3 Verstoß von Bundesbehörden gegen Geheimschutzvorgaben gefährdet Sicherheit sensibler Daten

Zusammenfassung

Viele Bundesbehörden haben ihre Behördennetze nicht ausreichend abgesichert und nicht für sensible, geheimhaltungsbedürftige Daten freigegeben. Gleichwohl sind sie an die ressortübergreifende Kommunikationsinfrastruktur „Netze des Bundes“ angebunden, über die sie auch solche Daten austauschen. Der Bundesrechnungshof sieht dadurch die Vertraulichkeit der Daten und die Sicherheit aller an den Netzen des Bundes teilnehmenden Bundesbehörden gefährdet.

Die meisten Bundesbehörden verarbeiten in ihren Behördennetzen auch sensible, geheimhaltungsbedürftige Daten (sog. Verschlusssachen). Dazu müssen die Behördennetze bestimmte Mindestanforderungen erfüllen und für die Verarbeitung von Verschlusssachen freigegeben sein. Neben den Behördennetzen gibt es für den Datenaustausch mit anderen Bundesbehörden die Netze des Bundes. Für deren Sicherheit ist das Bundesamt für Sicherheit in der Informationstechnik (BSI) zuständig. 80 % der Bundesbehörden missachten wesentliche Pflichten, die sie erfüllen müssen, wenn sie die Netze des Bundes nutzen. Auch verstoßen sie gegen Vorgaben für die Verarbeitung von Verschlusssachen. Das BSI hatte nicht geprüft, inwieweit die Bundesbehörden die Voraussetzungen für die Teilnahme an den Netzen des Bundes erfüllten. Ihm war bekannt, dass die Mehrzahl der Behördennetze nicht für die Verarbeitung von Verschlusssachen freigegeben ist. Der Bundesrechnungshof hatte den Haushaltsausschuss des Deutschen Bundestages bereits im Jahr 2019 über Gefahren für die Vertraulichkeit der Daten und für die Sicherheit aller an den Netzen des Bundes teilnehmenden Bundesbehörden unterrichtet. Das BMI hatte daraufhin zugesagt, die Mängel für die Netze des Bundes bis zum Jahr 2020 zu beheben. Diese Zusage galt jedoch nicht für die Behördennetze. Dort bestehen die Mängel fort.

Das BMI hat dringend auf alle Bundesbehörden einzuwirken, damit diese ihre Behördennetze endlich absichern und für die Verarbeitung von Verschlusssachen freigeben. Bis dahin muss es die Risiken für die Netze des Bundes minimieren. Zudem muss das BSI künftig zeitnah reagieren, wenn Bundesbehörden ihren Verpflichtungen im Geheimschutz nicht nachkommen. Dies hat das BMI im Wege seiner Aufsichtspflicht sicherzustellen.

3.1 Prüfungsfeststellungen

Teilnahme an den Netzen des Bundes nur für sichere und freigegebene Behördennetze

Der Eigenschutz staatlicher Strukturen ist – wie das BMI z. B. in seiner Cybersicherheitsagenda darstellt – grundlegend für eine handlungsfähige Bundesverwaltung. In Zeiten zunehmender Bedrohung aus dem Cyberraum gilt dies besonders für Behörden, die geheimhaltungsbedürftige Daten verarbeiten.

Das BMI ist auch für den staatlichen Geheimschutz zuständig. Es hat im Jahr 2006 die „Allgemeine Verwaltungsvorschrift zum materiellen Geheimschutz“ (Verschlusssachenanweisung) erlassen und diese im Jahr 2018 novelliert. Darin ist geregelt, wie die Bundesverwaltung mit geheimhaltungsbedürftigen Daten umzugehen hat. Darunter fallen auch Daten des Geheimhaltungsgrades „VS – NUR FÜR DEN DIENSTGEBRAUCH“ (VS-NfD). Dieser wird für Daten verwendet, deren Kenntnisnahme durch Unbefugte für die Interessen der Bundesrepublik Deutschland oder eines ihrer Länder nachteilig sein kann. Die Verschlusssachenanweisung regelt u. a., wie Verschlusssachen elektronisch zu verarbeiten sind. Das BSI soll die Bundesbehörden bei organisatorischen und technischen Sicherheitsmaßnahmen unterstützen und beraten.

