TLP:WHITE

Bundesamt
für Sicherheit in der
Informationstechnik

Informationsbroschüre

Unterstützung bei der Vorfallsbearbeitung

Übersicht über die Unterstützungsmöglichkeiten des BSI

Änderungshistorie

Version	*Datum*
Initiale Version v1.0	25.01.2021
v1.1	01.04.2021
v1.2	18.06.2021

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
Internet: https://www.bsi.bund.de
Service-Center (Telefon): 0800 2741000
Service-Center (E-Mail): service-center@bsi.bund.de
Einen Vorfall melden: https://www.allianz-fuer-cybersicherheit.de/Webs/ACS/DE/IT-Sicherheitsvorfall/Unternehmen/Online-Meldung/online-meldung_node.html
Für die Zielgruppen und Partner des BSI gelten darüber hinaus die üblichen Meldewege.

Inhalt

1 Externe Hilfe bei IT-Sicherheitsvorfällen

📣 Wichtiger Hinweis
Bei jedem IT-Sicherheitsvorfall gilt: Bewahren Sie Ruhe, handeln Sie nicht übereilt und holen Sie sich bei Bedarf frühzeitig externe Unterstützung!

Neben professionellen Incident Response Dienstleistern bieten auch diverse deutsche Behörden sowie Netzwerke (wie z.B. die Allianz für Cybersicherheit (ACS)) Unterstützung bei einem IT-Sicherheitsvorfall:

☞ Für die **Strafverfolgung und Täterermittlung** sind die **Polizeien** zuständig, die Sie z.B. über die Zentralen Ansprechstellen Cybercrime (ZAC)[1] der jeweiligen Landeskriminalämter (LKÄ) erreichen können.

☞ Bei Verdacht auf **Wirtschaftsspionage** erhalten Sie bei dem für Sie zuständigen **Landesamt - bzw. dem Bundesamt für Verfassungsschutz** (LfV / BfV)[2] kompetente Unterstützung.

☞ Auch das **Bundesamt für Sicherheit in der Informationstechnik (BSI)** kann im Rahmen seines gesetzlichen Auftrags[3] bestimmte Betroffene bei der **Bewältigung von IT-Sicherheitsvorfällen** tatkräftig unterstützen. Zu den Zielgruppen des BSI zählen demnach derzeit grundsätzlich:

- **Betreiber von Kritischen Infrastrukturen (gem. BSI-KritisV)**
- **Institutionen der Bundesverwaltung/Stellen des Bundes**
- **Unternehmen im besonderen öffentlichen Interesse**

ⓘ Ausnahme: Begründete Einzelfälle (BSIG § 5b, Satz 7)
In begründeten Einzelfällen kann das BSI auch bei solchen Institutionen tätig werden, die nicht zu den drei vorhergenannten Zielgruppen zählen. Ein begründeter Einzelfall liegt insbesondere dann vor, wenn es sich um einen Angriff von besonderer technischer Qualität handelt, die zügige Wiederherstellung der Sicherheit oder Funktionsfähigkeit des betroffenen informationstechnischen Systems von besonderem öffentlichem Interesse ist oder eine Stelle eines Landes betroffen ist.

📣 Wichtiger Hinweis
Diese Broschüre richtet sich vornehmlich an Betroffene der oben aufgelisteten Zielgruppen des BSI. Sollten Sie **nicht** zu einer der Zielgruppen gehören, so finden Sie am Ende dieser Broschüre in den FAQ weitergehende Hinweise für Unterstützungsangebote.

Eine Übersicht über alle externen Unterstützungsmöglichkeiten finden Sie auch am Ende dieser Broschüre.

[1] https://www.allianz-fuer-cybersicherheit.de/Webs/ACS/DE/IT-Sicherheitsvorfall/Unternehmen/Kontakt-zur-Polizei/kontakt-zur-polizei_node.html
[2] https://www.wirtschaftsschutz.info/DE/Ansprechpartner/Verfassungsschutz/verfassungsschutz_node.html
[3] Die Unterstützung des BSI erfolgt aufgrund des § 5b BSIG zur „Wiederherstellung der Sicherheit oder Funktionsfähigkeit informationstechnischer Systeme in herausgehobenen Fällen“. Handelt es sich bei einem Vorfall bei einer Stelle des Bundes oder eines Betreibers einer Kritischen Infrastruktur oder eines Unternehmens im besonderen öffentlichen Interesse um einen herausgehobenen Fall, so kann das Bundesamt auf Ersuchen der betroffenen Stelle oder des betroffenen Betreibers die Maßnahmen treffen, die zur Wiederherstellung der Sicherheit oder Funktionsfähigkeit des betroffenen informationstechnischen Systems erforderlich sind (BSIG § 5b, Satz 1).

