Kurzinformation
Behördliche Meldepflichten von IT-Sicherheitslücken

Gefragt wird, ob Beschäftigte von Sicherheitsbehörden verpflichtet sind, beim Auffinden von Sicherheitslücken in informationstechnischen Systemen diese zu melden.

Eine **spezialgesetzliche Handlungspflicht** existiert in Form von **§ 4 Abs. 3 des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (BSIG)**[1]. Seit dem 1. Januar 2010 müssen alle Bundesbehörden dem Bundesamt für Sicherheit in der Informationstechnik (BSI) unverzüglich Informationen, welche für die Erfüllung von Aufgaben oder die Sicherheit der Informationstechnik anderer Behörden von Bedeutung sind, mitteilen, soweit andere Vorschriften dem nicht entgegenstehen. Das **Meldeverfahren** und der **Umfang der Meldepflicht** sind in der gemäß § 4 Abs. 6 BSIG erlassenen Allgemeinen Verwaltungsvorschrift über das Meldeverfahren gemäß § 4 Abs. 6 BSIG[2] **(Allgemeine Verwaltungsvorschrift BSIG)** näher geregelt.

Meldepflichtig sind **alle** für die Abwehr von Gefahren für die Sicherheit in der Informationstechnik **erforderlichen Informationen,** insbesondere zu Sicherheitslücken, Schadprogrammen, erfolgten oder versuchten Angriffen auf die Sicherheit in der Informationstechnik und der dabei beobachteten Vorgehensweise, wozu auch IT-Sicherheitsvorfälle gehören, § 1 Abs. 1 S. 1 der Allgemeinen Verwaltungsvorschrift BSIG. Nicht erforderlich sind bereits öffentlich zugängliche Informationen wie beispielsweise Informationen von Herstellern über Sicherheitslücken und Sicherheitspatches, § 1 Abs. 1 S. 2 der Allgemeinen Verwaltungsvorschrift BSIG. **Ausgenommen** von der Meldepflicht sind **Informationen,** die aufgrund von Regelungen zum **Geheimschutz** oder **Vereinbarungen mit Dritten** nicht weitergegeben werden dürfen oder deren Weitergabe im **Widerspruch zu der verfassungsrechtlichen Stellung** eines Abgeordneten des Bundestages oder eines Verfassungsorgans oder der gesetzlich geregelten Unabhängigkeit einzelner Stellen stünde, § 4 Abs. 4 BSIG. Sofern möglich, werden diese Informationen von meldepflichtigen Informationen

1 BSI-Gesetz vom 14. August 2009 (BGBl. I S. 2821), zuletzt geändert durch Art. 19c des Gesetzes vom 3. Juni 2021 (BGBl. I S. 1309).

2 Allgemeine Verwaltungsvorschrift über das Meldeverfahren gemäß § 4 Abs. 6 BSIG, abrufbar unter https://www.verwaltungsvorschriften-im-internet.de/bsvwvbund_08122009_IT5606000111.htm (Stand 16. Juni 2021).

WD 3 - 3000 - 119/21 (16. Juni 2021)

getrennt, damit eine Meldung an das BSI möglich wird. Die Anzahl von Fällen, in denen meldepflichtige Stellen von dieser Ausnahmeregelung Gebrauch gemacht haben, sind dem BSI halbjährlich jeweils zum 30. März und 30. September bekannt zu geben, § 2 Abs. 3 S. 3 der Allgemeinen Verwaltungsvorschrift BSIG. Der Bundesnachrichtendienst ist von dieser Meldepflicht ausgenommen, § 2 Abs. 3 S. 4 der Allgemeinen Verwaltungsvorschrift BSIG.

Meldepflichtig sind grundsätzlich **alle Bundesbehörden**. **Stellen,** denen Kraft Verfassung oder Gesetz eine **besondere Unabhängigkeit** zukommt, wie den Bundesgerichten (soweit sie nicht öffentlich-rechtliche Verwaltungsaufgaben wahrnehmen), dem Bundesrechnungshof, dem Bundesbeauftragten für Datenschutz und Informationsfreiheit oder den Verfassungsorganen Bundestag, Bundesrat und dem Bundespräsidenten, sind **von der Meldepflicht ausgenommen, wenn** eine Übermittlung im **Widerspruch zu dieser Unabhängigkeit** stehen würde. Nicht meldepflichtige Stellen des Bundes können sich **freiwillig** an dem Verfahren beteiligen und an das BSI melden, (siehe zum Ganzen § 3 Abs. 1 der Allgemeinen Verwaltungsvorschrift BSIG). Die Meldung erfolgt grundsätzlich durch den IT-Sicherheitsbeauftragten der jeweiligen Bundesbehörde, § 3 Abs. 2 S. 1 der Allgemeinen Verwaltungsvorschrift BSIG.

Die spezielle Meldepflicht des § 4 Abs. 3 BSGI schließt nicht aus, dass Sicherheitsbehörden im Rahmen ihrer allgemeinen Gefahrabwendungspflichten vor IT-Sicherheitslücken warnen.[3]

Auf **Landesebene** finden sich entsprechende Meldepflichten etwa in Bayern,[4] Niedersachsen[5] und Rheinland-Pfalz[6].

***

3 Siehe die Gesetzesbegründung zum BSIG, BT-Drs. 16/11967, S. 12; beispielhaft für eine Warnung des BKA siehe https://www.bka.de/SharedDocs/Kurzmeldungen/DE/Warnhinweise/210416_Emotet.html (Stand 16. Juni 2021).

4 Art. 11 Abs. 2 des Gesetzes über die elektronische Verwaltung in Bayern (Bayerisches E-Government-Gesetz - BayEGovG) vom 22. Dezember 2015 (GVBl. S. 458, BayRS 206-1-D), zuletzt geändert durch § 1 Abs. 138 der Verordnung vom 26. März 2019 (GVBl. S. 98), abrufbar unter: https://www.gesetze-bayern.de/Content/Document/BayEGovG-11 (Stand 16. Juni 2021).

5 § 14 Abs. 2 des Niedersächsisches Gesetzes über digitale Verwaltung und Informationssicherheit (NDIG) vom 24. Oktober 2019 (Nds. GVBl. 2019, 291), abrufbar unter http://www.nds-voris.de/jportal/?quelle=jlink&query=DigVwInfSichG+ND&psml=bsvorisprod.psml&max=true&aiz=true (Stand 16. Juni 2021).

6 § 17 Abs. 3 des Landesgesetzes zur Förderung der elektronischen Verwaltung in Rheinland-Pfalz (E-Government-Gesetz Rheinland-Pfalz - EGovGRP) vom 15. Oktober 2020, GVBl. 2020, 573, abrufbar unter http://landesrecht.rlp.de/jportal/?quelle=jlink&psml=bsrlpprod.psml&feed=bsrlp-lr&docid=jlr-EGovGRPrahmen (Stand 16. Juni 2021).