Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

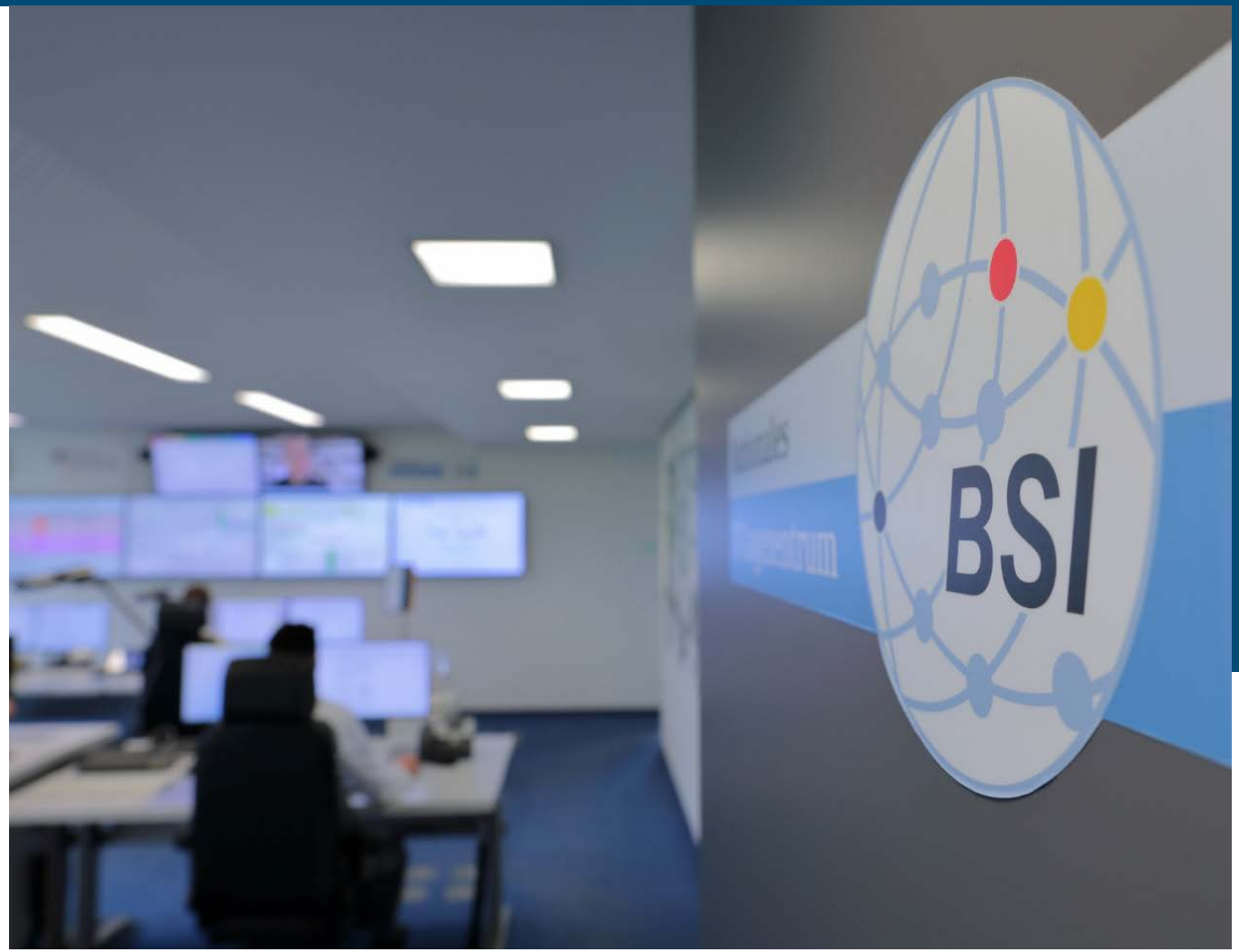
Nationales IT-Lagezentrum –
oder:
Wann müssen Sicherheitsvorfälle an das BSI gemeldet werden, und was passiert dort mit diesen Meldungen?

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?



