Anlage 2
zu Allgemeine Verwaltungsvorschrift über
das Meldeverfahren gemäß BSIG § 4 Abs. 6

Meldeprozess

Der Meldeprozess ist ein wesentlicher Bestandteil des IT-Sicherheitsmanagements der Bundesverwaltung und kann der erste Schritt eines Krisenmanagementprozesses sein. In diesem Dokument werden die beteiligten Stellen, die formalen Schritte und definierten Reaktionen für die zentrale Meldestelle für die Sicherheit in der Informationstechnik (BSIG § 4) beschrieben.

Verantwortliche Stelle

IT-Lage- und Analysezentrum (IT-LZ)

Die zentrale Meldestelle ist ein organisatorischer Teilbereich des IT-Lage- und Analysezentrums des Bundesamtes für die Sicherheit in der Informationstechnik (BSI).

Meldungstypen

Die meldepflichtigen Ereignisse sind in der Anlage 1 dieser Verwaltungsvorschrift dargestellt. In Abhängigkeit von Eskalationsmerkmalen, die im Wesentlichen auf der Dringlichkeit des zu meldenden Vorfalls beruhen, werden zwei Meldungstypen unterschieden, die zu verschiedenen Reaktionszeiten führen.

- SOFORT-Meldung
- Statistische Gesamtmeldung

Die SOFORT-Meldung ist als Einzelmeldung, die das konkrete Ereignis beinhaltet, unverzüglich an die zentrale Meldestelle zu melden. Im Gegensatz dazu ist die statistische Gesamtmeldung jeweils monatlich in Form einer Sammelmeldung an die zentrale Meldestelle zu berichten. Die dazugehörigen formalen Vorgaben sind als Meldeformulare am Ende dieser Anlage festgelegt.

SOFORT-Meldung

Sachverhalte, bei denen eine unmittelbare Gefahr für die Sicherheit der Informationstechnik des Bundes nicht ausgeschlossen werden kann, sind unverzüglich nach entsprechender Lagefeststellung durch die Behörde an die zentrale Meldestelle zu melden.

Beispiel 1: Vorfälle mit Frühwarnungspotenzial

Dies schließt alle Informationen mit IT-Bezug oder über IT-Vorfälle ein, die für andere Behörden zur Abwehr akut drohender Schäden von Bedeutung sind, unabhängig davon ob ein Schaden bereits eingetreten ist oder der Schaden vor Ort abgewendet werden konnte. Im Vordergrund steht hierbei die Absicht noch nicht betroffene oder kaum betroffene Behörden schnellst möglich durch die Frühwarnung in die Lage zu versetzen, geeignete Gegenmaßnahmen zu ergreifen.

Konkretisierung: Neues, von AV-Programmen noch nicht erkennbares Schadprogramm mit aggressiver Verbreitungsroutine.

Beispiel 2: Erfolgreiche Angriffe, insbesondere gezielte Angriffe

Dies schließt jeden erfolgreichen Angriff ein, der in der Regel dadurch charakterisiert ist, dass sich der Angreifer unbefugt Daten verschafft oder rechtswidrig Daten löscht, unterdrückt, unbrauchbar macht oder verändert.

Konkretisierung: Systemeinbruch auf einem Webserver mit anschließender Veränderung der Inhalte, beispielsweise für sinnentstellende Darstellungen oder zur Kritikäußerung (engl, „defacement").

Die überwiegende Mehrzahl von IT-Angriffen erfolgt ungerichtet und semi-automatisiert. Sobald Indizien darauf hindeuten, dass der vorliegende IT-Sicherheitsvorfall das Ergebnis eines gezielten, d. h. bewusst auf die betroffene Behörde ausgerichteten Angriffs ist, erhöht sich die Gefährdungseinschätzung drastisch. Zusätzliche Eskalationsschritte sind durch die betroffene Behörde und die zentrale Meldestelle in Betracht zu ziehen.

Konkretisierung: Vortäuschung (engl, „spoofing") eines real existierender Kommunikationspartners als Absender und Verwendung von kontextbezogenem, eventuell auch internem Wissen als Social Engineering Angriffsvektor. Dies kann insbesondere Innentäter mit einschließen.

