Foto: Gina Sanders – Fotolia

Informationen für mehr Sicherheit

Meldung von IT-Störungen an das BSI

Von Randolf Skerka und Prof. Dr. Andreas Becker

Krankenhäuser, die unter die BSI-KritisV fallen, sind ab dem 1. Januar 2018 verpflichtet, dem Bundesamt für Sicherheit in der Informationstechnik (BSI). „Außergewöhnliche IT-Störung“ oder IT-Störungen, die einen „Ausfall oder Beeinträchtigung“ zur Folge haben zu melden. Aus Sicht des BSI können IT-Störungen als außergewöhnlich bezeichnet werden, wenn sie „nur mit erheblichem beziehungsweise deutlich erhöhtem Ressourcenaufwand bewältigt werden können“. Das BSI nutzt das BSI die mitgeilten Informationen dazu, die IT-Störung zu analysieren, sie durch weitere Erkenntnisse zu ergänzen und gegebenenfalls Vorschläge für Gegenmaßnahmen zu entwickeln.

Keywords: *IT-Sicherheitsgesetz, IT-Störungen, Meldepflicht, BSI*

Ab dem 1. Januar 2018 sind Krankenhäuser, die unter die BSI-KritisV fallen verpflichtet, dem Bundesamt für Sicherheit in der Informationstechnik (BSI) „Außergewöhnliche IT-Störung“ oder IT-Störungen, die einen „Ausfall oder Beeinträchtigung“ zur Folge haben, über eine bis zum 29. Dezember 2017 einzurichtende und dem BSI zu benennende Kontaktstelle zu melden (▶Abb. 1).

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

Schnelligkeit vor Vollständigkeit

Die Meldung an das BSI erfolgt hierbei über ein „Meldeformular nach § 8b Absatz 4 BSIG (▶Abb. 2, Seite 70). Um sicherzustellen, dass das BSI möglichst frühzeitig über IT-Störungen, von denen potenziell auch andere Krankenhäuser, die betroffen sein können, zu informieren, erfolgt die Erstmeldung nach dem Motto: Schnelligkeit vor Vollständigkeit. Hierdurch ist das BSI in der Lage frühzeitig Warnungen an andere Krankenhäuser herauszugeben, wenn zu erwarten ist, dass es sich bei der IT-Störung um einen gezielten Angriff auf Krankenhäuser handelt. Des Weiteren gilt, dass die Meldung unverzüglich nach Erkennung der IT-Störung erfolgen muss, also ohne schuldhaftes Zögern. Die Meldepflicht nach § 8b Absatz 4 BSIG zur IT-Störung endet mit dem beim BSI

