Foto: Denys Rudyi – Fotolia

IT-Sicherheitsgesetz – Vom Risiko zur Maßnahme

Identifikation der Top-Risiken und Definition angemessener Maßnahmen

Von Randolf Skerka und Prof. Dr. Andreas Becker

Der Artikel erläutert ein alternatives Modell der IT-Risikoanalyse, welches deutlich von den in der Literatur beschriebenen üblichen Vorgehensweisen abweicht. Sie hat bewusst einen weniger systematischen Ansatz und ist fokussiert lediglich auf das Ziel, die kritischsten IT-Risiken und mögliche Maßnahmen identifizieren zu können. Die Vorgehensweise eignet sich v.a., um einen Einstieg in die Thematik der IT-Risikoanalyse zu finden.

Keywords: *Risikomanagement, IT, Kosten*

Die unter die BSI-KritisV fallenden Krankenhäuser sind gemäß § 8a Absatz 3 BSIG verpflichtet, bis zum 30. Juni 2019 den Nachweis zu erbringen, dass ein angemessenes Maß an IT-Sicherheit erreicht ist. Das wesentliche Ziel des IT-Sicherheitsgesetztes ist es sicherzustellen, dass Betreiber Kritischer Infrastrukturen durch das nachgewiesene Maß an IT-Sicherheit die Versorgungssicherheit ihrer für die Bevölkerung kritischer Dienstleistungen (kDL) gewährleisten können. Für Krankenhäuser ist die stationäre medizinische Versorgung als kritische Dienstleitung relevant. Da es noch keine einheitliche Meinung über das durch ein Krankenhaus zu erreichende Maß an IT-Sicherheit gibt, ist die größte Herausforderung für alle Betreiber Kritischer Infrastrukturen (KRITIS-Betreiber) die Ermittlung eben dieses zu erreichenden Niveaus.

Herkömmliche Risikoanalysen sind wenig sinnvoll

Als zentraler Bestandteil eines Risikomanagementsystems haben sich Risikoanalysen als effektive Vorgehensweise etabliert, um mit einem optimal eingesetzten aber begrenzten Budget ein angemessenes Sicherheitsniveau zu erreichen. Vereinfacht dargestellt ist das Ziel einer Risikoanalyse, Schadensereignisse zu identifizieren, die Wahrscheinlichkeit des Eintritts des Schadens und der Höhe des Schadens abzuschätzen. Das Risiko stellt dann das Produkt aus Eintrittswahrscheinlichkeit und Höhe des Schadens dar (▶ Abb.1).

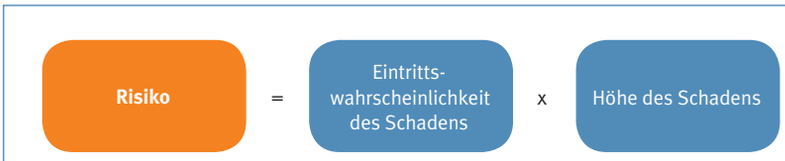

Abb. 1: Risikoanalyse

Im Bereich der Versicherungswirtschaft wird dieses Verfahren genutzt, um anhand statistischer Informationen die zu versichernden ▶

Risiken zu bewerten. Die Versicherungswirtschaft kann in vielen Fällen sowohl bei der Ermittlung der Eintrittswahrscheinlichkeit, wie auch der Schadenshöhe auf statistische Daten und sehr gute Erfahrungswerte zurückgreifen. Ein gutes Beispiel hierfür ist die Bewertung von Brandrisiken, in dessen Berechnung z. B. die Lage und das Baujahr eines Objektes eingeht.

Für IT-Risiken sind derartige statistische Daten nur eingeschränkt verfügbar und wenn sie verfügbar sind, können sie nur sehr eingeschränkt von einem Unternehmen auf ein anderes übertragen werden. In der Konsequenz müssen IT-Risiken in der Regel individuell betrachtet und bewertet werden. Aus diesem Grund sind in der Fachliteratur diverse Methoden zur Durchführung von IT-Risikoanalysen beschrieben, welche jedoch oftmals den Nachteil aufweisen, dass sie auf vermeintliche Vollständigkeit der ermittelten Risiken und größtmögliche Genauigkeit hinsichtlich der Bewertung der Risiken abzielen. Hiermit wird oft der Eindruck einer mathematischen Genauigkeit der ermittelten Ergebnisse vermittelt, welcher aber nicht möglich ist, da es wahrscheinlich ist, dass

- relevante Schadensereignisse unbeachtet bleiben,
- irrelevante Schadensereignisse berücksichtigt werden,
- die Eintrittswahrscheinlichkeiten falsch abgeschätzt werden oder
- die resultierende Schadenshöhen falsch abgeschätzt werden.