Beispiel 3: Extern verursachte, schwerwiegende Störung der IT
Im Falle einer andauernden, schwerwiegenden Störung der IT einer Behörde, die durch externe Einflüsse verursacht wird, prüft die zentrale Meldestelle anhand der Angaben in der Einzelmeldung die potentielle Betroffenheit weiterer Behörden und leitet zentrale Gegenmaßnahmen an den Schnittstellen des Regierungsnetzes ein.

Konkretisierung: Mehrstündige Überlastung von Netzkoppelelementen, beispielsweise aufgrund eines DDoS-Angriffs.

Beispiel 4: Öffentlich bekannt werdende IT-Störungen
IT-Störungen, die öffentlich bekannt geworden sind oder von denen anzunehmen ist, dass sie öffentlich bekannt werden, sind mit Nachdruck zu beseitigen, um sowohl potentielle Reputationsverluste, als auch konkrete Schäden gering zu halten.

Konkretisierung: Erhebliche Performanzeinbußen oder Schwachstellen in einer eGovernment-Anwendung.

STATISTISCHE Gesamtmeldung

Alle weiteren meldepflichtige Ereignisse (gem. Anlage 1), die nicht bereits als SOFORT-Meldungen erfasst wurden, sind als statistische Gesamtmeldungen an die zentrale Meldestelle zu melden. Dies dient insbesondere der konsolidierten Langzeitanalyse der IT-Sicherheitslage. Hierbei wird insbesondere die Angemessenheit bzw. Wirksamkeit und Wirtschaftlichkeit vorhandener zentraler Schutzmaßnahmen geprüft sowie der Bedarf erweiterter oder noch erforderlicher Schutzmaßnahmen festgestellt.

Meldeweg

Die meldepflichtige Behörde oder ein im Auftrag dieser Behörde agierender Dritter (vgl. § 3 W zum Meldeverfahren) melden **grdsl. elektronisch** an das IT-LZ. Dabei sind SOFORT-Meldungen am Anfang der Betreffzeile mit [SOFORT] zu kennzeichnen, STATISTISCHE Gesamtmeldungen mit [Statistik].
Das IT-LZ ist wie folgt erreichbar:

E-Mail: lagezentrum@bsi.bund.de
Telefon: 022899 9582 5110
022899 9582 5499

Vertraulichkeit

Bei Bedarf stehen für die geschützte elektronische Übermittlung folgende Möglichkeiten zur Verfügung:

- Übertragung innerhalb des Regierungsnetzes ohne zusätzliche Verschlüsselung
- Softwareverschlüsselung mit PGP oder S/MIME (sensitiv, nicht eingestuft)
- Chiasmus (VS-NfD)
- Kryptotelefon und Kryptofax (VS-V und höher)

Quittierung der Meldung

Jede eingehende SOFORT-Meldung wird durch das IT-LZ quittiert. Dies erfolgt durch eine E-Mail an den Meldenden und an den für die Behörde registrierten Alarmierungskontakt. Erhält der Meldende im Falle einer schriftlichen Meldung nicht innerhalb von 30 Minuten eine Eingangsbestätigung, so muss er die Meldung über alternative Kommunikationsmittel absetzen oder das IT-LZ unmittelbar kontaktieren.

Informationsauswertung

Die eingehenden Meldungen werden durch das IT-LZ ausgewertet und ggf. Maßnahmen eingeleitet. Für die Entscheidungsfindung durch das IT-LZ ist neben dem kontinuierlich erstellten Gesamtlagebild, welches die eingehenden Meldungen aller meldepflichtigen Behörden konsolidiert und in Beziehung setzt, die Erstbewertung des Sachverbalts durch den Meldenden von besonderer Bedeutung.

