VERBAND DER UNIVERSITÄTSKLINIKA DEUTSCHLANDS

Handlungsempfehlung

IT-Sicherheit

Allgemeine Grundsätze und Empfehlungen zum Meldewesen nach dem BSI-Gesetz

30. November 2017

Inhaltverzeichnis

Anlage 01:
Beispiele für IT-Sicherheitsvorfälle in der Branche „Medizinische Versorgung“

1 Vorbemerkung

Dieses Dokument wurde von der vom VUD-IT-Ausschuss eingesetzten „AG Informationssicherheit“ erstellt. Es dient den Universitätsklinika als eine unverbindliche Handlungsempfehlung zur Einrichtung und zum Betrieb der nach dem BSI-Gesetz (BSIG) vorgeschriebenen Meldestellen. Die hier wiedergegebenen Hinweise wurden teilweise dem Informationsangebot des Bundesamtes für Sicherheit in der Informationstechnik (BSI) entnommen und durch die AG um die besonderen Informationsbedürfnisse der Universitätsklinika ergänzt. Wir möchten Sie bitten, sich für aktuelle Informationen und Auslegungen des Verordnungstextes immer auch auf den Internetseiten des BSI zu informieren.

2 Ausgangspunkt und Zielsetzung

Die zunehmende digitale Durchdringung unseres gesamten Lebensraumes bei gleichzeitig immer professioneller ausgeführten Cyber-Angriffen erfordert den Schutz wichtiger Infrastruktureinrichtungen. Vor diesem Hintergrund trat am 25.06.2015 das Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz – ITSiG) als eines der ersten konkreten Umsetzungsergebnisse der Digitalen Agenda der Bundesregierung in Kraft. Das ITSiG als Artikelgesetz ändert und ergänzt diverse Fachgesetze, wie zum Beispiel das BSIG, hinsichtlich der IT-Sicherheitsanforderungen an Betreiber Kritischer Infrastrukturen.

> **Kritische Infrastrukturen** sind Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden.
>
> *Bundesministerium des Innern: Nationale Strategie zum Schutz Kritischer Infrastrukturen (KRITIS-Strategie)*

Nach dem BSI-Gesetz müssen Krankenhäuser als Teile des Sektors „Gesundheit“ die Versorgung der Bevölkerung mit Gesundheitsdienstleistungen auch in Krisensituationen gewährleisten.
Ende Juni 2017 ist die BSI Kritisverordnung (BSI-KritisV) Korb 2 in Kraft getreten, welche die Anlagenkategorien und Schwellenwerte für Einrichtungen der Kritischen Infrastruktur definiert. Nach der Verordnung sind Krankenhäuser mit mehr als 30.000 stationären Fällen pro Jahr (Schwellenwert) als kritische Infrastruktur im Sinne des BSI-Gesetzes definiert. Als Anlagekategorie wird dabei das komplette Krankenhaus betrachtet. Nach dieser Definition sind in Deutschland alle Uniklinika als kritische Infrastruktur einzustufen.

> **Krankenhaus** ist ein Standort oder Betriebsstätte eines nach § 108 des fünften Buches Sozialgesetzbuch in der jeweils geltenden Fassung zugelassenen Krankenhauses, der oder die für die Erbringung stationärer Versorgungsleistungen notwendig sind.
>
> *BSI-KritisV Korb 2, Anhang 5 (zu § 1 Nummer 4 und 5, § 6 Absatz 6 Nummer 1 und 2) Anlagenkategorien und Schwellenwerte im Sektor Gesundheit)*

Alle Krankenhäuser, welche diesen Schwellenwert erreichen oder überschreiten, müssen innerhalb von 6 Monaten (bis Ende 2017) einen Meldeprozess für IT-Störungen (IT-Sicherheitsvorfälle) aufgebaut haben.
Erreicht ein Krankenhaus den Schwellenwert erst zukünftig, also nach dem Jahr des Inkrafttretens der BSI-KritisV, so gilt es als kritische Infrastruktur ab dem 1.April des Kalenderjahres, das auf das Kalenderjahr des erstmaligen Erreichen oder Überschreiten des Schwellenwertes folgt. Für diese Fälle gilt die Meldepflicht dann unmittelbar ab Einstufung als kritische Infrastruktur.

Zudem sind innerhalb von 2 Jahren **angemessene** Schutzmaßnahmen nach dem Stand der Technik für diese IT-Infrastrukturen zu implementieren. Es sind entsprechende organisatorische und technische Vorkehrungen zur Vermeidung von IT-Störungen der informationstechnischen Systeme zu treffen und regelmäßig nachzuweisen. Dies betrifft insbesondere die Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit der IT-Systeme und Daten.
Einen Überblick vermitteln die folgenden Dokumente:

- „IT-Sicherheit – Allgemeine Grundsätze und Empfehlungen zum Informationssicherheitsmanagement von Universitätsklinika“ veröffentlicht von der Deutschen Hochschulmedizin
- „Handlungsempfehlungen zur Verbesserung der Informationssicherheit an Kliniken“ veröffentlicht vom UP KRITIS Branchenarbeitskreis Medizinische Versorgung

Dieses Dokument „Allgemeine Grundsätze und Empfehlungen zum Meldewesen nach IT-Sicherheitsgesetz“ soll eine Handlungsempfehlung zum Aufbau des geforderten Meldeprozesses geben, um die Meldepflichten über IT-Störungen an das BSI quantitativ und qualitativ sicherzustellen. Es basiert auf dem IT-Sicherheitsgesetz, sowie der zugehörigen Rechtsverordnung und ist eine auf die besondere Situation der Universitätsklinika angepasste Zusammenfassung der vom BSI herausgegebenen Informationen und FAQ.
In der Anlage 01 werden einige praktische Beispiele für meldepflichtige IT-Vorfälle aus dem Umfeld eines Krankenhauses beschrieben. Diese Fallsammlung ist nur exemplarisch und wird regelmäßig ergänzt.