Für die sichere Kommunikation und den Datenaustausch bis zum Geheimhaltungsgrad VS-NfD nutzt die Bundesverwaltung die Netze des Bundes als ressortübergreifende Kommunikationsinfrastruktur. Das BSI hat deren Informationssicherheit zu gestalten und zu prüfen. Hierzu hat es Schutzmechanismen für die Netze des Bundes zentral vorgegeben.

Um an den Netzen des Bundes teilzunehmen, muss jede Bundesbehörde die sogenannten „Nutzerpflichten Netze des Bundes“ (Nutzerpflichten) erfüllen. Dazu gehört, dass sie ihr Behördennetz für die Verarbeitung von VS-NfD absichern und anschließend freigeben muss. Diese Verschlusssachen-Freigabe ist u. a. daran gebunden, dass die Bundesbehörde ein aktuelles Informationssicherheitskonzept hat. Dafür muss sie bestehende Risiken für die Informationssicherheit ermitteln, bewerten und ihnen ggf. begegnen. Stellt eine Bundesbehörde Sicherheitsmängel fest, muss sie diese unmittelbar beheben.

Bundesbehörden nehmen trotz IT-Sicherheitsmängeln und fehlender Verschlusssachen-Freigabe an den Netzen des Bundes teil

Der Bundesrechnungshof hat in den Jahren 2017 bis 2022 bei 19 Prüfungen zur Informationssicherheit in der Bundesverwaltung gleichgelagerte Verstöße gegen die Nutzerpflichten und die Verschlusssachenanweisung festgestellt. Bundesbehörden hatten u. a.

- keine, keine vollständigen oder veraltete Informationssicherheitskonzepte,
- ihre Netze nicht ausreichend abgesichert,

- veraltete Betriebssysteme auf Servern im Einsatz,
- Server, Clients und Datenbanken nicht genügend gegen Cyberangriffe geschützt und
- IT-Personal eingesetzt, das nicht sicherheitsüberprüft war, obwohl es mit sicherheitsempfindlichen Tätigkeiten betraut war.

Die Bundesbehörden nahmen an den Netzen des Bundes teil, obwohl ihre Behördennetze weder die Nutzerpflichten noch die Verschlusssachenanweisung erfüllten. Entsprechend hatte auch keine dieser Bundesbehörden ihr Netz für die Verarbeitung von VS-NfD freigegeben.

Das BSI hatte zuletzt im Jahr 2021 die Verschlusssachen-Freigabe von Behördennetzen abgefragt. 21 der insgesamt 105 an den Netzen des Bundes teilnehmenden Bundesbehörden meldeten dem BSI, ihr Behördennetz oder Teile davon für die Verarbeitung von VS-NfD freigegeben zu haben. Auf die geringe Anzahl der Rückmeldungen reagierte das BSI nicht.

Verschärfte Vorgaben für „Dienststellen mit besonderem Geheimschutzbedarf“

Das BMI hat insgesamt 18 Bundesbehörden, darunter acht aus seinem Geschäftsbereich, als „Dienststellen mit besonderem Geheimschutzbedarf“ festgelegt. Deren Verschlusssachen sind in besonderem Maße Ziel von Angriffen. Diese Bundesbehörden müssen gemeinsam mit dem BSI weitere Sicherheitsvorkehrungen treffen. U. a. müssen sie sich mindestens alle vier Jahre vom BSI umfassend beraten und prüfen lassen.

Einige Bundesbehörden gaben an, dass sie infolge mangelnder Ressourcen beim BSI keine oder keine zeitnahe Geheimschutzberatung erhalten hätten. Inwieweit sie noch angemessen geschützt seien, könnten sie deshalb nicht einschätzen.

BMI waren Mängel schon im Jahr 2019 bekannt

Der Bundesrechnungshof hatte den Haushaltsausschuss des Deutschen Bundestages bereits im Jahr 2019 über fehlende Verschlusssachen-Freigaben und Sicherheitsmängel bei Behördennetzen unterrichtet. Das BMI sagte daraufhin zu, die Verschlusssachen-Freigabe für die Netze des Bundes bis zum Jahresbeginn 2020 abschließen zu wollen. Die Netze des Bundes haben zwischenzeitlich eine Verschlusssachen-Freigabe mit Auflagen bis zum Jahr 2023 erhalten. Auf die Verschlusssachen-Freigabe für die Behördennetze ging das BMI in seiner damaligen Stellungnahme nicht ein. Dort bestehen die Mängel fort.

