Cybersicherheit in der Buchhaltung

Herausforderungen aus der Sicht der externen Finanzkontrolle des Bundes

*Marie Bergmann/Inga Schedler**

Behörden nutzen in der Regel eigene IT-Systeme, um Haushaltsmittel des Bundes zu verwalten und Zahlungen anzuordnen. Der Bundesrechnungshof prüft neben dem Rechnungsabschluss des Bundes auch den ordnungsmäßigen Einsatz dieser IT-Systeme. Regelmäßig deckt er hierbei Mängel auf. Diese sind teilweise technisch und teilweise organisatorisch begründet. Wenn sich die Bundesverwaltung den Herausforderungen der Digitalisierung stellt, kann sie die Risiken beim Betrieb der IT-Systeme jedoch auf ein vertretbares Maß begrenzen.

Früher war alles anders

In der computerlosen Zeit konnten Behörden eine ordnungsmäßige Buchführung noch mit vergleichsweise einfachen Mitteln sicherstellen. Alle Vorgänge wurden auf Papier bearbeitet und kontrolliert. Das Interne Kontrollsystem (IKS) war somit überschaubar. Es bestand im Wesentlichen aus visuellen und physischen Merkmalen, wie Unterschriften und Schrankschlüsseln.

Im Mittelpunkt der Rechnungsbearbeitung stand das Anordnungsformular mit Durchschlag. Die Anordnung wurde mit den Unterschriften für die sachliche und rechnerische Richtigkeit sowie der Unterschrift der oder des Anordnenden gültig. Zwei unterschiedliche Unterschriften auf der Anordnung sollten das Vier-Augen-Prinzip gewährleisten. Den Durchschlag und die Belege bewahrte die Behörde auf, das Original der Anordnung erhielt die Bundeskasse. Diese prüfte die Anordnung auf Vollständigkeit und Echtheit. Dafür verglich sie die Unterschrift der oder des Anordnenden mit einer Unterschriftenprobe.

Von früher nach übermorgen

Heute setzt die Verwaltung in der Regel IT-Systeme ein, um Zahlungen und Buchungen im zentralen Verfahren für das Haushalts-, Kassen- und Rechnungswesen des Bundes (HKR) anzuordnen. An das zentrale HKR-Verfahren sind alle Behörden und Einrichtungen angebunden, die Haushaltsmittel des Bundes bewirtschaften. Dies gilt auch für Bewirtschafter aus Länder- oder Kommunalverwaltungen sowie aus sonstigen öffentlich-rechtlichen Einrichtungen. Mehr als 95 Prozent der Bewirtschafter nutzen IT-Systeme, um die Anordnungsdaten zu erstellen. Das Anordnungsformular wird durch eine Anordnungsdatei ersetzt, in der die Behörden durchaus mehrere tausend Anordnungen auf einmal zur Bundeskasse senden können. Formulare für Einzelanordnungen kommen nur noch in Ausnahmefällen zum Einsatz. Daher ist eine papiergebundene Kontrolle heute ohne Blick in die Systeme nicht mehr zweckmäßig. Das Vier-Augen-Prinzip ist meist über klar abgegrenzte Rechte im IT-System umgesetzt.

Die Buchung wird überwiegend in den unterschiedlichen IT-Systemen der Behörden belegt. Somit erstreckt sich die Buchführung des Bundes über eine komplexe, heterogene und spezialisierte Systemlandschaft (siehe Abb. 1).

Das IKS der Papierwelt lässt sich nicht eins-zu-eins auf die digitale Welt übertragen. Von manchen liebgewonnen Kontrollen auf Basis von Papierbelegen sollte sich die Bundesverwaltung daher verabschieden. Im Gegenzug muss sie die Kontrollen an die neuen Gefährdungen der IT-Welt anpassen. Grundsätzlich gilt dabei: Je komplexer die Abläufe der Rechnungsbearbeitung und Buchführung sind – etwa bei einer Verteilung der Arbeitsschritte auf mehrere Systeme und Standorte – umso größer ist auch das Fehlerpotenzial.

Allerdings bietet die IT-Welt auch die Chance, Kontrollen mit geringerem Aufwand durchzuführen und dabei sogar teilweise wirksamer als in der Papierwelt zu sein.

