Bundesministerium für Wirtschaft und Energie (BMWi)
(Einzelplan 09)

9 Bekannte IT-Sicherheitsmängel im Bundeskartellamt bestehen nach zehn Jahren immer noch

(Kapitel 0917)

Zusammenfassung

Das Bundeskartellamt stellt Sicherheitsmängel in seiner Informationstechnik (IT) über zehn Jahre hinweg nicht vollständig ab, obwohl es dies mehrfach zugesichert hat. Damit gefährdet es seine Arbeitsfähigkeit und die von ihm verarbeiteten sensiblen Daten.

Aufgabe des Bundeskartellamts ist es, den Wettbewerb in Deutschland zu schützen. Es muss dabei die Sicherheit der in seinem Haus verarbeiteten Daten gewährleisten. Bereits im Jahr 2011 hatten der Bundesrechnungshof und das Bundesamt für Sicherheit in der Informationstechnik (BSI) das Bundeskartellamt auf erhebliche Mängel in der IT-Sicherheit hingewiesen. Im Jahr 2018 stellte der Bundesrechnungshof fest, dass es diese nicht vollständig behoben hatte. Zwei Jahre später musste das Bundeskartellamt erneut einräumen, mit einigen Sicherheitsmaßnahmen lediglich begonnen zu haben. Als zentrale Ursache führte es fehlendes Fachpersonal an.

Das Bundeskartellamt muss die Sicherheit und den Notfallschutz seiner IT gewährleisten. Indem es bekannte Sicherheitsmängel über viele Jahre nicht behebt, geht es ein erhebliches, vermeidbares Risiko ein. U. a. könnten Unbefugte an sensible Daten gelangen. Das Bundeskartellamt muss unverzüglich alle Mängel beheben sowie notwendige Konzepte erarbeiten, umsetzen und regelmäßig aktualisieren. Die dafür notwendigen finanziellen und personellen Ressourcen hat das BMWi bei Bedarf zu ergänzen.

9.1 Prüfungsfeststellungen

IT-Sicherheit ist notwendige Daueraufgabe

Das Bundeskartellamt ist eine unabhängige Behörde im Geschäftsbereich des BMWi. Seine Aufgabe ist es, den Wettbewerb in Deutschland zu schützen. Beispielsweise beaufsichtigt es marktbeherrschende Unternehmen und überprüft die Vergabe öffentlicher Aufträge des

Bundes. Das Bundeskartellamt verarbeitet Daten von Wirtschaftsunternehmen. Es muss die Sicherheit dieser sensiblen und besonders schützenswerten Daten gewährleisten.

Das Bundeskartellamt ist verpflichtet, seine IT zu schützen. Hierzu muss es Konzepte, Grundlagendokumente und Handbücher erarbeiten, diese kontinuierlich fortschreiben und die darin enthaltenen Vorgaben umsetzen. Zudem ist das Bundeskartellamt verpflichtet, seine IT-Sicherheitsmaßnahmen mindestens alle drei Jahre z. B. in Form von Informationssicherheitsrevisionen (IS-Revisionen) zu überprüfen. Die Ergebnisse sind zu dokumentieren. IS-Revisionen zielen darauf ab, die Informationssicherheit zu verbessern und Fehlentwicklungen zu vermeiden. Das BSI bietet den Bundesbehörden an, diese IS-Revisionen durchzuführen.

IT-Sicherheit im Bundeskartellamt war lückenhaft

Der Bundesrechnungshof hatte bereits Anfang 2011 das unvollständige und veraltete IT-Sicherheitskonzept des Bundeskartellamts bemängelt. Das BMWi räumte seinerzeit ein, das Bundeskartellamt habe das IT-Sicherheitskonzept in der Vergangenheit nicht im notwendigen Maße fortgeschrieben. Der Grund habe insbesondere in personellen Engpässen gelegen. Zudem sagte das BMWi zu, das Bundeskartellamt werde mithilfe eines externen Dienstleisters ein umfassendes IT-Sicherheitskonzept erstellen. In den Folgejahren könne eigenes Personal dieses dann fortschreiben.

Im gleichen Jahr ließ das Bundeskartellamt eine IS-Revision durch das BSI vornehmen. Dieses stellte technische Mängel fest. Darüber hinaus beanstandete das BSI fehlende Vorgaben zum IT-Notfallmanagement des Bundeskartellamts.