3.2 Würdigung

Die Bedrohung der Bundesverwaltung durch Cyberangriffe verschärft sich seit Jahren. Dennoch missachten Bundesbehörden den staatlichen Geheimschutz in ihren Behördennetzen

und erfüllen nicht die Mindestanforderungen. Dies ist nicht hinnehmbar. Eine Bundesbehörde gefährdet nicht nur die Sicherheit ihrer eigenen Daten, wenn sie wesentliche Vorgaben der Verschlusssachenanweisung und der Nutzerpflichten nicht beachtet. Sie gefährdet vielmehr die Sicherheit aller anderen Bundesbehörden, die an den Netzen des Bundes teilnehmen. Die zentral bereitgestellten Schutzmechanismen für die Netze des Bundes reichen allein **nicht** aus, wenn Behördennetze nur unzureichend abgesichert sind.

Der Bundesrechnungshof hatte bereits im Jahr 2019 darauf hingewiesen, dass die Behördennetze zeitnah zu überprüfen sind. Er hat in seinen Prüfungen immer wieder Mängel bei der Informationssicherheit in Behördennetzen festgestellt. Zwar sind die Netze des Bundes zwischenzeitlich für Verschlusssachen freigegeben. Dies reicht jedoch nicht aus, wenn Bundesbehörden an den Netzen des Bundes teilnehmen, obwohl sie die Nutzerpflichten nicht erfüllen. Dieser Zustand dauert bereits seit Jahren an. Dies birgt erhebliche Risiken für den Schutz der geheimhaltungsbedürftigen Verschlusssachen. Das BSI ist sowohl für die Informationssicherheit der Netze des Bundes als auch der gesamten Bundesverwaltung verantwortlich. Es hätte kontrollieren müssen, ob **ausschließlich** Bundesbehörden an den Netzen des Bundes teilnehmen, die in ihren Behördennetzen die Mindestanforderungen erfüllen.

Seit fast einem Jahr ist dem BSI bekannt, dass 80 % der an Netzen des Bundes teilnehmenden Bundesbehörden ihre Behördennetze nicht für Verschlusssachen freigegeben haben. Es hat bislang weder die Gründe hierfür ermittelt noch die Bundesbehörden auf ihre Pflichten hingewiesen. Das BSI hätte diese kontrollieren und zusätzliche Schutzmaßnahmen verlangen müssen.

Angesichts der aktuellen Bedrohungslage im Cyberraum stellen „Dienststellen mit besonderem Geheimschutzbedarf“ herausgehobene Angriffsziele dar. Dies auch, weil diese Dienststellen viele Verschlusssachen in ihren Behördennetzen verarbeiten. Das BMI hätte daher besonders darauf achten müssen, dass diese Bundesbehörden, vor allem in seinem eigenen Geschäftsbereich, ihre Beratungs- und Prüfpflichten einhalten. Indem es diese Pflichten nicht aktiv einforderte, war der Schutz der dort verarbeiteten Verschlusssachen gefährdet.

Das BMI muss darauf hinwirken, dass **jede** an den Netzen des Bundes teilnehmende Bundesbehörde ihr Behördennetz für die Verarbeitung von VS-NfD umfassend absichert und anschließend für die Verarbeitung von Verschlusssachen freigibt.

3.3 Stellungnahme

Das BMI hat darauf hingewiesen, dass die Behördennetze bereits Anfang des Jahres 2019 in die Netze des Bundes aufgenommen worden seien. Die Nutzerpflichten dafür seien jedoch erst im September 2019 in Kraft getreten. In der Folge habe sich ein Teil der betroffenen Bundesbehörden außerstande gesehen, die Anforderungen der Nutzerpflichten zu erfüllen. Es sei jedoch weder realistisch, praktikabel noch erwünscht gewesen, Bundesbehörden von den Netzen des Bundes abzukoppeln. Alle Beteiligten würden daran arbeiten, die fehlenden Verschlusssachen-Freigaben schnellstmöglich nachzuholen. Einige Bundesbehörden könnten

die Sicherheitsvorgaben der Nutzerpflichten auch perspektivisch nicht erfüllen. Für diese habe das BMI damit begonnen, ein eigenes Netz aufzubauen; die sogenannte „Grundschutzzone/Extranet“.

Das BSI habe bei der Geheimschutzberatung und -kontrolle seine Belastungsgrenze überschritten. Beträchtliche Ressourcen seien für Geheimschutzaspekte in verschiedensten Projekten gebunden. Daher habe das BSI bereits seit längerer Zeit nicht mehr alle Bundesbehörden beraten können. Von den „Dienststellen mit besonderem Geheimschutzbedarf“ sei bislang nur eine einzige mit einem entsprechenden Beratungs- und Prüfbedarf an das BSI herangetreten.