Dr. Marie Bergmann
Dipl.-Informatikerin, Prüferin im Prüfungsgebiet „Prüfung Rechnungsabschluss Bund“, Bundesrechnungshof

Inga Schedler
Dipl.-Informatikerin, Prüferin im Prüfungsgebiet „Prüfung Rechnungsabschluss Bund“, Bundesrechnungshof

* Der Aufsatz gibt ausschließlich die persönlcihe Meinung der Autorinnen wieder.

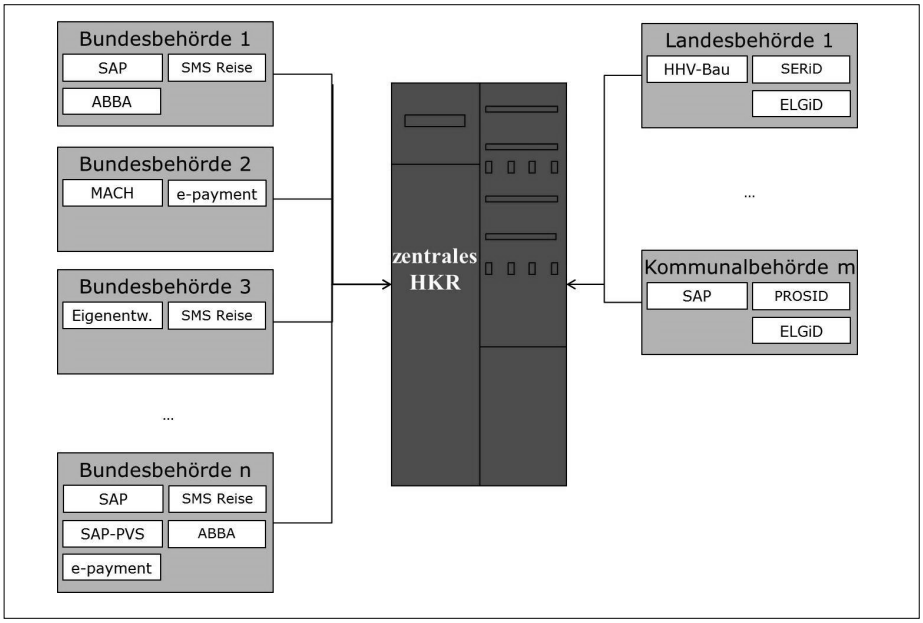

Abb. 1: Viele Bewirtschafter liefern Daten aus unterschiedlichen Systemen an das zentrale HKR-System des Bundes (Beispiele)

Die Digitalisierung der Buchführung schreitet ohnehin weiter voran: die ersten Behörden empfangen und verarbeiten schon die E-Rechnung und bewahren digitale Belege (in E-Akten) auf. Vereinzelt arbeiten Behörden bereits an voll automatisierten Rechnungsbearbeitungsprozessen, die das Eingreifen der Sachbearbeitung nur in Ausnahmefällen erfordert. Auch wenn viele Behörden hier noch am Anfang stehen, ist die Tendenz in Richtung Dunkelverarbeitung im Rechnungswesen des Bundes erkennbar. Etwa bei der Zahlung von Bezügen, Beihilfe oder Reisekosten sowie bei der Rückerstattung von Steuern oder Zöllen wird kaum noch manuell eingegriffen. Diese Entwicklung erfordert, das IKS und dessen Prüfungen anzupassen.

IT-Systemprüfungen des Bundesrechnungshofes

Der Bundesrechnungshof hat die Herausforderungen der Digitalisierung angenommen. Mit angepassten Prüfungsansätzen hat er sich auf die veränderte Situation in den Haushaltsreferaten der Behörden eingestellt: Seit fünf Jahren prüft der Bundesrechnungshof neben den Belegen auch die für die Rechnungslegung eingesetzten IT-Systeme. Der Prüfungsansatz orientiert sich an nationalen wie internationalen Prüfungsstandards. Er berücksichtigt auch die von der Internationalen Organisation der Obersten Rechnungskontrollbehörden (INTOSAI) empfohlenen International Standards of Supreme Audit Institutions (ISSAI).

