Bundesamt
für Sicherheit in der
Informationstechnik

Fragen und Antworten für Betreiber Kritischer Infrastrukturen zur Meldepflicht nach dem IT-Sicherheitsgesetz

Wer muss dem BSI melden? Die Meldepflicht gem. § 8b Absatz 4 BSI-Gesetz betrifft Betreiber Kritischer Infrastrukturen, die anhand der in der BSI-Kritisverordnung festgesetzten Schwellenwerte als Kritische Infrastrukturen im Sinne des BSI-Gesetzes identifiziert wurden.

Mit Inkrafttreten des "Gesetzes zur Umsetzung der EU-Richtlinie über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union" (NIS-Richtlinien-Umsetzungsgesetz) am 30.06.2017 ergeben sich für Betreiber von Energieversorgungsnetzen, öffentlichen Telekommunikationsnetzen und öffentlich zugänglichen Telekommunikationsdiensten folgende Neuregelungen:

1. Betreiber von Energieversorgungsnetzen

Die Verpflichtung zur Meldung von IT-Störungen an das BSI betraf bisher nur die Betreiber von Energieversorgungsnetzen, deren Anlagen nach der BSI-Kritisverordnung als Kritische Infrastrukturen bestimmt wurden. Mit dem Gesetz zur Umsetzung der NIS-Richtlinie erweitert sich diese Meldepflicht auf alle Energieversorgungsnetzbetreiber.

2. Betreiber von öffentlichen Telekommunikationsnetzen und Erbringer öffentlich zugänglicher Telekommunikationsdienste

Mit dem Gesetz zur Umsetzung der NIS-Richtlinie erweitert sich ebenfalls die bereits bestehende Meldepflicht gemäß **§ 109 Absatz 5 TKG** insofern, dass Beeinträchtigungen von Telekommunikationsnetzen und -diensten, sofern diese zu beträchtlichen Sicherheitsverletzungen führen oder führen können, sowohl an die **Bundesnetzagentur** als auch an das **BSI** gemeldet werden müssen.

Für die Meldung an das BSI kann ebenfalls das Mitteilungsformular der Bundesnetzagentur unter Beachtung des Umsetzungskonzeptes verwendet werden, welche sich auf der Webseite der Bundesnetzagentur finden lassen.

Für eine vertrauliche Übermittlung des Mitteilungsformulars gem. § 109 Absatz 5 TKG an das BSI wird nachfolgend als Textdatei ein öffentlicher PGP-Schlüssel zur Verfügung gestellt:

PublicKey
Datum der Erstellung: 17.07.2017
Schlüssel-ID: 6977BB6EB4D9BD70
Fingerprint: C02C B80C 09A6 235F AA52 4A8B 6977 BB6E B4D9 BD70

Schlüssel-ID und Fingerprint des öffentlichen PGP-Schlüssels können nach dem Import in Ihre eigene PGP-Schlüsselsammlung auf Übereinstimmung überprüft werden.

Betreiber Kritischer Infrastrukturen gemäß BSI-Kritisverordnung, die ein öffentliches Telekommunikationsnetz betreiben oder öffentlich zugängliche Telekommunikationsdienste erbringen, müssen eine Kontaktstelle beim BSI registrieren.

Ausgehend vom Gesetzestext heißt es im § 8b (4) BSIG:

Wann muss dem BSI gemeldet werden?

"Betreiber Kritischer Infrastrukturen haben folgende Störungen unverzüglich über die Kontaktstelle an das Bundesamt zu melden:

- *Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die zu einem Ausfall oder zu einer erheblichen Beeinträchtigung der Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen geführt haben,*
- *erhebliche Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die zu einem Ausfall oder zu einer erheblichen Beeinträchtigung der Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen führen können. […]"*

Abbildung 1 verdeutlicht die verschiedenen Fälle, wann eine Meldung erforderlich ist.