3 Meldepflicht

3.1 Wer muss melden?

Die Meldepflicht gem. § 8b Absatz 4 BSI-Gesetz betrifft Betreiber Kritischer Infrastrukturen, die anhand der in der BSI-KritisV festgesetzten Schwellwerte als Kritische Infrastrukturen im Sinne des BSI-Gesetzes identifiziert wurden. Für die Medizinische Versorgung sind dies Krankenhäuser, die genau oder mehr als 30.000 stationäre Fälle pro Jahr aufweisen.

3.2 Was sind meldepflichtige Ereignisse?

Im Kapitel 4 „Meldungen von IT-Störungen“ erfolgt eine Definition der möglichen meldepflichtigen IT-Vorfälle. Gerade in der ersten Umsetzungsphase des IT-SiG fehlen aber noch praktische Beispiele aus dem Umfeld der Branche „Medizinische Versorgung“, so dass die Anlage 01 zukünftig mit weiteren Beispielen aufgebaut werden wird. Als generelle Empfehlung für die Anfangszeit gilt daher zunächst:

„Besser eine IT-Störung mehr melden, als zu wenig!“

Am wichtigsten sind dabei Meldungen von bzw. Hinweise auf IT-Störungen, von denen andere betroffene Infrastrukturen in Zukunft profitieren können. Somit soll der Aufbau eines qualitativ hochwertigen und im praktischen Umfeld der medizinischen Versorgung einsetzbaren Meldewesens beim BSI gefördert werden.

3.3 An wen muss gemeldet werden?

Gemäß § 8b Absatz 1 BSI-Gesetz fungiert das BSI als zentrale Meldestelle. Die Behörde hat sich in einer Selbstverpflichtung dazu erklärt, dass Meldungen zeitgerecht, sicher und vertrauensvoll entgegengenommen werden.
Ziel ist aber auch, aus diesen Meldungen und aus diversen weiteren Informationen gewonnene Erkenntnisse in einem Sicherheitslagebild für alle Betreiber Kritischer Infrastrukturen zur Verfügung zu stellen, damit diese ihre Informationstechnik angemessen schützen können. Unter Umständen können Sicherheitslagebilder aber auch nur direkt betroffene Branchen oder Sektoren zur Verfügung gestellt werden (Beispiel: ein Sicherheitsvorfall bei einem PACS-System wird nur an die Branche Medizinische Versorgung verteilt).

3.4 Ab wann muss gemeldet werden?

Mit der Benennung einer Kontaktstelle sind IT-Störungen sofort meldepflichtig!
Der in der Folge beschriebene Registrierungsprozess zur Benennung einer Kontaktstelle beim BSI ist zwar einfach und schnell durchzuführen, aber jedes Krankenhaus hat zuvor die notwendigen Anpassungen der internen Organisationsstruktur vorzunehmen! Dabei muss sichergestellt werden, das die Meldungen ab dem 1. April des Kalenderjahres in dem das Krankenhaus meldepflichtig wird, erfolgen können (s.u.).

3.5 Benennung einer Kontaktstelle

Bis zum 30.12.2017 haben alle betroffenen Infrastrukturen (in diesem Fall alle Uniklinika) dem BSI eine Kontaktstelle für IT-Störungen zu benennen.
Erreicht oder überschreitet ein Krankenhaus erst im Jahr 2017 oder später den Schwellenwert, so gilt es als Betreiber Kritischer Infrastrukturen ab dem 1.April des Kalenderjahres, das auf das Kalenderjahr des erstmaligen Erreichen oder Überschreiten des Schwellenwertes folgt. Solche Betreiber Kritischer Infrastrukturen haben dann sofort eine Kontaktstelle zu benennen.

Die Benennung einer Kontaktstelle gem. § 8b Absatz 3 BSI-Gesetz erfolgt mit der Registrierung unter:

Praktische Hinweise zum Ausfüllen der Registrierung:

- Punkt 3.5 Registereintrag / Handelsregisternummer: Sofern im Feld 3.4 als Rechtsform eine Anstalt öffentlichen Rechts (AöR) angegeben wurde, kann dieses Feld freigelassen werden. Stattdessen ist das Feld 3.6 „Alternative zum Registereintrag“ anzukreuzen und ein (formloses) Beiblatt mit entsprechendem Hinweis auf die Rechtsform dem Antrag hinzuzufügen
- Punkt 4.1 Sektor / Branche: hier haben auch die Krankenhäuser, welche eigene Labore oder Apotheken unterhalten, nur das Feld Gesundheit – Medizinische Versorgung zu aktivieren!
- Punkt 5.1 Ansprechpartner der Organisation: es wird empfohlen, keine Angaben zu tätigen, so dass die angegebene Kontaktstelle unter Punkt 5.2 auch organisatorischen Fragestellungen des BSI als zentraler Kontakt übernimmt.
- Anlage 2 Punkt 1.3 Kritische Infrastruktur: hier wird der Name des Krankenhauses erwartet (z.B. Uniklinikum Musterstadt)
- Nicht alle Punkte sind Pflichtangaben - es gibt auch optionale Felder, aber eine möglichst detaillierte Angabe aller Informationen wird empfohlen.
- Spätere Änderungen der ausgefüllten Angaben, sollten auch immer zeitnah dem BSI mitgeteilt werden!