Die Prüfung umfasst mit dem zu prüfenden IKS des Bewirtschafters sowohl die ordnungsmäßige Anwendung haushaltsrechtlicher Regelungen als auch den sicheren Einsatz der IT. Sie soll eine Aussage ermöglichen, inwieweit ein Bewirtschafter die allgemeinen Anforderungen für die Ordnungsmäßigkeit der Rechnungslegung erfüllt sowie die Vertraulichkeit, Integrität, Verfügbarkeit, Autorisierung, Authentizität und Verbindlichkeit sicherstellt. Daher sind für die Prüfung rechnungslegungsrelevanter IT-Systeme vornehmlich die Prüfungsfelder relevant, die die Richtigkeit, Vollständigkeit und Unveränderbarkeit der begründenden Unterlagen gewährleisten.

Die IT-Systemprüfungen sind vielschichtig angelegt: Die Prüferinnen und Prüfer sichten die Verfahrensdokumentation, beobachten den Rechnungsbearbeitungsprozess, führen Gespräche, prüfen Systemeinstellungen sowie vergebene Rechte und analysieren Buchungsdaten. Genau wie andere Behörden muss der Bundesrechnungshof daher bereits bei seiner Personalauswahl auch auf fundierte IT-Kenntnisse achten.

Der Bundesrechnungshof hat bei seinen IT-Systemprüfungen schon behördenübergreifend zahlreiche Kontrolllücken aufgedeckt. Bereits in den Jahren 2014 und 2016 hat er das Parlament über seine Feststellungen unterrichtet.[1] Dieser Beitrag greift wesentliche Punkte auf.

Normengerüst

Die zentrale Grundlage für die Prüfungen des Bundesrechnungshofes bildet das vom Bundesministerium der Finanzen (BMF) erlassene Normengerüst. Dieses umfasst insbesondere die Verwaltungsvorschriften für Zahlungen, Buchführung und Rechnungslegung[2], die Grundsätze ordnungsgemäßer Buchführung bei Einsatz automatisierter Verfahren[3] und die Bestimmungen über die Mindestanforderungen für den Einsatz automatisierter Verfahren[4].

Im Falle eines größeren Systemzusammenbruches, etwa im Krisen- oder Notfall, muss sichergestellt sein, dass keine Daten verloren gehen, der Bewirtschafter zahlungsfähig bleibt und sowohl das IT-System als auch die Buchungsdaten in

1 Bundesrechnungshof: Bemerkungen 2014 Nr. 03 „Risiken beim Betrieb zahlungsrelevanter IT-Systeme“ und Bericht nach § 88 Absatz 2 BHO vom 13.05.2016 „Automatisierte Verfahren zur Bewirtschaftung von Haushaltsmitteln des Bundes.“ Vgl. https://www.bundesrechnungshof.de/de/veroeffentlichungen/bemerkungen-jahresberichte/jahresberichte/2014/teil-ii-uebergreifende-und-querschnittliche-pruefungserkenntnisse/2014-bemerkungen-nr-03-risiken-beim-betrieb-zahlungsrelevanter-it-systeme und https://www.bundesrechnungshof.de/de/veroeffentlichungen/beratungsberichte/2016-bericht-automatisierte-verfahren-zur-bewirtschaftung-von-haushaltsmitteln-des-bundes.

2 Verwaltungsvorschrift für Zahlungen, Buchführung und Rechnungslegung (§§ 70 bis 72 und 74 bis 80 BHO) - VV-ZBR BHO. Vgl. https://www.jurion.de/gesetze/vv_zbr_bho/

3 Anlage 1 VV-ZBR BHO – Grundsätze ordnungsgemäßer Buchführung bei Einsatz automatisierter Verfahren im Haushalts-, Kassen- und Rechnungswesen des Bundes (GoBIT-HKR). Vgl. https://www.jurion.de/gesetze/vv_zbr_bho/anlage_1/

4 Bestimmungen über die Mindestanforderungen für den Einsatz automatisierter Verfahren im Haushalts-, Kassen- und Rechnungswesen des Bundes (BestMaVB-HKR). Vgl. https://www.jurion.de/gesetze/bestmavb_hkr-1/

geplanter Zeit wiederhergestellt werden können. Dabei muss jede Behörde für sich entscheiden, wie wichtig das jeweilige IT-System für ihre Buchhaltung und Arbeitsabläufe ist. Daher decken die haushaltsrechtlichen Normen mittelbar auch den informationstechnischen Bereich mit ab. Denn sie fordern gleichermaßen, dass die Standards des Bundesamtes für Sicherheit in der Informationstechnik (BSI) eingehalten werden. Diese Standards werden immer wieder dem aktuellen Stand der Informationstechnik angepasst, zuletzt im Oktober 2017.