Zudem erfordert die Durchführung von IT-Risikoanalysen, wenn präzise Ergebnisse erzielt werden sollen, einen großen Erfahrungsschatz sowie tiefe Kompetenz im Bereich der IT-Sicherheit. Darüber hinaus fließen in die Abschätzung der Eintrittswahrscheinlichkeit und der Schadenshöhe erfahrungsgemäß oft subjektive Empfindungen mit ein. Im Ergebnis besteht die Gefahr, dass die Ergebnisse von IT-Risikoanalysen nicht der tatsächlichen Risikolage entsprechen, Budgets falsch eingesetzt und nicht die optimalen Ergebnisse erzielt werden.

Die Besonderheit von IT-Risikoanalysen

Unter der Annahme, dass eine IT-Risikoanalyse fehleranfällig ist und nur in selten Fällen genaue und optimale Ergebnisse liefert, kann eine initiale IT-Risikoanalyse mit einem anderen Anspruch durchgeführt werden. Einerseits sollte der Anspruch bestehen, dass die Ergebnisse der IT-Risikoanalyse im Rahmen eines Risikomanagementsystems regelmäßig aktualisiert und zunehmend „passender“ für das Unternehmen werden. Andererseits sollten erstmalig durchgeführte IT-Risikoanalysen lediglich mit dem Anspruch durchgeführt werden, Antworten auf die folgenden Fragen zu geben:

- Welche Schadensereignisse sind für unser Unternehmen die kritischsten?
  – Durch welche Schadensereignisse werden 80 % der Schäden verursacht?
- Mit welchen Maßnahmen lässt sich die größte Wirkung erzielen?
  – Durch welche Maßnahmen werden 80 % der Risiken reduziert?
- Wie lässt sich das verfügbare Budget derart einsetzen, dass das Risiko möglichst weit reduziert wird?

Ziel ist es, die kritischsten Risiken zu identifizieren und das verfügbare Budget dahingehend einzusetzen, dass das Risikopotenzial möglichst weit reduziert wird.

Im Kontext der BSI-KritisV wird es im ersten Schritt für ein Krankenhaus von besonderer Bedeutung sein zu ermitteln, welche (Schadens-)Ereignisse dazu führen können, dass kurz-, mittel- oder langfristig die stationäre Patientenversorgung nicht aufrechterhalten werden kann. Im Rahmen des Risikomanagements können die initial erarbeiteten Ergebnisse zukünftig verbessert, weitere Risiken betrachtet und neue Maßnahmen definiert werden. Um dieses Ziel zu erreichen, kann ein pragmatischer Ansatz einer IT-Risikoanalyse durchgeführt werden, welcher aus den folgenden Schritten besteht. Die erarbeiteten Ergebnisse müssen angemessen dokumentiert werden, so dass die Ergebnisse zu einem späteren Zeitpunkt genutzt und die Bewertungen nachvollzogen werden kann.

Schritt 1 – Relevante Bereiche ermitteln

Im ersten Schritt werden diejenigen Bereiche identifiziert, die für die Erbringung der kritischen Dienstleistung erforderlich sind. Im Falle eines Krankenhauses und der stationären Patientenversorgung können dies u.a. die zentrale Notaufnahme, das Labor, die Intensivstation, die Radiologie, der Operationssaal und die Normalstationen sein.

Schritt 2 – IT-Durchdringung ermitteln

Im zweiten Schritt wird ermittelt, wie stark die Prozesse in den identifizierten Bereichen durch IT-Prozesse unterstützt werden. Hierzu ist es erforderlich zu erheben, welche IT-Komponenten (z. B. KIS, RIS, LIS, PACS, Medizin-IT) innerhalb der einzelnen Bereiche genutzt werden. Sofern im Vorfeld eine IT-Strukturanalyse erstellt wurde, können diese Ergebnisse eine wertvolle Grundlage für diesen Schritt sein. In der Praxis bedeutet dies, dass Gespräche mit den jeweiligen Leitungsfunktionen der identifizierten Bereiche durchgeführt werden, um zu ermitteln, wie stark die medizinischen Prozesse von der eingesetzten IT unterstützt werden.