Die Kommunikation zwischen dem Krankenhaus und dem BSI erfolgt in der Regel über das Melde- und Informationsportal des BSI, in Ausnahme auch per E-Mail oder telefonisch.
Die Funktions-E-Mail-Adresse der Kontaktstelle wird vom BSI für eventuelle Rückfragen (z.B. Einschätzungen / Bearbeitungsstatus) zu IT-Störungsmeldungen verwendet, sowie zum Zustellen von IT-Sicherheitsinformationen (Sicherheitslagebild).
Die Kontaktstelle muss lt. BSIG (§ 8b (3) Satz 2) „jederzeit erreichbar“ sein. D.h. die eingehende E-Mail muss vom empfangenden E-Mail-System angenommen werden und in angemessener Zeit durch einen zuständigen Mitarbeiter bearbeitet werden. Ein Beispielprozessablauf für eine interne Bearbeitung von IT-Sicherheitsinformationen des BSI wird in der Anlage 01 unter Punkt 6 dargestellt.

Empfohlen wird die Einbindung der angegebenen Funktions-E-Mail-Adresse in ein eventuell vorhandenes Incidentmanagement (zentraler IT-Service) und technisch in das verwendete zentrale IT-Ticketsystem, um alle eingehenden BSI Meldungen optimal erfassen und bearbeiten zu können.
Zudem wird die Einbindung weiterer meldepflichtiger Stellen empfohlen (siehe Punkt 7)

Um die Meldungen nach der Registrierung ausführen zu können, stellt das BSI nach der Registrierung ein Informationspaket (mit Zugangsbeschreibung zum Meldeportal und drei Hardware Token für die 2-Faktor-Authentifizierung) zur Verfügung. Zu beachten ist aber, dass IT-

Störungen schon mit der Registrierung meldepflichtig sind. Bis zum Erhalt des Informationspaketes und dem Einrichten des Zugangs, müssen IT-Störungen via Telefon (siehe Kontaktdaten – BSI Lagezentrum) mitgeteilt werden!
Sollten mehr als drei Hardware Token benötigt werden, so ist dem KRITIS-Büro (siehe Kontaktdaten) eine E-Mail mit der gewünschten Anzahl und einer Begründung zu senden!

3.6 Gemeinsam übergeordnete Ansprechstelle (GÜAS)

Betreiber Kritischer Infrastrukturen können neben der Kontaktstelle eine gemeinsame übergeordnete Ansprechstelle (GÜAS) benennen. Hierzu müssen sich einerseits die geplante GÜAS beim BSI registrieren und andererseits die Betreiber, die diese GÜAS nutzen wollen, dies in ihrer Benennung der Kontaktstelle angeben.
Bei der Benennung von GÜAS sind folgende Punkte zu beachten:

- Eine GÜAS kann nur von Betreibern benannt werden, die dem gleichen Sektor angehören.
- Die Aufgabe der GÜAS ist es, die vom BSI versandten Informationen stellvertretend für den Betreiber entgegenzunehmen sowie die Vorfalls Meldungen nach § 8b BSIG im Auftrag der Betreiber an das BSI zu melden.
- Wenn eine GÜAS benannt wurde, erfolgt der Informationsaustausch zwischen dem BSI und dem Betreiber in der Regel über diese. Parallel wird allerdings auch immer die Kontaktstelle des Betreibers angeschrieben. Daher ist hier aus Eigeninteresse der Betreiber nur eine GÜAS zu benennen, der seitens der Betreiber volles Vertrauen entgegengebracht wird.
- Die GÜAS muss eine sogenannte "Traffic Light Protocol (TLP – Details unter Punkt 8)"-Erklärung unterzeichnen, da sie entsprechend eingestufte Dokumente zur Weiterleitung an die angeschlossenen Betreiber erhalten wird.
- Die GÜAS leiten die vom BSI erhaltenen Informationen nur an Betreiber einer Kritischen Infrastruktur im Sinne von § 2 Absatz 10 BSIG weiter.

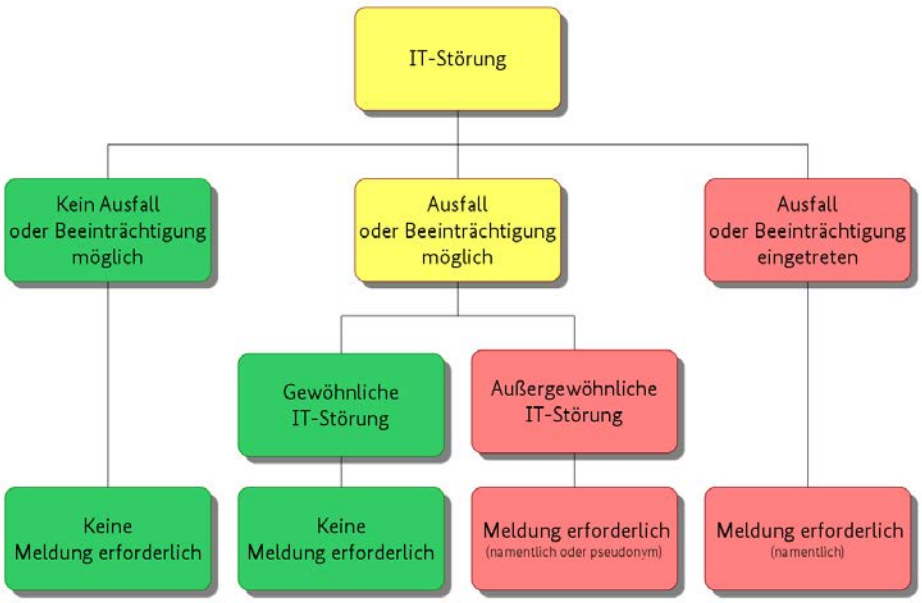
4 Meldungen von IT-Störungen

Betreiber Kritischer Infrastrukturen müssen erhebliche Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer IT-Systeme, IT-Komponenten und IT-Prozesse (IT-Störung), die zu einem Ausfall oder einer Beeinträchtigung der kritischen Infrastruktur führen könnten oder bereits geführt haben, dem BSI melden (gemäß § 8b Absatz 4 BSI-Gesetz)!