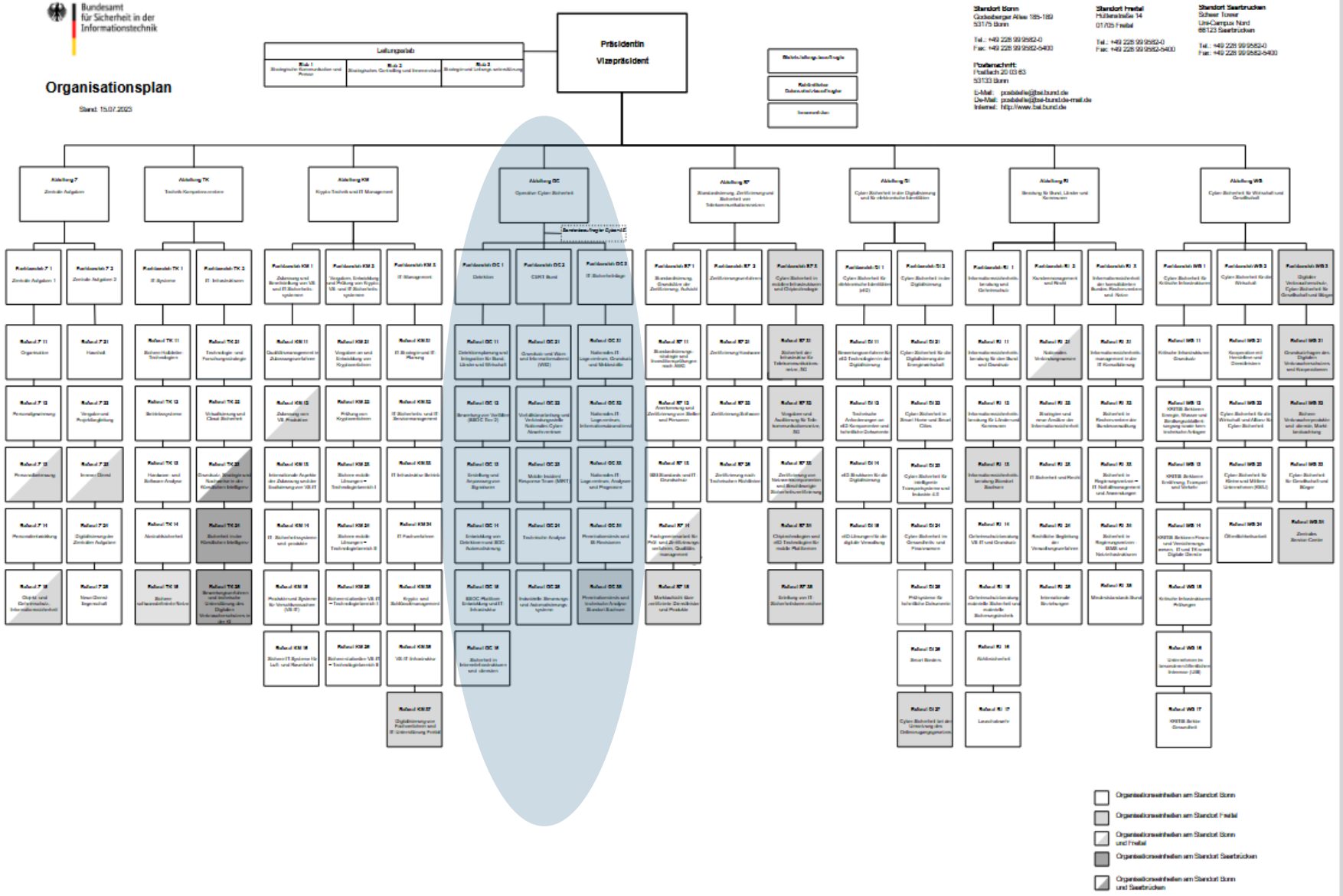
Das BSI

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

Bundesamt für Sicherheit in der Informationstechnik

Organisationsplan

Stand: 15.07.2023



Nationales IT-Lagezentrum

BSI

Nationales IT-Krisenreaktionszentrum

BSI

BSOC

CERT Bund

MIRT

NATIONALES CYBER-ABWEHRZENTRUM

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

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