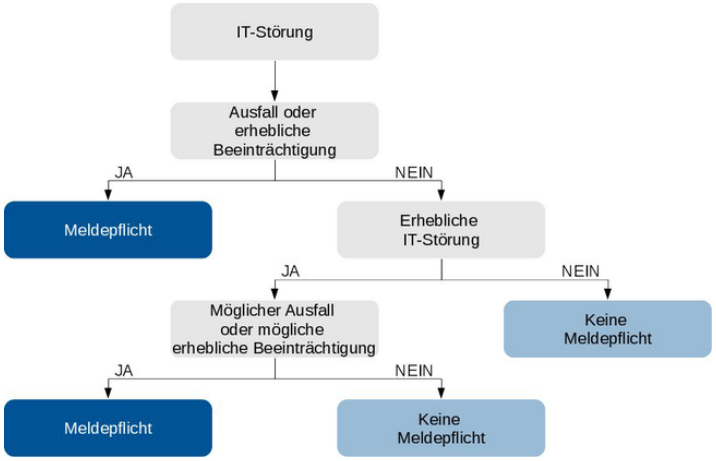

Abbildung 1: Meldekriterien für IT-Störungen Quelle: *Bundesamt für Sicherheit in der Informationstechnik*

Sollte es trotz aller Erläuterungen nicht eindeutig möglich sein, festzustellen, um was für eine IT-Störung es sich handelt, können aus praktischer Erfahrung und pragmatischer Sicht folgende Fragen eine zusätzliche Hilfestellung bieten, ob die Störung zu melden ist:

- Hätte es mir geholfen, wenn ich Warnungen über diese Art von Vorfall von einem anderen Betreiber bekommen hätte?
- Ist die (mögliche) Einschränkungen relevant für die Versorgungslage?

Im Zweifelsfall suchen Sie den Kontakt zum BSI. Die Mitarbeiter und Mitarbeiterinnen unserer Meldestelle werden Sie gerne hinsichtlich der Meldepflicht beraten.

Was ist eine IT-Störung?

Zur IT-Störung findet sich in der Begründung des IT-Sicherheitsgesetzes folgende Erläuterung:

"Eine [IT-]Störung im Sinne des BSI-Gesetzes liegt daher vor, wenn die eingesetzte Technik die ihr zugedachte Funktion nicht mehr richtig oder nicht mehr vollständig erfüllen kann oder versucht wurde, entsprechend auf sie einzuwirken." (siehe BT-Drs 18/4096, 28)

Beispiele für IT-Störungen, die keine IT-Sicherheitsvorfälle sind und trotzdem meldepflichtig sind, können sein:

- ein Bagger, der ein Kabel durchtrennt,
- ein Ausfall der Kühlung eines Rechenzentrums,
- ein falsch konfiguriertes System,
- ein fehlerhaftes Update oder ein fehlerhafter Patch, der eingespielt wird.

Wann ist eine IT-Störung erheblich? § 8b Abs. 4 Nr. 2 BSIG sagt, dass eine IT-Störung erheblich sein muss, um den Tatbestand der Meldepflicht zu erfüllen. Eine eindeutige, umfassend geltende Antwort, wann eine Störung erheblich ist, ist nicht möglich. Stattdessen ist es erforderlich, dass die Verantwortlichen in KRITIS-Unternehmen Einzelfallentscheidungen treffen.

Die folgende Liste an Beispielkriterien dient nur als Orientierungshilfe, um einen ersten Maßstab anlegen zu können. Die Beispielkriterien berücksichtigen dabei die IT-seitigen Auswirkungen der IT-Störung, nicht jedoch ihren Einfluss auf die kritische Dienstleistung. Diese ist erst in einem zweiten Schritt zu betrachten.

