TÜV Media

IT-Risikomanagement für medizinische Einrichtungen

Matthias Knoll – Jörg Schönefeld

TÜVRheinland
Genau. Richtig.

IMPRESSUM

Autoren

Matthias Knoll

Jörg Schönfeld

Bibliografische Informationen der Deutschen Nationalbibliothek

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie.

Detaillierte bibliografische Daten sind im Internet über portal.dnb.de abrufbar.

ISBN 978-3-7406-0816-3

www.tuev-media.de

Arbeitshilfen

Checkliste Cybersicherheit für vernetzte Medizinprodukte

Die Checkliste berücksichtigt alle Rahmenbedingungen für die Cybersicherheit vernetzter Medizinprodukte. Sie können sie frei verwenden und an Ihre Einrichtung anpassen.

CYBERSICHERHEIT_FÜR_VERNETZTE_MEDIZINPRODUKTE.DOCX

Inhalt

Zum Inhalt

Dieser Beitrag richtet sich an alle medizinischen Einrichtungen, die über eine eigene Organisationseinheit für den IT-Betrieb und gegebenenfalls die Entwicklung von eigenen IT-Lösungen verfügen. Die in diesem Beitrag diskutierten Aspekte können jedoch auch für kleinere medizinische Einrichtungen, die ihre IT von einem spezialisierten Dienstleister betreuen lassen, interessant sein. Schließlich können auch niedergelassene Ärzte für ihren täglichen Umgang mit der IT profitieren. Für diese beiden letzten Zielgruppen sind spezielle Hinweise im Text ergänzt, die erläutern, wie einzelne Themen auf die Einrichtungsgröße angepasst betrachtet und umgesetzt werden können.

Dieser Beitrag unterstützt beim Aufbau von Fachwissen, wie mit Risiken im IT-Kontext im Alltag umgegangen werden muss, indem er in das Thema „IT-Risikomanagement" einführt und zeigt, wie sowohl in medizinischen als auch in nicht medizinischen Bereichen auf die Herausforderungen durch Risiken im Kontext der IT mit Blick auf das Patientenwohl ganzheitlich, strukturiert, besonnen und nicht zuletzt mit wirtschaftlichem Augenmaß reagiert werden kann.

1 Warum IT-Risikomanagement?

Sicherheitskultur im Krankenhaus

In der Vergangenheit gab es in vielen medizinischen Einrichtungen keine IT-spezifische Sicherheitskultur und damit auch kein IT-Risikomanagement. Die Sicherheitskultur eines Krankenhauses bedeutete vorrangig, eine fehler- und schadensfreie medizinische Behandlung und Versorgung umzusetzen. Gefördert wurde diese Sichtweise vor allem durch die Grundsätze der Medizinethik, die Umsetzung des Patientenrechtegesetzes und weitere qualitätssichernde Maßnahmen, wie etwa das erprobte Critical Incident Reporting System (CIRS), das medizinische (Beinahe-)Fehler und kritische Ereignisse periodisch zusammenfassend darstellt. Ähnliche Ansätze sind auch aus produzierenden Unternehmen im Kontext der Unfallverhütung bekannt und erprobt.

Schneller Zugriff vs. IT-Sicherheit?

Hintergrund für diese Betrachtung ist der bislang vielfach noch gültige Grundsatz, dass im klinischen Diagnostik- und Behandlungsalltag der schnelle und unkomplizierte Zugriff auf Patientendaten aus ärztlicher und pflegerischer Sicht wichtiger ist als die Sicherheit des Zugangs zu klinischen Daten innerhalb von IT-Anwendungen oder die sichere Nutzung von vernetzten Medizingeräten. In kritischen Situationen ist beispielsweise ein Zeitverlust durch umfangreiche Anmeldeprozesse an IT-Anwendungen nicht hinnehmbar. Gleichzeitig jedoch ist die Sicherstellung der Integrität der hochsensiblen Patienteninformationen und der Funktionalität ebendieser Anwendungen von ebenso zentraler Bedeutung. Denn falsche, lückenhafte oder insgesamt nicht verfügbare Informationen können ebenso wie fehlerhaft arbeitende oder nicht verfügbare Diagnose- oder Therapie-Technik Patienten unmittelbar gefährden.