Datenverwendung

Bei Bedarf können durch IT-LZ im Rahmen der IT-Vorfallsbearbeitung erforderliche, soweit möglich und notwendig anonymisierte Teilirrformationen an Dritte weitergegeben werden, soweit die Ursachen für den IT-Vorfall bei diesen Dritten liegen. Die Weitergabe der Informationen darf ausschließlich der Beseitigung oder der Minderung der Ursachen des IT-Vorfalls bei dem jeweiligen Dritten dienen[1)].
Nach Abschluss der durch die Meldungen ausgelösten Vorgänge erfolgt die Aufbereitung der Informationen für das Berichtswesen. Die Berichterstattung und Lagebilddarstellung erfolgt in anonymisierter Form. Bei sensitiven Sachverhalten ist die Freigabe durch die meldende Behörde erforderlich.

Meldezyklus

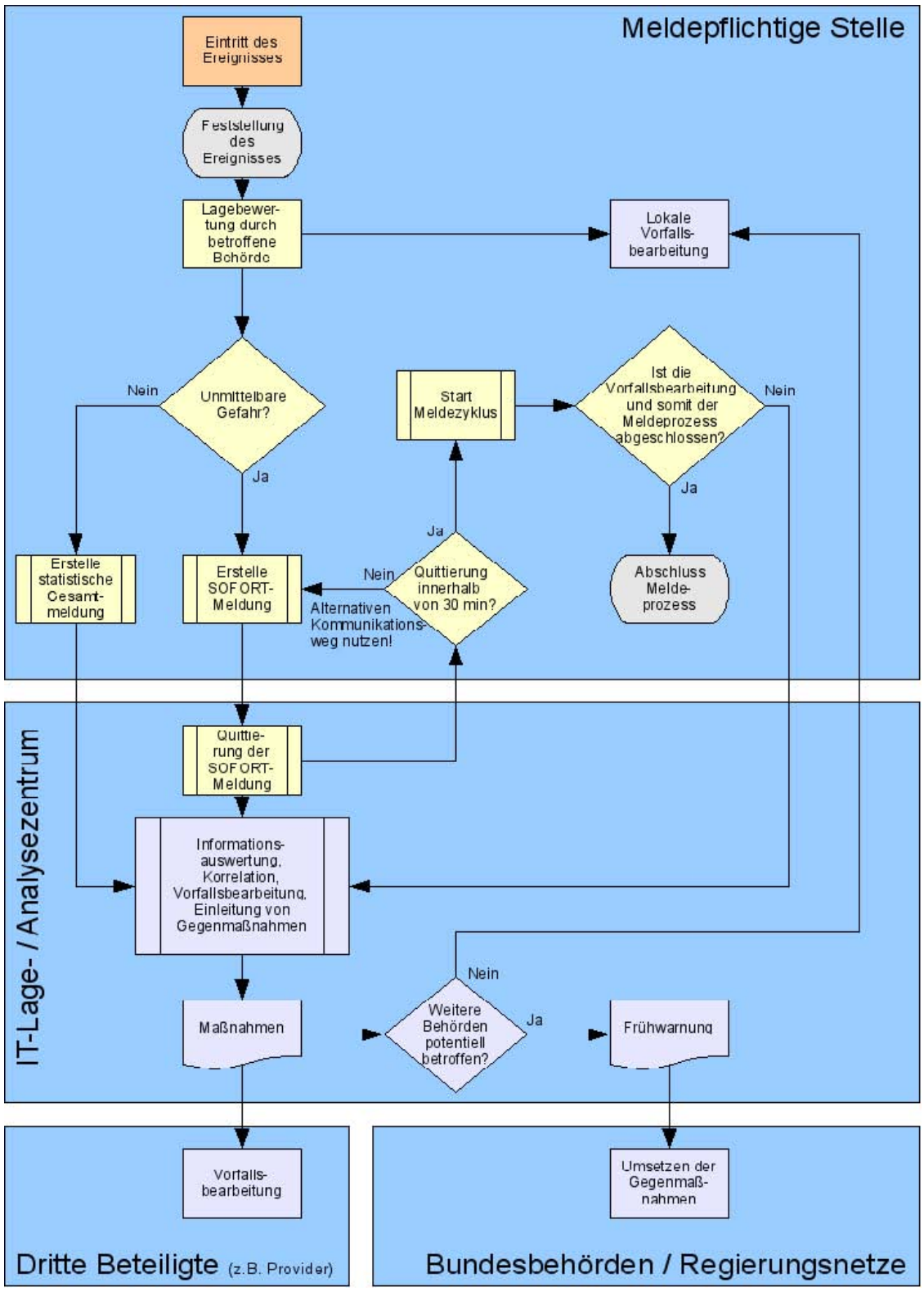
Bis zur Beendigung des Sachverhalts und der eingeleiteten Maßnahmen erfolgt in Absprache mit der zentralen Meldestelle in regelmäßigen Abständen eine Aktualisierung der Lage der betroffenen Behörde aus der Sicht des Meldenden.