Das BMI hat angekündigt, das BSI nunmehr in die Lage zu versetzen, seinen gesetzlichen Aufgaben besser nachzukommen. Hierzu wolle es das BSI zu einer umfassenden Aufgabenkritik und -priorisierung auffordern. Auch sei das Freigabeverfahren für Verschlusssachen-IT wegen unterschiedlicher rechtlicher Grundlagen für Geheimschutz und Informationssicherheit nicht praktikabel. Es prüfe aktuell, dieses anzupassen.

3.4 Abschließende Würdigung

Die Stellungnahme des BMI verdeutlicht: Die Mängel bei der Absicherung und der Verschlusssachen-Freigabe der Behördennetze sind nicht Folge eines Erkenntnis-, sondern eines Umsetzungsdefizits. BMI und BSI hatten alle erforderlichen Informationen schon seit längerer Zeit. Sie traten den Verstößen der Bundesbehörden gegen die Geheimschutzvorgaben jedoch nicht wirksam entgegen.

Die Argumentation des BMI, die Nutzerpflichten seien erst nach der Aufnahme der Bundesbehörden in die Netze des Bundes in Kraft getreten, geht fehl. Sie verkennt, dass die Vorgaben der Verschlusssachenanweisung zum ausschließlichen Einsatz von für Verschlusssachen freigegebener IT bereits viel früher galten. Hiergegen verstieß die Mehrzahl der Bundesbehörden schon, bevor sie in die Netze des Bundes aufgenommen wurden. Solange die IT-Sicherheitsmängel in den Bundesbehörden nicht abgestellt sind, verbleiben erhebliche Risiken für den Schutz der Verschlusssachen: Das schwächste Glied in der Kette der an den Netzen des Bundes teilnehmenden Bundesbehörden bestimmt die Sicherheit im gesamten Kommunikationsverbund.

Die „Grundschutzzone/Extranet“ kann für einige Bundesbehörden eine angemessene Lösung darstellen; für die Mehrzahl ist sie das jedoch nicht. Die Ankündigung des BMI, die fehlenden Verschlusssachen-Freigaben schnellstmöglich nachzuholen, reicht hier nicht aus. Es ist unklar, bis wann dies abgeschlossen sein soll. Angesichts der teils gravierenden Defizite in der Informationssicherheit der Bundesbehörden sind Verschlusssachen-Freigaben kurzfristig nicht realistisch zu erwarten. Das BMI sollte daher zunächst die Ursachen für die fehlenden Verschlusssachen-Freigaben ermitteln und diese anschließend beheben. Hierzu hat es mit den betroffenen Bundesbehörden einen risikoorientierten Zeitplan zu erarbeiten. Für die

Zwischenzeit muss das BMI Ausgleichsmaßnahmen vorsehen, um die Risiken für die Netze des Bundes zu minimieren.

Der Bundesrechnungshof stimmt mit dem BMI darin überein, dass das BSI seine vielfältigen Aufgaben kritisch analysieren und anschließend priorisieren muss. Einen Schwerpunkt sollte das BSI dabei auf die Geheimschutzberatung und -kontrolle legen. Hier muss es deutlich aktiver werden. Erst recht gilt dies für die „Dienststellen mit besonderem Geheimschutzbedarf". Es ist unverständlich, dass das BMI für diese Bundesbehörden einerseits feststellt, sie seien in besonderem Maße das Ziel von Angriffen auf ihre Verschlusssachen, andererseits die verschärften Vorgaben daraus aber nicht konsequent umsetzt. Dies betrifft insbesondere die acht Bundesbehörden im eigenen Geschäftsbereich. Das BMI muss hier seine Aufsichtspflicht intensiver wahrnehmen.

Angesichts der fortschreitenden Digitalisierung in der Bundesverwaltung erachtet es der Bundesrechnungshof als sachgerecht, zu überprüfen, ob die Prozesse zur Freigabe von Verschlusssachen-IT anzupassen sind. Unabhängig davon bleibt er bei seiner Auffassung, dass die Bundesbehörden ihre Informationssicherheit deutlich steigern müssen. Nur so lassen sich die Verschlusssachen, die Behördennetze und die Netze des Bundes auch in Zeiten stetig zunehmender Bedrohungen wirksam schützen.