Bundesministerium der Finanzen (BMF)
(Einzelplan 08)

6 BMF toleriert Mängel beim Einsatz eines IT-Verfahrens in nachgeordneten Behörden

(Kapitel 0813)

Zusammenfassung

Das BMF muss darauf hinwirken, dass die Behörden in seinem Geschäftsbereich IT-Verfahren zur Bewirtschaftung von Haushaltsmitteln ordnungsgemäß einsetzen. Die Bundeszollverwaltung hält die haushaltsrechtlichen Vorschriften beim Einsatz eines solchen IT-Verfahrens derzeit nicht ein.

Der Bundesrechnungshof stellte beim Einsatz eines IT-Verfahrens in der Bundeszollverwaltung erhebliche zahlungs- und buchführungsrelevante Mängel fest. Diese betreffen auch andere Behörden der Bundesfinanzverwaltung sowie ein anderes Bundesministerium, die dasselbe IT-Verfahren nutzen. Darin sind zu weitreichende Berechtigungen vergeben. Zudem werden Datenänderungen unzureichend protokolliert. Dadurch ist es möglich, dass Beschäftigte des anderen Bundesministeriums unbemerkt auf Daten der Bundeszollverwaltung zugreifen.

Um Risiken für die Mittelbewirtschaftung zu vermeiden, muss das BMF darauf hinwirken, dass alle Datenänderungen im IT-Verfahren protokolliert werden. Zudem muss es sicherstellen, dass alle an das IT-Verfahren angeschlossenen Bewirtschafter nur auf ihre eigenen Daten zugreifen können. Dies erfordert geschäftsbereichsübergreifend klare und einheitliche Regelungen für die Rechtevergabe und die Protokollierung.

6.1 Prüfungsfeststellungen

Haushaltsrechtliche Vorschriften

Um eine ordnungsgemäße Mittelbewirtschaftung mit IT-Verfahren sicherzustellen, hat das BMF verschiedene haushaltsrechtliche Vorschriften erlassen. Sie dienen dazu, finanzielle Risiken für den Bundeshaushalt zu vermeiden. Die Vorschriften sehen u. a. vor, dass alle Buchungen und Zahlungen nachvollziehbar und unveränderlich sein müssen. Dies setzt insbesondere voraus, dass die in ein IT-Verfahren eingestellten Daten eines Geschäftsvorfalls

einem Verursacher eindeutig zuzuordnen sind. Hierzu müssen alle Änderungen an zahlungsrelevanten Daten protokolliert werden. Zudem müssen die Protokollierungen erkennen lassen, welche Person die Änderungen vorgenommen hat.

Bewirtschafter, die ein IT-Verfahren einsetzen, müssen dieses der Bundeskasse melden und die Einhaltung der haushaltsrechtlichen Vorschriften erklären. Wenn sie wesentliche Änderungen am IT-Verfahren vornehmen, müssen sie dies ebenfalls mitteilen. Für die Einhaltung der Vorschriften ist neben dem Bewirtschafter die oberste Bundesbehörde verantwortlich, in deren Geschäftsbereich das IT-Verfahren eingesetzt wird.

Bundeszollverwaltung verstößt beim Einsatz ihres IT-Verfahrens zur Bewirtschaftung von Haushaltsmitteln gegen haushaltsrechtliche Vorschriften

Der Bundesrechnungshof prüfte seit dem Jahr 2021 das IT-Verfahren mit dem die Bundeszollverwaltung ihren Sachhaushalt bewirtschaftet. Dieses Verfahren nutzten neben der Generalzolldirektion (GZD) auch weitere Behörden der Bundesfinanzverwaltung sowie ein anderes Bundesministerium. Die GZD zahlte mit dem Verfahren im Jahr 2021 insgesamt mehr als 700 Mio. Euro aus.

