

Nationales IT-Lagezentrum –

oder:

Wann müssen Sicherheitsvorfälle an das BSI gemeldet werden, und was passiert dort mit diesen Meldungen?

Isabel Münch, Fachbereichsleiterin IT-Sicherheitslage

GI SECMGT-Workshop, Frankfurt 24.11.2023

Gliederung

- Das BSI
- Wann muss ich melden?
- Wie melde ich?
- Wo landen die Meldungen?



Das BSI



Bundesamt
für Sicherheit in der
Informationstechnik

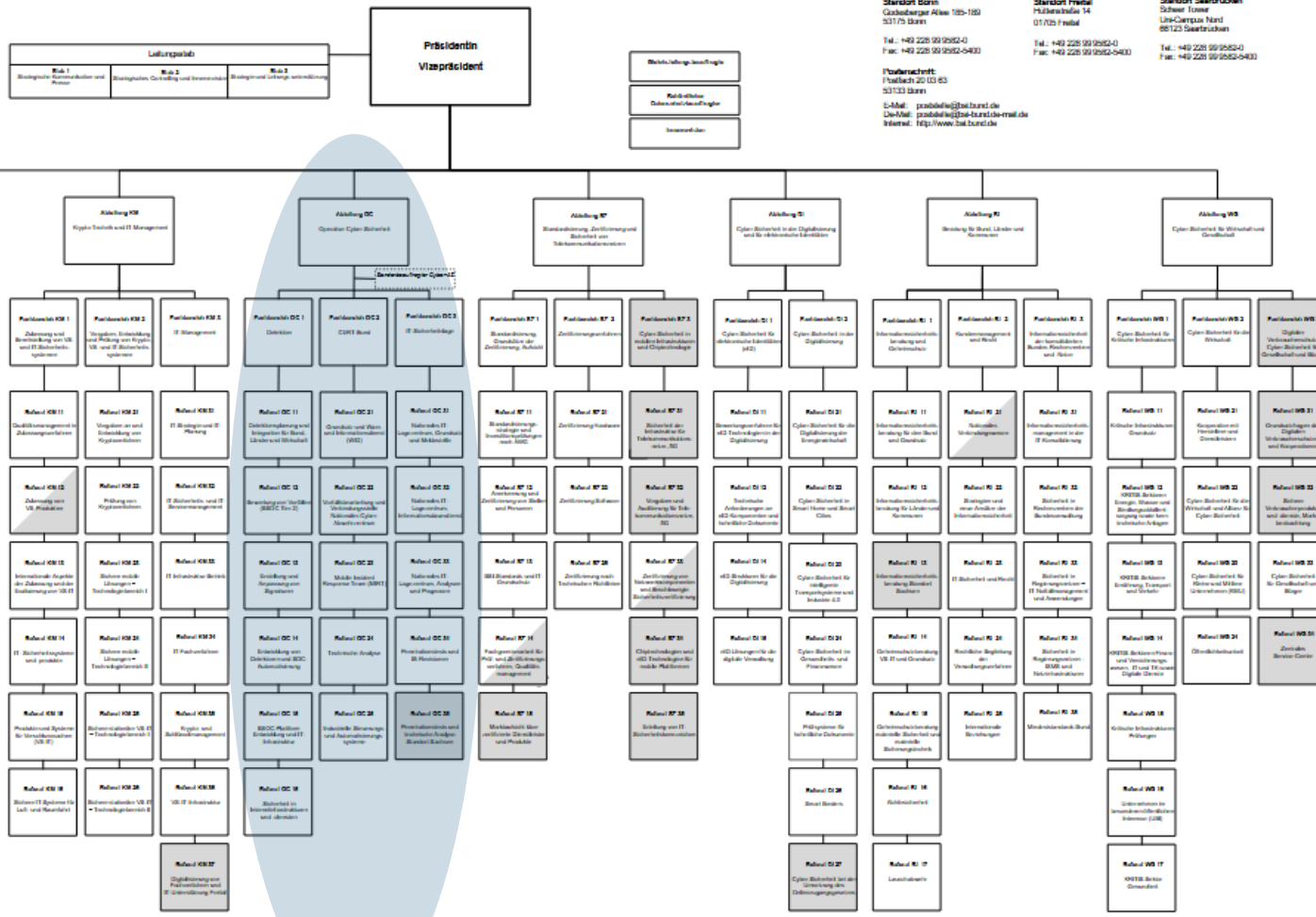
Deutschland
Digital•Sicher•BSI•

Das BSI als die Cyber-Sicherheitsbehörde des Bundes gestaltet Informationssicherheit in der Digitalisierung durch Prävention, Detektion und Reaktion für Staat, Wirtschaft und Gesellschaft.