Das Normengerüst soll – richtig vom Bewirtschafter angewandt – dafür sorgen, dass die Zahlungen und Buchungen ordnungsmäßig und sicher durchgeführt werden. Damit gibt es trotz zunehmenden IT-Einsatzes eine Konstante für das IKS – zumindest solange der Mensch den Ablauf der Rechnungsbearbeitung bestimmt: Damals wie heute regelt eine Dienstanweisung Abläufe, Kontrollen und Befugnisse. Nur wenn die Behördenleitung die Rechte und Pflichten klar regelt, können die Beschäftigten auch die volle Verantwortung für ihr Verwaltungshandeln im Rechnungswesen der Behörde übernehmen.

Dokumentation ist die Basis

Die Dokumentation des Verfahrens spielt eine wichtige Rolle im IKS. Sie ist kein Selbstzweck, sondern die Basis für wirksame interne Kontrollen. Zunächst sind die Gefährdungen für den IT-unterstützten Rechnungsbearbeitungsprozess und die sich daraus ergebenden finanziellen Risiken für den Behördenhaushalt zu analysieren und zu dokumentieren. Häufig verzichten Bewirtschafter jedoch auf diese Analyse. Infolgedessen fehlen entweder Konzepte zur Risikominimierung oder die Kontrollen sind nicht ausreichend wirksam.

Eine fehlende Verfahrensdokumentation bereitet schon im alltäglichen Betrieb des IT-Systems schnell Probleme, etwa im Vertretungsfall oder bei Neueinstellungen. An den Notfall oder Systemausfall denken die wenigsten. So fehlen den Beschäftigten häufig Informationen, um Rechnungen rechtzeitig bezahlen oder notwendige Softwareanpassungen durchführen zu können.

Riskante Medienbrüche

An alten haushaltstechnischen Gepflogenheiten wird oftmals festgehalten. So bescheinigen viele Bewirtschafter die Feststellung der sachlichen und rechnerischen Richtigkeit immer noch gern papiergebunden. Der IT-Prozess wird um diese Bescheinigungen herum konzipiert. Dies führt zu Medienbrüchen. Infolgedessen steigt das Risiko voneinander abweichender Daten zwischen Papier- und Systembelegung. Im Übrigen verzichten Bewirtschafter bei Medienbrüchen gerne auf systemseitige Unterstützungen, wie die Kontrolle des Vier-Augen-Prinzips oder Plausibilitätsprüfungen. Diese sind in vielen IT-Systemen integriert und können Fehleingaben verhindern. Bleiben sie ungenutzt, müssen Kontrollen anderweitig sichergestellt werden.

Das Optimierungspotenzial einer vollständigen Datenverarbeitung im Systemverbund mit anderen Systemen bleibt ungenutzt, etwa für die Beschaffung, Bestandsverwaltung, Korruptionsprävention etc. Die Behörde lässt sich so die Chance entgehen, von der Bedarfsanforderung bis zur Bezahlung den Belegpflichten durch systemseitige Protokollierung zu genügen.

Protokollierung

Die digitale Buchführung kennt das Radierverbot und verlangt eine eindeutige Zuordnung zwischen Buchung und Buchführenden. Um feststellen zu können, wer welche Daten wann geändert hat, muss das IT-System alle relevanten Datenänderungen protokollieren. Wenn eine zweite Person die Zahlung angeordnet hat, darf es an den Daten keine Änderungen mehr zulassen.

Wenn ein IT-System jedoch auf Datenbankebene ermöglicht, dass Buchungsdaten unprotokolliert geändert werden können, ist der Verursacher später nicht mehr zuverlässig zu ermitteln. Diese so genannte Prüfspur bei auffälligen Buchungen ist mindestens „verwischt".

Wenn IT-Systeme auch die Änderungen an Systemeinstellungen nicht protokollieren, lassen sich Fehlerursachen oder gar Manipulationen in der Regel nicht mehr systemseitig nachweisen. Somit besteht das Risiko, dass die Behörden eine grob fahrlässige Handlung oder gar einen etwaigen Missbrauch weder belegen noch entkräften können. Zudem wird es ohne Protokollierung noch schwieriger, den Umfang oder den Ursprung eventueller Angriffe von außen zu ermitteln.