2 Das Bundesamt für Sicherheit in der Informationstechnik (BSI)

Eine zentrale Anlaufstelle

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) ist die Cyber-Sicherheitsbehörde des Bundes[4]. Mit den Fachreferaten des Computer Emergency Response Team des Bundes (CERT-Bund) und dem Nationalen IT-Lagezentrum ist das BSI die zentrale Anlaufstelle für präventive und reaktive Maßnahmen mit Bezug auf sicherheits- und verfügbarkeitsrelevante Vorfälle in Computersystemen. Mit der Zentralen Meldestelle und dem Nationalen IT-Lagezentrum verfügt das BSI über einen Single Point of Contact (SPOC), in dem alle Meldungen zu Sicherheitsvorfällen in Deutschland zentral zusammengeführt werden.

Vorfallsbearbeitung unter der Federführung von CERT-Bund

Die Vorfallsbearbeitung wird federführend durch die Fachreferate des CERT-Bund durchgeführt. Dabei wird im Bedarfsfall auch auf die gesamte Expertise des BSI zurückgegriffen. Dazu zählen u.a. Experten für Cyber-Sicherheit in Industrieanlagen, Forensiker und Malware-Reverse-Analysten im Bereich der technischen Analysen, sowie Penetrationstester und dedizierte Incident Responder aus dem Mobile Incident Response Team (MIRT). Die meisten Experten des BSI verfügen über jahrelange Einsatzerfahrung und haben bereits eine Vielzahl an Behörden und Unternehmen bei schweren Cyber-Sicherheitsvorfällen erfolgreich unterstützt.

Über das ebenfalls beim BSI angesiedelte Nationale Cyber-Abwehrzentrum (Cyber-AZ) können bei Bedarf zudem auch weitere Sicherheitsbehörden zur Vorfallsbearbeitung hinzugezogen werden.

[4]Weitere Informationen finden Sie unter: www.bsi.bund.de

3 Die Unterstützungsangebote des BSI

Im Folgenden werden die wichtigsten Unterstützungsmöglichkeiten des BSI bei IT-Sicherheitsvorfällen kurz beschrieben. Die Auswahl der am besten geeigneten Maßnahmen erfolgt dabei jeweils fallabhängig.

Triage

Das Nationale IT-Lagezentrum führt zusammen mit dem CERT-Bund eine **Erstbewertung** einer Vorfallsmeldung durch. Dazu wird in der Regel eine sogenannte Triage-Besprechung mit dem Betroffenen durchgeführt. In dieser Besprechung, die in der Regel in Form einer Video-/ Telefonkonferenz abgehalten wird, wird ein gemeinsames Verständnis des Vorfalls erarbeitet., sowie mögliche Maßnahmen diskutiert. Darauf aufbauend werden dann die am besten geeigneten weiteren Maßnahmen ausgewählt.

Produkte und Dokumente

Das BSI bietet eine Vielzahl an **Produkten und Dokumenten** an, die Betroffenen präventiv und/oder im Rahmen der Vorfallsbearbeitung zur Verfügung gestellt werden können.

Dazu zählen z.B. insbesondere Dokumente zur Prävention, Detektion und Reaktion bei APT-Vorfällen[5], Hilfsdokumente für die Vorfallsbearbeitung bei schweren IT-Sicherheitsvorfällen bzw. Ransomware-Vorfällen[6] und viele mehr. Auch zum Thema IT-Krisenmanagement und Krisenkommunikation bietet das BSI entsprechende Dokumente als Hilfestellung an.

Auf viele der genannten Dokumente sowie auf eine Vielzahl weiterer Papiere können Unternehmen auch selbstständig, über den **internen Bereich der Allianz für Cyber-Sicherheit**, zugreifen[7].

