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.