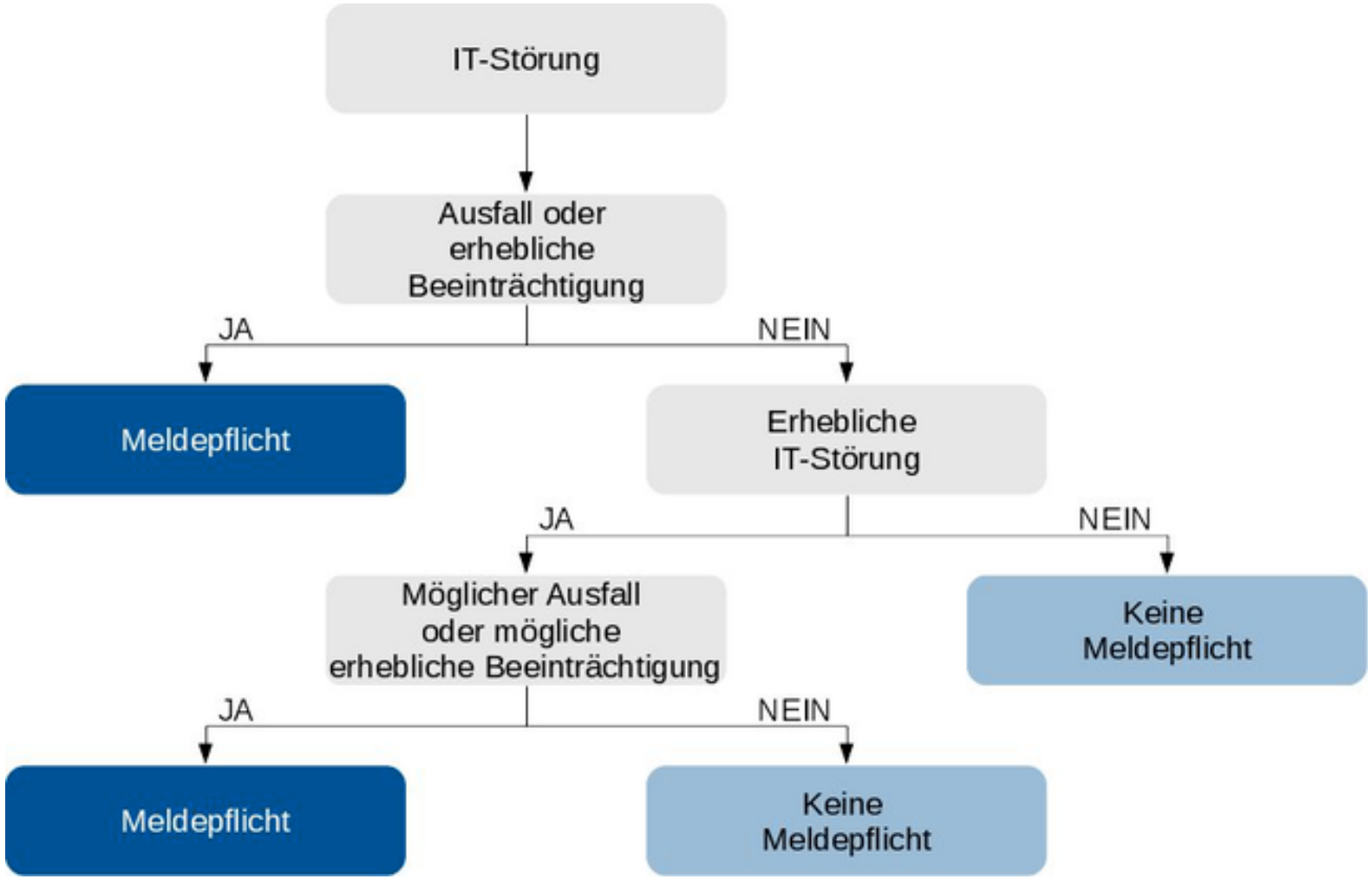
- DER.2.1.A1 Definition eines Sicherheitsvorfalls
- DER.2.1.A2 Erstellung einer Richtlinie zur Behandlung von Sicherheitsvorfällen
- DER.2.1.A3 Festlegung von Verantwortlichkeiten und Ansprechpartnern bei Sicherheitsvorfällen
- DER.2.1.A4 Benachrichtigung betroffener Stellen bei Sicherheitsvorfällen
- 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:

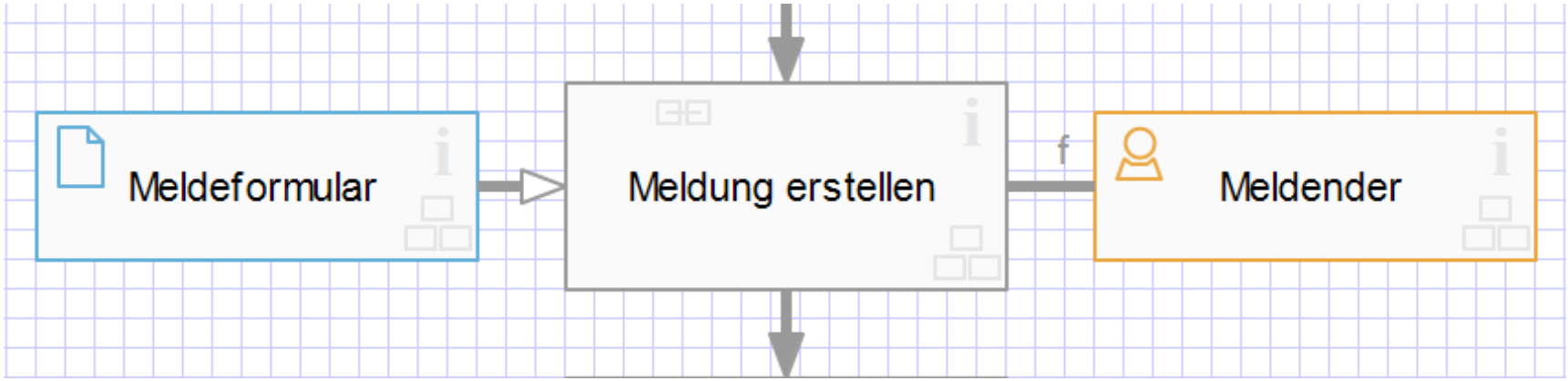
Eine [IT-]Störung im Sinne des BSI-Gesetzes liegt daher vor, wenn die eingesetzte Technik die ihr zugedachte Funktion nicht mehr richtig oder nicht mehr vollständig erfüllen kann oder versucht wurde, entsprechend auf sie einzuwirken.

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.

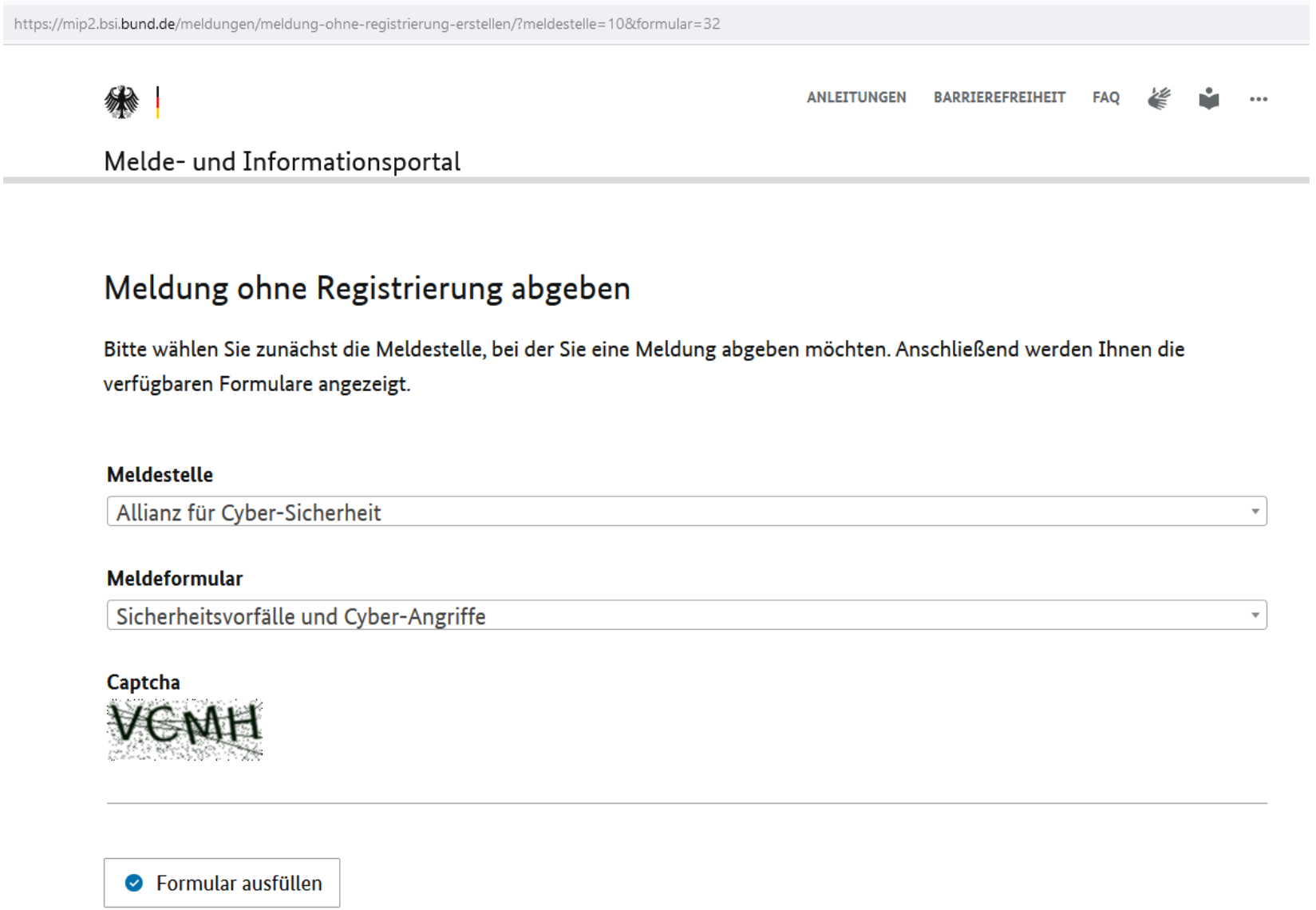
Wie melde ich?