»Nur wenn die Behördenleitung Rechte und Pflichten klar regelt, können die Beschäftigten auch die volle Verantwortung für ihr Verwaltungshandeln im Rechnungswesen der Behörde übernehmen.«

Passwörter sind Schlüssel

Früher wirkten der Unterschriftenvergleich bei der papiergebundenen Rechnungsbearbeitung und die damit verbundene Berechtigungsprüfung wie ein Türschlüssel. Dieser Schlüssel wird heute ersetzt durch Benutzerkennungen mit einer spezifischen Rechte- und Rollenkonfiguration im System. Die oder der Beauftragte für den Haushalt muss die Rechte so vergeben, dass jeder nur die ihm zugewiesenen Aufgaben im System durchführen kann. So muss z.B. sichergestellt sein, dass nur Anordnungsbefugte Zahlungen anordnen können. Da die Anordnungsbefugten die Einzelanordnung digital im IT-System „unterschreiben", obliegt die

Kontrolle der Berechtigungen heute dem Bewirtschafter und nicht mehr der Bundeskasse.

Zu häufig pflegen Bewirtschafter mit den Benutzerkennungen oder Passwörtern allerdings denselben Umgang wie mit Türschlüsseln: Wenn es erforderlich oder bequem erscheint, wird der Schlüssel auch schon mal an Kolleginnen und Kollegen großzügig weitergegeben. Dies passiert meistens nicht mit böser Absicht und führt in der Regel nicht zu finanziellen Schäden für den Bund. Dennoch ist der leichtfertige Umgang – auch aus Datenschutzgründen – ein Problem. Denn schon beim reinen Lesezugriff gilt das „Need-to-know-Prinzip", also Zugriff nur, falls die Aufgabe es erfordert.

Manche vergebenen Rechte können mitunter mit einem ganzen Schlüsselbund verglichen werden. Die IT-Systemprüfung trifft leider noch zu häufig auf diese Art Generalschlüssel, etwa den Einsatz des SAP_ALL Profils für SAP-Systeme. Manche Administratoren vergeben diese Rechte aus Bequemlichkeit oder Unwissenheit immer noch zu leichtfertig.

Auch Zugriffsrechte auf Daten außerhalb des Anordnungssystems können eine Gefahr darstellen, z.B. wenn Daten auf Gruppenlaufwerken gespeichert werden. Wird die dezidierte Rechtestruktur des Anordnungssystems nicht auf die Laufwerksebene übertragen, besteht zudem das Risiko eines Datenschutzverstoßes.

Oftmals ließe sich schon der Zugang zu den Systemen einschränken und damit das Risiko unberechtigter Datenzugriffe begrenzen. So sperrt z.B. eine automatische Bildschirmsperre den Zugang zu den Anwendungsdaten im IT-System für Unbefugte, sollte das manuelle Sperren des Bildschirms beim Verlassen des Arbeitsplatzes ausbleiben.

Funktionstrennung ist wichtig

Das Vier-Augen-Prinzip der Rechnungsbearbeitung soll sicherstellen, dass nicht eine Person alleine eine Zahlung veranlassen kann. Diese Trennung der Funktionen Datenerfassung und -freigabe gibt es auch für den Betrieb des IT-Systems: Niemand darf das System administrieren, entwickeln und damit Rechnungen bearbeiten. In der IT-Systemprüfung wird insbesondere die Trennung kritischer Funktionen geprüft. So sollte etwa die Benutzer- und Rechteverwaltung nicht in einer Hand bei den Fachadministratoren liegen. Sonst könnten sie sich zusätzliche Benutzer anlegen und damit das Vier-Augen-Prinzip umgehen.

Wenn eine Person mehrere Funktionen ausübt, sammelt sie auch ein umfangreicheres Wissen an. Verlässt sie die Behörde, geht viel mehr Wissen verloren als bei einer etablierten Funktionstrennung. Zudem ist diese Person für Innen- und Außentäter ein attraktiveres Angriffsziel.

»Das Vier-Augen-Prinzip soll sicherstellen, dass nicht eine Person alleine eine Zahlung veranlassen kann. Diese Trennung gibt es auch für den Betrieb des IT-Systems: Niemand darf das System administrieren, entwickeln und damit Rechnungen bearbeiten.«

Die Gründe für fehlende Funktionstrennung sind vielfältig, etwa beibehaltene Rechte nach einer Vertretungssituation, nach dem Wechsel in eine andere Organisationseinheit oder aus der Entwicklungsphase eines Verfahrens. Nicht selten haben daher auch Externe weiterhin unberechtigten Zugriff auf Daten.