Organisationsplan

Stand: 15.07.2025



Standort Bonn
Godesberger Allee 185-189
53175 Bonn
Tel.: +49 228 99 9582-0
Fax: +49 228 99 9582-6400

Standort Freibal
Hübenerstraße 14
01705 Freibal
Tel.: +49 228 99 9582-0
Fax: +49 228 99 9582-6400

Standort Saarbrücken
Schwarzer Tower
Linien-Campus Nord
66123 Saarbrücken
Tel.: +49 228 99 9582-0
Fax: +49 228 99 9582-6400

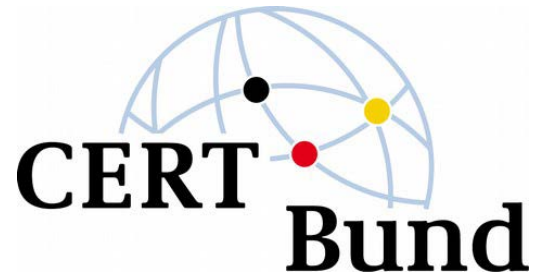
Funktionen:
1. Juli 2025 03:05
53133 Bonn
E-Mail: problemliste@bsi.bund.de
De-Mail: problemliste@bsi.bund.de-trial.de
Internet: <http://www.bsi.bund.de>

- Organisationsstellen am Standort Bonn
- Organisationsstellen am Standort Freibal
- Organisationsstellen am Standort Saarbrücken
- Organisationsstellen am Standort Bonn und Saarbrücken

Nationales
IT-Lagezentrum



BSOC



MIRT

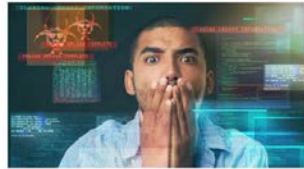


Wann muss ich melden?



Melden Sie!

- Alle Meldungen helfen – Ihnen, uns und anderen!



Ich habe einen Vorfall – Was soll ich tun?

> Mehr



Ich habe einen Vorfall – Checkliste Organisatorisches

> Mehr



Ich möchte einen IT-Sicherheitsvorfall melden.

> Mehr

Unternehmen: Einen Vorfall
bewältigen, melden, sich informieren,
vorbeugen

IT-Grundschutz (Baustein DER.2.1 - „Behandlung von Sicherheitsvorfällen“)

- DER.2.1.A1 Definition eines Sicherheitsvorfalls
- DER.2.1.A2 Erstellung einer Richtlinie zur Behandlung von Sicherheitsvorfällen
- DER.2.1.A3 Festlegung von Verantwortlichkeiten und Ansprechpartnern bei Sicherheitsvorfällen
- DER.2.1.A4 Benachrichtigung betroffener Stellen bei Sicherheitsvorfällen
- DER.2.1.A5 Behebung von Sicherheitsvorfällen
-
- DER.2.1.A9 Festlegung von Meldewegen für Sicherheitsvorfälle
-
- DER.2.1.A22 Überprüfung der Effizienz des Managementsystems zur Behandlung von Sicherheitsvorfällen