Abschluss des Meldeprozesses

Die meldende Behörde teilt dem IT-LZ mit, wenn aus ihrer Sicht der Meldeprozess beendet werden kann. Dies geht üblicherweise einher mit dem Abschluss der Vorfallsbehandlung oder des daraus erwachsenem Krisenmanagements, kann aber auch direkt bei Eingangsbestätigung oder unmittelbar nach der Erstbewertung der eingehenden Meldung durch das IT-LZ erfolgen.

[1)] Die Weitergabe von Informationen aus dem Geschäftsbereich des BMVg an Dritte bedarf der Zustimmung durch den Meldepflichtigen. Gemäß Begründung zu § 3 BSIG ergreift das BMVg eigene Maßnahmen zur Abwehr von Gefahren für seine Information- und Kommunikationstechnik. Die Entscheidung, ob Dritte oder das IT-LZ entsprechende Maßnahmen an der Technik des Geschäftsbereichs des BMVg oder eines anderen Ressons durchfühlen, verbleibt beim BMVg bzw. dem jeweils zuständigen Ressort. Die Entscheidungskompetenz hinsichtlich der Durchführung von Gegenmaßnahmen ist nichc Gegenstand der Vcrwaltungsvorschrift.

Graphische Darstellung des Meldeprozesses



Formular SOFORT-Meldung IT-Vorfall

Einstufung:	☐ Offen	☐ VS-NfD	☐ VS-Vertraulich	Ohne Einstufung: OFFEN Bei Einstufung: VSA beachten!
SOFORT-Meldung IT-Vorfall				
Behörde:				
Meldender:				
Erreichbarkeit:	(Telefon)		(E-Mail)	
Rückfragen:	(Telefon)		(E-Mail)	Sofern abweichend von Erreichbarkeit Meldender
Datum:		**Uhrzeit:**		Wann ist das Ereignis eingetreten?
Vorläufige Klassifizierung durch den Meldenden:				Vgl. mit Anlage 1 der Verwaltungsvorschrift
Externer Angriff	☐ gezielt	☐ Abgewehrtes 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 Lagebericht	☐ Explizite Freigabe der Endfassung 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 anderen Organisationen 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 Analysezenrum; <lagezentrum@bsi.bund.de>; 022899 9582 5110			

Formular Statistische Gesamtmeldung IT-Vorfälle

Einstufung:	☐ Offen	☐ VS-NfD	☐ VS-Vertraulich	Ohne Einstufung: OFFEN Bei Einstufung: VSA beachten!
Statistische Gesamtmeldung IT-Vorfälle				
Behörde:				
Meldender:				
Erreichbarkeit:	(Telefon)		(E-Mail)	
Rückfragen:	(Telefon)		(E-Mail)	Sofern abweichend von Erreichbarkeit Meldender
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 Analysezenrum; <lagezentrum@bsi.bund.de>; 022899 9582 5110			

Einstufung: ☐ Offen ☐ VS-NfD ☐ VS-Vertraulich	Ohne Einstufung: OFFEN Bei Einstufung: VSA beachten!

Statistische Gesamtmeldung IT-Vorfälle (Teil II)

OPTIONAL: Angabe von Detailinformationen (Datum, Sachverhalt)	Verweis auf beigefügte Zusatzdokumente möglich
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

GMBl 2009, S. 1665