Niemand ist sicher

Einschlägige aktuelle Beispiele zeigen eindringlich, dass es daher sowohl technischer als auch organisatorischer Maßnahmen zur Verbesserung der Sicherheit von Informationen und IT-Systemen bedarf. Denn es ist – leider – auch in medizinischen Einrichtungen zunehmend keine Frage, ob, sondern nur wann und wie oft sie Opfer von gezielten Angriffen, zufälligen Beeinträchtigungen aufgrund von Angriffen an anderer Stelle oder allgemeinen technischen Störungen sind. Alleine die starke Zunahme von IT lässt solche Szenarien künftig statistisch viel wahrscheinlicher werden.

Lücken finden, Maßnahmen ergreifen

Es müssen also Lösungen geschaffen werden, die einerseits die ärztlichen und pflegerischen Anforderungen, andererseits aber auch die durch verstärkten Einsatz von IT entstehenden neuen Kontexte beherrschen. Das IT-Risikomanagement hilft als Teildisziplin des Risikomanagements unter Beachtung aller weiterhin gültigen nichttechnischen Rahmenbedingungen dabei, in enger Zusammenarbeit mit weiteren Disziplinen aus der IT, insbesondere der IT-Sicherheit, Lücken im Kontext des IT-Einsatzes rechtzeitig zu identifizieren und nachhaltige Maßnahmen zu ergreifen, um die Situation im Kontext der Nutzung von IT zu verbessern.

Was ist wichtig?

Als wesentliche Anforderungen an ein gutes IT-Risikomanagement gelten daher:

- die Einrichtung einer sinnvoll bemessenen IT-Risikomanagement-Organisation,
- seine Angemessenheit (Eignung für die medizinische Einrichtung) und
- seine Wirksamkeit (Funktionsfähigkeit der Elemente des IT-Risikomanagements).

Damit das IT-Risikomanagement angemessen ist, müssen dazu weitere Anforderungen berücksichtigt werden:

- **Integrationsfähigkeit**
  Auch wenn es auf den ersten Blick einfacher und ausreichend erscheinen mag: Eine isolierte Behandlung von technisch geprägten Risiken in der IT wäre aufgrund bereichsübergreifender Ursache-Wirkung-Beziehungen nicht ausreichend. Vielmehr ist eine intensive Kooperation der IT-Risikomanagement-Organisation und der IT insgesamt mit medizinischen und technischen Fachleuten aus allen Bereichen der medizinischen Einrichtung mit IT-Bezug notwendig, um ein gemeinsames Verständnis dafür zu schaffen, wo, wie und mit welchen Folgen ein Risiko im IT-Kontext wirken kann.
- **Anpassungsfähigkeit**
  Genauso wenig wie die medizinische und technische Entwicklung auf einem bestimmten Niveau verharrt, darf auch das IT-Risikomanagement nicht verharren. Es muss fortlaufend an die veränderte Situation beim Einsatz von und im Umgang mit der IT angepasst werden. Genutzte Methoden müssen dazu fortlaufend geprüft und gegebenenfalls angepasst oder ergänzt werden, ebenso die gewählte Software zur Unterstützung.

- **Wirtschaftlichkeit**
  Je umfassender die IT-Durchdringung ist, desto aufwendiger werden Maßnahmen zur Beherrschung der damit verbundenen Risiken ausfallen müssen. Denn IT-Systeme neuester Generation sind so komplex, dass sie eine immer aufwendigere Analyse erfordern. Die Elemente des IT-Risikomanagements müssen daher als eigene Position im IT-Budget eingeplant und mit den etablierten Methoden und Werkzeugen, etwa einer SWOT-Analyse und/oder Nutzwertanalyse, betriebswirtschaftlich beurteilt werden.