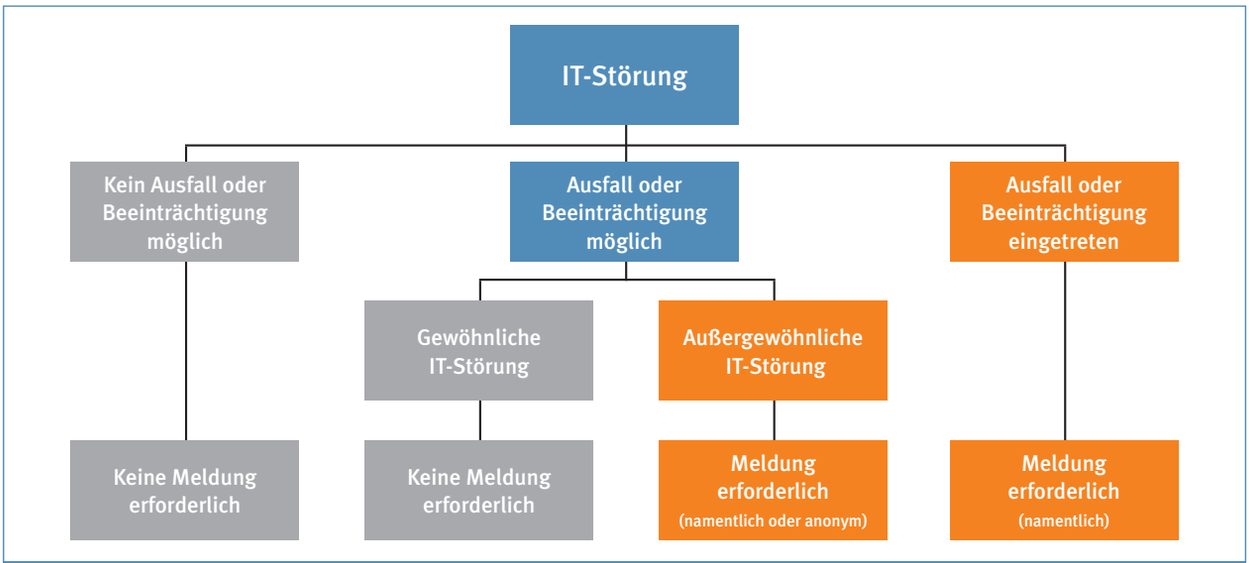

Abb. 1: Meldeprozess „IT-Störungen“

eingereichten Abschlussbericht, sofern sich das BSI nicht innerhalb von fünf Arbeitstagen beim Krankenhaus meldet (z. B. zur Klärung eventueller Rückfragen zur IT-Störung). Im Rahmen der Meldung müssen im Meldeformular eine Vielzahl von Angaben zur IT-Störung gemacht werden, welche das BSI in die Lage versetzen soll, die Situation zu bewerten und gegebenenfalls, mit dem KRITIS-Betreiber Kontakt aufzunehmen. Aus diesem Grund ist es verständlich, dass das BSI die Meldung unter dem Motto „Schnelligkeit vor Vollständigkeit“ versteht. Das Meldeformular ist so aufgebaut, sodass es im Rahmen der Behandlung der IT-Störung fortgeschrieben werden kann. Zu Beginn des Formulars werden damit Informationen erfasst, die allgemeiner Natur sind beziehungsweise generelle Informationen zur Störung erfassen.

Welche Informationen benötigt das BSI?

Der erste Teil des Meldeformulars beinhaltet „Allgemeine Informationen zum Meldenden“, welche unter anderem den Namen der Kontaktstelle (oder der GÜAS), die betroffene Anlage und Kontaktdaten eines technischen Ansprechpartners enthalten. Diese Informationen sollten natürlich bereits in der Erstmeldung enthalten sein, damit das BSI in der Lage ist den Meldenden zu identifizieren und gegebenenfalls Rückfragen zu stellen.

Im restlichen Meldeformular müssen Details zur Störung, den Ursachen, ergriffene Maßnahmen etc. angegeben werden. Zu den „Allgemeinen Informationen zum Vorfall“ zählen Informationen wie die Meldungsart (z.B. Erst- oder Folgemeldung), der (vermutete) Zeitpunkt des Vorfalls, die betroffene kritische Dienstleistung (kDL) und der betroffene Anlagentyp. Zudem sind „Details zur IT-Störung“ anzugeben, also welche Systeme von der Störung betroffen sind, eine Beschreibung des Vorfalls, Ursachen, Konsequenzen und Symptome sowie die Information, ob die IT-Störung noch anhält.

Folgemeldungen möglich

Im Laufe der Behandlung der Störung ist zu erwarten, dass weitere Details bekannt werden. Diese sind dann im Meldeformular anzugeben. An dieser Stelle wird deutlich, dass auch dem BSI bewusst ist, dass zu Beginn einer Störung nicht alle Details vorliegen, son- ▶

dern sich die Informationslage erst im Laufe der Behandlung des Vorfalls entwickelt. Demzufolge können dem BSI neue Informationen als „Folgemeldung“ mitgeteilt werden.

Zu solchen Informationen gehören z. B. die „Details zu den vermuteten Ursachen“, welche in den Kategorien „Physikalischer Schaden“, „Technisches Versagen“, „Organisatorische Ursache“, „Versagen der genutzten Infrastruktur“ und „Technischer Angriff“, sowie „Sonstiges“ unterteilt ist. Im Falle eines vermuteten „Technischen Angriffs“ können weitere Informationen angegeben werden, zum Beispiel hinsichtlich der Frage, ob es sich um einen Denial-of-Service Angriff, einen Missbrauch durch einen Innentäter oder einen gezielten Angriff handelt.

Sofern Anzeichen dafür vorhanden sind, dass es sich um einen „informationstechnischen Angriff“ handelt, sind zum Beispiel die Angriffsart (gezielt / ungerichtet), die vermutete Motivation und die Frage, ob die Ermittlungsbehörden bereits einbezogen wurden, anzugeben.

Auswirkungen der Störung sind anzugeben

Wahrscheinlich bereits in einer früheren Phase der Störung kann das Krankenhaus abschätzen, welche Auswirkung die IT-Störung auf die kritische Dienstleitung hat, beispielsweise ob es überhaupt zu einer Beeinträchtigung der Funktionsfähigkeit kommt, ob die Möglichkeit besteht, dass die Kritische Infrastruktur beeinträchtigt ist, wie viele Personen (Bevölkerung) betroffen sein können, welche geographische Verbreitung die Auswirkung hat etc. Solche Informationen sind ebenfalls im Meldeformular anzugeben.

Angabe der Gegenmaßnahmen

Abschließend ist dem BSI mitzuteilen, welche Maßnahmen ergriffen wurden, um die Beeinträchtigung zu mindern oder zu beheben. Es ist daher erforderlich die Störung ausgiebig zu dokumentieren, um folgende Fragen beantworten zu können:

- Wer hat wann, welche Maßnahme ergriffen und warum?
- Wer hat wann, von welchem Sachstand erfahren?
- Wer hat wann, welche Information an wen weitergeleitet?
- Wer hat wann, welche Information von wem erhalten?