Das BMF hatte die Zuständigkeit für die Meldung des IT-Verfahrens im Jahr 2014 seinem damaligen IT-Dienstleister übertragen. Dieser erklärt auch gegenüber der Bundeskasse, dass die haushaltsrechtlichen Vorschriften eingehalten werden. Er kann dafür Teilbestätigungen der Dienststellen einholen, die das IT-Verfahren einsetzen. Die GZD gab gegenüber dem aktuellen IT-Dienstleister Informationstechnikzentrum Bund (ITZBund) zuletzt Anfang des Jahres 2021 eine solche Teilbestätigung ab.

Das IT-Verfahren kann in Mandanten und Buchungskreise gegliedert werden. Die Bundesfinanzverwaltung und das andere Bundesministerium waren als Mandanten eingerichtet. Dem Mandanten der Bundesfinanzverwaltung waren zudem Buchungskreise für die GZD und für weitere Behörden zugeordnet. Die Behörden können sowohl die Mandanten als auch die Buchungskreise unabhängig voneinander nutzen. Zugriffe aus anderen Mandanten oder Buchungskreisen können sie verhindern, indem sie Berechtigungen einschränken.

Die Benutzerverwaltung überwacht, wer in welcher Form auf das IT-Verfahren zugreifen darf. Sie richtet hierzu Benutzer mit verschiedenen Berechtigungen ein. Mit einem umfassenden Berechtigungsprofil kann ein Benutzer alle Aufgaben im gesamten IT- Verfahren uneingeschränkt durchführen und seine Aktivitäten löschen. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) empfiehlt daher, das umfassende Berechtigungsprofil sowie auch Rechte zum elektronischen Radieren nur in Notfällen und zeitlich befristet einzusetzen. Zudem sollten alle Änderungen protokolliert werden, die mit diesem Berechtigungsprofil vorgenommen werden.

Der Bundesrechnungshof stellte fest, dass die GZD im IT-Verfahren nur die vom Hersteller eingerichteten Standardprotokollierungen nutzte. Damit war z. B. nachvollziehbar, wann welcher Benutzer Ein- und Auszahlungen erfasst, geändert, geprüft oder freigegeben hatte. Benutzer können zahlungsrelevante Daten (wie Bankverbindungen von Zahlungspartnern) aber auch direkt in Tabellen ändern, auf die das Verfahren bei den einzelnen Buchungen zugreift. Diese Änderungen konnte die GZD nicht zuverlässig nachhalten. Die Tabellenprotokollierung des Verfahrens hatte sie nicht aktiviert. Auch kritische Aktivitäten bei den Systemeinstellungen (wie Anmeldungen mit Notfallbenutzerkennungen, denen das umfassende Berechtigungsprofil zugeordnet war) protokollierte sie nicht. Damit konnte die GZD nicht gewährleisten, dass die Zahlungen und Buchungen im IT-Verfahren nachvollziehbar waren. Sie konnte daher etwaige Fehler oder Missbräuche auch im Nachhinein nicht aufdecken oder nachvollziehen. Die Protokollierungseinstellungen galten auch für die anderen Behörden, die das IT-Verfahren einsetzten.

Darüber hinaus hatte die GZD verschiedenen Beschäftigten über ihre fachlichen Aufgaben hinaus weitreichende Berechtigungen zugewiesen (wie elektronisches Radieren). Einzelne dieser Berechtigungen hätten es den Beschäftigten ermöglicht, Zahlungsdaten und Systemeinstellungen sowohl der GZD als auch der anderen Behörden unbemerkt zu verändern.