Meldung erstellen und versenden



Melde- und Informationsportal (MIP)

Allianz für Cybersicherheit

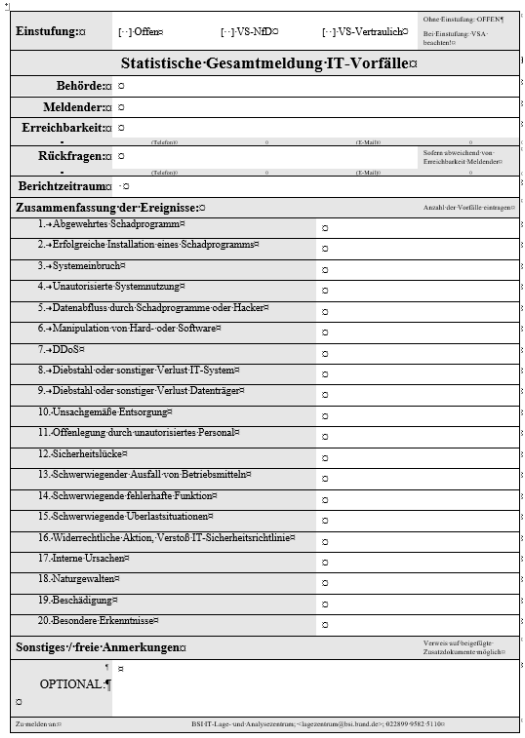


§ 4 BSIG + Verwaltungsvorschrift

SOFORT-Meldung

STATISTISCHE Gesamtmeldung

Einstufung:	[ ] Offen	[ ] VS-NfD	[ ] VS-Vertraulich	Ohne Einstufung: OFFEN Bei Einstufung: VSA beachten!
SOFORT-Meldung IT-Vorfall				
Behörde:				
Meldender:				
Erreichbarkeit:				
	(Telefon)		(E-Mail)	
Rückfragen:				Sofern abweichend von Erreichbarkeit Meldender
	(Telefon)		(E-Mail)	
Datum:		**Uhrzeit:**		Wann ist das Ereignis eingetreten?
Vorläufige Klassifizierung durch den Meldenden:				Vgl. mit Anlage 1 der Verwaltungsvorschrift
Externer Angriff	[ ] gezielt	[ ] Abgewehrter Schadprogramm	[ ] Erfolgreiche Installation eines Schadprogramms	[ ] Systemeinbruch
	[ ] Unautorisierte Systemnutzung	[ ] Datenabfluss durch Schadprogramme/Hacker	[ ] Manipulation von Hard- oder Software	[ ] DDoS
Datenverlust	[ ] Diebstahl oder sonstiger Verlust IT-System	[ ] Diebstahl oder sonstiger Verlust Datenträger	[ ] Unsachgemäße Entsorgung	[ ] Offenlegung durch unautorisiertes Personal
Sicherheitslücke				
Störung von SW/HW/ Komponenten	[ ] Schwerwiegender Ausfall von Betriebsmitteln	[ ] Schwerwiegende fehlerhafte Funktion	[ ] Schwerwiegende Überlastsituationen	
Widerrechtl. Aktion	[ ]			
Interne Ursachen	[ ]			
Externe Einflüsse	[ ] Naturgewalten	[ ] Beschädigung		
Bes. Erkenntnisse	[ ]			
Zweck der Information / Erwartete Reaktion durch das BSI-IT-LZ				Mehrfachauswahl möglich
	[ ] Zur Kenntnisnahme	[ ] Freigabe zur Aufnahme in Lageberichte	[ ] Explizite Freigabe der Einflussung zur Aufnahme in Lagebericht durch Meldenden erforderlich	
	[ ] Bitte um Rückruf	[ ] Bitte um Einschätzung/ Stellungnahme	[ ] Unterstützung erforderlich	[ ] Vorfallsbearbeitung durch BSI-IT-LZ
Sachverhalt				Verweis auf beigefügte Zusatzdokumente möglich