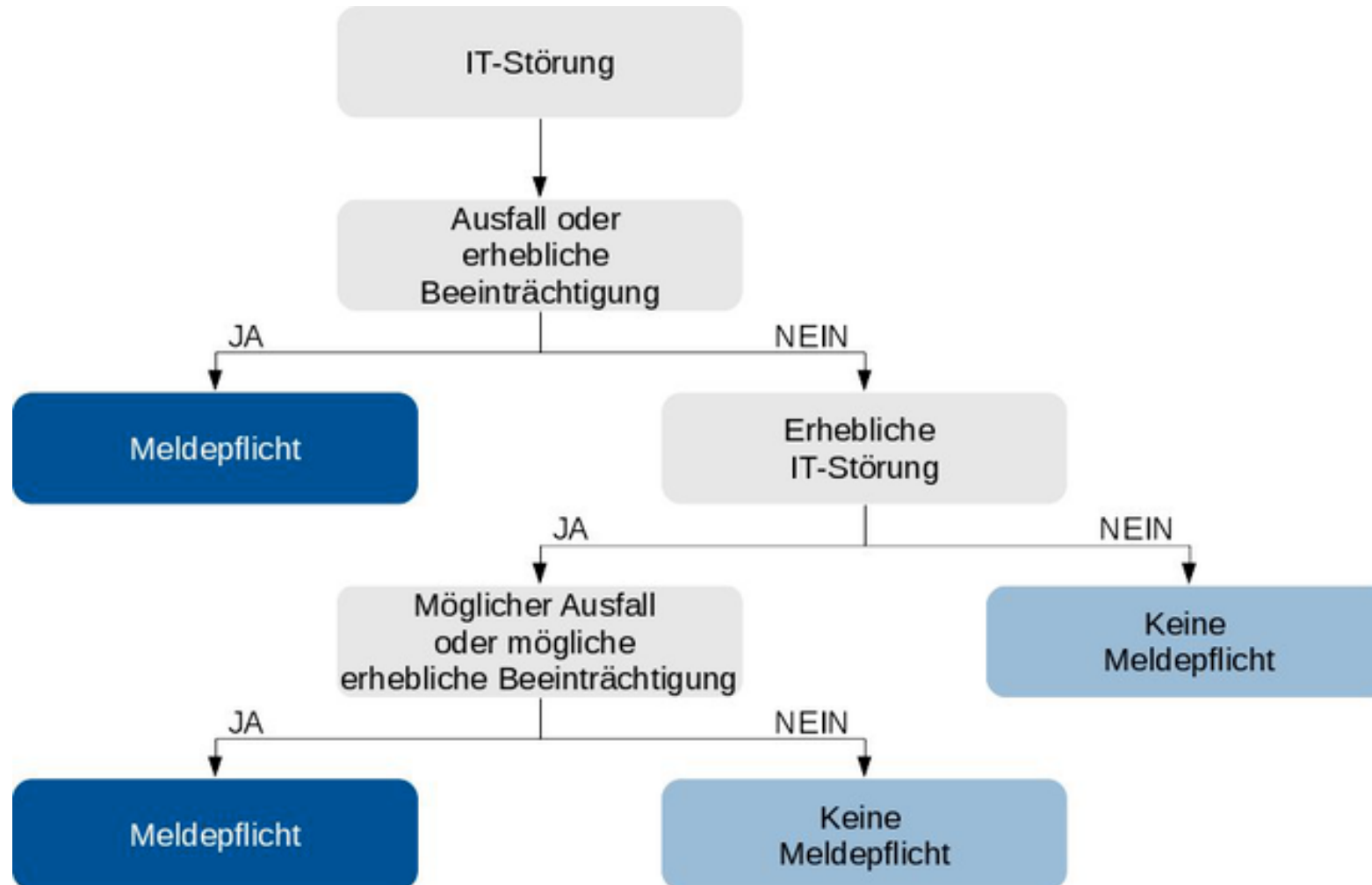
Kritische Infrastrukturen (als Beispiel)

Gesetzestext des § 8b Absatz 4 BSIG:

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

1. 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,
2. 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. [...]

Meldekriterien für IT-Störungen



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.

