05. Oktober 2017

Verbindliches Meldeverfahren zum Informationsaustausch über IT-Sicherheitsvorfälle im VerwaltungsCERT-Verbund (VCV) - (Meldestandard)

Präambel

Die im März 2013 vom IT-Planungsrat beschlossene Leitlinie für die Informationssicherheit in der öffentlichen Verwaltung von Bund und Ländern trägt dem Bedarf der übergreifenden Zusammenarbeit Rechnung und formuliert u.a. die gemeinsame Abwehr von IT-Angriffen als Strategie zur Umsetzung der Ziele der Informationssicherheit. Diese Leitlinie stellt einen IT-Sicherheitsstandard im Sinne von § 3 Abs. 1 des IT-Staatsvertrags dar und ist damit für Bund und Länder verbindlich, soweit dies zum bundländerübergreifenden Datenaustausch notwendig ist.

In Umsetzung der o.g. Strategie wurde in der Leitlinie die Zusammenarbeit im Rahmen eines VerwaltungsCERT-Verbunds (VCV) vereinbart. Dieser Verbund dient der frühzeitigen Erkennung und der Abwehr von IT-Angriffen und besteht aus den Länder-CERTs sowie dem CERT-Bund, welche wiederum den angeschlossenen Verwaltungen der Länder bzw. des Bundes relevante Informationen zur Wahrung der Informationssicherheit bereitstellen

Vor diesem Hintergrund werden folgende Regelungen für den Informationsaustausch im VerwaltungsCERT-Verbund (VCV) auf Beschluss des IT-Planungsrates Nr. 2017/35 für Bund und Länder als IT-Sicherheitsstandard im Sinne von § 3 Absatz 1 des IT-Staatsvertrags verbindlich vereinbart:

§ 1 - Zweck

Cyberangriffe sind eine zunehmende Bedrohung für die Verwaltungen von Bund und Ländern. Geeignete Schutz- und Abwehrmaßnahmen sind unabdingbar. Der gegenseitige Austausch von relevanten Informationen zur Informationssicherheit hat dabei besonderes Gewicht.

Die Regelung legt hierzu fest, welche Informationen für den Schutz der Informationstechnik der Teilnehmer des VCV relevant und daher im VCV bereitzustellen sind.

§ 2 - Meldepflichtige Informationen

Absatz 1:

1. Zu melden sind IT-Sicherheitsvorfälle, bei denen Auswirkungen auf die Länder oder den Bund nicht ausgeschlossen werden können oder die auch für andere als relevant eingeschätzt werden.
2. Nicht meldepflichtig sind bereits öffentlich zugängliche Informationen, wie beispielsweise Informationen von Herstellern über Sicherheitslücken und Sicherheitspatches.

Absatz 2:

Die IT-Sicherheitsvorfälle sind gemäß den in Anlage 1 verzeichneten Kategorien einzuordnen.

Absatz 3:

Grundsätzlich dürfen zu meldende Informationen keine personenbezogenen Daten enthalten. Sofern ausnahmsweise personenbezogene Daten gemeldet werden, sind diese auf das erforderliche Minimum zu beschränken.

§ 3 - Meldepflichtige Stellen

Meldepflichtig sind alle Teilnehmer des VCV (Bund und Länder).

§ 4 - Meldeverfahren

1. Die Teilnehmer des VCV stellen die unverzügliche Meldung nach Feststellung der Meldewürdigkeit des Ereignisses sicher.
2. Die Meldung erfolgt an alle Teilnehmer des VCV zeitgleich und unter Angabe des in Anlage 2 bezeichneten Informationsumfangs.
3. CERT-Bund bestätigt gegenüber dem Absender unverzüglich den Eingang der Meldung (siehe Anlage 3).
4. Die eingehenden Informationen werden von den Teilnehmern des VCV unverzüglich ausgewertet. Die Teilnehmer des VCV informieren sich gegenseitig im Wege der Frühwarnung unverzüglich über alle für die Abwehr von Gefahren für die Sicherheit in der Informationstechnik relevanten Informationen.

§ 5 - Bericht durch das BSI

1. Das BSI berichtet der Arbeitsgruppe Informationssicherheit kalenderjährlich jeweils bis zum 31.03. des dem Berichtsjahr folgenden Jahres zu den eingegangenen Meldungen. Der Bericht soll Rückschlüsse auf die meldenden Stellen vermeiden.
2. Die Arbeitsgruppe Informationssicherheit wertet diesen Bericht aus und legt das Ergebnis dem IT-Planungsrat zeitnah vor.