In komplexen Störungssituationen ist es daher unabdingbar, dass sich eine Person ausschließlich mit der Dokumentation beschäftigt.

Freiwillige Angaben

Darüber hinaus können außerdem weitere freiwillige Angaben zur Störung im Meldeformular gemacht werden, die in den vorangegangenen Abschnitten keinen Platz gefunden haben. Das sind beispielsweise weiterführende Informationen, weiterführende Bewertungen und Sonstiges.

Wofür benötigt das BSI die Informationen?

Von großem Interesse von Seiten der Krankenhäuser ist natürlich die Frage, wofür genau das BSI die Informationen aus dem Meldeformular benötig und verwertet sowie die Frage danach, auf welche Weise das BSI die Informationen der Krankenhäuser, die aus den Störungsmeldungen hervorgehen, behandelt.

Die Informationen aus den ersten beiden Abschnitten, also die Allgemeinen Informationen zum Meldenden sowie Allgemeine Informationen zum Vorfall nutzt das BSI hauptsächlich für die Kontaktaufnahme zum meldenden Betreiber, der Betroffenheitskorrelation und der statistischen Nachbereitung.

Die weiteren vier Abschnitte, in denen genauere Details zu dem IT-Sicherheitsvorfall mitgeteilt werden, verwendet das BSI für die:

- Kritikalitätsbewertung aus IT-Sicherheitssicht,
- Erstellung eines bundesweiten IT-Lagebilds,
- Warn- oder Informationsmeldungen an potentiell weitere betroffene Betreiber des Sektors,

Bundesamt für Sicherheit in der Informationstechnik

Nationales IT-Lagezentrum BSI

MUSTER

Meldeformular

nach § 8b Absatz 4 BSIG

0. Allgemeine Informationen zum Meldenden

0.1	Name des meldenden Unternehmens bzw. der meldenden GÜAS	Trinkwasser-Mustergewinnungswerk
0.2	Betroffene Anlage (Kritische Infrastruktur gemäß BSI-KritisV) (Name und Ort)	Trinkwasser-Mustergewinnungswerk, Musterstadt
0.3	Name des Ansprechpartners für technischen Rückfragen	Frau Erika Mustermann
0.4	Kontaktdaten des Ansprechpartners (E-Mail, Telefonnummer)	e.mustermann@twgw.muster, Tel.: 0000 – 99 99-9099

Abb. 2: Meldeformular des BSI

- statistische Nachbereitung und
- Analyse der potenziellen Auswirkungen auf die Verfügbarkeit Kritischer Infrastrukturen.

Zusammenfassend nutzt das BSI die mitgeilten Informationen dazu, die IT-Störung zu analysieren, sie durch weitere Erkenntnisse zu ergänzen und gegebenenfalls Vorschläge für Gegenmaßnahmen zu entwickeln. Des Weiteren fließen die gewonnenen Erkenntnisse in die Erstellung eines Gesamtlagebildes ein und bei Relevanz für weitere Krankenhäuser, z.B. wenn es sich um einen gezielten Angriff auf Krankenhäuser handeln könnte, erstellt das BSI eine Warn- oder Informationsmeldung. Das bedeutet auch, dass verschiedene Krankenhäuser voneinander profitieren können, indem durch eine schnelle Meldung einer betroffenen Einrichtung andere Einrichtungen aus dem Sektor Gesundheit vor einer übergreifenden IT-Störung gewarnt und geschützt werden können. Die datenschutzrechtliche Behandlung der Störungsmeldung durch das BSI ist selbstverständlich vertraulich. Das ergibt sich bereits aus § 8e BSIG, der die Weitergabe von Informationen an Dritte deutlich einschränkt. Ein Zugang zu personenbezogenen Daten wird nicht gewährt. Eine Auskunft durch das BSI darf nur in dem Fall erteilt werden, wenn schutzwürdige Interessen des Betreibers dem nicht entgegenstehen und durch die Auskunft keine Beeinträchtigung wesentlicher Sicherheitsinteressen zu erwarten ist. Die Erstellung einer Warn- oder Informationsmeldung erfolgt anonymisiert, der Name des meldenden Krankenhauses wird nicht genannt.

Fazit

Die Meldung von IT-Störungen an das BSI stellt den zweiten Schritt zur Umsetzung der Anforderungen des IT-Sicherheitsgesetzes dar. Das BSI gibt den Krankenhäusern in Form des vorgefertigten Meldeformulars bereits eine erhebliche Hilfestellung mit auf den Weg, ferner können auf der Webseite des BSI weitere Hilfestellungen zum Ausfüllen des Formulars gefunden werden. Eine gewissenhafte Durchführung der Meldung trägt nicht nur zur Schutz der eigenen kritischen Infrastrukturen bei, sie hilft dem BSI durch stetige Informationsgewinnung auch dabei ein Gesamtlagebild, sowie Warn- oder Informationsmeldungen an weitere Krankenhäuser zu erstellen und zu versenden. ■

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

Randolf Skerka

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