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

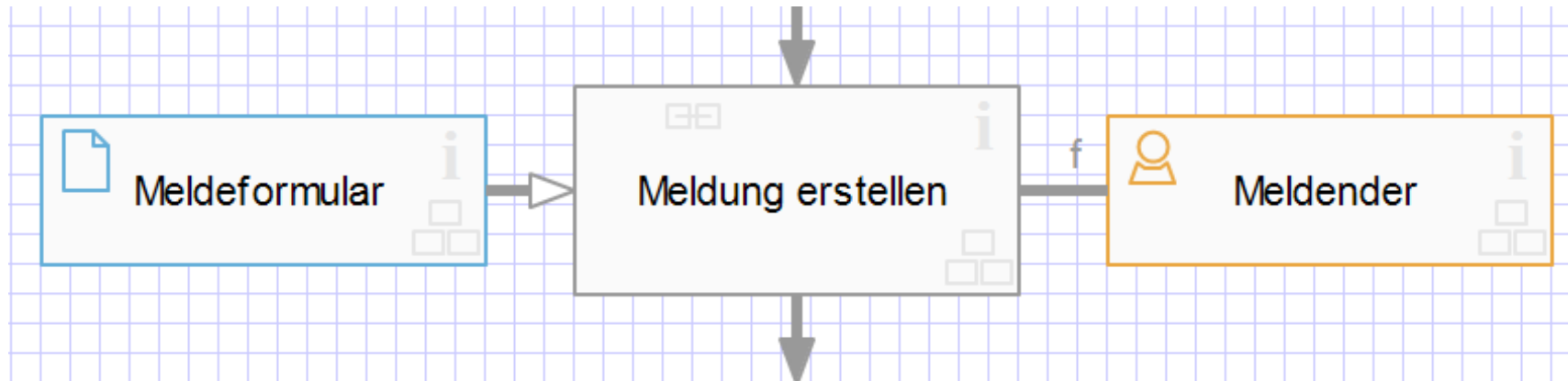
- ein Bagger, der ein Kabel durchtrennt,
- ein Ausfall der Kühlung eines Rechenzentrums,
- ein falsch konfiguriertes System,
- ein fehlerhaftes Update oder ein fehlerhafter Patch, der eingespielt wird.



Wie melde ich?



Meldung erstellen und versenden



- 01 LP-Burel
- 02 LP-KOITSE
- 03 KTH
- 04 NAB
- 05 VOV
- 06 AIG-gau
- 07 TKS-gau
- 08 sonstige Meldung
- 09 KKH (gau-gau)
- 10 BUND-g11 (g)
- 11 Demand (g11-g)
- 12 GEP-g11-gau
- 13 eGAP
- 14 MBO
- 15 ACP
- 16 PECO (g11-gau)
- 17 LUB
- 18 eC
- 19 Burel
- 20 LUB

Melde- und Informationsportal (MIP)

<https://mip2.bsi.bund.de/meldestellen-uebersicht/>



ANLEITUNGEN BARRIEREFREIHEIT FAQ   ...

Melde- und Informationsportal

Übersicht und Erläuterung der Meldestellen

- Meldestelle Allianz für Cybersicherheit
- Meldestelle Bund (§ 4 BSIG)
- Meldestelle KRITIS
 - IT-Sicherheitsgesetz, BSI-Gesetz und BSI-Kritisverordnung
 - Kontaktstelle benennen
 - Meldepflicht
 - Registrierung
 - Registrierung für Behörden / Aufsichtsbehörden/ Zentrale Kontaktstellen der Länder
 - Änderungen an den Registrierungsdaten an das BSI übermitteln
- Meldestelle Schwachstellen und Sicherheitslücken



Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI

Allianz für Cybersicherheit

https://mip2.bsi.bund.de/meldungen/meldung-ohne-registrierung-erstellen/?meldestelle=10&formular=32



ANLEITUNGEN BARRIEREFREIHEIT FAQ   ...

Melde- und Informationsportal

Meldung ohne Registrierung abgeben

Bitte wählen Sie zunächst die Meldestelle, bei der Sie eine Meldung abgeben möchten. Anschließend werden Ihnen die verfügbaren Formulare angezeigt.