§ 6 - Verfahren zur Änderung der Anlagen

Änderungen in den Anlagen 1 und 2 zu diesem Standard sind durch die Arbeitsgruppe Informationssicherheit einvernehmlich zu beschließen.

§ 7 - Inkrafttreten

Dieser Standard tritt am 01.01.2018 in Kraft.

Es gelten folgende Anlagen:

Anlage 1: Meldungskategorien

Anlage 2: Meldeformular

Anlage 3: Meldeprozess

Meldekategorien im VCV

Bei IT-Sicherheitsvorfällen, die den nachstehend aufgeführten Kategorien bzw. den aktuell wesentlichen Gefährdungen[1] zuzuordnen sind, steht die Meldewürdigkeit grundsätzlich zu vermuten.

Können bei derartigen Vorfällen Auswirkungen auf andere Teilnehmer des VCV nicht ausgeschlossen werden oder könnten die Informationen zum jeweiligen Vorfall für andere Teilnehmer des VCV sonst relevant sein, ist die mit der VCV-GO Tz. 4.1 vereinbarte Meldung an das Lagezentrum des BSI (CERT-Bund) zu veranlassen. Die Meldung erfolgt gem. der in der Anlage zu diesem Dokument bestimmten Form, vorzugsweise per E-Mail.

CERT-Bund stellt die nach Bewertung durch das BSI zur Abwehr bestehender Gefährdungen erforderlichen Informationen im VCV unverzüglich zur Verfügung.

Erreichbarkeit Lagezentrum BSI:

E-Mail: lagezentrum@bsi.bund.de

Telefon: 022899 9582 - 5110 oder - 5499

Kategorie	Aktuell wesentliche Gefährdungen (Erläuterungen)
1) Externer Angriff	Versuchte Clientseitig detektierte und abgewehrte Installation eines Schadprogramms
	Erfolgreiche Installation eines Schadprogramms[2]
	Systemeinbruch (z.B. Hacking, Exploiting, Missbrauch von Passwörtern)
	Unautorisierte Systemnutzung (z.B. Hacking, Defacement, Manipulation Datenbestand, Botnet-Client, Spam-Relay, Dropzone)
	Datenabfluss durch Schadprogramme oder durch Hacking
	Manipulation von Hard- oder Software
	(Distributed) Denial of Service [(D)DoS]
2) Datenverlust	Diebstahl oder sonstiger Verlust von IT-Systemen oder mobilen Geräten, die dienstliche Informationen enthalten, die öffentlich nicht zugänglich und schützenswert sind
	Diebstahl oder sonstiger Verlust von Datenträgern, soweit diese dienstliche Informationen enthalten, die öffentlich nicht zugänglich und schützenswert sind[3]
	Unsachgemäße Entsorgung von IT-Systemen, mobilen Geräten sowie von Datenträgern[4], soweit diese dienstliche Informationen enthalten, die öffentlich nicht zugänglich und schützenswert sind
	Datenabfluss bzw. Offenlegung durch unautorisiertes Personal hinsichtlich dienstlicher Informationen, die öffentlich nicht zugänglich und schützenswert sind.

[1] Die Kategorien und die derzeit aktuellen meldepflichtigen Gefährdungen orientieren sich am Gefährdungskatalog der IT-Grundschutz-Kataloge und der ISO 27005.
[2] Auch wenn das Schadprogramm nach einem gewissen Zeitraum durch ein AV-Produkt entdeckt und entfernt wird, gilt es dennoch als erfolgreiche Installation.
[3] Sofern die Informationen auf den Datenträgern nur verschlüsselt vorliegen und die eingesetzte Verschlüsselung den Vorgaben des BSI bzgl. des jeweiligen Schutzbedarfs entspricht, kann von der Meldung des Verlustes abgesehen werden.
[4] Sofern die Informationen auf den Datenträgern nur verschlüsselt vorliegen und die eingesetzte Verschlüsselung den Vorgaben des BSI bzgl. des jeweiligen Schutzbedarfs entspricht, kann von der Meldung der unsachgemäßen Entsorgung der Datenträger abgesehen werden.