Bundeszollverwaltung wollte Mängel nicht beseitigen – BMF nahm dies hin

Der Bundesrechnungshof bat die GZD, ihre Stellungnahme zu seinen Prüfungserkenntnissen mit dem BMF abzustimmen. Die GZD teilte darin mit, dass sie ihren Beschäftigten die kritischen Berechtigungen entzogen habe, sofern diese nicht zur Erfüllung administrativer Aufgaben erforderlich seien. Zur Protokollierung im IT-Verfahren vertrat die GZD die Auffassung, dass sie solche Systemeinstellungen nicht beeinflussen könne. Dafür sei das ITZBund verantwortlich. Darüber hinaus teilte sie mit, dass kein Anlass bestehe, das IT-Verfahren erneut der Bundeskasse zu melden. Diese Aussage hatte sie mit dem BMF abgestimmt.

Weitere Erkenntnisse

Im Jahr 2023 prüfte der Bundesrechnungshof die bewirtschafterübergreifende Konfiguration von automatisierten Verfahren beim ITZBund. Dabei stellte er fest, dass die Protokollierung von Tabellenänderungen und kritischen Aktivitäten in dem von der GZD genutzten IT-Verfahren noch nicht aktiviert war. Die Prüfung ergab zudem, dass auch außerhalb der GZD zahlreiche Personen weitreichende Berechtigungen in diesem IT-Verfahren hatten. So war 12 Benutzerkennungen der Bundesfinanzverwaltung und 15 Benutzerkennungen des anderen Bundesministeriums zum Jahresende 2022 das umfassende Berechtigungsprofil zugeordnet.

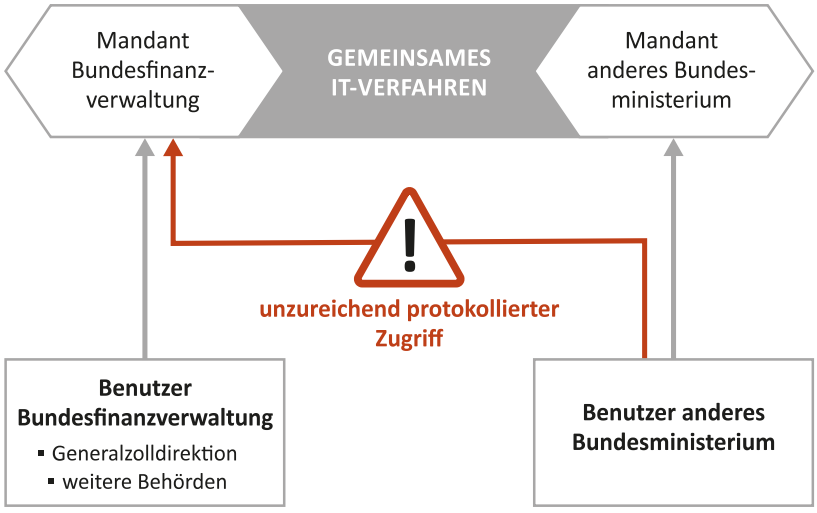
Im Mandanten der Bundesfinanzverwaltung fand der Bundesrechnungshof keinen Anhaltspunkt dafür, dass das umfassende Berechtigungsprofil im Zeitraum Januar 2021 bis August 2022 vergeben oder entzogen worden war. Im Mandanten des anderen Bundesministeriums

hatten im gleichen Zeitraum sieben Benutzer dieses Berechtigungsprofil neu erhalten. Nur in einem Fall hatte das andere Bundesministerium dieses Berechtigungsprofil anschließend wieder entzogen. Mit dem umfassenden Berechtigungsprofil hatten Benutzer des anderen Bundesministeriums unzureichend protokollierte Zugriffsmöglichkeiten auf die Haushaltsdaten der GZD.

Abbildung 6.1

Haushaltsdaten der GZD vor fremden Zugriffen unzureichend geschützt

Ein anderes Bundesministerium kann mit dem umfassenden Berechtigungsprofil auf den Mandanten der Bundesfinanzverwaltung im gemeinsam genutzten IT-Verfahren zugreifen. Da derartige Zugriffe unzureichend protokolliert werden, sind sie nicht nachvollziehbar.



Grafik: Bundesrechnungshof.