Meldestelle

Allianz für Cyber-Sicherheit

Meldeformular

Sicherheitsvorfälle und Cyber-Angriffe

Captcha



Formular ausfüllen



Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

§ 4 BSIG + Verwaltungsvorschrift

SOFORT-Meldung

STATISTISCHE Gesamtmeldung

Einstufung	(-) Offen	(-) VS-ND	(-) VS-Vertraulich	Über-Einstufung OFFEN bei Einstufung VAA beachten!
SOFORT-Meldung-IT-Vorfall				
Behörde				
Meldender				
Erreichbarkeit				
Rückfragen				
Datum				
Uhrzeit				
Vorläufige Klassifizierung durch den Meldenden				
Externer Angriff	(-) ja/nein	(-) Abgewehrt-Schadprogramm	(-) Erfolgreiche Installation eines Schadprogramms	(-) Systemsturz
Datenverlust	(-) Inaktiviert-Sperre	(-) Datenabfluss durch Spionage	(-) Manipulation von Hard- oder Software	(-) DDoS
Sicherheitslücke	(-) Diebstahl oder sonstiger Verlust IT-Systeme	(-) Diebstahl oder sonstiger Verlust Daten	(-) Unschlüssige Entwertung	(-) Offenlegung durch unautorisiertes Personal
Störung von SW/HW-Komponenten	(-) Schweregradiger Ausfall von Betriebsmitteln	(-) Schweregradige fehlerhafte Funktion	(-) Schweregradige Überlastsituation	
Widerrechtl. Aktion	(-) ja			
Interne Ursachen	(-) ja			
Externe Einflüsse	(-) Naturgeschehen	(-) Beschädigung		
Bes. Erkenntnisse	(-) ja			
Zweck der Information / Erwartete Reaktion durch das BSI-IT-LZ				
	(-) Zur Kenntnisnahme	(-) Freigabe zur Aufhebung von Lagerbeständen	(-) Explizite Freigabe der Freilassung zur Aufhebung von Lagerbeständen	(-) Nachvollziehbarkeit durch BSI-IT-LZ
	(-) Bitte um Rückmeldung	(-) Bitte um Einreichung von Stellungnahmen	(-) Umstellung auf andere Verfahren	(-) Nachvollziehbarkeit durch BSI-IT-LZ
Sachverhalt				
Textfeld für den Sachverhalt: Was ist passiert? Was ist die Ursache? Welche Schäden wurde bereits beobachtet? In wie weit ist die betroffene Komponente betroffen? Welche bereits (Jahre) Maßnahmen wurden ergriffen? Was ist die Ursache? Welche bereits (Jahre) Maßnahmen wurden ergriffen?				
Vorschläge des Meldenden zum weiteren Vorgehen				
OPTIONAL				
Sonstiges / freie Anmerkungen				
OPTIONAL				
Zurücksenden	BSI IT-Lage- und Analysezentrum ->lagenstrom@bsi.bund.de; 02299 9502 5110			

Einstufung	(-) Offen	(-) VS-ND	(-) VS-Vertraulich	Über-Einstufung OFFEN bei Einstufung VAA beachten!
Statistische Gesamtmeldung-IT-Vorfälle				
Behörde				
Meldender				
Erreichbarkeit				
Rückfragen				
Berichtszeitraum				
Zusammenfassung der Ereignisse				
Anzahl der Vorfälle insgesamt				
1. Abgewehrtes Schadprogramm	<input type="checkbox"/>			
2. Erfolgreiche Installation eines Schadprogramms	<input type="checkbox"/>			
3. Systemeinbruch	<input type="checkbox"/>			
4. Unautorisierte Systemnutzung	<input type="checkbox"/>			
5. Datenabfluss durch Schadprogramme oder Hacker	<input type="checkbox"/>			
6. Manipulation von Hard- oder Software	<input type="checkbox"/>			
7. DDoS	<input type="checkbox"/>			
8. Diebstahl oder sonstiger Verlust IT-Systeme	<input type="checkbox"/>			
9. Diebstahl oder sonstiger Verlust Datenträger	<input type="checkbox"/>			
10. Unschlüssige Entsorgung	<input type="checkbox"/>			
11. Offenlegung durch unautorisiertes Personal	<input type="checkbox"/>			
12. Sicherheitslücke	<input type="checkbox"/>			
13. Schweregradiger Ausfall von Betriebsmitteln	<input type="checkbox"/>			
14. Schweregradige fehlerhafte Funktion	<input type="checkbox"/>			
15. Schweregradige Überlastsituation	<input type="checkbox"/>			
16. Widerrechtliche Aktion, Verstoß IT-Sicherheitsrichtlinie	<input type="checkbox"/>			
17. Interne Ursachen	<input type="checkbox"/>			
18. Naturgeschehen	<input type="checkbox"/>			
19. Beschädigung	<input type="checkbox"/>			
20. Besondere Erkenntnisse	<input type="checkbox"/>			
Sonstiges / freie Anmerkungen				
OPTIONAL				
Zurücksenden	BSI IT-Lage- und Analysezentrum ->lagenstrom@bsi.bund.de; 02299 9502 5110			

Wie schnell muss ich melden?