Leitfragen: Was wurde festgestellt / was ist passiert? Wer, bzw. was ist betroffen? Welcher Schaden wurde bereits festgestellt? Ist eine Kompromittierung weiterer Systeme in analysierten Segmenten wahrscheinlich? Wurden bereits (Gegen-) Maßnahmen ergriffen? Wenn ja, welche? Wurden bereits weitere Stellen informiert?				
Vorschläge des Meldenden zum weiteren Vorgehen				Verweis auf beigefügte Zusatzdokumente möglich
OPTIONAL:				
Sonstiges / freie Anmerkungen				Verweis auf beigefügte Zusatzdokumente möglich
OPTIONAL:				
Zu melden an	BSI IT-Lage- und Analysezentrum, <lagezentrum@bsi.bund.de>; 022899 9582-5110			



Einstufung:	[ ] Offen	[ ] VS-NfD	[ ] VS-Vertraulich	Ohne Einstufung: OFFEN Bei Einstufung: VSA beachten!
Statistische Gesamtmeldung IT-Vorfälle				
Behörde:				
Meldender:				
Erreichbarkeit:				
	(Telefon)		(E-Mail)	
Rückfragen:				Sofern abweichend von Erreichbarkeit Meldender
	(Telefon)		(E-Mail)	
Berichtzeitraum				
Zusammenfassung der Ereignisse:				Anzahl der Vorfälle eintragen
1. Abgewehrtes Schadprogramm				
2. Erfolgreiche Installation eines Schadprogramms				
3. Systemeinbruch				
4. Unautorisierte Systemnutzung				
5. Datenabfluss durch Schadprogramme oder Hacker				
6. Manipulation von Hard- oder Software				
7. DDoS				
8. Diebstahl oder sonstiger Verlust IT-System				
9. Diebstahl oder sonstiger Verlust Datenträger				
10. Unsachgemäße Entsorgung				
11. Offenlegung durch unautorisiertes Personal				
12. Sicherheitslücke				
13. Schwerwiegender Ausfall von Betriebsmitteln				
14. Schwerwiegende fehlerhafte Funktion				
15. Schwerwiegende Überlastsituationen				
16. Widerrechtliche Aktion, Verstoß IT-Sicherheitsrichtlinie				
17. Interne Ursachen				
18. Naturgewalten				
19. Beschädigung				
20. Besondere Erkenntnisse				
Sonstiges / freie Anmerkungen				Verweis auf beigefügte Zusatzdokumente möglich
OPTIONAL				
Zu melden an	BSI IT-Lage- und Analysezentrum, <lagezentrum@bsi.bund.de>; 022899 9582-5110			