Vereinbarungen zum IT-Betrieb

Behörden müssen mit ihrer IT-Abteilung oder ihrem behördeninternen IT-Dienstleister eindeutige Vereinbarungen zum Betrieb der IT-Systeme treffen, beispielsweise zu maximalen Systemausfallszeiten, Wartungsfenstern oder Notfallszenarien. Ohne diese Vereinbarungen riskiert die Fachseite letztlich längerfristige Systemausfälle.

Eine mangelnde Notfallvorsorge zeigt sich in der Prüfung unter anderem darin, dass Notfallprozesse ungeregelt, Wiederanlaufpläne nicht vorhanden und Notfallpläne nicht eingeübt sind. Den Beschäftigten der IT- und der Haushaltsabteilung sind ihre Aufgaben in Notfallsituationen nicht vertraut. Damit wird der Notfall zu einem Vabanquespiel.

Um im Notfall handlungsfähig zu sein, bedarf es Vorkehrungen im Regelbetrieb: Datensicherungen und die regelmäßige Kontrolle der Datenaufbewahrung sind die entscheidende Grundlage dafür, dass die Daten weitgehend vollständig und konsistent wieder hergestellt werden können. Dabei sollten die Daten so gesichert werden, dass sie konsistent zueinander sind. Wenn zeitkritische Prozesse eine hohe Systemverfügbarkeit erfordern, muss diese etwa durch kürzere Sicherungszyklen, Rufbereitschaften bei der Administration oder Ausweichrechenzentren mit vorinstallierten Systemen sichergestellt sein.

Kontrolle Externer

Viele Behörden lassen ihr IT-System von externen Dienstleistern entwickeln und betreiben. Infolgedessen fehlt es bisweilen an eigener Expertise für das System. Die Behörde kann die Anforderungen an das IT-System nicht vollständig spezifizieren und läuft Gefahr, dem externen Dienstleister blind vertrauen zu müssen. Ohne diese selbst formulierten Anforderungen fehlt der Behörde sowohl eine Grundlage für den Vertrag als auch für den eigenen Test und die Abnahme vor Inbetriebnahme des IT-Systems.

Die Ursachen für ein mangelhaftes IKS stecken beim Outsourcing daher häufig schon in den Verträgen. Einerseits mangelt

es an eindeutigen Vorgaben für die Entwicklung bzw. den Betrieb. Andererseits verzichten die Behörden als Auftraggeber ohne eigene Expertise auch mal auf eine hinreichende Vertragsgrundlage für eine regelmäßige Kontrolle der Vertragsleistungen, etwa über Nachweise der Leistungserbringung, IT-Revisionen oder Zertifikatsnachweise.

Was muss die Behörde tun?

Auf Digitalisierung einstellen

Entsprechend der E-Rechnungs-Verordnung[5] muss die Bundesverwaltung bis zum 27. November 2019 elektronische Rechnungen empfangen und verarbeiten können – Bundesministerien und Verfassungsorgane haben ein Jahr weniger Zeit. Zudem verpflichtet das E-Government-Gesetz[6] die Bundesbehörden ab dem Jahr 2020 zur vollständigen elektronischen Aktenführung.

Sollte eine Behörde weiterhin Vorgänge parallel hierzu auf Papier bearbeiten wollen, drohen zusätzliche und in der Regel vermeidbare Kontrollrisiken durch Medienbrüche. Beispielsweise muss sich der Datenprüfer als zweites Augenpaar bei der Belegprüfung sicher sein können, dass die ausgedruckte Rechnung dem elektronisch eingegangenen Original entspricht. Dies verursacht zusätzlichen Aufwand, der oft an anderer Stelle eingespart wird und dort zu Lücken im Kontrollsystem führt.

Die Verwaltung sollte daher Medienbrüche soweit wie möglich vermeiden und stattdessen die Chancen einer digitalisierten Rechnungsbearbeitung und Rechnungslegung konsequent nutzen. Hierzu gehört auch, die damit verbundenen Möglichkeiten gezielter Datenanalysen und automatisierter Kontrollen voll auszuschöpfen.

Vor allem in Massenantragsverfahren der Verwaltung steckt ein hohes Potenzial, mit Datenanalysen Buchungsfehler zu vermeiden (Bsp. Doppelbuchungen) oder Betrug zu verhindern. Auffällige Buchungen und Beschaffungsvorgänge lassen sich viel gezielter aus einer großen Gesamtheit von Datensätzen ermitteln als bei zufälligen Stichproben.