Die Meldung nach § 8b BSIG 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.**

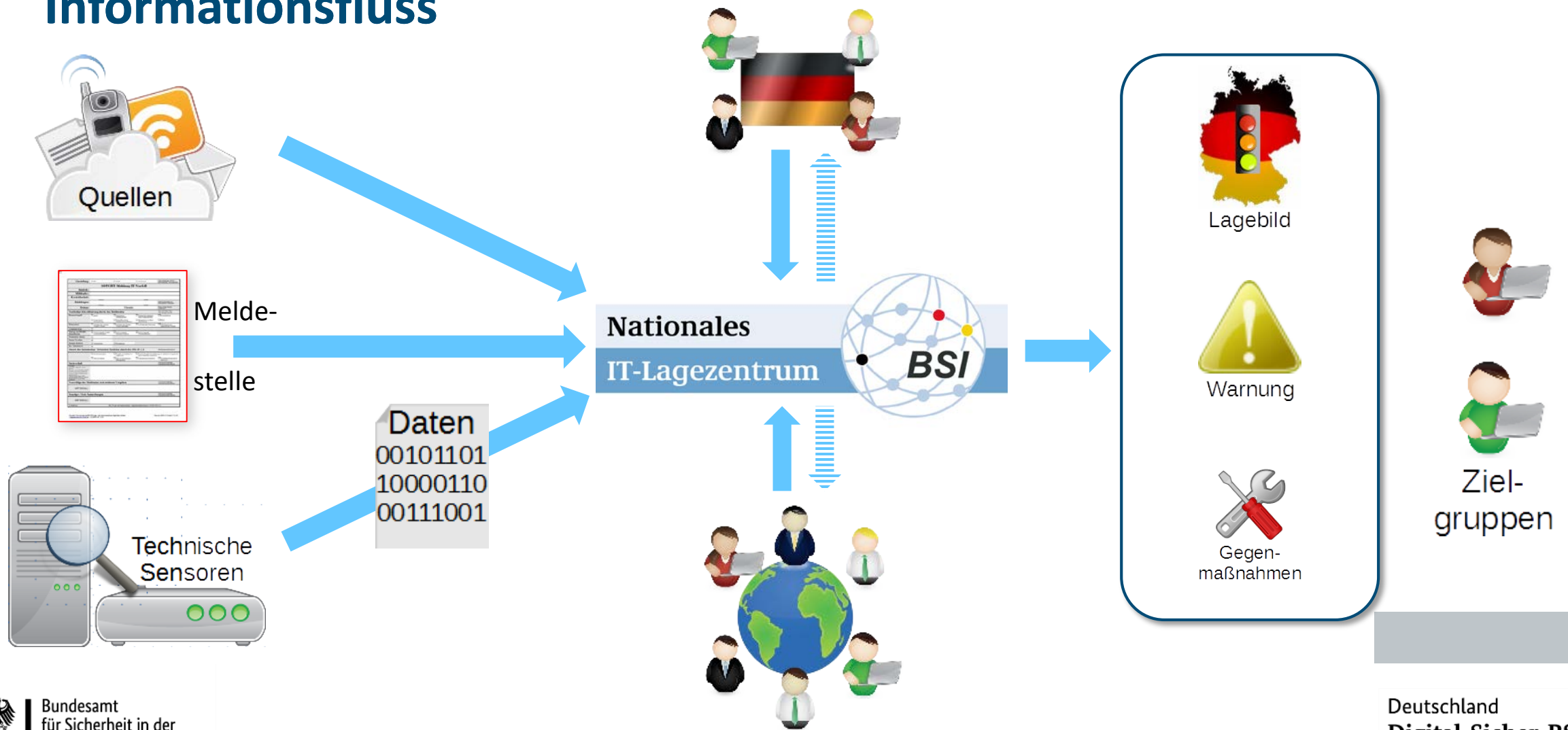
Wo landen die Meldungen?