Persönliche Beratung

Das BSI kann Behörden und Unternehmen insbesondere hinsichtlich

- des **koordinierten und strukturierten Vorgehens** bei Sicherheitsvorfällen
- der **Umsetzung** von **geeigneten Maßnahmen**
- der Durchführung eines angemessenen **IT-Krisenmanagements**
- der passenden **Krisenkommunikation**

beraten. Wie bereits beschrieben, kann dafür auf die gesamte Expertise des BSI zurückgegriffen werden.

Weitergehende Unterstützung

Neben der reinen Beratung, kann das BSI auch bei der **Lagefeststellung und Lagebeurteilung** unterstützen. Hierzu können auch Besprechungen mit technischen Experten/-innen durchgeführt werden, die Ihnen für vertiefende Fachdiskussionen im Rahmen des Vorfalls zur Verfügung stehen.

Darüber hinaus verfügt das BSI über eine Vielzahl **technischer Indikatoren zur Angriffserkennung** (sogenannte Indicators of Compromise (IOC)) und kann Ihnen ggf. passende Indikatoren zur Aufklärung bzw. zum Schutz Ihrer Netze übermitteln.

[5] https://www.allianz-fuer-cybersicherheit.de/Webs/ACS/DE/Informationen-und-Empfehlungen/Empfehlungen-nach-Gefaehrdungen/APT/apt_node.html. Bei Bedarf auch in Englisch verfügbar.
[6] https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Analysen-und-Prognosen/Fortschrittliche-Angriffe/fortschrittliche-angriffe_node.html
[7] https://www.allianz-fuer-cybersicherheit.de: Um alle Dokumente einsehen zu können, ist eine *kostenlose* Registrierung notwendig.

Das BSI bietet Betroffenen zudem an, anonymisierte Angriffs-Indikatoren aus dem Vorfall **mit vertrauenswürdigen Dritten zu teilen**. Dadurch können wertvolle Rückmeldungen, wie weitere Indikatoren oder gar Analysen zurückfließen, ohne dass die Identität des Betroffenen den Dritten bekannt wird.

Technische Analysen

Das BSI verfügt unter anderem über Expertise im Bereich Reverse Engineering, Forensik, Event-/ Loganalysen und Industriesteuerungen. Die entsprechenden Experten können aus dem BSI heraus **Analysen zu einzelnen technischen Fragestellungen** im Rahmen eines Vorfalles durchführen und sie so, z.B. bei der Aufklärung eines Vorfalls, unterstützen.

Mobiles Incident Response Teams (MIRT)

In besonders herausgehobenen Fällen kann das BSI einen **Vor-Ort Einsatz** mit einem Mobilen Incident Response Team (MIRT) durchführen. Das MIRT kann das Unternehmen in einer Vielzahl von Bereichen unterstützen:

- Erstbewertung und Vor-Ort Beratung u.a. zu Maßnahmen und zur Entscheidungsunterstützung
- Grobanalyse und Abschätzung der Konsequenzen
- Sichtung von Logdaten und Alarmen, z.B. aus dem IDS oder SIEM
- Technische Beweissicherung, wie Erstellung von Festplatten-Images oder Aufzeichnung von Netzwerkverkehr sowie technische Analyse im Backoffice
- Beratende Unterstützung des lokalen Betriebspersonals bei der Bereinigung
- Empfehlungen zur Härtung der Systeme