Insgesamt ist festzustellen, dass hier vor dem Hintergrund der Ausführung des Gesetzgebers in der Begründung des Gesetzesvorhabens von einem eher weiten Störungsbegriff ausgegangen wird.

Eine Meldung ist immer erforderlich, wenn es bereits zu einem Ausfall oder zu einer Beeinträchtigung der betriebenen Kritischen Infrastruktur gekommen ist. Ist ein Ausfall oder eine Beeinträchtigung zwar möglich, aber (noch) nicht eingetreten, so ist eine Meldung nur erforderlich, wenn es sich um eine außergewöhnliche IT-Störung handelt.

Die folgende Grafik stellt dar, wann gemeldet werden soll:



Quelle: *Bundesamt für Sicherheit in der Informationstechnik*

4.1 Beschreibung für gewöhnliche IT-Störungen

IT-Störungen können als gewöhnlich bezeichnet werden, wenn sie mit den nach "Stand der Technik" umgesetzten Maßnahmen (die Maßnahmen können sowohl technisch als auch organisatorisch sein) abgewehrt wurden und ohne nennenswerte Probleme oder ohne erhöhten Ressourcenaufwand bewältigt wurden.
Beispiele für gewöhnliche IT-Störungen werden in der Anlage 01 gesammelt und bewertet!

4.2 Beschreibung für außergewöhnliche IT-Störungen

IT-Störungen können aus Sicht der VUD AG Informationssicherheit als **außergewöhnlich** bezeichnet werden, wenn sie nicht bereits automatisiert mithilfe der als "Stand der Technik" beschriebenen Maßnahmen abgewehrt wurden. Sie sind dann außergewöhnlich, wenn sie nur mit **erheblichem** bzw. **deutlich erhöhtem Ressourcenaufwand** (z. B. erhöhtem Koordinie-

rungsaufwand, Hinzuziehen zusätzlicher Experten, Nutzung einer besonderen Aufbauorganisation, Einberufung eines Krisenstabs) sowie mit Maßnahmen, die nicht dem Stand der Technik entsprechen, bzw. über diesen hinausgehen, bewältigt werden können.
Beispiele für außergewöhnliche IT-Störungen werden in der Anlage 01 gesammelt und bewertet!

4.3 Was ist unter einem Ausfall der Funktionsfähigkeit der betriebenen Kritischen Infrastruktur zu verstehen?

Unter einem **Ausfall der Funktionsfähigkeit** der Kritischen Infrastruktur versteht das BSI, dass die betroffene Anlage (in diesem Fall das Krankenhaus) **aufgrund einer Störung der Informationstechnologie** nicht mehr in der Lage ist, den von ihm erbrachten Anteil an der Erbringung der kritischen Dienstleistung, somit der stationären Versorgung, zu leisten.
Beispiele für einen Ausfall der Funktionsfähigkeit werden in der Anlage 01 gesammelt und bewertet!

4.4 Was ist unter einer Beeinträchtigung der Funktionsfähigkeit der betriebenen Kritischen Infrastruktur zu verstehen?

Unter **Beeinträchtigung der Funktionsfähigkeit** der Kritischen Infrastruktur versteht das BSI, dass das betroffene Krankenhaus **aufgrund einer Störung der Informationstechnologie** nicht mehr in der Lage ist, den von ihr erbrachten Anteil an der Erbringung der kritischen Dienstleistung (stationäre Versorgung) **voll umfänglich**, also in der erwarteten Quantität (Menge pro Zeit) zu erbringen.
Das Kriterium der Beeinträchtigung tritt dann ein, wenn die Quantität (Leistung bzw. versorgte Personen) der erbrachten kritischen Dienstleistung der Anlage um mindestens 50 % der im Durchschnitt erbrachten Leistung oder versorgten Personen gemindert ist. Geplante Ausfallzeiten (z.B. durch Wartung, Baumaßnahmen) sind davon ausgenommen.
Aufgrund der Komplexität und der Heterogenität der kritischen Dienstleistung eines großen Krankenhauses kann eine Quantifizierung einer Beeinträchtigung nur schwer vorgenommen werden. So kann z.B. der IT-Bedingte Ausfall von einzelnen „Sekundärdienstleistern“ wie Sterilisation, Labor oder Radiologische Diagnostik zu Beeinträchtigung (z.B. Reduktion der Anzahl von OPs) oder (partiellen) Ausfällen der kritischen Dienstleistung führen.
Beispiele für eine Beeinträchtigung der Funktionsfähigkeit werden in der Anlage 01 gesammelt und bewertet!