Nationales IT-Lagezentrum

Das IT-Lagezentrum verfügt **jederzeit** über ein **verlässliches Bild** der **aktuellen IT-Sicherheitslage** in Deutschland, um den **Handlungsbedarf** und die **Handlungsoptionen** bei IT-Sicherheitsvorfällen sowohl auf staatlicher Ebene als auch in der Wirtschaft **schnell und kompetent einschätzen zu können**.

Informationsfluss



IT-Lageberichte

jede Zielgruppe hat anderen Bedarf:

... andere Themen (technisch vs. politisch)

... andere Freigaben/Vertraulichkeitsvereinbarungen

... andere Passwörter für Verschlüsselung

... andere Formatvorlagen (z.B. auch Kategorien)

... andere Empfänger

... andere Abhängigkeiten

... usw.

Übersicht

Nr.	Titel	Version	Zielgruppen	Grundeinstufung	Status
2021-180976 (01.02.2021, 21:49)	0-day Schwachstelle der SonicWall Secure Mobile Access Serie		BY: offen, bu, LPK: offen, rest, VCV: offen, rest, ACS: offen, rest, CV: offen, rest, Fra4: offen, rest, IT-SIG: offen, rest	offen, bu / offen, rest	abgeschlossen GF
2021-180841 (16.01.2021, 14:38)	Schwachstelle in ABB PLCs der Reihe ACS100 V2	1.0	Energie: TLP:GREEN, Wasser: TLP:GREEN	offen, bu / TLP:GREEN	abgeschlossen GF
2021-180708 (05.01.2021, 15:01)	Veröffentlichung eines Exploit-Codes für die kritische Schwachstelle in SAP Solution Manager 7.2 (CVE-2020-6207)	1.0	BY: offen, bu, LPK: TLP:GREEN, VCV: TLP:GREEN, ACS: TLP:GREEN, CV: TLP:GREEN, Fra4: TLP:GREEN, IT-SIG: TLP:GREEN	offen, bu / TLP:GREEN	abgeschlossen GF
2021-180557 (19.01.2021, 16:48)	Schwachstelle in Bachmann Controllern	1.0	UStk: TLP:AMBER	VS: MID / TLP:AMBER	abgeschlossen GF
2020-533849 (02.12.2020, 16:12)	Schwachstellen in Komponenten des Netzwerkstack von Treck	1.0	LPK: TLP:GREEN, ACS: TLP:GREEN, IT-SIG: TLP:GREEN	offen, bu / TLP:GREEN	abgeschlossen GF
2020-533721 (02.12.2020, 16:05)	Schwachstellen in FTC Keypware KEP Server	1.0	UKEnergie: TLP:GREEN, UWasser: TLP:GREEN, Energie: TLP:GREEN, Wasser: TLP:GREEN	offen, bu / TLP:GREEN	abgeschlossen GF
2020-533588 (21.12.2020, 11:26)	Schwachstellen in ABB Symphony, Harmony und Melody Produkten sowie CLS	1.0	UKEnergie: TLP:GREEN, UWasser: TLP:GREEN, Energie: TLP:GREEN, Wasser: TLP:GREEN	offen, bu / TLP:GREEN	abgeschlossen GF
2020-533036 (11.12.2020, 22:42)	Online-Kampagne ruft zur massenhaften Kontaktierung von COVID-19 Impfstoffherstellern auf	1.0	Man: TLP:GREEN	offen, bu / TLP:GREEN	abgeschlossen GF
2020-532768 (01.12.2020, 11:06)	Schwachstellen in Open Source Netzwerkstacks (AMNESIA-33)		BY: offen, bu, LPK: TLP:GREEN, VCV: TLP:GREEN, ACS: TLP:GREEN, CV: TLP:GREEN, Fra4: TLP:GREEN, IT-SIG: TLP:GREEN	VS: MID / offen, rest	abgeschlossen GF
2020-516205 (01.11.2020, 11:39)	Schwachstelle in RTU Easergy T300 von Schneider Electric	1.0	UStk: TLP:GREEN, UStk: TLP:GREEN	offen, bu / TLP:GREEN	abgeschlossen GF
2020-516141 (11.11.2020, 18:39)	Kritische Schwachstellen in Apple iOS mit Auswirkung auf SecurePM	1.0	BY: VS: MID	VS: MID / TLP:RED	abgeschlossen GF

Wie bedroht ist Deutschlands Cyberraum?