Vermittlung von externen Experten

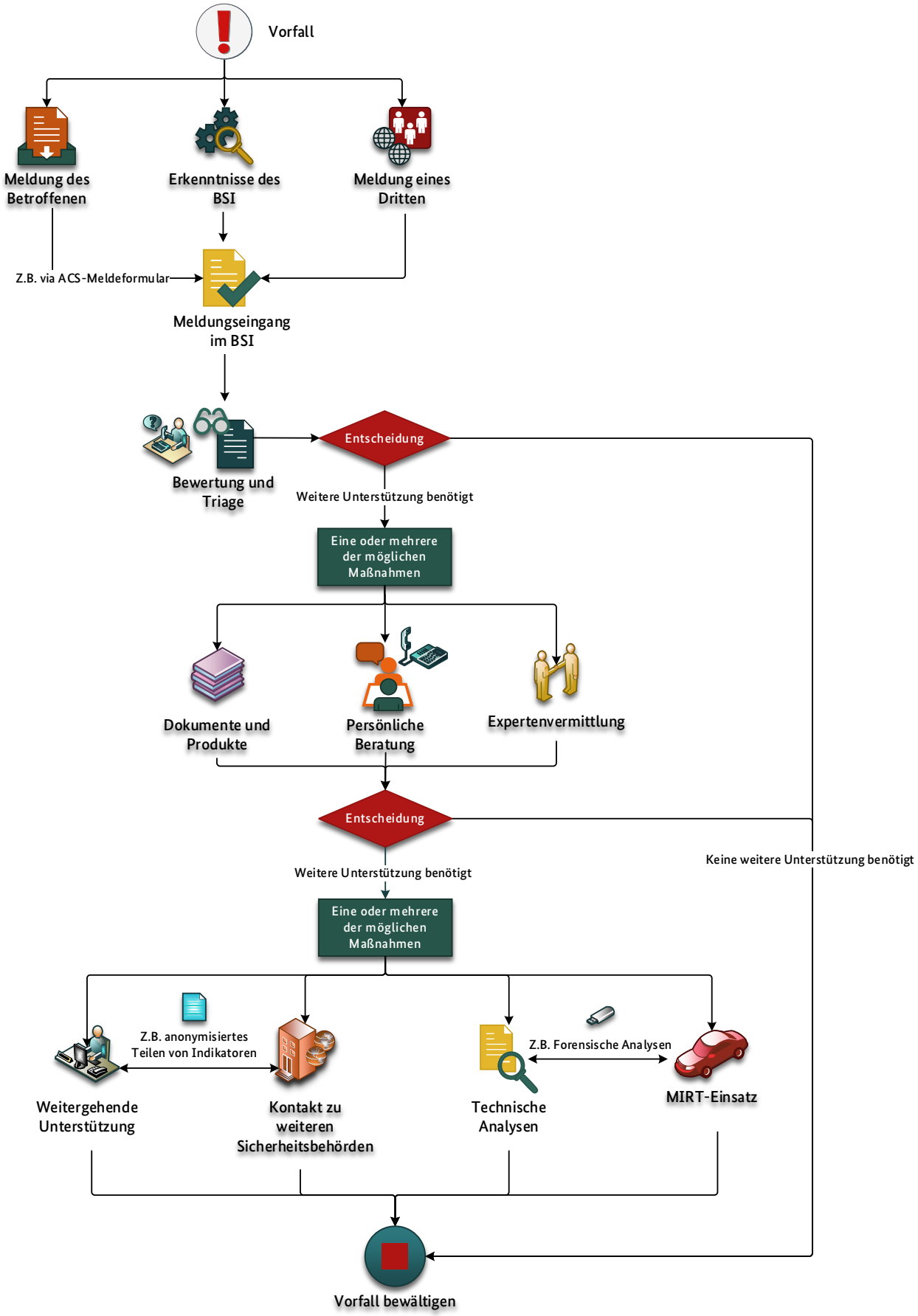
Das BSI kann Unternehmen nicht nur mit der eigenen Expertise unterstützen, sondern auch bei der **Suche nach geeigneten Incident-Response-Dienstleistern** helfen. Hierfür hat das BSI eine Liste **qualifizierter APT-Response-Dienstleister** veröffentlicht[8]. Alle darauf befindlichen Dienstleister wurden anhand der vom BSI festgelegten Kriterien auf ihre Kompetenz beim Umgang mit schwerwiegenden IT-Sicherheitsvorfällen überprüft und konnten sich entsprechend qualifizieren.

Kontakt zu weiteren Sicherheitsbehörden

Das BSI kann die betroffene Organisation **mit Strafverfolgungsbehörden und/oder dem Verfassungsschutz vernetzen**. Diese verfügen mit Einheiten wie der Quick Reaction Force des Bundeskriminalamts (BKA) und den Zentralen Ansprechstellen Cybercrime (ZAC) der Länder über kompetente Ansprechstellen bei IT-Sicherheitsvorfällen. Über die Einbindung weiterer Behörden entscheidet der Betroffene selbst.