Eine erhebliche IT-Störung liegt insbesondere vor, wenn

- eine Nicht-Behandlung zu immer weiterführenden negativen Auswirkungen führen würde (zum Beispiel wenn der Ausfall einer Anlagensteuerung zu immer umfangreicheren Schäden oder der Zerstörung einer Anlage führen würde)
- zusätzliche Aufwände und Mittel eingesetzt oder eingeplant werden, die über die Aufwände und Mittel des Regelbetriebs oder bereits geplanter Arbeiten hinausgehen (zum Beispiel zusätzliche Mitarbeiter, Überstunden, Einsatz von Ersatzkapazitäten, zusätzliche Geld- oder Sachmittel)
- ihre Behandlung durch speziell vorgehaltene Incident-Responder oder Störfallteams durchgeführt werden muss
- wichtige IT-Systeme oder Komponenten zur Vermeidung weiterer Auswirkungen abgeschaltet oder isoliert werden
- für den Bewältigungszeitraum Betriebsprozesse geändert werden
- sie einen hohen finanzielle Schaden verursacht
- die Vermutung naheliegt, dass das Unternehmen Ziel eines neuartigen, außergewöhnlichen, zielgerichteten oder aus technischer Sicht bemerkenswerten Angriffs oder Angriffsversuchs ist zum Beispiel ein sogenannter Advanced Persistent Threat (APT)
- besondere Berichtspflichten gegenüber der Unternehmensleitung für solche IT-Störungen bestehen

Auch wenn erst im Nachhinein festgestellt wurde, dass die IT-Störung erheblich im Sinne des BSIG war, ist sie ab diesem Zeitpunkt meldepflichtig.

Wie schnell muss dem BSI 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.

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.

Eine Abschlussmeldung kann nach vollständiger Umsetzung aller Maßnahmen zur Vorfallsbearbeitung erfolgen. Mit der Abschlussmeldung hat der Betreiber seine Meldepflicht zu dieser IT-Störung gegenüber dem BSI vollständig erfüllt, sofern sich das BSI nicht binnen fünf Arbeitstagen anderweitig gegenüber dem Betreiber äußert (z. B. durch weitere Nachfragen zum Vorfall).

Was ist ein Ausfall? Ein Ausfall liegt vor, wenn die Funktionsfähigkeit einer KRITIS nicht mehr gegeben ist. Eine geplante Betriebsunterbrechung gilt nicht als Ausfall.

Was ist eine erhebliche Beeinträchtigung einer Kritischen Infrastruktur? Eine erhebliche Beeinträchtigung liegt insbesondere vor, wenn eine KRITIS nicht mehr in der Lage ist, ihre Versorgungsleistung wie geplant oder erwartet zu erbringen, zum Beispiel weil ihre Funktionsfähigkeit nur noch in Teilen gegeben ist, und die darauf entstandene Minderleistung erheblich ist. Wann eine Minderleistung erheblich ist, muss im Verhältnis zur Betroffenheit der Versorgten gesehen werden.

Beispielsweise kann von einer erheblichen Beeinträchtigung ausgegangen werden, wenn:

- eine große Anzahl von Nutzern betroffen ist
- eine große Anzahl von Geschäftsprozessen betroffen ist
- die Auswirkungen die öffentliche Aufmerksamkeit auf sich ziehen

Was ist ein möglicher Ausfall oder eine mögliche erhebliche Beeinträchtigung?

§ 8b Absatz 4 Satz 1 Nummer 2 BSIG setzt voraus, dass eine erhebliche IT-Störung zu einem Ausfall oder einer Beeinträchtigung der betriebenen Kritischen Infrastrukturen hätte führen können – in diesem Fall wäre die erhebliche IT-Störung meldepflichtig.

Folgende Beispiele dienen der Orientierung:

- Es treten erhebliche IT-Störungen während einer geplanten Betriebsunterbrechung auf, die sich auf die Funktionsfähigkeit der Kritischen Infrastruktur negativ auswirken. Aufgrund der geplanten Betriebsunterbrechung ist die zu diesem Zeitpunkt geplante Versorgungsleistung bereits 0 und wird durch die zusätzliche Störung nicht weiter verringert.
  Z. B.: ein Patch wird während einer Betriebsunterbrechung eingespielt, der die Funktionsfähigkeit der Anlage stört.
- Es treten erhebliche IT-Störungen während einer geplanten Betriebsunterbrechung auf, die dazu führen, dass die Betriebsunterbrechung länger als geplant andauert, aber nicht zwingend zu einer Verringerung der Versorgungsleistung führt.
- Es treten erhebliche IT-Störungen auf, die nicht alle, aber mehrere Schutzmechanismen, die vor IT-Störungen oder Einschränkungen schützen sollen, überwinden.
  Z. B.: Ein Angreifer verschafft sich Zugang zum Netz der Kritischen Infrastruktur, die Versorgungsleistung wird dadurch aber nicht gemindert.
- Es treten erhebliche IT-Störungen auf, die zu einem Ausfall oder einer erheblichen Beeinträchtigung von Teilen einer Kritischen Infrastruktur führen, aber die Versorgungsleistung über ihre Dauer nicht tatsächlich mindern. Dies könnte der Fall sein, wenn ein Teil der Produktions- oder Logistikkette innerhalb der Kritischen Infrastruktur ausfällt, die Versorgung aber zumindest zeitweilig durch Lagerbestände aufrechterhalten werden kann.
- Werden Angriffe auf die Kritische Infrastruktur unter Verwendung von neuartigen, außergewöhnlichen, zielgerichteten oder aus technischer Sicht bemerkenswerten Angriffsverfahren entdeckt, muss davon ausgegangen werden, dass eine Einwirkung auf die Kritische Infrastruktur möglich ist, sobald sich die Angreifer dazu entschließen.

Was mache ich, wenn ich keine Quittierung durch das BSI erhalte? Sollten Sie nach spätestens 30 Minuten keine Quittierung Ihrer Meldung durch das BSI erhalten, wenden Sie sich bitte zusätzlich telefonisch an das BSI. Sie erreichen das BSI über die Ihnen nach der Registrierung mitgeteilten Kontaktdaten.

Wo finde ich Hilfe beim Ausfüllen des Meldeformulars? Sollten Sie Fragen beim Ausfüllen des Meldeformulars haben, wenden Sie sich bitte an die Ihnen nach der Registrierung mitgeteilten Kontaktdaten.

Wenn aufgrund einer anhaltenden IT-Störung noch nicht alle Fragen zum Zeitpunkt Ihrer Meldung beantwortet werden können, sind diese später in der Folgemeldung oder Abschlussmeldung zu ergänzen.

Bitte machen Sie in dem Meldeformular mit Kennzeichnung der Abschlussmeldung klar, wenn Sie keine zusätzlichen Informationen mehr erwarten. Spätestens mit der Abschlussmeldung sollen die für die Statistik und das Gesamtlagebild erforderlichen Angaben (Abschnitt 3) zu den vermuteten oder tatsächlichen Ursachen gemacht werden.

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 haben Sie die Möglichkeit zu ergänzenden Angaben (*Abschnitt 6*).

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 **Bundesamt für Bevölkerungsschutz und Katastrophenhilfe** (BBK) zu analysieren“.
Im Bedarfsfall geht das BSI hierzu auf die zuständigen Aufsichtsbehörden und/oder das BBK zu. Ggf. leitet das BSI Ihre Meldung dabei anonymisiert (ohne den Abschnitt 0) an die zuständigen Aufsichtsbehörden weiter.
Sofern Sie eine Nennung Ihres Unternehmens gegenüber der Aufsichtsbehörde vermeiden wollen, achten Sie bitte darauf, dass im Text der anderen Abschnitte KEINE HINWEISE auf IHR UNTERNEHMEN stehen, die eine Identifizierung ermöglichen.

Falls Sie im Meldeformular angegeben haben, bei wem Sie Anzeige erstattet haben, und kennzeichnen, dass Sie eine entsprechende Weiterleitung explizit wünschen, wird das BSI diese Meldung, als Ergänzung zu Ihrer Zusammenarbeit mit den lokalen Strafverfolgern, dem **BKA** im Rahmen seiner gesetzlichen Zuständigkeit für Kritische Infrastrukturen weiterleiten. Damit steht Ihnen 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 **BfV** im Rahmen seiner gesetzlichen Zuständigkeit durch das BSI unterrichtet werden.

In Einzelfällen muss das BSI seine Fachaufsicht im BMI über einen IT-Sicherheitsvorfall und die zugehörigen technischen Aspekte unterrichten. Das BSI wird Maßnahmen ergreifen, die übergebenen Informationen angemessen zu schützen, um die Interessen des Betroffenen zu wahren.