Tipp

Tipp für kleine Einrichtungen: IT-Risikomanagement ist dann **angemessen**, wenn:

- *Integrationsfähigkeit:*
  … der jeweilige IT-Dienstleister gemeinsam mit dem medizinischen Personal die relevanten Themen bespricht und darauf achtet, dass ein gemeinsames Verständnis erzielt wird. Dies kann regelmäßig, sinnvollerweise jährlich, etwa im Rahmen eines halbtägigen Workshops geschehen, oder auch immer dann, wenn größere Änderungen an der IT vorgenommen oder neue Geräte installiert werden. Zudem sollte neu eingestelltes Personal umgehend entsprechend sensibilisiert und geschult werden.
- *Anpassungsfähigkeit:*
  … die gewählte Lösung so gestaltet ist, dass sie sich einerseits einfach nutzen lässt, andererseits aber auch leicht auf neue Verhältnisse angepasst werden kann. Einfache Checklisten oder Tabellen genügen dafür vielfach vollkommen. Wichtig ist, dass sie genutzt und fortlaufend aktualisiert werden. Auch hier kann der jeweilige Dienstleister oder eine dritte Partei (unabhängige Sachverständige) unterstützen.
- *Wirtschaftlichkeit*:
  … für das Thema ausdrücklich Mittel für die dedizierte Bezahlung von Fachleuten vorgesehen sind, etwa über Rücklagen. Grundsatz: Kosten in diesem Kontext dürfen nicht „überraschen“. Sie existieren – auch wenn das gerne vermieden würde – und können nicht eingespart werden.

- **Wirksamkeit**
  Die Wirksamkeit ist dann sichergestellt, wenn im Rahmen von regelmäßig wiederholten Tests und Prüfungen (Audits), zunächst durch die Risikomanagement-Organisation selbst sowie unabhängige Dritte, in der Regel spezialisierte Dienstleister, im nächsten Schritt durch die einrichtungseigene Revision oder von ihr beauftragte Dienstleister, festgestellt wird, dass die eingerichteten Mechanismen und gewählten Maßnahmen wie erwartet funktionieren, Risiken also gezielt minimiert oder gar vermieden werden.

Tipp

Tipp für kleine Einrichtungen:

IT-Risikomanagement ist dann wirksam, wenn regelmäßige, unter Umständen auch gegenseitige nicht formalisierte Beobachtungen und Gespräche zeigen, dass das Thema bei allen Beteiligten präsent ist, etwa auch, indem vereinbarte Vorgehensweisen eingehalten werden. Bei technischen Lösungen reicht häufig aus, wenn der beauftragte IT-Dienstleister durch Vorlage anerkannter Zertifikate (mit Gültigkeitsdatum) nachweisen kann, dass die Lösung dem aktuellen Stand der Technik entspricht. Bei Beschaffungen können Testergebnisse aus Fachmagazinen unterstützen, um die Qualität der gewählten Lösung zu dokumentieren.

Auf medizinische Einrichtungen kommen also zahlreiche Herausforderungen zu, die sie erfüllen müssen. Denn der Risikobegriff, der im nachfolgenden Abschnitt näher betrachtet wird, ist durch fortschreitende Nutzung der IT auch in der Medizin („Digitale Transformation“) vielschichtiger und bedeutsamer geworden.

2 Informationssysteme in der Medizin

Ein IT-Risikomanagement ist notwendig und muss bestimmte Anforderungen erfüllen, weil jede medizinische Einrichtung abhängig von ihrer Größe, ihren medizinischen Schwerpunkten und ihren im Gesundheitswesen darüber hinaus zugedachten Aufgaben (etwa Notfallversorgung) mehr oder weniger stark von IT durchdrungen ist. Um den Sachverhalt besser strukturieren und aufzeigen zu können, wie vielschichtig das Themengebiet ist, wird der Begriff des Informationssystems genutzt.

Eine medizinische Einrichtung lebt von und wird durch das medizinische und nicht medizinische Personal getragen. Es bestimmt, wie fachliche Prozesse gestaltet sind, welche Daten relevant sind und kann (mehr oder weniger stark) Einfluss darauf nehmen, in welcher Form es durch IT-Systeme und deren Prozesse (IT-Prozesse) unterstützt wird. Bei der notwendigerweise umfassenden Betrachtung möglicher Risiken sind also alle Bestandteile des IT-Systems einzubeziehen.

Dies betrifft sowohl die Anwendungssysteme in den nicht medizinischen Bereichen, die Medizintechnik selbst als Teil der sogenannten „Operational Technology“ (OT), weitere OT-Elemente (beispielsweise Elemente für die Gebäudeautomation), die Systemsoftware, also beispielsweise Betriebssysteme wie Windows oder Linux, weitere notwendige Hardware sowie das IT-Netzwerk.