Der gesamte Unterstützungsprozess des BSI ist auf der nächsten Seite in Abbildung 1 noch einmal schematisch dargestellt.

[8] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Dienstleister_APT-Response-Liste.pdf?__blob=publicationFile&v=5



1 Schematische Darstellung des Unterstützungsprozesses

4 Frequently Asked Questions (FAQ)

4.1 Muss ich jeden IT-Sicherheitsvorfall an das BSI melden?

Grundsätzlich erfolgt die Meldung eines Sicherheitsvorfalls **auf freiwilliger Basis**. Neben den freiwilligen Meldungen gibt es aber auch einige gesetzliche Regelungen, aufgrund derer eine Meldung an das BSI verpflichtend erfolgen muss. Dazu gehören u.a.:

1. Für Bundesbehörden gilt nach § 4 Abs. 3 BSIG eine Pflicht, das BSI unverzüglich zu unterrichten, wenn dort für die Abwehr von Gefahren für die Sicherheit in der Informationstechnik erforderliche Informationen (insbesondere zu Sicherheitslücken, Schadprogrammen sowie erfolgten oder versuchten Angriffen und der dabei beobachteten Vorgehensweise) bekannt werden. Die genauen Details zur Meldepflicht können der Allgemeinen Verwaltungsvorschrift über das Meldeverfahren gemäß § 4 Abs. 6 BSIG entnommen werden.
2. Für Betreiber Kritischer Infrastrukturen, die oberhalb der Schwellenwerte der BSI-Kritisverordnung liegen, gilt bei IT-Störungen die Meldepflicht des § 8b Absatz 4 BSIG. Mit dem Gesetz zur Umsetzung der europäischen Richtlinie zur Gewährleistung einer hohen Netzwerk- und Informationssicherheit (NIS-Richtlinie) erweiterte sich diese Meldepflicht auf alle Energieversorgungsnetzbetreiber gemäß § 11 Absatz 1c EnWG.
3. Für Betreiber Kritischer Infrastrukturen unterhalb der Schwellenwerte der BSI-Kritisverordnung, gilt die unter Punkt 1 aufgeführte Meldepflicht nicht, mit Ausnahme der Betreiber von Energieversorgungsnetzen. Sie können dennoch freiwillige Meldungen über IT-Sicherheitsvorfälle und Cyber-Angriffe über die Meldestelle der Allianz für Cyber-Sicherheit abgeben.
4. Für Anbieter digitaler Dienste (Online-Marktplätze, Online-Suchmaschinen, Cloud-Computing-Dienste) gilt die Meldepflicht auf Grundlage des § 8c Absatz 3 BSIG. Die Meldepflicht gilt für Sicherheitsvorfälle, die erhebliche Auswirkungen auf die Bereitstellung digitaler Dienste haben, die innerhalb der Europäischen Union erbracht werden.
5. Betreiber von Telekommunikationsnetzen und Telekommunikationsdiensten haben bei Sicherheitsverletzungen die Meldepflicht gemäß § 109 Absatz 5 TKG zu befolgen und diese an das BSI sowie die Bundesnetzagentur zu melden.
6. Gemäß der eIDAS-Verordnung sind qualifizierte und nicht qualifizierte Vertrauensdiensteanbieter dazu verpflichtet, dem BSI unverzüglich jede Sicherheitsverletzung oder jeden Integritätsverlust zu melden, die bzw. der sich erheblich auf den erbrachten Vertrauensdienst oder die darin vorhandenen personenbezogenen Daten auswirkt. Die Meldung hat in jedem Fall innerhalb von 24 Stunden nach Kenntnisnahme von dem betreffenden Vorfall zu erfolgen.

4.2 Wie kann ich das BSI erreichen?

✋ ACHTUNG ✋
Es sollte **keine Kommunikation über ein vermeintlich kompromittiertes Netzwerk** initiiert werden. Nutzen Sie für die Erst-Kommunikation einen Festnetz-Anschluss, sofern dieser nicht intern als IP-Telefonie ausgeführt und mit ihrem Netzwerk gekoppelt ist. Alternativ nutzen sie ein Handy, welches nicht mit dem Unternehmensnetzwerk synchronisiert ist.