Schritt 3 – Schadensereignisse bewerten und Gegenmaßnahmen erarbeiten

Der dritte Schritt des Prozesses stellt den Kern der IT-Risikoanalyse und auch der Risikobehandlung dar. Es müssen relevante Schadensereignisse identifiziert und deren Auswirkung auf die medizinischen Prozesse – insbesondere die stationäre Patientenversorgung – bewertet werden. Aus den oben genannten Gründen ist dies erfahrungsgemäß derjenige Schritt, in dem das größte Fehlerpotenzial vorhanden ist. Auch der dritte Schritt wird im Rahmen von Gesprächen mit den jeweiligen Leitungsfunktionen der identifizierten Bereiche durchgeführt.

Im pragmatischen Ansatz sollten, ausgehend von konkreten Scha-

densszenarien, die folgenden Fragen beantwortet werden:

- Welche Schutzmaßnahmen sind, bezogen auf das betrachtete Schadensereignis, bereits umgesetzt?
- Wie wahrscheinlich ist es, dass das jeweilige Schadensereignis eintrifft?
- Welche Auswirkung hat das Eintreten des betrachteten Schadensereignisses auf den medizinischen Prozess – insbesondere auf die stationäre Patientenversorgung?
- Wenn die Auswirkungen nicht tragbar sind, welche Maßnahmen können ergriffen werden, um die Auswirkungen zu reduzieren?

Die Herausforderung ist, relevante Schadensereignisse zu identifizieren und zu bewerten. Ausgangspunkt für die zu betrachtenden Schadensereignisse können z.B. der Gefährdungskatalog „Elementare Gefährdungen“ sowie die Bedrohungskategorien aus der „Orientierungshilfe zu Inhalten und Anforderungen an branchenspezifische Sicherheitsstandards (B3S) gemäß § 8a (2) BSIG“ des Bundesamt für Sicherheit in der Informationstechnik (BSI) sein.

Werden die oben genannten vier Fragen systematisch für alle Schadensszenarien bewertet, lässt sich ein guter Überblick über die relevanten Risiken und mögliche Gegenmaßnahmen verschaffen.

Schritt 4 – Maßnahmenplan erarbeiten

Im Ergebnis des dritten Schrittes wurden Maßnahmen identifiziert, die erforderlich sind, um die Auswirkungen der betrachteten Schadensszenarien zu reduzieren. Im letzten Schritt ist die Planung der Maßnahmenumsetzung erforderlich. Hierzu ist insbesondere die Priorisierung der Maßnahmen vorzunehmen. Zum einen sollten die identifizierten, nicht tragbaren Schadensszenarien mit entsprechenden Maßnahmen hinterlegt werden, zum anderen ist die Berücksichtigung des verfügbaren Budgets bei der Planung der Maßnahmenumsetzung notwendig. Aus dem Maßnahmenplan muss hervorgehen, wann welche Maßnahmen umgesetzt werden und welche Maßnahmen nicht umgesetzt werden. Der bewusste Verzicht auf eine Maßnahme kann für solche Fälle sinnvoll sein, bei denen der zu erwartende Schaden geringer ist als die Kosten für die Maßnahme.

Die beschriebene Vorgehensweise weicht deutlich von den in der Literatur, z.B. ISO27005, ISO 31000 oder BSI Standard 100-3, beschriebenen Vorgehensweisen zur Durchführung von IT-Risikoanalysen ab. Sie ist bewusst weniger systematisch und fokussiert lediglich auf das Ziel, die kritischsten IT-Risiken und mögliche Maßnahmen identifizieren zu können. Die Vorgehensweise ist geeignet, einen Einstieg in die Thematik der IT-Risikoanalyse zu finden. Sie soll die in der Literatur beschriebene Vorgehensweise nicht ersetzen, sondern es den Krankenhäusern ermöglichen, perspektivisch ein den Regeln der Technik entsprechendes IT-Risikomanagement aufzubauen. Üblicherweise sind in den Krankenhäusern ohnehin bereits Risikomanagementsysteme vorhanden, so dass es langfristig sinnvoll ist, das IT-Risikomanagement in die vorhandenen Managementsysteme zu integrieren. ■

Randolf Skerka
SRC Security Research & Consulting GmbH
Emil-Nolde-Str. 7
D-53113 Bonn

Randolf Skerka

Prof. Dr. Andreas Becker
Institut Prof. Dr. Becker
Rösrath

FACHWISSEN
KU FACHBÜCHER

Mediengruppe Oberfranken –
Fachverlage GmbH & Co. KG
Tel. 09221/949-311
ku-gesundheitsmanagement.de

KU GESUNDHEITSMANAGEMENT