Zur konkreten Fallbearbeitung geht das BSI nur in Absprache mit Ihnen auf **weitere Behörden** zu.

Was macht das BSI mit meinen Meldungen?

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 BBK und Aufsichtsbehörden zudem die potentiellen Auswirkungen der IT-Störung auf die Verfügbarkeit Kritischer Infrastrukturen.

Wie schützt das BSI meine Informationen? Das BSI behandelt Ihre 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 Ihrer 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 Ihres Unternehmens öffentlich bekannt werden.

Sollte ich bei einem IT-Angriff Anzeige erstatten? Die Sichtbarkeit von IT-Angriffen, wie sie durch die Meldestelle des BSI verfolgt wird, sollte sich auch in der Strafverfolgung und der Kriminalstatistik wiederfinden. Unterstützend dazu finden Sie auf den Internetseiten des BKA Handlungsempfehlungen für die Wirtschaft in Fällen von Cybercrime.

Bitte prüfen Sie bei Angriffen und Schäden in Ihrem Betrieb daher aktiv, ob die Erstattung einer Anzeige möglich ist.

Was erhalte ich vom BSI? Aus der stetigen Informationsgewinnung des BSI oder durch die Meldungen von Betroffenen erstellt das BSI sanitarisierte Warn- oder Informationsmeldungen, die an registrierte Betreiber zielgruppenorientiert versendet werden.

Zusätzlich stellt das BSI allen meldepflichtigen Betreibern und ggf. darüber hinaus Dritten ein Gesamtlagebild zur Verfügung.

Eine Reihe von weiteren Produkten und Dienstleistungen sind in Vorbereitung.

Was bedeutet die Anforderung "jederzeit erreichbar" gemäß § 8b (3) BSIG für KRITIS-Betreiber konkret?

Das BSI versteht unter der Formulierung "jederzeit erreichbar" gemäß § 8b (3) BSIG, dass Betreiber über die registrierte Kontaktstelle rund um die Uhr (24/7) in der Lage sind, BSI-Produkte zur Warnung und Information von KRITIS-Betreibern, im Folgenden kurz BSI-Produkte, (Cyber-Sicherheitswarnungen, Lageinformationen etc.) entgegenzunehmen und unverzüglich zu sichten und zu bewerten (Bearbeitung der Informationen auf Zuruf).
In der Regel werden BSI-Produkte während der normalen Geschäftszeiten versendet. Es ist jedoch nicht auszuschließen, dass das BSI in Ausnahmefällen dringende Warnungen auch außerhalb der normalen Geschäftszeiten (an Feiertagen, Wochenenden oder nachts) versendet.
Das BSI gestaltet die Cyber-Sicherheitswarnungen so, dass Dringlichkeit und (potentieller) Handlungsbedarf aus der E-Mail-Betreffzeile (automatisiert) herausgelesen werden können. Somit können bereits existierende dauerhaft erreichbare Stellen in der Institution, z. B. Pforte, Werkschutz oder sonstige Bereitschaftsdienste, akuten Handlungsbedarf erkennen und ggf. eine Alarmierung bzw. Weiterleitung an geeignete Ansprechpartner vornehmen. Geeignete Ansprechpartner verfügen über die fachliche Kompetenz zur Beurteilung des konkreten Vorfalls und sind in die Organisation und Prozesse zur Vorfallsbewältigung eingebunden.
Gesteigerte Anforderungen an die Verfügbarkeit einer Kontaktstelle des Betreibers ergeben sich nach einer Meldung einer IT-Störung gegenüber dem BSI. Um eine reibungslose Vorfallsbewältigung in Zusammenarbeit mit dem BSI sicherzustellen, sollen interne (Weiterleitungs-)Prozesse eingerichtet werden, die eine Alarmierung geeigneter Ansprechpartner nach Eingang der Information auch außerhalb der normalen Geschäftszeiten sicherstellen. Dies gilt insbesondere, wenn Sie eine IT-Störung an das BSI gemeldet haben und mit Rückfragen des BSI zu rechnen ist.