Freiwillige Meldungen können am einfachsten über das **Online-Meldeformular der Allianz für Cybersicherheit**[9] abgegeben werden. Dort können Sie auch angeben, ob Sie eine Kontaktaufnahme bzw. Unterstützung durch das BSI wünschen.

Unterstützungsersuchen bei Vorfällen bei Betreibern Kritischer Infrastrukturen (gem. BSI-Kritisverordnung) und Institutionen der Bundesverwaltung werden zentral durch das Nationale IT-Lagezentrum des BSI entgegengenommen. Dieses können Sie rund um die Uhr (24/7) erreichen.

Die Kontaktdaten liegen den jeweiligen Zielgruppen als „Visitenkarte Lagezentrum“ vor und sind auch im Melde- und Informationsportal (MIP) des BSI im Nutzerbereich verfügbar.

4.3 Behandelt das BSI meine Meldung vertraulich?

Das BSI behandelt Meldungen strikt nach dem "**Need-to-know-Prinzip**". Das bedeutet, dass die Quelle durchgängig Herr der von ihr zur Verfügung gestellten Informationen ist. Der Betroffene bestimmt selbst, welche Informationen durch das BSI anonymisiert oder sanitarisiert an Dritte weitergegeben werden können. Ausgenommen davon sind etwaige gesetzliche Verpflichtungen.

Das BSI befürwortet grundsätzlich, dass IT-Sicherheitsvorfälle, gerade wenn es sich um Spionage oder Sabotage handelt, zur Anzeige gebracht werden. Hierüber entscheidet aber der Betroffene. Das BSI ist nicht verpflichtet in solchen Fällen Strafanzeige zu stellen.

Meldungen von Betreibern von Kritischen Infrastrukturen (gem. BSI-Kritisverordnung) sowie die im Rahmen von Meldungen behandelten Vorfälle sind zudem von Anfragen nach dem Informationsfreiheitsgesetz (IFG) ausgenommen (BSIG §8e).

4.4 Was kostet mich die Unterstützungsleistung des BSI?

Soweit das BSI erste Maßnahmen zur Schadensbegrenzung und Sicherstellung des Notbetriebes vor Ort ergreift, werden hierfür keine Gebühren oder Auslagen für die Tätigkeit des Bundesamtes erhoben. Hiervon unberührt bleiben etwaige Kosten für die Hinzuziehung qualifizierter Dritter (BSIG § 5b, Satz 1).

[9] https://www.allianz-fuer-cybersicherheit.de/Webs/ACS/DE/IT-Sicherheitsvorfall/Unternehmen/Online-Meldung/online-meldung_node.html

4.5 Wie kann das BSI mir helfen, wenn ich keiner der gesetzlich definierten Zielgruppen angehöre?

Auch wenn Sie keiner der gesetzlich definierten Zielgruppen angehören, kann das BSI Sie bei einem IT-Sicherheitsvorfall unterstützen:

Zertifizierte APT-Response- und IT-Sicherheits-Dienstleister

Auf den Webseiten des BSI findet man **Listen mit zertifizierten APT-Response- und IT-Sicherheits-Dienstleistern**. Das BSI hat bei diesen Dienstleistern eine Kompetenzfeststellung durchgeführt. Sollten Sie Unterstützung bei einem Vorfall benötigten, empfiehlt das BSI einen dieser Dienstleister zu beauftragen:
https://www.bsi.bund.de/DE/Themen/ZertifizierungundAnerkennung/Listen/Listen_node.html
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Dienstleister_APT-Response-Liste.html

Allianz für Cybersicherheit

Viele Informationen und Hilfsdokumente zum Thema IT-Sicherheit finden Sie auf den Seiten der **Allianz für Cybersicherheit**: https://www.allianz-fuer-cybersicherheit.de.
*Hinweis: Um alle Dokumente einsehen zu können, ist eine *kostenlose* Registrierung notwendig.*

