiert vorgenommen, die zugleich Aufschluss darüber geben, ob die installierte Software überhaupt genutzt bzw. aktuell ist. Nicht aktualisierte Software kann erhebliche Sicherheitslücken enthalten und Angriffspunkte für künftige Cyberangriffe darstellen. Im Ergebnis trägt SAM nicht nur zu einer richtigen Lizenzierung bei, sondern hilft zugleich kritische Anwendungen zu identifizieren und potenzielle Schwachstellen zu beseitigen.

Solidaris

**3. Europäische Datenschutzgrundverordnung (DSGVO)**

Im Zuge der zunehmenden digitalen Transformation kommt dem Datenschutz eine immer wichtigere Bedeutung zu. Die Europäische Datenschutzgrundverordnung, welche ab dem 25. Mai 2018 unmittelbar geltendes Recht sein wird, bildet einen völlig neuen datenschutzrechtlichen Rahmen mit zum Teil grundlegend neuen datenschutzrechtlichen Instrumenten und verschärften Pflichten und Rechten. Andererseits werfen die Schnittstellen von neuem europäischen Datenschutz zu nationalem Datenschutz insbesondere zum Sozialdatenschutz sowie kirchlichen Datenschutz erhebliche, zum Teil noch nicht geklärte Fragen auf. Erst jetzt wurde mit der Vorlage des Entwurfs für das Allgemeine Bundesdatenschutzgesetz ein erster nationaler Regelungskatalog erkennbar. Gleichwohl ist die Übergangszeit bis zum In-Kraft-Treten der DSGVO für die datenschutzrechtliche Anpassung der komplexen technischen und organisatorischen Prozesse im Krankenhaus zu nutzen.

Die fundierte rechtliche Information über die Grundprinzipien des künftigen europäischen, nationalen, sozial- und kirchenrechtlichen Datenschutzes ist ebenso unerlässlich, wie das Wissen um die Prinzipen „privacy by design“ und „privacy by default“ oder das neue Instrument der Datenschutzfolgeabschätzung in ihren Auswirkungen auf den Betrieb im Krankenhaus.

Weiterführende Informationen und konkrete Hilfestellungen aus und für die Praxis erhalten Sie auf unserer exklusiven Veranstaltung IT-Governance-Tag: Steuerung von IT-Risiken für Krankenhausverantwortliche am **28. November 2016 in Köln,** zu der wir Sie hiermit herzlich einladen.

## Unser Veranstaltungstipp: IT-Governance-Tag

| | |
|---|---|
| **Teilnehmergebühr:** | 200,00 EUR + 19 % MwSt. Diese Schutzgebühr beinhaltet Tagungsunterlagen (als elektronische Datei), Snacks, Getränke sowie ein Mittagessen und wird bei Erhalt der Rechnung fällig. |
| **Termin:** | 28. November 2016, von 10:00 bis 16:00 Uhr |
| **Ort:** | Maternushaus, Kardinal-Frings-Straße 1-3, 50668 Köln, Tel. 0221 . 6310 |
| **Anmeldung:** | unter **www.solidaris.de**, per E-Mail an **j.ruppenthal@solidaris.de**, per Post oder per Fax an 02203 . 8997-199 |
| **Anmeldeschluss:** | 21. November 2016 |

*Anmeldeformular rückseitig*

Solidaris

## Ihre Ansprechpartner

**Oliver Schikora**
Dipl.-Betriebswirt (FH)

Certified Information Systems Auditor (CISA)
IT-Sicherheitsbeauftragter (TÜV)
KompetenzTeam IT-Revision
Solidaris Revisions-GmbH
WPG StBG

02203 . 8997-228
o.schikora@solidaris.de

**Fach- und Branchenerfahrung**

- Langjährige Erfahrung als Prüfungsleiter und IT-Systemprüfer bei gemeinnützigen Organisationen im Bereich des Gesundheits- und Sozialwesens
- Referent bei verschiedenen internen und externen Fortbildungsveranstaltungen
- Umfassende Beratungsleistungen im Bereich der IT-Sicherheit, IT-Revision sowie der Entwicklung zukunftsweisender Strategien im Hinblick auf IT-spezifische Fragestellungen

**Ingo Kreutz**
Dipl.-Wirtschaftsinformatiker

Certified Information Systems Auditor (CISA)
Certified Information Security Manager (CISM)
KompetenzTeam IT-Revision
Solidaris Revisions-GmbH
WPG StBG

02203 . 8997-217
i.kreutz@solidaris.de

**Fach- und Branchenerfahrung**

- Langjährige Erfahrung als verantwortlicher Leiter von IT-Systemprüfungen in Unternehmen unterschiedlicher Branchen, u. a. im Bereich des Gesundheits- und Sozialwesens
- Umfassende Beratungsleistungen im Bereich der Ordnungsmäßigkeit und Sicherheit von IT-Systemen, Risikomanagementsystemen sowie internen Kontrollsystemen
- Projektbegleitende Qualitätssicherung im Rahmen von Softwaremigrationen

*Hier abtrennen – bitte Fensterumschlag benutzen*

*oder faxen an: 02203 . 8997-199*

**An dem IT-Governance-Tag der Solidaris**
Montag, 28. November 2016 im Maternushaus,
Kardinal-Frings-Straße 1-3, 50668 Köln,
**nehme ich teil.**

**Solidaris Revisions-GmbH**
**Frau Jacqueline Ruppenthal**
**Von-der-Wettern-Straße 13**
**51149 Köln**

**Absender**

Organisation

Name, Vorname

Straße / Hausnummer

PLZ / Ort

Telefon

E-Mail