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?


microsoft
windows

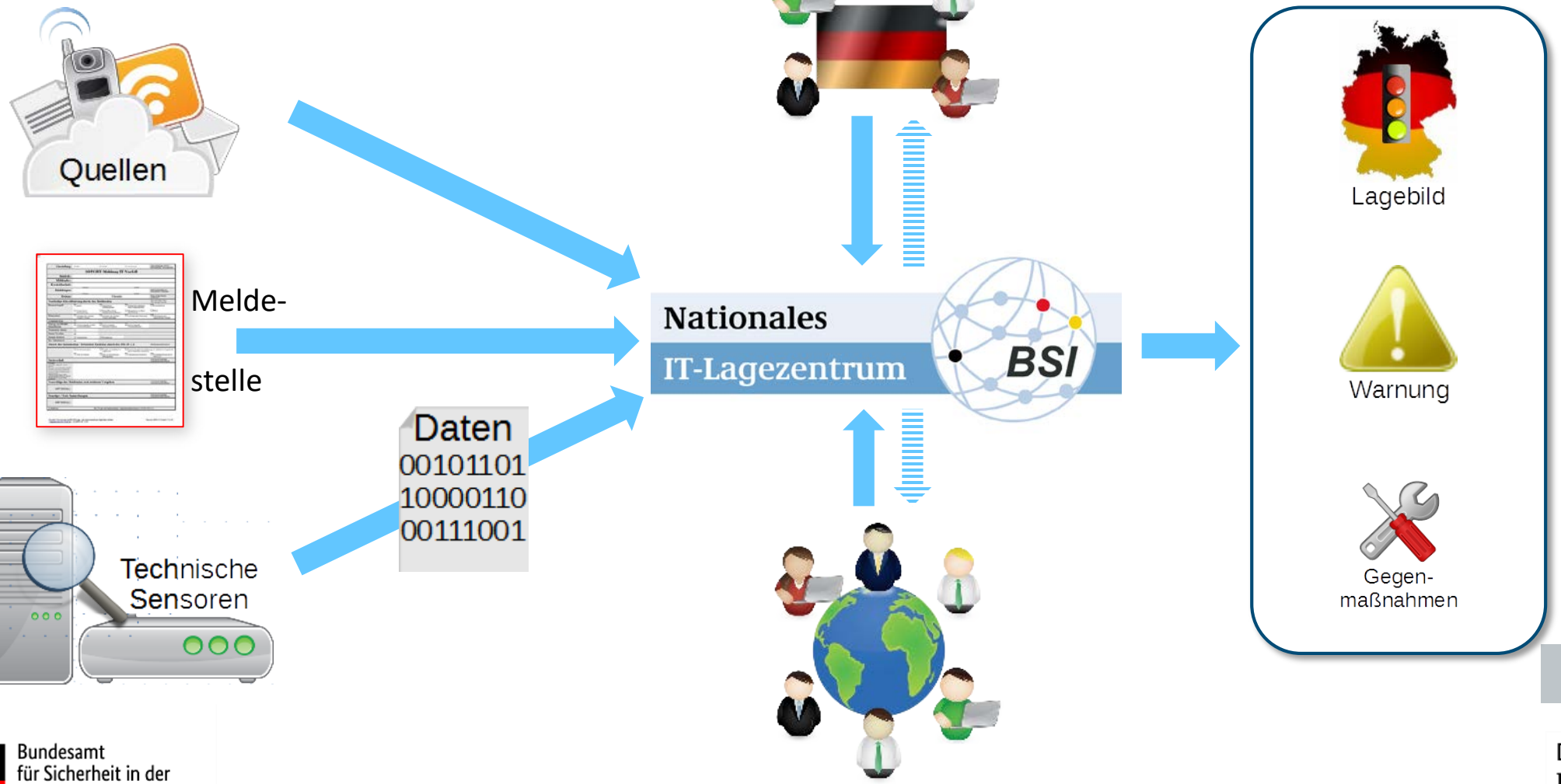

Taranis

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

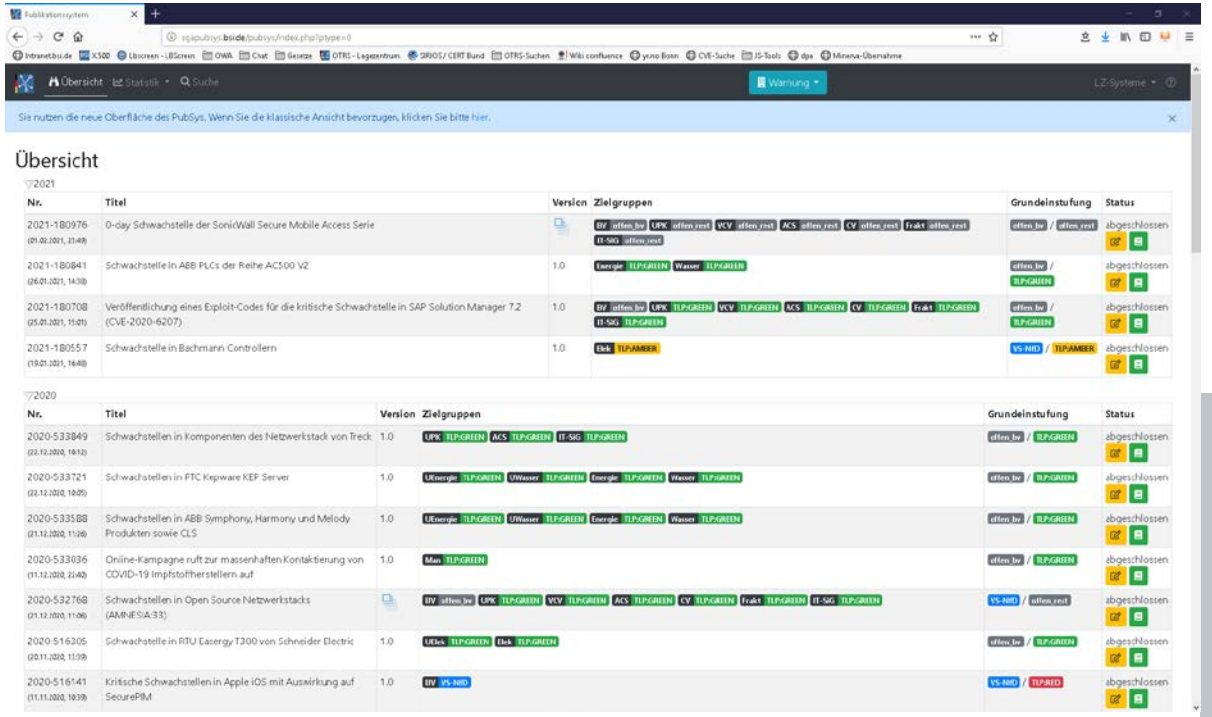
… andere Passwörter für Verschlüsselung

… andere Formatvorlagen (z.B. auch Kategorien)

… andere Empfänger

… andere Abhängigkeiten

… usw.



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


Bundesamt für Sicherheit in der Informationstechnik

BSI-IT-Sicherheitswarnung

SCHWACHSTELLE

Unsichere Signaturen in PDF-Dokumenten

Zahlreiche Dokumentenbetrachter weisen Schwachstellen auf

Nr. 2019-173145-1000, Version 1.0, 22.02.2019

IT-Bedrohungslage*: 2 / Gelb

Sachverhalt

IT-Krisenreaktionszentrum

Das IT-Krisenreaktionszentrum stellt die **schnelle Reaktion** auf **schwerwiegende Vorfälle** sicher, um so **rechtzeitige Gegenmaß-nahmen** 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

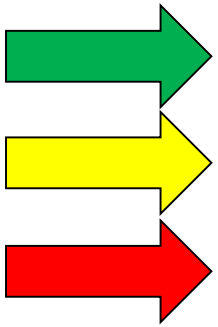
Zusammenfassung

Zusammenfassung

Vorfall ⇨ Meldewege

Information ⇨ Meldeformulare

Bearbeitung im Nationalen IT-Lagezentrum



Lagebild

Warnung

Gegenmaßnahmen

Vielen Dank
für Ihre Aufmerksamkeit!

Deutschland
Digital•Sicher•BSI•

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

Bundesamt
für Sicherheit in der
Informationstechnik