01/07 Finanzen / Haushalt / Bewirtschaftung

Zugangs- und Zugriffskontrollen bei automatisierten Verfahren zur Bewirtschaftung von Haushaltsmitteln des Bundes

Leitsätze

(1) Zu automatisierten Verfahren im Haushalts-, Kassen und Rechnungswesen des Bundes dürfen nur befugte Personen Zugang haben. Dies ist durch geeignete technische Vorkehrungen abzusichern (z. B. personenbezogene und ausreichend starke Passwörter, Zugangssperren nach mehreren Fehleingaben).

(2) Der Beauftragte für den Haushalt muss regeln, wer bei diesen Verfahren auf welche zahlungsrelevante Daten und Funktionen zugreifen darf. Basis der Zugriffsrechtevergabe muss ein aktuelles und vollständiges Berechtigungskonzept sein. Seine Einhaltung ist regelmäßig zu kontrollieren.

(3) Die Zugriffsrechte müssen aufgabenbezogen auf das notwendige Maß beschränkt sein. Hierbei sind das Vier-Augen-Prinzip und weitere Funktionstrennungen zu beachten. Entwickler dürfen allenfalls lesende Zugriffsrechte auf produktiv eingesetzte automatisierte Verfahren haben.

(4) Benutzerkennungen für automatisierte Verfahren dürfen grundsätzlich nur personenbezogen vergeben werden.

(5) In den automatisierten Verfahren ist systemseitig zu protokollieren, wer zu welchem Zeitpunkt über welche Zugriffsrechte verfügte und wann welche Daten geändert hat.

(6) Nicht bzw. seit längerem nicht verwendete Benutzerkennungen sind generell zu sperren oder zu löschen.

Hintergründe

Beim Einsatz automatisierter Verfahren zur Bewirtschaftung von Haushaltsmitteln des Bundes sind verschiedene haushaltsrechtliche Vorschriften zu beachten. So fordern die vom Bundesministerium der Finanzen herausgegebenen Mindestanforderungen für den Einsatz automatisierter Verfahren im Haushalts-, Kassen- und Rechnungswesen des Bundes (BestMaVB-HKR) in Verbindung mit den Vorgaben zum IT-Grundschutz[1] des Bundesamtes für Sicherheit in der Informationstechnik u. a. wirksame Zugangs- und Zugriffskontrollen. Die Bewirtschafter müssen vor allem dafür Sorge tragen, dass

- ausschließlich berechtigte Benutzer Zugang zum automatisierten Verfahren haben,
- die Benutzer innerhalb des automatisierten Verfahrens nur Zugriff auf die von ihnen benötigten haushaltsrelevanten Daten haben,
- dokumentiert ist, welche Zugriffsrechte den Benutzern eingerichtet werden sollen und
- die eingerichteten Zugriffsrechte und die haushaltswirksamen Datenänderungen anhand von Systemprotokollen nachvollziehbar sind.

(1) Der Bundesrechnungshof stellt bei seinen Prüfungen regelmäßig fest, dass bei automatisierten Verfahren der Zugangsschutz unzureichend umgesetzt wurde. So ist die Passwortstärke nicht ausreichend und entspricht nicht dem IT-Grundschutz.[2] Benutzerkennungen werden nach mehreren Falschanmeldungen häufig nicht gesperrt. Folglich können Angreifer Passwörter im Extremfall beliebig oft ausprobieren. Das Kennwortrücksetzungsverfahren ist teilweise missbrauchsanfällig, indem z. B. neue Passwörter nicht nur für die eigene, sondern auch für andere Benutzerkennungen angefordert und eingesetzt werden können.