- **Ransomware** ist weiterhin die größte Bedrohung.
- Vermehrt wurden **kleine und mittlere Unternehmen (KMU) sowie Kommunalverwaltungen und kommunale Betriebe** angegriffen.
- Mehr als **zwei erfolgreiche Ransomware-Angriffe** auf Kommunalverwaltungen oder kommunale Betriebe wurden im Durchschnitt **in jedem Monat** bekannt.
- Außerdem hat das BSI den **Ausbau einer Schattenwirtschaft** cyberkrimineller Arbeitsteilung beobachtet.



IT-Sicherheitswarnungen

Verschiedene Warnstufen

- Grau:** Information/Kenntnisnahme → einige
- Gelb:** zeitnahes Handeln erforderlich → Regel
Schwachstelle von hoher Relevanz,
Wurmausbruch
- Orange:** unmittelbare Reaktion erforderlich → Dutzende
Schwerwiegende Schwachstelle,
Sicherheitsvorfall
- Rot:** schnellstmögliche Reaktion → Sehr selten
Sehr schwerwiegender Sicherheitsvorfall,
IT-Krise



IT-Krisenreaktionszentrum

Das IT-Krisenreaktionszentrum stellt die **schnelle Reaktion** auf **schwerwiegende Vorfälle** sicher, um so **rechtzeitige Gegenmaßnahmen** zu ermöglichen und **Schäden** in größerem Ausmaß zu **vermeiden**.



Aufwuchs zum IT-Krisenreaktionszentrum

Vorbereitete Räumlichkeiten (LZ) mit technischer Unterstützung (z.B. SATCOM, 2. TK-Anlage, Notstrom, BOS-Digitalfunk, ...) und Verfahren (Stabarbeitshilfen ...)

Aufwuchs aus dem Nationalen IT-Lagezentrum (Das Lagezentrum bleibt als Konstante erhalten!)

Krisenlagenbezogene Stabsorganisation (BAO)

Besetzung Meldungseingang (Meldekopf, Sichter)

→ zentraler Ein-/Ausgang zur Kanalisierung von Informationsflüssen

Rollen Lagebeobachter, Dokumentation, Visualisierung

Stabsgebiet „Lage“ (S2) / Koordinierungsgruppe

Leiter Krisenreaktion (LKR) nach Redundanzmodell

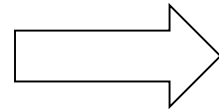
Nachalarmierte Experten aus den Fachreferaten nach Redundanzmodell



Zusammenfassung

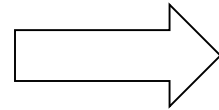
Zusammenfassung

Vorfall



Meldewege

Information

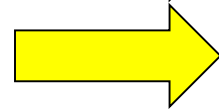


Meldeformulare

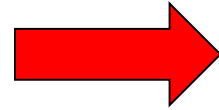
Bearbeitung im Nationalen IT-Lagezentrum



Lagebild



Warnung



Gegenmaßnahmen

Vielen Dank für Ihre Aufmerksamkeit!

Kontakt

Isabel Münch

Fachbereichsleiterin OC3

isabel.muench@bsi.bund.de

Tel. +49 (0) 228 9582 5367

Fax +49 (0) 228 10 9582 5367

Bundesamt für Sicherheit in der
Informationstechnik (BSI)

Godesberger Allee 185-189

53175 Bonn

www.bsi.bund.de

www.bsi-fuer-buerger.de

Deutschland
Digital•Sicher•BSI•



Bundesamt
für Sicherheit in der
Informationstechnik