Foto: Jenny Sturm – Fotolia

IT-Sicherheitsgesetz: Kontaktstelle mitteilen

Auf Sicherheitsmeldungen des BSI reagieren und Sicherheitsvorfälle melden

Von Randolf Skerka und Prof. Dr. Andreas Becker

Mit der am 30. Juni 2017 erfolgten Veröffentlichung der ersten Verordnung zur Änderung der BSI-Kritisverordnung (KritisV) sind nun die unter die Verordnung fallenden Krankenhäuser, verpflichtet Sicherheitsmaßnahmen nach dem Stand der Technik umzusetzen und Sicherheitsvorfälle an das BSI zu melden. Kurzfristig muss dem BSI bis zum 30. Dezember 2017 eine Kontaktstelle benannt werden, über die das Krankenhaus jederzeit, das heißt 24 Stunden am Tag, sieben Tage die Woche, erreichbar ist. An diese Adresse wird das BSI IT-Sicherheitsinformationen versenden.

Kontaktstelle einrichten

Das geänderte BSI-Gesetz (§ 8b) verpflichtet die unter die BSI-Kritisverordnung fallenden Krankenhäuser sowohl dem BSI erhebliche IT-Störungen in anonymisierter Form zu melden, als auch dafür Sorge zu tragen, dass das BSI ständig (24 Stunden am Tag an sieben Tagen in der Woche) in der Lage ist, dem Krankenhaus IT-Sicherheitsinformationen über eine zu benennende Kontaktstelle mitzuteilen. Aus Sicht des BSI ist die Einrichtung eines Funktionspostfaches, das nicht einem einzelnen, sondern einer Gruppe von Mitarbeitern zugeordnet ist, geeignet, die erforderliche Erreichbarkeit zu gewährleisten. Auch ist es möglich, dass sich mehrere Krankenhäuser zusammenschließen und eine gemeinsame übergeordnete Ansprechstelle (GÜAS) definieren.

Denkbar ist dies zum Beispiel für Klinik-Gruppen oder Klinikverbünde, die bereits an anderen Stellen interne Prozesse zusammengeführt oder den Betrieb der IT zusammengelegt haben. Flächendeckend werden sich GÜAS aber wahrscheinlich erst in den kommenden Jahren etablieren.

Aus den eingegangenen Meldungen beabsichtigt das BSI für jeden KRITIS-Sektor ein Lagebild abzuleiten, das die Grundlage etwa für Warn- und Alarmierungsmeldun- ▶

Das Thema IT-Sicherheit gewinnt im Gesundheitswesen zunehmend an Bedeutung. Die Digitalisierung von Prozessen und die Vernetzung von Programmen erhöht zwar die Effektivität, macht Krankenhäuser jedoch auch angreifbar. Der Gesetzgeber folgte dem Ruf nach mehr Sicherheit mit dem im Juli 2015 in Kraft getretene IT-Sicherheitsgesetz. Doch wie wirken sich die Gesetzesvorschriften konkret aus? Diese Fragen beantworten Randolf-Heiko Skerka, Experte für Informationssicherheits-Managementsysteme, und Prof. Dr. Andreas Becker, Berater für Einrichtungen im Gesundheitswesen.

Keywords: *IT-Sicherheit, Geltungsbereich, Strukturanalyse, BSIG*

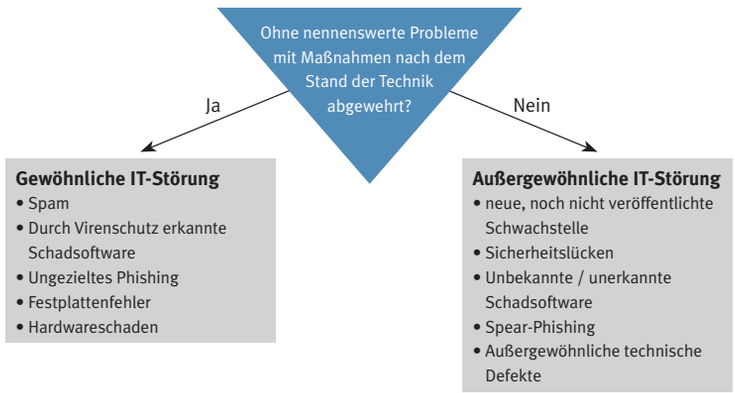

Abb. 1: Meldeprozess „IT-Störungen“

gen sowie konkrete Handlungsempfehlungen zur Vermeidung von Schäden ist. Ziel ist es, die Betreiber kritischer Infrastrukturen frühzeitig auf erwartete Angriffe oder Ausfälle vorzubereiten beziehungsweise Abwehrmaßnahmen zu ergreifen. In den letzten Monaten wurden über diesen Kanal beispielsweise bereits Meldungen zu WannaCry an die registrierten Kontaktstellen verteilt.