5 Meldeprozess

Grundsätzlich hat jedes Krankenhaus einen internen Prozess zur Behandlung von IT-Störung zu definieren (Incidentmanagement). Zudem muss der Meldeprozess, die Zuständigkeiten bis hin zur Dokumentation, ausreichend beschrieben werden.
Ein Beispielprozessablauf für einen Meldeprozess an das BSI wird in der Anlage 01 und dem Punkt 5 dargestellt.
Zum Meldeprozess nach IT-SiG hat das BSI die folgenden Informationen veröffentlicht:

Wie melde ich eine IT-Störung:
https://www.bsi.bund.de/DE/Themen/Industrie_KRITIS/IT-SiG/Was_tun/Vorfaelle_melden/vorfaelle_melden_node.html

Benutzeranleitung für das Melde-und Informationsportal:
https://mip.bsi.bund.de/Anleitung-MIP.pdf

Weitere Informationen zum Meldeprozess erhalten die Betreiber Kritischer Infrastrukturen nach der Registrierung innerhalb des Infopaketes.
In der Folge werden die wesentlichen Punkte auf Grundlage der genannten BSI Informationen zusammengestellt und geben einen groben ersten Überblick, ohne Anspruch auf Vollständigkeit und Aktualität.

5.1 Wie schnell muss gemeldet werden?

Die Meldung muss unverzüglich nach Erkennung der IT-Störung erfolgen, d. h. ohne schuldhaftes Zögern. Alle Erkenntnisse, die zum Zeitpunkt der Meldung vorliegen, müssen an das BSI gemeldet werden.
Beispiele:

- Der IT-Bereich erhält im Rahmen der IT-Rufbereitschaft außerhalb der Servicezeiten z.B. Freitagnachts eine Meldung, dass ein Verschlüsselungstrojaner auf einem IT-System zugeschlagen hat. Die Rufbereitschaft aktiviert die entsprechenden Mitarbeiter zur Beseitigung der IT-Störung. Die für die Meldung der Vorfälle und als Kontaktstelle beim BSI bekannte zuständige Stelle wird noch am Wochenende informiert, benötigt aber die organisationsbedingte Freigabe der Rechtsabteilung, welche keinen Bereitschaftsdienst hat, und kann dadurch die Meldung erst am Montagvormittag zu den üblichen Bürozeiten an das BSI melden
  -> nach Einschätzung der VUD-AG Informationssicherheit liegt dann kein schuldhaftes Zögern vor!
- Die für die Meldung der Vorfälle und als Kontaktstelle beim BSI bekannte zuständige Stelle wird in der üblichen Bürozeit über eine IT-Störung informiert. Durch organisatorische Vorgaben soll diese Stelle aber die Freigabe des Vorstandes abwarten, um den Vorfall an das BSI melden zu können. Der Vorstand meldet sich nicht in angemessener Zeit zurück **und** es erfolgt auch keine andere Kommunikationsaufnahme zum Vorstand. Erst 5 Tage später meldet sich der Vorstand und erteilt die Freigabe
  -> es liegt ein schuldhaftes Verzögern vor!

Können im Rahmen dieser unverzüglichen Meldung noch nicht alle erforderlichen Angaben zur IT-Störung gemacht werden, ist die Meldung als Erstmeldung zu kennzeichnen. Sobald fehlende Informationen bekannt sind, ist eine Folgemeldung und letztendlich eine Abschlussmeldung vorzulegen.

Im Zweifelsfall ist die Meldung nachrangig gegenüber der Eindämmung der akuten Folgen der IT-Störung.

Für die Erstmeldung gilt grundsätzlich Schnelligkeit vor Vollständigkeit!

Es wird empfohlen, dass die Betreiber Kritischer Infrastrukturen entsprechende Organisationsstrukturen (Verantwortlichkeiten, Kommunikationswege) aufbauen, die eine Meldung ohne schuldhaftes Zögern sicherstellen! Dies kann z.B. durch Arbeitsanweisungen oder Sicherheitsrichtlinien erfolgen, in der u.a. die folgenden Prozesse definiert werden:

- Meldung aller IT-Störungen, verdächtiger Aktivitäten und Vorfälle an eine zentrale Stelle - dem IT-Servicemanagement. Das IT-Servicemanagement beurteilt die Lage, koordiniert Maßnahmen und bindet eine Melderolle mit ein, welche u.a. für die Weiterleitung meldepflichtiger IT-Störungen an das BSI verantwortlich ist.

5.2 Ausfüllen des Meldeformulars

Grundsätzlich sollen alle Meldungen über das Melde- und Informationsportal des BSI abgegeben werden. In Ausnahmefällen können Meldungen aber auch per E-Mail oder per Telefon abgegeben werden. Die unterschiedlichen Kommunikationswege werden den Betreibern Kritischer Infrastrukturen mit der Benennung einer Kontaktstelle (Registrierung) mitgeteilt.

Muster des Meldeformulars nach §8b Absatz 4 BSIG:
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/IT_SiG/Meldeformular_BSIG8b_Muster.pdf?__blob=publicationFile&v=3

Wenn aufgrund einer anhaltenden IT-Störung noch nicht alle Fragen zum Zeitpunkt der Meldung beantwortet werden können, sind diese später in der Folgemeldung oder Abschlussmeldung zu ergänzen.
Die Abschlussmeldung kann nach vollständiger Umsetzung aller Maßnahmen zur Vorfallsbearbeitung erfolgen. Spätestens mit der Abschlussmeldung sollen die für die Statistik und das Gesamtlagebild erforderlichen Angaben zu den vermuteten oder tatsächlichen Ursachen gemacht werden.

Mit der Abschlussmeldung hat der Betreiber einer Kritischen Infrastruktur seine Meldepflicht zu dieser IT-Störung gegenüber dem BSI erfüllt.

Um das Ausfüllen des Meldeformulars innerhalb der Kritischen Infrastruktur zu schulen, ist es möglich, sogenannte Testmeldungen vorzunehmen. Dazu ist sie in einen der ersten Felder des Formulars klar und deutlich als „TESTMELDUNG“ zu bezeichnen. Zudem sollten Testmeldungen innerhalb normaler Bürozeiten (Mo-Fr 8-16 Uhr) erfolgen.
In einer der nächsten Updates des Melde- und Informationsportal soll es ermöglicht werden, Meldungen zum Testen und Schulen der internen Prozesse einfacher & eindeutiger markieren zu können.

