Der Bundesbeauftragte
für Wirtschaftlichkeit in
der Verwaltung

Leitsätze 08 Informations- und Kommunikationstechnik

Leitsatz 08/07 Freigabe von Verschlusssachen-Informationstechnik (VS-IT)

Leitsätze

(1) Verarbeitet eine Behörde Verschlusssachen elektronisch, muss die Dienststellenleitung die dafür eingesetzte IT als VS-IT freigeben.

(2) Sie kann die Freigabe mit Auflagen erteilen, wenn sie u. a.

- **die noch bestehenden Risiken aus noch nicht umgesetzten Sicherheitsmaßnahmen strukturiert und nachvollziehbar ermittelt, analysiert und bewertet hat,**
- **einen realistischen Umsetzungsplan für die ausstehenden Sicherheitsmaßnahmen erstellt hat und**
- **schriftlich die Risikoübernahme erklärt.**

(3) Die Freigabe mit Auflagen sollte sie für nicht länger als ein Jahr erteilen.

Hintergründe

Die Verschlusssachenanweisung (VSA) gilt gemäß § 1 Absatz 1 für Bundesbehörden und bundesunmittelbare öffentlich-rechtliche Einrichtungen (Dienststellen). Diese dürfen Verschlusssachen nur mit dafür von der Dienststellenleitung freigegebener VS-IT verarbeiten (§ 50 Absatz 1 Satz 1 VSA). Will die Dienststellenleitung die VS-IT freigeben, muss die Dienststelle grundsätzlich die Standards zur Informationssicherheit des Bundesamtes für Sicherheit in der Informationstechnik (BSI) (§ 50 Absatz 2 VSA) und die Geheimschutzanforderungen (§ 50 Absatz 3 VSA) erfüllen.

§ 50 Absatz 1 Satz 2 i. V. m. § 8 VSA ermöglicht eine Freigabe von VS-IT mit Auflagen. Hierzu muss eine Dienststelle entsprechend dem BSI-Standard 200-2 alle für ihre VS-IT zu erfüllenden Sicherheitsanforderungen und die notwendigen Sicherheitsmaßnahmen ermitteln und einen IT-Grundschutzcheck (Soll-Ist-Vergleich) durchführen. Weiter muss sie klären, welche Sicherheitsmaßnahmen noch umzusetzen sind und welche Risiken verbleiben.

§ 50 Absatz 1 Satz 2 VSA fordert nicht explizit das Vorliegen eines Sicherheitskonzepts. Gleichwohl ist nach dem maßgeblichen BSI-Standard 200-2 das Sicherheitskonzept das wichtigste Element der

strukturierten Vorgehensweise. Ohne Sicherheitskonzept kann die Dienststelle keinen fundierten IT-Grundschutzcheck durchführen und keinen Umsetzungsplan entwickeln. Weicht die Dienststellenleitung von dieser auf einem Sicherheitskonzept beruhenden strukturierten Vorgehensweise ab, geht sie ein Risiko ein, wenn sie die VS-IT dennoch freigibt.

Übergangsweise kann sie auf ein dokumentiertes Sicherheitskonzept verzichten, wenn die Vorarbeiten hierfür soweit abgeschlossen sind, dass die Dienststelle die Risiken für die freizugebende VS-IT erkennen und bewerten kann. Die Dienststelle sollte hierzu einen Umsetzungsplan erstellen, der ausweist, bis wann sie welche noch fehlende Sicherheitsmaßnahme realisiert. Auf der Grundlage des IT-Grundschutzchecks und des Umsetzungsplans kann die Dienststellenleitung bewerten, ob eine Risikoübernahme sachgerecht ist.

Das Bundesministerium des Innern hat als zeitliche Obergrenze für eine Freigabe mit Auflagen ein Jahr festgelegt.

(1) Der Bundesrechnungshof untersuchte in den Jahren 2017 bis 2019 bei 19 Bundesbehörden die Informationssicherheit und stellte dabei u. a. fest, dass viele Bundesbehörden gegen die VSA verstießen, da sie in ihren Behördennetzen Daten des Geheimhaltungsgrades „VS – NUR FÜR DEN DIENSTGEBRAUCH“ (VS-NfD) verarbeiteten und die Behördennetze nicht als VS-IT freigegeben hatten. Dennoch nutzten sie die ressortübergreifende Kommunikationsinfrastruktur „Netze des Bundes“ (NdB), um Daten bis zum Geheimhaltungsgrad VS-NfD auszutauschen.

(2) Prüfungserkenntnisse des Bundesrechnungshofes zeigen, dass Dienststellen die Vorschrift der VSA zur Freigabe mit Auflagen unterschiedlich auslegen. Trotz vielfältiger Mängel bei der Informationssicherheit und beim Geheimschutz gaben einzelne Dienststellen z.B. ihr Hausnetz als VS-IT für Verarbeitung von VS-NfD frei, ohne zuvor ein Sicherheitskonzept erstellt zu haben. Andere taten dies u. a. mit der Auflage, das Sicherheitskonzept fertigzustellen und Risikoanalysen durchzuführen. Ohne ein Sicherheitskonzept ist die strukturierte Bewertung der Risiken der Dienststelle jedoch nicht möglich. Darin muss sie die für den Betrieb ihrer VS-IT erforderlichen Sicherheitsanforderungen und -maßnahmen beschreiben. Liegt noch kein verabschiedetes Sicherheitskonzept vor, müssen zumindest die Vorarbeiten für ein solches soweit abgeschlossen sein, dass die Dienststellenleitung die Risiken für die freizugebende VS-IT erkennen und bewerten kann.

(3) Die Freigaben mit Auflagen waren zeitlich nicht befristet. Ohne eine Befristung ist nicht sichergestellt, dass die erkannten und akzeptierten Risiken in einer angemessenen Zeit behoben werden.

Anmerkungen

Der Rechnungsprüfungsausschuss des Deutschen Bundestages hat die Bemerkung „Verstoß von Bundesbehörden gegen Geheimschutzvorgaben gefährdet Sicherheit sensibler Daten“, welche den

oben beschriebenen Sachverhalt behandelt, am 10. Februar 2023 zustimmend zur Kenntnis genommen und die Empfehlungen des Bundesrechnungshofes durch Beschlüsse in den Jahren 2024 und 2025 weiter gestützt.