Es darf erwartet werden, dass das BSI an die Kontaktstelle in Krankenhäusern insbesondere sehr spezifische Meldungen, vergleichbar zur Meldung über die seit zwei Jahren bestehende Schwachstelle, die in Tomografen festgestellt wurden (ICSMA-17-215-02), verteilt. Die Meldepflicht der Krankenhäuser besteht bei Störungen, die bereits zu einem Ausfall oder einer Beeinträchtigung geführt haben oder hierzu führen können.

Um die Meldungen geordnet vom BSI entgegen zu nehmen oder an dieses abzugeben, ist die Einrichtung geeigneter Meldeprozesse erforderlich. In der Regel sind bereits entsprechende Alarm- und Kommunikationspläne innerhalb eines Krankenhauses vorhanden, so dass diese genutzt und angepasst werden können, um die Anforderungen des BSI-Gesetzes zu erfüllen.

Vorhandene Kommunikationsstruktur anpassen

Die Registrierung beim BSI setzt einige Vorarbeiten voraus, die innerhalb des Krankenhauses zu erledigen sind, um eine erfolgreiche Registrierung durchführen zu können.

Schritt 1: Festlegung des Ansprechpartners der Organisation
Im Rahmen des Registrierungsprozesses muss die Organisation gegenüber dem BSI einen Ansprechpartner benennen. Gemäß Registrierungsformular ist die „Aufgabe des Ansprechpartners der Organisation […], dem BSI gegenüber Änderungen bzgl. der Kontaktstelle mitzuteilen. Das BSI kontaktiert den Ansprechpartner bei allen organisatorischen Fragestellungen, zum Beispiel zur Überprüfung und/oder Ergänzung der Kontaktdaten“. Die Benennung des Ansprechpartners ist jedoch optional, wird kein Ansprechpartner benannt, wird das BSI die Kontaktstellen in den genannten Fällen kontaktieren.

Schritt 2: Einrichtung und Etablierung einer Kontaktstelle gemäß § 8b Abs. 3 BSIG
Damit das BSI dem KRITIS-Betreiber IT-Sicherheitsinformationen zukommen lassen kann, ist die Erreichbarkeit der Kontaktstelle an 24 Stunden sieben Tage die Woche zu gewährleisten. Da das BSI an die Qualität der eigenen Meldungen in Richtung der KRITIS-Betreiber, wie auch die aus Richtung der KRITIS-Betreiber kommenden Meldungen, gewisse Anforderungen stellt und die Erreichbarkeit der Kontaktstelle sichergestellt werden muss, sind in der Regel geeignete Meldeprozesse aufzubauen und zu etablieren.

Schritt 3: Registrierung auf dem Melde- und Informationsportal für Betreiber Kritischer Infrastrukturen im Rahmen des IT-Sicherheitsgesetzes
Um der Meldepflicht nachzukommen, muss die Organisation eine