Keine grundlegende Verbesserung nach sieben Jahren

Im Jahr 2018 prüfte der Bundesrechnungshof die IT-Sicherheit beim Bundeskartellamt erneut. Entgegen der Zusage des BMWi aus dem Jahr 2011 war das IT-Sicherheitskonzept des Bundeskartellamts weder vollständig noch aktuell. Rund 1 000 Einzelmaßnahmen daraus hatte das Bundeskartellamt erst teilweise, rund 800 noch gar nicht umgesetzt. Auch bearbeitete es geheimhaltungsbedürftige Daten (sog. Verschlusssachen) auf nicht dafür freigegebenen IT-Systemen. Sicherheitsmängel, die das BSI bereits im Jahr 2011 festgestellt hatte, hatte das Bundeskartellamt nicht vollständig behoben. Darüber hinaus erkannte der Bundesrechnungshof weitere Sicherheitsmängel. Seit dem Jahr 2011 hatte das Bundeskartellamt zudem keine IS-Revisionen veranlasst.

Erneut sicherte das BMWi zu, das Bundeskartellamt werde die Mängel beheben. U. a. solle es

- das IT-Sicherheitskonzept aktualisieren, vervollständigen und kontinuierlich fortschreiben und
- anschließend eine neue IS-Revision veranlassen.

Für das IT-Notfallmanagement sei bereits ein Dienstleister beauftragt und vor Ort tätig. Der Informationssicherheitsbeauftragte des Bundeskartellamts werde regelmäßig die IT-Sicherheit kontrollieren und die Ergebnisse sowie daraus resultierende Maßnahmen dokumentieren. Gleichwohl schränkte das BMWi ein, das Bundeskartellamt müsse bei den Maßnahmen seine vorhandenen Ressourcen berücksichtigen.

Daueraufgabe IT-Sicherheit weiterhin verbesserungsfähig

Der Bundesrechnungshof fragte Ende des Jahres 2020 den Sachstand ab. Das Bundeskartellamt räumte ein, bis zu neun Jahre bekannte Mängel noch nicht vollständig behoben zu haben. Es erklärte z. B.,

- das Projekt für das neue IT-Sicherheitskonzept befinde sich in der Planungsphase,
- die Erarbeitung eines IT-Notfallkonzepts habe es auf die Jahre 2021 und folgende verschieben müssen und
- eine IS-Revision, regelmäßige Sicherheitskontrollen durch den Informationssicherheitsbeauftragten und die Freigabe für die Verarbeitung von Verschlusssachen werde es erst nach Aktualisierung des IT-Sicherheitskonzepts veranlassen.

Das Bundeskartellamt begründete dies u. a. mit knappen Ressourcen und teilweise anderen Prioritäten.

In einem Schreiben an den Präsidenten des Bundeskartellamts wies dessen Informationssicherheitsbeauftragter im Jahr 2020 auf einzuhaltende Vorgaben hin. Er führte aus, das Bundeskartellamt müsse für die IT-Sicherheit bestehende Konzepte weiterentwickeln und neue erstellen. Dies gewährleiste, dass das Bundeskartellamt die von ihm verwalteten Informationen ihrem Schutzbedarf angemessen behandele. Andernfalls verschlechtere sich das gesamte Sicherheitsniveau und die Arbeitsfähigkeit des Bundeskartellamts sei mittelbar gefährdet.

9.2 Würdigung

Es ist nicht akzeptabel, dass das Bundeskartellamt im Jahr 2011 festgestellte Mängel bei der IT-Sicherheit noch nicht vollständig behoben hat.

Das Bundeskartellamt benötigt ein vollständiges, umfassendes und aktuelles IT-Sicherheitskonzept. Nur damit kann es den zunehmenden, von außen und innen drohenden Gefahren für die IT angemessen begegnen. Dabei muss es die für die Bundesverwaltung vorgegebenen Standards erfüllen. Das Schreiben des Informationssicherheitsbeauftragten aus dem Jahr 2020 belegt, dass sich das Bundeskartellamt dieser Mängel bewusst war. Umso unverständlicher ist, dass es wissentlich über viele Jahre hinweg ein erhebliches, vermeidbares Risiko eingegangen ist. Ein erfolgreicher Hacker-Angriff könnte die Arbeitsfähigkeit des

Bundeskartellamts beeinträchtigen und sensible, besonders schützenswerte Daten könnten an Unbefugte gelangen.