Meldekategorien im VCV

3) Sicherheitslücke	Neuartige Sicherheitslücken oder Schwachstellen in IT-Produkten, die durch den Meldenden aufgedeckt wurden
4) Störung von Soft- oder Hardwarekomponenten	Schwerwiegender[5] Ausfall von technischen Systemen und/oder deren Komponenten (z.B. Ausfall Telekommunikationsanlage, defekte Hardware) soweit nicht von Ziffer 6 oder 7 erfasst
	Schwerwiegende fehlerhafte Funktion von technischen Systemen und/oder deren Komponenten oder Software (z.B. erratisches, nicht-deterministisches Verhalten, Systemabsturz, kein Wiederanlaufen eines Fachverfahrens nach Softwareupdates) soweit nicht von Ziffer 6 oder 7 erfasst
	Schwerwiegende Überlastsituationen (z.B. bei Ausfall von Teilsystemen) soweit nicht von Ziffer 6 oder 7 erfasst
5) Widerrechtliche Aktion - Verstoß gegen IT-Sicherheitsrichtlinien	Schwerwiegender, üblicherweise durch Innentäter verursachter Missbrauch von technischen Systemen und/oder deren Komponenten, Unautorisierte Erstellung von Kopien, Datenmanipulation oder Unzulässige Datenverarbeitung
6) Interne Ursachen	Schwerwiegender betriebsrelevanter Ausfall von technischen Systemen und/oder deren Komponenten durch Ausfall der Strom- oder Wasserversorgung (z.B. Sicherungen, USV, Kühlkreislauf, Klimaanlage Rechenzentrum)
7) Externe Einflüsse	Schwerwiegender betriebsrelevanter Ausfall von technischen Systemen und/oder deren Komponenten durch Naturgewalten bzw. höhere Gewalt (z.B. Feuer, Wasser, Hitze, Kälte)
	Schwerwiegender betriebsrelevanter Ausfall von technischen Systemen und/oder deren Komponenten durch Beschädigung (z.B. durch Bauarbeiten, Unfälle)
8) Besondere Erkenntnisse	Sonstige relevante Ereignisse mit IT-Bezug, die nach Einschätzung des Meldenden für die Gewährleistung des Schutzes der Informationstechnik anderer und damit auch für die Abwehr von Gefahren für die Informationstechnik der Teilnehmer des VCV von Bedeutung sind.

[5] Bei der Einschätzung, ob ein Ausfall schwerwiegend ist, kann die meldende Stelle auch berücksichtigen, ob das Ereignis für die Gewährleistung des Schutzes der Informationstechnik anderer Teilnehmer des VCV und damit auch für die Abwehr von Gefahren für die Informationstechnik anderer Teilnehmer des VCV Bedeutung haben könnte. Dies gilt auch im Folgenden, soweit bei den wesentlichen Gefährdungen das Merkmal „schwerwiegend“ Erwähnung findet.

Formular Meldung IT-Vorfall

TLP:	☐ White	☐ Green	☐ Amber	☐ Red
Meldung IT-Vorfall				
Organisation:				
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:		**Sachverhalt** Verweis auf beigefügteZusatzdokumente möglich
Externer Angriff	☐	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?
Datenverlust	☐	
Sicherheitslücke	☐	
Störung von SW/HW-Komponenten	☐	
WiderrechtlicheAktion	☐	
Interne Ursachen	☐	
Externe Einflüsse	☐	
Besondere Erkenntnisse	☐	

Zweck der Information / Erwartete Reaktion durch BSI Mehrfachauswahl möglich

☐ Zur Kenntnisnahme	☐ Freigabe zur Aufnahmein Lagebericht	☐ Explizite Freigabe der Endfassung zur Aufnahme in Lagebericht durch Meldenden erforderlich	
☐ Bitte um Rückruf	☐ Bitte um Einschätzung / Stellungnahme	☐ Unterstützung erforderlich	☐

Optional: Vorschläge des Meldenden zum weiteren Vorgehen Verweis auf beigefügte Zusatzdokumente möglich

Optional: Sonstiges / freie Anmerkungen Verweis auf beigefügte Zusatzdokumente möglich

Zu melden an: BSI IT-Lage- und Analysezentrum; <lagezentrum@bsi.bund.de>; Telefon: 022899 9582 -5110 oder -5499

VCV – Referenz-Meldeprozess