(2) Die Bewirtschafter dürfen ein automatisiertes Verfahren erst produktiv nutzen, nachdem sie ein Berechtigungskonzept in Kraft gesetzt und systemseitig umgesetzt haben.[3] Im Berechtigungskonzept sind Befugnisse festzulegen und die dafür benötigten Zugriffsrechte möglichst in Rollen zusammenzufassen. Die geprüften Einrichtungen hatten vielfach kein oder kein aktuelles Berechtigungskonzept. Sofern ein Berechtigungskonzept vorhanden war, entsprachen die in dem automatisierten Verfahren vergebenen Zugriffsrechte diesem oft nicht. Zudem

[1] Diese Empfehlungen sind gemäß Nr. 3 (1) BestMaVB-HKR zu beachten.
[2] M 2.11 der IT-Grundschutz-Kataloge, ab 1. Februar 2018: ORP.4.A8 IT-Grundschutz-Kompendium.
[3] Als Teil des in Nr. 6.4 VV-ZBR BHO geforderten Ordnungsmäßigkeitskonzeptes.

verzichteten die geprüften Einrichtungen häufig darauf, die Berechtigungskonzepte und die eingerichteten Zugriffsrechte regelmäßig zu überprüfen. Damit war nicht sichergestellt, dass die vergebenen Zugriffsrechte zur Aufgabenerfüllung noch erforderlich waren.

(3) Benutzer dürfen nur die Zugriffsrechte haben, die sie zur Aufgabenerfüllung benötigen. Das Berechtigungskonzept hat als Teil des Ordnungsmäßigkeitskonzeptes die haushaltsrechtlich geforderten Funktionstrennungen vorzusehen. Um das Vier-Augen-Prinzip einzuhalten, sind von einer Person die zahlungsrelevanten Daten eines Beleges zu erfassen und von einer zweiten vor der Freigabe zur weiteren Datenverarbeitung zu prüfen (Anordnung). Das Vier-Augen-Prinzip gilt auch zwischen Feststellung[4] und Anordnung.[5]

Zudem muss ein Zugriff auf Programme, die sich im Wirkbetrieb befinden, für die Funktionsbereiche Systemprogrammierung, Verfahrensentwicklung und –pflege ausgeschlossen sein.[6] Dies bedeutet, dass Entwickler zu keinem Zeitpunkt in der Lage sein dürfen, produktiv genutzte automatisierte Verfahren nach deren Abnahme bzw. Freigabe unautorisiert und unprotokolliert zu modifizieren. Auch dürfen Entwickler niemals Rechte zum Haushaltsvollzug haben.[7]

Der Bundesrechnungshof hat regelmäßig festgestellt, dass die vorgeschriebenen Funktionstrennungen nicht umgesetzt waren. So hatten in den produktiv genutzten automatisierten Verfahren vielfach Entwickler umfassende Buchungsrechte. Viele nicht-personenbezogene Benutzerkennungen hatten ebenfalls Rechte zum Haushaltsvollzug und zur Systemadministration. Den Beauftragten für den Haushalt war dies oft nicht bekannt. Hierdurch waren sensible Buchhaltungsbereiche nicht hinreichend aufgabenbezogen abgrenzt.

(4) Die oder der Beauftragte für den Haushalt muss die im Berechtigungskonzept festgelegten Befugnisse verantwortlichen Personen zuweisen.[8] Damit dies auch systemseitig nachvollzogen werden[9] kann, dürfen Zugriffsrechte grundsätzlich nur personenbezogen vergeben werden. Hiervon ausgenommen sind systemtechnische Benutzerkennungen, z. B. für Schnittstellenprogramme.

---

[4] Wahrnehmung der Verantwortungsbereiche nach Nr. 1.2 VV-ZBR BHO (entspricht der Feststellung der sachlichen und rechnerischen Richtigkeit bei manuellen Verfahren gemäß Nr. 2.2.2 und Nr. 2.2.3 der Anlage 2 zur VV-ZBR BHO).
[5] Nrn. 2 (2a), 5.2 (1) und 5.4 (1) BestMaVB-HKR.
[6] Nr. 2 (4) Satz 1 BestMaVB-HKR.
[7] Nr. 2 (4) Satz 2 BestMaVB-HKR.
[8] Nr. 6.5.1 VV-ZBR BHO.
[9] Siehe hierzu auch M 2.587 der IT-Grundschutz-Kataloge, ab 1. Februar 2018: ORP.4.A15 IT-Grundschutz Kompendium.

