§ 15 BSIG 2025 — Detektion von Angriffsmethoden und von Sicherheitsrisiken für die Netz- und IT-Sicherheit

BSI-Gesetz
Stand: 07.12.2025 (konsolidierte Textfassung, kein amtliches Inkrafttretensdatum)

(1) Das Bundesamt kann im Rahmen seiner Aufgaben nach § 3 Absatz 1 Satz 2 Nummer 1 zur Detektion von bekannten Schwachstellen und anderen Sicherheitsrisiken Abfragen an den Schnittstellen öffentlich erreichbarer informationstechnischer Systeme zu öffentlichen Telekommunikationsnetzen durchführen,

1. um festzustellen, ob diese Schnittstellen unzureichend geschützt und dadurch in ihrer Sicherheit oder Funktionsfähigkeit gefährdet sein können, oder
2. wenn die Einrichtungen der Bundesverwaltung, der besonders wichtigen oder der wichtigen Einrichtungen die entsprechenden Einrichtungen darum ersuchen.

Erlangt das Bundesamt dabei Informationen, die durch Artikel 10 des Grundgesetzes geschützt sind, darf es diese nur zum Zwecke der Übermittlung nach § 8 Absatz 6 und 7 verarbeiten. Sofern die Voraussetzungen des § 8 Absatz 6 und 7 nicht vorliegen, sind Informationen, die durch Artikel 10 des Grundgesetzes geschützt sind, unverzüglich zu löschen.

(2) Wird durch Abfragen gemäß Absatz 1 Satz 1 eine bekannte Schwachstelle oder ein anderes Sicherheitsrisiko eines informationstechnischen Systems erkannt, informiert das Bundesamt als allgemeine Meldestelle für die Sicherheit in der Informationstechnik nach § 5 darüber unverzüglich die für das informationstechnische System Verantwortlichen. Gehört das informationstechnische System zu einer Einrichtung der Bundesverwaltung, sind zugleich die Informationssicherheitsbeauftragten der betroffenen Einrichtung der Bundesverwaltung nach § 45 und des übergeordneten Ressorts nach § 46 zu informieren. Das Bundesamt soll dabei auf bestehende Möglichkeiten zur Abhilfe des Sicherheitsrisikos hinweisen. Sind dem Bundesamt die Verantwortlichen nicht bekannt oder ist ihre Identifikation nur mit unverhältnismäßigem Aufwand oder über eine Bestandsdatenabfrage nach § 12 möglich, so ist hilfsweise der betreibende Dienstleister des jeweiligen Netzes oder Systems unverzüglich zu benachrichtigen, wenn überwiegende Sicherheitsinteressen nicht entgegenstehen.

(3) Das Bundesamt unterrichtet die Bundesbeauftragte oder den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit jeweils bis zum 30. Juni des Folgejahres über die Anzahl der gemäß Absatz 1 durchgeführten Abfragen.

(4) Das Bundesamt legt der Bundesbeauftragten oder dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit zu den Abfragen nach Absatz 1 auf Anforderung eine Liste der geprüften Systeme der Einrichtungen der Bundesverwaltung, der besonders wichtigen Einrichtungen und der wichtigen Einrichtungen zur Kontrolle vor.

(5) Das Bundesamt darf zur Erfüllung seiner Aufgaben Systeme und Verfahren einsetzen, die einem Angreifer einen erfolgreichen Angriff vortäuschen, um den Einsatz von Schadprogrammen oder andere Angriffsmethoden zu erheben und auszuwerten. Das Bundesamt darf dabei die zur Auswertung der Funktionsweise der Schadprogramme und Angriffsmethoden erforderlichen Daten verarbeiten.