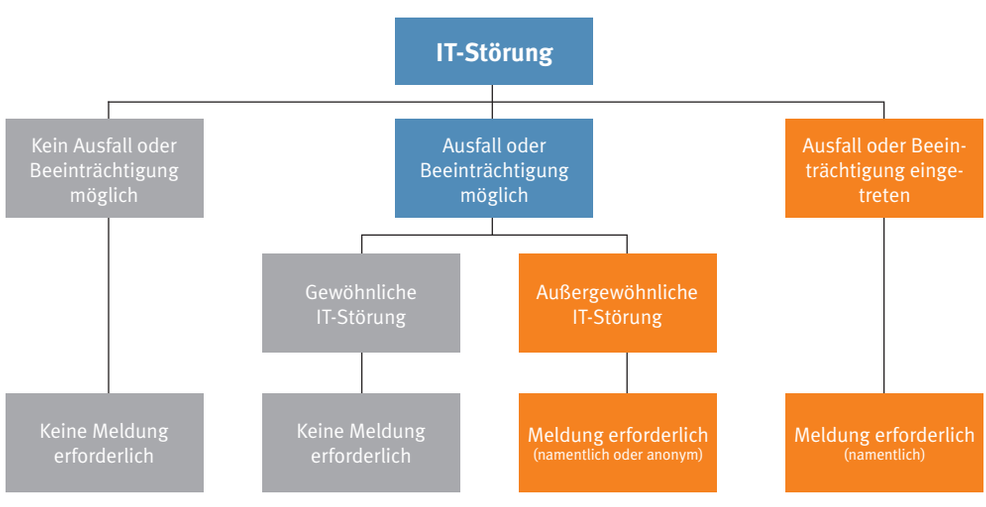

Abb. 2: Gewöhnliche und außergewöhnliche IT-Störungen

Registrierung auf dem „Melde- und Informationsportal für Betreiber Kritischer Infrastrukturen im Rahmen des IT-Sicherheitsgesetzes“ vornehmen. Anschließend werden die zur Meldepflicht erforderlichen Informationen (Meldeformular, Anleitung zur Durchführung einer Meldung) bereitgestellt. Die Homepage des BSI lautet: https://mip.bsi.bund.de/register

Meldungen an das BSI

Dem BSI sind nur relevante Vorfälle mitzuteilen. Zunächst sind nur Meldungen relevant, die die betroffene kritische Dienstleistung nach KritisV, wie etwa die „stationäre medizinische Versorgung“, betreffen. Ereignisse, die somit keine Auswirkungen auf die kritische Dienstleistung haben, müssen dem BSI nicht gemeldet werden.

Es lassen sich drei Fälle unterscheiden, die in der nachfolgenden Abbildung dargestellt sind (▶Abb. 1):

1. Ein Ausfall oder eine Beeinträchtigung der kritischen Dienstleistung ist nicht möglich.
   Eine Meldung ist nicht erforderlich.

2. Ein Ausfall oder eine Beeinträchtigung der kritischen Dienstleistung ist möglich (auch wenn keine Störung eingetreten ist).
   Eine Meldung ist nur in dem Fall erforderlich, wenn es sich um eine außergewöhnliche IT-Störung handelt. Aufgetretene Schadsoftware, die durch die vorhandenen Maßnahmen erfolgreich abgewehrt wurde, ist damit nicht meldewürdig.

3. Ein Ausfall oder eine Beeinträchtigung der kritischen Dienstleistung ist eingetreten.
   Eine namentliche Meldung ist nun zwingend erforderlich.

In der Praxis wird die interessante Frage sein, was als „außergewöhnliche Störung“ zu verstehen ist. Das BSI definiert zunächst die gewöhnliche IT-Störung als solche, die durch übliche Maßnahmen nach dem Stand der Technik abgewehrt werden können. Hierzu dürfen zum Beispiel die erfolgreiche Abwehr von Schadsoftware durch entsprechende Anti-Viren Mechanismen zählen (▶Abb. 2).

Aus Sicht des BSI können IT-Störungen als außergewöhnlich bezeichnet werden, wenn sie „nur mit erheblichem bzw. deutlich erhöhtem Ressourcenaufwand (zum Beispiel erhöhtem Koordinierungsaufwand, Hinzuziehen zusätzlicher Experten, Nutzung einer besonderen Aufbauorganisation, Einberufung eines Krisenstabs) bewältigt werden können“.

Die Benennung der Kontaktstelle stellt den ersten Schritt zur Umsetzung der Anforderungen des IT-Sicherheitsgesetzes dar. Das BSI gibt viele Hilfestellungen, so dass sich ein Besuch der Webseite zu diesem Thema lohnen und Klarheit bringen dürfte. Da üblicherweise bereits etablierte Kommunikationsstrukturen für Not- und Katastrophenfälle im Krankenhaus vorhanden sind, besteht die Herausforderung darin, diese auf den neuen „externen Kommunikationspartner“ hin anzupassen und stärker auf IT-Themen auszurichten. ■

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

Randolf Skerka

Prof. Dr. Andreas Becker
Qualifikation
“Spezielle Prüfverfahrens-Kompetenz
für § 8a BSIG“
Institut Prof. Dr. Becker