Von dem Jahr 2011 bis heute hätte das Bundeskartellamt mindestens drei IS-Revisionen veranlassen müssen. Das BSI hätte hierbei immer wieder andere Schwerpunkte zur IT des Bundeskartellamts untersuchen und so Hinweise zum Status der IT-Sicherheit geben können. Auf dieser Grundlage hätte das Bundeskartellamt seine IT-Sicherheitsrisiken minimieren können. Aktuell besteht die Gefahr, dass Risiken unerkannt geblieben sind und es gegen diese erst zu einem späteren Zeitpunkt Maßnahmen ergreifen wird.

Das BMWi muss darauf hinwirken, dass das Bundeskartellamt nunmehr unverzüglich alle Mängel beseitigt. Die erforderlichen Konzepte muss das Bundeskartellamt nach den Vorgaben des BSI erarbeiten, umsetzen und regelmäßig fortschreiben. Künftige Sicherheitsmängel muss das Bundeskartellamt zeitnah beheben, um Risiken möglichst gering zu halten.

Das BMWi muss sicherstellen, dass das Bundeskartellamt seine personellen und finanziellen Mittel für die IT-Sicherheit zielgerichtet verwendet und ggf. fehlende Mittel erhält.

9.3 Stellungnahme

Das BMWI hat erklärt, das Bundeskartellamt habe sein IT-Sicherheitskonzept zuletzt in den Jahren 2011/2012 aktualisiert. Damit habe es der Empfehlung des Bundesrechnungshofes entsprochen. Aufgrund der hohen Personalfluktuation sei es dem Bundeskartellamt nur bedingt möglich gewesen, das IT-Sicherheitskonzept fortzuschreiben. In den nachfolgenden Jahren habe das Bundeskartellamt jedoch sein IT-Sicherheitsmanagement weiterentwickelt und verbessert. Es habe Richtlinien, Leitlinien und Konzepte zur IT-Sicherheit entwickelt, Beschäftigte sensibilisiert und technische Maßnahmen umgesetzt.

Die vom BSI bei der IS-Revision im Jahr 2011 festgestellten Mängel habe das Bundeskartellamt nahezu vollständig abgearbeitet. Im Jahr 2012 habe es ein Konzept zum IT-Krisenmanagement verabschiedet. Die bis zum Jahr 2016 erstellten Entwürfe für eine IT-Notfallleitlinie und ein IT-Notfallvorsorgekonzept habe das Bundeskartellamt wegen erneuter personeller Wechsel nicht fertigstellen können. Auch ein im Jahr 2018 begonnenes Projekt zum IT-Notfallmanagement habe es aufgrund knapper Personalressourcen und anderer Prioritäten wieder zurückstellen müssen. Vordringlich wolle es nun das IT-Sicherheitskonzept aktualisieren. Dieses benötige das Bundeskartellamt, damit es Verschlusssachen verarbeiten darf.

Noch im Jahr 2018 habe das Bundeskartellamt damit begonnen, einige vom Bundesrechnungshof festgestellte Mängel der IT, des IT-Sicherheitskonzepts und des IT-Notfallmanagements zu beheben. Mehrere Maßnahmen habe es bereits vollständig umgesetzt. Wenn das Bundeskartellamt das IT-Sicherheitskonzept aktualisiert hat, beabsichtige es, seine IT-Sicherheit regelmäßig selbst zu kontrollieren und IS-Revisionen zu beauftragen.

Die Leitung des Bundeskartellamts messe der IT-Sicherheit eine hohe Bedeutung bei und unterstütze Maßnahmen dazu uneingeschränkt.

Das Bundeskartellamt verarbeite in nur sehr eingeschränktem Umfang Verschlusssachen.

Das BMWi hat die IT-Sicherheitssituation des Bundeskartellamts u. a. mit einer überdurchschnittlichen Personalfluktuation begründet. Mitarbeitende seien wegen finanzieller Anreize und attraktiveren Beschäftigungs- und Einstellungsbedingungen zu anderen Behörden gewechselt. Seit dem Jahr 2015 hätten 14 Beschäftigte mit unmittelbarem oder mittelbarem Bezug zu Aufgaben der IT-Sicherheit das Bundeskartellamt verlassen. So sei zuletzt im April 2021 auch der Informationssicherheitsbeauftragte nach gut einem Jahr Amtszugehörigkeit gegangen. Es sei in den letzten Jahren äußerst schwierig gewesen, geeignetes Personal zu gewinnen. Das Bundeskartellamt stehe in sehr harter Konkurrenz mit finanzkräftigen Unternehmen und anderen Behörden um qualifiziertes Personal.