UP KRITIS

Darüber hinaus informiert das BSI staatliche Stellen, Kritische Infrastrukturen und wichtige andere Organisation regelmäßig mit relevanten und wichtigen Warnmeldungen. Hierfür müssen die in Frage kommenden Organisationen dem BSI aber bekannt sein. Daher gibt es für bestimmte Organisationen die Möglichkeit, dem **UP KRITIS** beizutreten. Die Teilnahme ist *kostenfrei*. Der UP KRITIS ist eine öffentlich-private Kooperation zwischen Betreibern Kritischer Infrastrukturen (KRITIS), deren Verbänden und den zuständigen staatlichen Stellen. Der UP KRITIS bietet diesen Organisationen, bei Betreibern Kritischer Infrastrukturen auch unabhängig davon, ob sie aufgrund ihrer Größe unter die Regulierung des BSI-Gesetzes (BSIG) fallen, eine unverbindliche Organisationsplattform. Dadurch haben Sie auch die Möglichkeit, sich vertraulich mit anderen Teilnehmern auszutauschen. Alle relevanten Informationen sowie Voraussetzungen für den Beitritt finden Sie unter den folgenden Links:
https://www.kritis.bund.de/SubSites/Kritis/DE/Aktivitaeten/Nationales/UPK/upk_node.html
https://www.kritis.bund.de/SubSites/Kritis/DE/Aktivitaeten/Nationales/UPK/Kontakt/UPK_Kontakt.html?nn=1902622
https://www.kritis.bund.de/SharedDocs/Downloads/Kritis/DE/UP_KRITIS_Flyer.pdf?__blob=publicationFile

Verbraucher*innen (ehemals „BSI für Bürger“)

Bürger finden Unterstützung auf den Webseiten des **BSI** und können sich mit ihren Fragen an das Service-Center wenden:
https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/verbraucherinnen-und-verbraucher_node.html
Service-Center Hotline: 0800 2741000
E-Mail: mail@bsi-fuer-buerger.de
Kostenlos aus dem deutschen Fest- und Mobilfunknetz, Erreichbarkeit: Mo. bis Fr. von 8:00 bis 18:00 Uhr

Abkürzungsverzeichnis

ACS	Allianz für Cybersicherheit
APT	Advanced Persistent Threat
BfV	Bundesamt für Verfassungsschutz
BKA	Bundeskriminalamt
BND	Bundesnachrichtendienst
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSIG	Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz - BSIG)
BSI-KritisV	Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-Kritisverordnung)
CERT	Computer Emergency Response Team
CYBER-AZ	Cyber-Abwehrzentrum
eIDAS	electronic Identification, Authentication and trust Services
EnWG	Energiewirtschaftsgesetz / Gesetz über die Elektrizitäts- und Gasversorgung
IDS	Intrusion Detection System
IFG	Informationsfreiheitsgesetz
IOC	Indicators of Compromise
LfV	Landesamt für Verfassungsschutz
LKA/LKÄ	Landeskriminalamt/Landeskriminalämter
MIRT	Mobile Incident Response Team
MIP	Melde- und Informationsportal
NIS	Netz- und Informationssicherheit
KRITIS	Kritische Infrastrukturen
SIEM	Security Information and Event Management
SPOC	Single Point of Contact
TKG	Telekommunikationsgesetz
UP KRITIS	Umsetzungsplan KRITIS
ZAC	Zentrale Ansprechstelle Cybercrime

Übersicht über externe Unterstützungsmöglichkeiten

Externer Experte	*Information*	*Link*
BSI	Meldeformular ACS	https://www.allianz-fuer-cybersicherheit.de/Webs/ACS/DE/IT-Sicherheitsvorfall/Unternehmen/Online-Meldung/online-meldung_node.html
	CERT-Bund	https://www.bsi.bund.de/CERT-Bund
Landes- bzw. Bundesamt für Verfassungsschutz	Liste der Erreichbarkeiten	https://www.wirtschaftsschutz.info/DE/Ansprechpartner/Verfassungsschutz/verfassungsschutz_node.html
Polizeien	Liste der Erreichbarkeiten	https://www.polizei.de/Polizei/DE/Einrichtungen/ZAC/zac_node.html
APT-Response Dienstleister	Qualifizierte APT-Response Dienstleister	https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Dienstleister_APT-Response-Liste.html
Initiative Wirtschaftsschutz	Kooperation von BfV, BKA, BND und BSI	https://www.wirtschaftsschutz.info
Allianz für Cyber-Sicherheit	Initiative von BSI und bitkom	https://www.allianz-fuer-cybersicherheit.de/