6.2 Würdigung

Die Ausführungen der GZD vom März 2022 haben gezeigt, dass das von ihr genutzte IT-Verfahren den haushaltsrechtlichen Vorschriften weiterhin nicht entsprechen wird. Das BMF hat dies hingenommen. Damit hat es weder seine Rechtsaufsicht über die GZD noch seine haushaltsrechtliche Verantwortung als zuständige oberste Bundesbehörde für das IT-Verfahren angemessen wahrgenommen.

Zudem hat es den Bewirtschaftern offenbar nicht ausreichend klar gemacht, dass sie für einen ordnungsgemäßen Verfahrenseinsatz verantwortlich bleiben. Dies gilt auch, wenn ein IT-Dienstleister das IT-Verfahren betreibt und es der Bundeskasse meldet.

Sowohl in der Bundesfinanzverwaltung als auch in dem anderen Bundesministerium waren darüber hinaus viele Benutzer eingerichtet, die mit dem umfassenden Berechtigungsprofil

dauerhaft auf das IT-Verfahren zugreifen konnten. Dies widerspricht den Empfehlungen des BSI.

Der Bundesrechnungshof hat das BMF aufgefordert sicherzustellen, dass die Bewirtschafter in seinem Geschäftsbereich die Nachvollziehbarkeit automatisierter Zahlungs- und Buchführungsprozesse gewährleisten. Hierzu muss es darauf hinwirken, dass auch Tabellenänderungen und kritische Aktivitäten bei den Systemeinstellungen protokolliert werden. Es darf darüber hinaus nicht zulassen, dass weitreichende Berechtigungen die Unveränderbarkeit von Zahlungsdaten und Systemeinstellungen sogar behördenübergreifend gefährden und Kontrollen ins Leere laufen lassen. Zudem muss es dafür sorgen, dass das ITZBund die Einhaltung der haushaltsrechtlichen Vorschriften erneut erklärt, sobald alle Beteiligten die Verfahrensmängel abgestellt haben.

6.3 Stellungnahme

Das BMF hat darauf hingewiesen, dass das ITZBund eine vollständige Protokollierung für das umfassende Berechtigungsprofil bisher aus Wirtschaftlichkeitsgesichtspunkten nicht in Betracht gezogen habe. Die Ausführungen des Bundesrechnungshofes deute es als Forderung nach einer maximal erreichbaren Sicherheit unter Außerachtlassung aller anderen Aspekte. Vor diesem Hintergrund würden die Tabellenprotokollierung und die Protokollierung kritischer Aktivitäten bei den Systemeinstellungen künftig standardmäßig für alle Benutzer aktiviert. Hierzu benötige das ITZBund Aufträge der Kundenbehörden. Das BMF werde diesen Prozess begleiten.

Die Berechtigungen zum elektronischen Radieren, zur Deaktivierung der Änderungsverfolgung sowie zur Änderung der Berechtigungsprüfung würden in der GZD nicht benötigt. Das ITZBund habe diese im Auftrag der GZD inzwischen gelöscht. Es werde die Zuweisung derartiger Berechtigungen an reine Anwender des IT-Verfahrens künftig noch kritischer hinterfragen und entsprechend ablehnen.

Im Mandanten der Bundesfinanzverwaltung sei das umfassende Berechtigungsprofil ausschließlich an technische und betrieblich notwendige Benutzerkennungen vergeben worden. Im ITZBund würden erweiterte Berechtigungen im Bereich der Systemadministration für den Mandanten der Bundesfinanzverwaltung nur temporär mit Begründung, Genehmigung und dokumentiertem Benutzerantrag vergeben. Seit dem Jahr 2022 fänden Erhebungen statt, um die tatsächlichen Erfordernisse von umfassenden Berechtigungsprofilen bei technischen Nutzerkennungen bewerten zu können.