5.3 Wofür werden die Informationen aus dem Meldeformular benötigt?

Das Meldeformular ist in sieben Abschnitte unterteilt. Dabei sind die Informationen, die in den ersten beiden Abschnitten von dem Meldenden zur Verfügung gestellt werden, wichtig für die

- Kontaktaufnahme (Abschnitt 0),
- Betroffenheitskorrelation (Abschnitt 0, Abschnitt 1) und
- (statistische) Nachbereitung (Abschnitt 1).

In den weiteren vier Abschnitten sollen genauere Details zu dem IT-Sicherheitsvorfall ermittelt werden. Diese Informationen werden verwendet für die

- Kritikalitätsbewertung aus IT-Sicherheitssicht (Abschnitt 1-4),
- Erstellung eines bundesweiten IT-Lagebilds (Abschnitt 1-4),
- Warn- oder Informationsmeldung an potentiell weitere Betroffene (Abschnitt 1-4),
- (statistische) Nachbereitung (Abschnitt 1-4, insbesondere Abschnitt 3) sowie
- Analyse der potentiellen Auswirkungen auf die Verfügbarkeit Kritischer Infrastrukturen (Abschnitt 1, Abschnitt 5).

Darüber hinaus hat man die Möglichkeit zu ergänzenden Angaben (Abschnitt 6).

5.4 Meldungsquittierung durch das BSI

Das BSI quittiert den Empfang der Meldung innerhalb von 30 Minuten. **Sollte nach 30 Minuten keine Quittierung erfolgt sein, ist zusätzlich telefonisch mit dem BSI der Kontakt aufzunehmen.**
Erreichbar ist das BSI über die nach der Registrierung mitgeteilten Kontaktdaten.

5.5 Was geschieht mit der Meldung beim BSI?

Das BSI analysiert die IT-Störung, korreliert sie mit weiteren vorliegenden Erkenntnissen und erarbeitet ggf. Vorschläge für Maßnahmen. Sollten zusätzliche Detailinformationen benötigt werden, wendet sich das BSI mit Rückfragen an den im Meldeformular für den Vorfall angegebenen Ansprechpartner oder ersatzweise an die benannte Kontaktstelle des Betreibers.

Bei Relevanz für andere Mitbetroffene erstellt das BSI eine Warn- oder Informationsmeldung. Des Weiteren fließen die Erkenntnisse kontinuierlich in die Erstellung eines Gesamtlagebildes mit ein.
Im Rahmen der Auswertung analysiert das BSI gemeinsam mit dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) und weiteren Aufsichtsbehörden zudem die potentiellen Auswirkungen der IT-Störung auf die Verfügbarkeit Kritischer Infrastrukturen.

5.6 Feedback und Mehrwertdienste durch das BSI

Aus der stetigen Informationsgewinnung des BSI und durch die Meldungen von Betroffenen erstellt das BSI sanitarisierte (d.h. Veränderung der betroffenen Namen und Institutionen in einem rückschlussfreien Ersatzkontext) Warn- oder Informationsmeldungen, die an registrierte Betreiber zielgruppenorientiert versendet werden.

Laut BSI FAQ Meldewesen

Zusätzlich stellt das BSI allen meldepflichtigen Betreibern und ggf. darüber hinaus Dritten ein Gesamtlagebild zur Verfügung.
Das BSI bietet den Betreibern der Kritischen Infrastruktur eine Task Force Einheit an, ähnlich dem der BKA Quick Reaction Force (QRF) Einheit, welche im Notfall und ausschließlich auf Anforderung des Betreibers der Kritischen Infrastruktur Unterstützung zur schnellen Wiederinbetriebnahme und der Analyse des Vorfalles anbietet!

5.7 Wie schützt das BSI die Informationen?

Das BSI behandelt die Störungsmeldungen vertraulich. § 8d BSIG schränkt die Weitergabe von Informationen an Dritte deutlich ein. Auskunft darf nur erteilt werden, wenn schutzwürdige Interessen des betroffenen Betreibers Kritischer Infrastrukturen dem nicht entgegenstehen und durch die Auskunft keine Beeinträchtigung wesentlicher Sicherheitsinteressen zu erwarten ist. Zugang zu personenbezogenen Daten wird nicht gewährt.

Sofern das BSI aufgrund einer Störungsmeldung eine anonymisierte Information erstellt hat, wird es den Betreibernamen nicht nennen. Dies gilt auch, sofern im Verlauf der Bearbeitung über andere Wege Informationen zur Betroffenheit eines Betreibers Kritischen Infrastrukturen öffentlich bekannt werden.

5.8 Sollte bei einem IT-Angriff Anzeige erstattet werden?

Die Sichtbarkeit von IT-Angriffen (technische Angriffe wie z.B. Hacking, Identitätsmissbrauch, Spear-Phishing), sollte sich auch in der Strafverfolgung und der Kriminalstatistik wiederfinden. Es wird daher bei IT-Angriffen und Schäden empfohlen, die Erstattung einer Anzeige bei einer polizeilichen Ermittlungsbehörde vorzunehmen.

Mehr Informationen und eine Übersicht der zentrale Ansprechstellen Cybercrime der Polizeien der Länder und des Bundes sind abrufbar unter:
https://www.polizei.de/Polizei/DE/Einrichtungen/ZAC/zac.html?nn=39938

5.9 Welche Schnittstellen gibt es zu den bestehenden Genehmigungs-/ Aufsichtsbehörden und sonstigen zuständigen Behörden des Bundes?