Die Corona-Pandemie habe auch das Bundeskartellamt erheblich belastet. Dadurch hätten sich die IT-Sicherheitsmaßnahmen, welche der Bundesrechnungshof empfohlen hatte, verzögert. Das Bundeskartellamt werde diese nun wieder zügig abarbeiten.

9.4 Abschließende Würdigung

Der Bundesrechnungshof erkennt an, dass das Bundeskartellamt nicht untätig war und zahlreiche Maßnahmen zur IT-Sicherheit durchgeführt hat. Er bleibt dennoch bei seiner Auffassung, dass das Bundeskartellamt gravierende, bis zu zehn Jahre bekannte Sicherheitsmängel nicht vollständig abgestellt hat. Hierzu gehören neben den konzeptionellen auch gravierende technische Sicherheitsmängel.

Ein IT-Sicherheitskonzept ist kein Selbstzweck. Sein Ziel ist es, notwendige Maßnahmen zu identifizieren, um die betroffenen Daten und IT-Systeme wirksam zu schützen. Da das Bundeskartellamt sein IT-Sicherheitskonzept nicht vollständig umsetzt und fortlaufend aktualisiert, verfehlt dieses seinen Zweck. Ausgaben und Aufwand dafür sind in Teilen vergebens. Das Bundeskartellamt entspricht damit bis heute nicht der Empfehlung des Bundesrechnungshofes aus dem Jahr 2011.

Bereits seit dem Jahr 2006 sind Bundesbehörden, die Verschlusssachen verarbeiten, verpflichtet, ihre IT dafür abzusichern und freizugeben. Dies setzt voraus, dass sie über ein aktuelles IT-Sicherheitskonzept verfügen und dieses auch umgesetzt haben. Dies gilt unabhängig von Umfang und Inhalt der von ihnen verarbeiteten Verschlusssachen. Schon aus diesem Grund hätte das Bundeskartellamt der IT-Sicherheit in den vergangenen Jahren einen höheren Stellenwert einräumen müssen.

Das BMWi hat nicht erklärt, weshalb das Bundeskartellamt mit IT-Sicherheitskontrollen und IS-Revisionen warten will, bis das IT-Sicherheitskonzept aktualisiert ist. Beide können

hilfreich sein, um Schwachstellen aufzudecken, und damit zur Güte des IT-Sicherheitskonzepts beitragen.

Die Corona-Pandemie beeinträchtigt alle Bundesbehörden und nicht nur das Bundeskartellamt erheblich. Hätte das Bundeskartellamt die Mehrzahl seiner Maßnahmen wie zugesichert vor der Pandemie abgeschlossen, so bestünde nun kein Maßnahmenstau. Dafür trägt allein das Bundeskartellamt die Verantwortung.

Der Fachkräftemangel im Bereich der IT-Sicherheit betrifft alle Behörden. Deshalb darf das Bundeskartellamt aber schwerwiegende Defizite in der IT-Sicherheit nicht jahrelang auf sich beruhen lassen. Sowohl das Bundeskartellamt als auch das BMWi hätten rechtzeitig gegensteuern müssen. Das BMWi sollte das Bundeskartellamt dabei unterstützen, das aus z. B. Zulagen, Prämien und familienfreundlichen Arbeitszeitmodellen bestehende Anreizsystem auszuschöpfen. Es kann dadurch die Arbeitsplätze in der IT-Sicherheit attraktiver gestalten und eigenes wie neues Personal besser binden. Zudem muss es durch Aus- und Fortbildung mehrerer Beschäftigter für die einzelnen Schlüsselrollen der IT-Sicherheit vorsorgen. So kann es drohende Vakanzen wie z. B. bei dem Informationssicherheitsbeauftragten schneller auffangen. Ist nachweislich kein geeignetes Personal zu finden, hätte es – wie andere Behörden – beispielsweise externe Dienstleister längerfristig beauftragen können.

Das BMWi hat dafür zu sorgen, dass das Bundeskartellamt

- seine personellen und finanziellen Mittel für die IT-Sicherheit zielgerichtet verwendet,
- für die IT-Sicherheit fehlende Mittel erhält,
- Sicherheitsmängel regelmäßig durch IT-Sicherheitskontrollen und IS-Revisionen erhebt und
- ihm bekannte Sicherheitsmängel nun ohne weitere Verzögerungen behebt.