Der Bundesrechnungshof hat wiederholt festgestellt, dass in automatisierten Verfahren auch nicht-personenbezogene Benutzerkennungen mit haushaltsrelevanten Zugriffsrechten für den Dialogbetrieb eingerichtet waren (z. B. 'AZUBI', 'ERFASSER' für mehrere Beschäftigte). Bei diesen Benutzerkennungen lässt sich nicht nachweisen, welche Person hiermit beispielsweise zahlungsrelevante Belegdaten erfasste oder Auszahlungen anordnete. Oftmals verfügen nicht-personenbezogene Benutzerkennungen (z. B. 'SYSTEM', 'NOTFALL' oder 'ADMIN') zudem über sehr umfassende Zugriffsberechtigungen (z. B. über umfassende Rollen oder Profile wie 'SAP_All' und 'SAP_NEW'). Sie bergen damit ein hohes Risiko für dolose Handlungen.

Der Bundesrechnungshof hat teilweise auch festgestellt, dass Beschäftigte ihre Benutzerkennungen an Kolleginnen oder Kollegen weitergaben und hierdurch das Vier-Augen-Prinzip wirkungslos wurde.

(5) Die Bewirtschafter protokollierten in ihren automatisierten Verfahren teilweise die Zugriffsrechteverwaltung sowie die Zugriffe auf haushaltsrelevante Daten nicht in der Form einer Änderungshistorie.

Entsprechend des IT-Grundschutzes ist zu protokollieren, wer zu welchem Zeitpunkt welche Zugriffsrechte hatte.[10] Darüber hinaus müssen u. a. Änderungen zentraler zahlungsrelevanter Daten (Stammdaten) systemseitig in der Form einer Änderungshistorie protokolliert werden.[11] Diese Systemprotokolle ermöglichen nachgelagerte Kontrollen. Sie bilden damit eine wesentliche Grundlage, um eventuelle Unregelmäßigkeiten aufzudecken.

(6) Der Bundesrechnungshof hat bei seinen Prüfungen automatisierter Verfahren festgestellt, dass nicht bzw. seit längerer Zeit nicht mehr verwendete Benutzerkennungen nach wie vor verwendbar waren. Dies betraf z. B. Benutzerkennungen von Beschäftigten, die zwischenzeitlich andere Aufgaben übernommen hatten oder ausgeschieden waren.

Benutzerkennungen sollten nur für den Zeitraum eingerichtet werden, für den sie benötigt werden. Oft findet der Bundesrechnungshof Benutzerkennungen, die seit mehr als 90 Tagen nicht oder noch nie verwendet wurden. Entsprechend des

[10] M 2.110 der IT-Grundschutz-Kataloge, ab 1. Februar 2018: ORP.4.A3 IT-Grundschutz-Kompendium.
[11] Nr. 5.7 BestMaVB-HKR.

IT-Grundschutzes sollten nicht mehr zu verwendende Benutzerkennungen gesperrt bzw. gelöscht werden.[12]

Anmerkungen

Weitere Prüfungserkenntnisse des Bundesrechnungshofes finden sich auch in den Bemerkungen 2014, Nr. 3 sowie einem Bericht nach § 88 Absatz 2 BHO an den Rechnungsprüfungsausschuss des Haushaltsausschusses des Deutschen Bundestages vom 13. Mai 2016. Der RPA hat das Bundesministerium der Finanzen und die anderen Ressorts aufgefordert, die haushaltsrechtlichen Vorgaben für den Betrieb aller zahlungsrelevanten IT-Systeme in ihrem jeweiligen Verantwortungsbereich einzuhalten.

[12] M 4.17 der IT-Grundschutz-Kataloge, ab 1. Februar 2018: ORP.4.A6-8 IT-Grundschutz-Kompendium.