Im Mandanten des anderen Bundesministeriums liege die Benutzer- und Rechteverwaltung nicht beim ITZBund, sondern ausschließlich beim Kunden. Das ITZBund sei hier als rein administrativer Dienstleister tätig. Es besitze keine (fachliche) Weisungsbefugnis. Es tausche sich aber bereits mit dem anderen Bundesministerium aus, um das umfassende Berechtigungsprofil zeitnah zu deaktivieren. Umsetzen müsse dies jedoch das andere Bundesministerium.

Das BMF hat eingeräumt, dass Benutzer des anderen Bundesministeriums mit dem umfassenden Berechtigungsprofil theoretisch Zugriff auf den Datenbestand aller Mandanten des IT-Verfahrens hätten. Es hat aber bestritten, dass derartige (theoretisch denkbare) Zugriffe auf Daten der GZD unbemerkt und unprotokolliert stattgefunden hätten. Dabei hat es auf die herstellerseitigen Standardprotokollierungsfunktionen verwiesen.

Im Übrigen habe das BMF kontinuierlich dafür gesorgt, die Vorgaben zur Verfahrenssicherheit in seinem Geschäftsbereich zu gewährleisten. Dabei habe es sich vor allem auf die Erstellung und stetige Fortschreibung der notwendigen Unterlagen konzentriert. Es werde künftig noch intensiver sicherstellen, dass den Bewirtschaftern die Maßgaben zum ordnungsgemäßen Verfahrenseinsatz verdeutlicht werden. Besonderes Augenmerk werde es auf die Rolle des ITZBund als zentrale Instanz für die Betreuung und Fortentwicklung des IT-Verfahrens legen. Das ITZBund werde die Abgabe einer aktualisierten Erklärung für das gesamte Verfahren prüfen. Das BMF werde mit den übrigen Bewirtschaftern der Bundesfinanzverwaltung den Prozess begleiten.

6.4 Abschließende Würdigung

Der Bundesrechnungshof bestreitet, dass seine Forderungen auf „eine Gewährleistung der maximal erreichbaren Sicherheit unter Außerachtlassung aller anderen Aspekte“ abstellen, wie vom BMF behauptet. Da das BSI die Aktivierung der Tabellenprotokollierung und die Protokollierung kritischer Aktivitäten bei den Systemeinstellungen empfiehlt, sollten diese vielmehr gängige Praxis sein.

Ungeachtet dessen erkennt der Bundesrechnungshof an, dass das BMF seiner Verantwortung als zuständige oberste Bundesbehörde inzwischen nachkommen will. Die Maßnahmen, die es angekündigt hat, um eine ordnungsgemäße Mittelbewirtschaftung mit dem IT-Verfahren in seinem Geschäftsbereich zu gewährleisten, gehen grundsätzlich in die richtige Richtung. Es sollte dabei jedoch die Risiken ernster nehmen, die sich aus dem geschäftsbereichsübergreifenden Verfahrenseinsatz ergeben.

Hierzu reicht es nicht aus, bei der Vergabe des umfassenden Berechtigungsprofils auf die unterschiedlichen Abläufe zur Berechtigungsvergabe in einzelnen Behörden oder Mandanten zu verweisen. Mit diesem Profil besteht das permanente Risiko, dass die Trennung der verschiedenen Mandanten unterlaufen wird. Außerdem ist es hiermit möglich, beliebige Informationen inklusive der Protokollierung zu ändern oder zu löschen. Das BSI empfiehlt daher, das umfassende Berechtigungsprofil und Rechte zum elektronischen Radieren nur in Notfällen zeitlich befristet zuzuweisen und deren Einsatz zu überwachen. Das BMF muss sich dafür einsetzen, dass sich sowohl das ITZBund als auch das andere Bundesministerium bei der Vergabe von Berechtigungen an diese Empfehlung halten. Anderenfalls kann es für die Behörden seines Geschäftsbereichs keinen ordnungsgemäßen Verfahrenseinsatz sicherstellen.