Gemäß § 8b Absatz 2 Nummer 2 BSIG ist das BSI verpflichtet, „potentielle Auswirkungen auf die Verfügbarkeit der Kritischen Infrastrukturen in Zusammenarbeit mit den zuständigen Aufsichtsbehörden und dem BBK zu analysieren“.
Im Bedarfsfall geht das BSI hierzu auf die zuständigen Aufsichtsbehörden und/oder das BBK zu.
Gegebenenfalls leitet das BSI die Meldung dabei anonymisiert (ohne den Abschnitt 0) an die zuständigen Aufsichtsbehörden weiter.

Sofern eine Nennung des Betreibers der Kritischen Infrastruktur gegenüber der Aufsichtsbehörde vermieden werden soll, ist unbedingt darauf zu achten, dass im Text der anderen Abschnitte KEINE HINWEISE auf den Namen der Kritischen Infrastruktur stehen, die eine Identifizierung ermöglichen.
Falls im Meldeformular angegeben wurde, bei wem die Anzeige erstattet wurde und eine entsprechende Weiterleitung explizit gewünscht wird, wird das BSI diese Meldung, als Ergänzung zur Zusammenarbeit mit den lokalen Strafverfolgern, dem BKA im Rahmen seiner gesetzlichen Zuständigkeit für Kritische Infrastrukturen weiterleiten. Damit steht die gesamte Bandbreite der polizeilichen Möglichkeiten zur Verfügung.

Sofern sich aus der Meldung Tatsachen ergeben, die einen terroristischen Hintergrund erkennen lassen, muss das BKA im Rahmen seiner gesetzlichen Zuständigkeit durch das BSI unterrichtet werden.

Sofern sich aus der Meldung Tatsachen ergeben, die eine sicherheitsgefährdende oder geheimdienstliche Tätigkeit für eine fremde Macht erkennen lassen, muss das Bundesamt für Verfassungsschutz (BfV) im Rahmen seiner gesetzlichen Zuständigkeit durch das BSI unterrichtet werden.

In Einzelfällen muss das BSI seine Fachaufsicht im Bundesministerium des Innern über eine IT-Störung und die zugehörigen technischen Aspekte unterrichten. Das BSI wird Maßnahmen ergreifen, die übergebenen Informationen angemessen zu schützen und die Interessen der betroffenen Kritischen Infrastruktur wahren.

Zur konkreten Fallbearbeitung geht das BSI nur in Absprache mit der betroffenen Kritischen Infrastruktur auf weitere Behörden zu.

6 Verstoß gegen die Meldepflicht?

Bei festgestellten Verstößen gegen die Pflichten aus dem IT-Sicherheitsgesetz, insbesondere die Pflicht zur Einrichtung angemessener technischer und organisatorischer Maßnahmen zum Schutz von IT-Systemen und Kundendaten, drohen Bußgelder von bis zu 50.000 € (vgl.: Art.

4 IT-Sicherheitsgesetz i.V.m. § 16 Abs. 2 TMG, Art. 5 IT-Sicherheitsgesetz i.V.m. 149 Abs. 2 TKG).

7 Meldeverpflichtungen auf Basis anderer Gesetze oder rechtlicher Grundlagen

Auf Grundlage der folgenden Verordnungen sind die entsprechenden Meldeverpflichtungen im Bedarfsfall ebenso zu beachten, einzuhalten und in den Meldeprozess zu integrieren:

- **Medizinprodukte Betreiberverordnung (MPBetreibV)**
  Meldung meldepflichtiger Vorkommnisse im Sinne der Medizinprodukte-Sicherheitsplanverordnung (MPSV) an das Bundesamt für Arzneimittel und Medizinprodukte (BfArM-Meldung).
- **EU Datenschutzgrundverordnung, Landesdatenschutzverordnung**
  Meldung meldepflichtiger Datenschutzvorfälle im Sinne der EU Datenschutzgrundverordnung oder der Landesdatenschutzverordnungen.

Unter Umständen kann es bei einer IT-Störung notwendig sein, auch eine Meldung auf Basis einer oder aller genannten Verordnungen tätigen zu müssen! Hier fehlen aktuell noch die praktischen Erfahrungen aus diesen neuen Verordnungen, so dass es zukünftig noch zu Änderungen bzw. Anpassungen kommen kann.

8 Kontaktdaten

- **Bundesamt für Sicherheit in der Informationstechnik**
  Godesberger Allee 185-189
  Postfach 20 03 63
  53133 Bonn

  E-Mail: bsi@bsi.bund.de
- **KRITIS Büro**
  Ist erste Anlaufstelle für:
  * Registrierung Kontaktstelle
  * Auslegung der BSI-KritisV
  * Fragen zur Umsetzung ITSiG
  Telefon: +49(0)228 99 9582 6166 (Montag-Freitag 08:00-15:30 Uhr)
  E-Mail: kritis-buero@bsi.bund.de
- **BSI Lagezentrum / Meldestelle**

  Alternativ, falls online nicht möglich:
  Telefon:
  09:00-16:00 Uhr: +49(0)228 99 9582 6171
  16:00-09:00 Uhr: +49(0)170 459 5627

9 Abkürzungen / Glossar / Literatur-Links

Abkürzungen:

BBK	Bundesamt für Bevölkerungsschutz und Katastrophenhilfe
BfArM	Bundesamt für Arzneimittel und Medizinprodukte
BfV	Bundesamt für Verfassungsschutz
BKA	Bundeskriminalamt
BMI	Bundesministerium des Innern
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSIG	BSI Gesetz
BSI-KritisV	BSI-Kritis-Verordnung
GÜAS	Gemeinsam übergeordnete Ansprechstelle
ITSiG	IT-Sicherheitsgesetz - Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme
KRITIS	Kritische Infrastrukturen
LKA	Landeskriminalamt
MIP	Melde- und Informationsportal des BSI
MP	Medizinprodukt
MPBetreibV	Medizinprodukte Betreiberverordnung
MPSV	Medizinprodukte-Sicherheitsplanverordnung
PACS	Picture Archiving and Communication System - Bildarchivierungssystem
QRF	Quick Reaction Force Einheit des BKA
SPOC	Single Point of Contact
TKG	Telekommunikationsgesetz
TLP	Traffic Light Protocol
WID	Warn- und Informationsportal des BSI

Glossar:

Cyber-Angriff	Ein Cyberangriff (Cyberattacke) ist der gezielte Angriff auf größere, für eine spezifische Infrastruktur wichtige Rechnernetze von außen.
DDOS	Mit „Distributed Denial of Service-Attacken" (DDoS) verfolgen Angreifer das Ziel, Server oder IT-Systeme mit einer großen Anzahl an Anfragen zu bombardieren, bis diese ihren Dienst einstellen und Internet-Services nicht mehr aufrufbar sind
Hardware Token	Ist eine Hardwarekomponente zur zusätzlichen Identifizierung und Authentifizierung von Benutzern
Kompromittierung	Ein System, eine Datenbank oder auch nur ein einzelner Datensatz wird als kompromittiert betrachtet, wenn Daten manipuliert sein könnten und wenn der Eigentümer des Systems keine Kontrolle über die korrekte Funktionsweise oder den korrekten Inhalt mehr hat, beziehungsweise ein Angreifer ein anderes Ziel der Manipulation erreicht hat.
Mitigation	Maßnahmen, um zu verhindern, dass der gleiche Angriff mehrfach Erfolg hat
UP KRITIS	Ist eine öffentlich-private Kooperation zwischen Betreibern Kritischer Infrastrukturen (KRITIS), deren Verbänden und den zuständigen staatlichen Stellen

Sanitarisierung	Veränderung der betroffenen Namen und Institutionen in einem rückschlussfreien Ersatzkontext
Stand der Technik	Ist ein Entwicklungsstand fortschrittlicher Verfahren, Einrichtungen und Betriebsweisen, der nach herrschender Auffassung führender Fachleute das Erreichen des gesetzlich vorgegebenen Zieles gesichert erscheinen lässt. Verfahren, Einrichtungen und Betriebsweisen oder vergleichbare Verfahren, Einrichtungen und Betriebsweisen müssen sich in der Praxis bewährt haben. (Quelle: Bundesministeriums für Justiz und Verbraucherschutz, Handbuch der Rechtsförmlichkeit - http://hdr.bmj.de/page_b.4.html). Das Anforderungsniveau der Klausel „Stand der Technik“ liegt zwischen den "allgemein anerkannte Regeln der Technik" und dem "Stand von Wissenschaft und Technik" Es definiert keine konkrete Maßnahme oder keinen technologischen Stand.
Spam	Unerwünschte Nachrichten (Informationen), die dem Empfänger unverlangt zugestellt werden und häufig werbenden Inhalt enthalten
Traffic Light Protocol	Vereinbarung zum Schutz von Informationen. Das TLP dient der Schaffung von Vertrauen bzgl. des Schutzes ausgetauschter Informationen durch Regelung der Weitergabe
Phishing	(engl. für Angeln) - Ist der Versuch, über gefälschte Webseiten oder E-Mails an persönliche Benutzerdaten zu gelangen, um damit Identitätsdiebstahl zu begehen
-Spear-Phishing	(engl. für Speer) - Spezialisierte Form des klassischen Phishing. Ist ein gezielter Angriff auf konkrete Organisationen.

Literatur-Links (Stand 29.11.2017):

BSI Gesetz: https://www.gesetze-im-internet.de/bsig_2009/
IT-Sicherheitsgesetz: http://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl115s1324.pdf
BSI FAQ IT-Sicherheitsgesetz: https://www.bsi.bund.de/DE/Service/FAQ/IT-Sicherheitsgesetz/faq_node.html
BSI FAQ Meldewesen: https://www.bsi.bund.de/DE/Service/FAQ/Meldepflicht/faq_node.html
Melden einer IT-Störung beim BSI: https://www.bsi.bund.de/DE/Themen/Industrie_KRITIS/IT-SiG/Was_tun/Vorfaelle_melden/vorfaelle_melden_node.html
Benutzeranleitung für das Melde-und Informationsportal: https://mip.bsi.bund.de/Anleitung-MIP.pdf
Zentrale Ansprechstellen Cybercrime der Polizeien der Länder und des Bundes: https://www.polizei.de/Polizei/DE/Einrichtungen/ZAC/zac.html?nn=39938
„IT-Sicherheit – Allgemeine Grundsätze und Empfehlungen zum Informationssicherheitsmanagement von Universitätsklinika“ veröffentlicht von der Deutschen Hochschulmedizin
„Handlungsempfehlungen zur Verbesserung der Informationssicherheit an Kliniken“ veröffentlicht vom UP KRITIS Branchenarbeitskreis Medizinische Versorgung

Kontakt
Verband der Universitätsklinika
Deutschlands e.V. (VUD)
Alt-Moabit 96
10559 Berlin
info@uniklinika.de
www.uniklinika.de

Oliver Stenzel
Politik- und Gremienarbeit
F. +49 (0)30 3940517-19
stenzel@uniklinika