Für die Analyse von Risiken und die Entwicklung der Kontrollen muss die Verwaltung qualifiziertes Personal aufbauen. Neben der Neueinstellung von IT-Experten kann sie auch ihre Beschäftigten fort- und weiterbilden. Eine breitere IT-Qualifikation auf Seiten der Fachseite und IT-Anwender im Rechnungswesen ist die Basis für ordnungsmäßige und sichere Buchungen und Zahlungen.

Kontrollsystem regelmäßig überprüfen

Der Einsatz der IT im Haushalts- und Rechnungswesen verändert die Anforderungen an funktionswirksame Kontrollen. Um neue Kontrolllücken wirksam schließen zu können, muss jede Behörde regelmäßig eine individuelle Gefährdungsanalyse durchführen und ihre technischen und organisatorischen Verfahrensabläufe anpassen.

Nicht zu vergessen sind in diesem Zusammenhang auch regelmäßige Prüfungen der Wirksamkeit des Kontrollsystems durch unabhängige Prüfinstanzen. Das Management sollte hierbei stets die Chance nutzen, den Ballast an unwirksamen Kontrollen abzuwerfen. Häufig erzielen automatisierte Kontrollen im System (z.B. Plausibilitätskontrollen, systemseitige Buchungslimits) eine bessere Wirkung als organisatorische bzw. manuelle Kontrollen. Zudem vereinfachen und beschleunigen sie die Prozesse.

Die Prüfungen des Bundesrechnungshofes bieten der Bundesverwaltung darüber hinaus einen externen und unabhängigen Blick auf die Sicherheit und Ordnungsmäßigkeit ihres IT-Systems. Sie ersetzten jedoch nicht die Pflicht der Behörden, die Gefährdungen ihres IT-Systems regelmäßig selbst zu analysieren und die Wirkung der Kontrollen zu überprüfen. Daher sind regelmäßige Prüfpflichten seit 2014 auch in den Normen verankert.

Zusammenfassung und Fazit

Die Bundesverwaltung ordnet Zahlungen überwiegend nur noch über IT-Systeme an. Nun hat ihr die Bundesregierung mit der E-Rechnung und der E-Akte weitere ambitionierte Ziele gesetzt. Das IKS der Papierwelt lässt sich allerdings nicht eins-zu-eins auf die digitale Welt übertragen. Das Festhalten an etablierten Kontrollen im Rechnungsbearbeitungsprozess wird den Risiken einer zunehmend elektronischen Rechnungsbearbeitung nicht gerecht. Nicht selten schwächt es wegen des zusätzlichen Aufwands sogar das Kontrollsystem.

Grundsätzliche Risiken zeigen sich einerseits in einer lückenhaften Dokumentation, im IT-seitig unzureichend umgesetzten Vier-Augen-Prinzip sowie in einer fehlenden Funktionstrennung aufgrund zu großzügig vergebener Berechtigungen. Unzureichende Betriebsüberwachung,

»Um neue Kontrolllücken wirksam schließen zu können, muss jede Behörde regelmäßig eine individuelle Gefährdunganalyse durchführen und ihre technischen und organisatorischen Verfahrensabläufe anpassen.«

5 Verordnung über die elektronische Rechnungsstellung im öffentlichen Auftragswesen des Bundes

6 Gesetz zur Förderung der elektronischen Verwaltung ist abrufbar unter http://www.gesetze-im-internet.de/egovg/EGovG.pdf

mangelnde Notfallvorsorge und fehlende IT-Fachkräfte erhöhen diese Risiken.

Die Bundesverwaltung kann jedoch mit vertretbarem Aufwand Kontrolllücken schließen, indem sie sich der Digitalisierung stellt, ihr IKS kontinuierlich an aktuelle Entwicklungen anpasst, auf liebgewonnene, aber wirkungslose Kontrollen aus dem „Papierzeitalter" verzichtet und stattdessen auch die Kontrollen automatisiert.

Aus Sicht des Bundesrechnungshofes bleibt die Eindämmung der Risiken beim Betrieb der zahlungs- und rechnungslegungsrelevanten IT-Systeme auf ein vertretbares Maß eine Daueraufgabe der Bundesverwaltung.