RECHNUNGSHOF
RHEINLAND-PFALZ

Auszug aus dem Jahresbericht 2021

Nr. 6 Berechtigungen im Integrierten Personalmanagementsystem IPEMA® - Berechtigungskonzept entsprach nicht den Anforderungen, Rechtevergabe war risikobehaftet -

Impressum:

Rechnungshof Rheinland-Pfalz
Gerhart-Hauptmann-Straße 4
67346 Speyer

Telefon: 06232 617-0
Telefax: 06232 617-100
E-Mail: poststelle@rechnungshof.rlp.de
Internet: https://rechnungshof.rlp.de

Nr. 6 Berechtigungen im Integrierten Personalmanagementsystem IPEMA®
- Berechtigungskonzept entsprach nicht den Anforderungen, Rechtevergabe war risikobehaftet -

Für die Zahlung von Bezügen und Reisekostenvergütungen von 5,9 Mrd. € jährlich setzt das Landesamt für Finanzen das Integrierte Personalmanagementsystem IPEMA® ein. Beim Einsatz des SAP-basierten IT-Verfahrens wurde nicht allen Anforderungen an die IT-Sicherheit Rechnung getragen:

- **Das Berechtigungskonzept genügte im Hinblick auf Vollständigkeit, Nachvollziehbarkeit und Aktualität nicht allen Standards des Bundesamts für Sicherheit in der Informationstechnik.**
- **Kritische Berechtigungen waren nicht vollständig identifiziert. Sie wurden zu häufig an Benutzer vergeben. Außerdem war ihre Vergabe nicht vollständig geregelt.**
- **Aktivitäten von Benutzern mit kritischen Berechtigungen wurden nicht wirksam überwacht. Ein Protokollierungskonzept fehlte.**
- **Benutzer- und Berechtigungsverwaltung waren nicht getrennt. Notwendige Kontrollen zur Kompensation der fehlenden Funktionstrennung unterblieben.**
- **Bei Benutzerkonten, auf die zeitweise bis zu vier Personen zugreifen konnten, war es nicht möglich, für bestimmte Änderungen verantwortliche Personen zu identifizieren.**
- **Nicht benötigte Berechtigungen wurden nicht regelmäßig entfernt. Wesentliche Änderungen am IPEMA®-Produktivsystem waren nicht immer dokumentiert.**
- **Die Verschlüsselung von Kennwörtern der IPEMA®-Benutzer entsprach nicht dem aktuellen Stand der Technik.**

1 Allgemeines

Das Landesamt für Finanzen zahlt unter anderem Bezüge und Reisekostenvergütungen aus. Es betreut 178.000 Bedienstete des Landes und verwaltet hierfür ein Gesamtausgabevolumen von 5,9 Mrd. € jährlich.[1]

Zur Erledigung dieser Aufgaben setzt das Landesamt das **I**ntegrierte **Pe**rsonal**ma**nagementsystem (IPEMA®) ein. Technische Grundlage dieses IT-Verfahrens ist die Standardsoftware SAP ERP 6.0.

---

[1] Vorwort zum Einzelplan 04 Ministerium der Finanzen, Kapitel 04 07 Landesamt für Finanzen (Haushaltsplan für die Haushaltsjahre 2019/2020).

IPEMA® wird auch von allen personalverwaltenden Dienststellen des Landes für die Bearbeitung von 110.000 Personalfällen genutzt. Ferner ermöglicht das Modul IPEMA®-Reisekostenportal die elektronische Beantragung, Genehmigung und Abrechnung von Reisekostenvergütungen für Dienstreisen.

Zum Zeitpunkt der Prüfung des Rechnungshofs wurde IPEMA® von 280 Abrechnungsbearbeitern des Landesamts, 1.300 Personalsachbearbeitern der Dienststellen des Landes sowie mehr als 60.000 Dienstreisenden[2] genutzt.

An die IT-Sicherheit von IPEMA® sind hohe Anforderungen zu stellen. Insbesondere müssen die Vertraulichkeit, Integrität und Verfügbarkeit der in IPEMA® enthaltenen Daten sichergestellt und missbräuchliche Aktivitäten vermieden werden.

Der Rechnungshof hat das Berechtigungskonzept des IT-Verfahrens IPEMA® beim Landesamt geprüft. Ziel der Prüfung war es insbesondere festzustellen, ob

- dem Einsatz von IPEMA® ein den Anforderungen entsprechendes Berechtigungskonzept zugrunde liegt,
- die im Berechtigungskonzept enthaltenen Regelungen sowohl in IPEMA® als auch organisatorisch bei der Administration umgesetzt sind und
- die Praxis bei der Vergabe von Berechtigungen die bestehenden datenschutzrechtlichen und haushaltswirtschaftlichen Risiken vermindern kann.

Die Prüfung erstreckte sich im Wesentlichen auf das IPEMA®-Produktivsystem.[3] Dort werden die Echtdaten der Landesbediensteten verarbeitet und die Personalverwaltung sowie die Bezüge- und Reisekostenabrechnung im laufenden Betrieb abgewickelt. Als Prüfungsmaßstäbe hat der Rechnungshof insbesondere die Standards und Umsetzungshinweise des Bundesamts für Sicherheit in der Informationstechnik (BSI) zum Einsatz von SAP-Systemen herangezogen.

2 Wesentliche Prüfungsergebnisse

2.1 Berechtigungskonzept nicht vollständig, nachvollziehbar und aktuell

Das Berechtigungskonzept stellt die elementare Sicherheitsfunktion in SAP-Systemen dar. Hierin werden die Zugriffsregelungen für einzelne Benutzer oder Benutzergruppen auf das IT-System festgelegt. Nach den Standards des BSI soll ein Berechtigungskonzept für ein SAP-System insbesondere Folgendes enthalten:

- alle vom Systembetreiber zu erfüllenden rechtlichen und internen Vorgaben,
- die Beschreibung der Prozesse der Benutzer- und Berechtigungsadministration und der vergebenen Rollen,
- Namenskonventionen über die Benennung von Rollen und Systembenutzern,
- die Identifizierung kritischer Berechtigungen und Regelungen für den Umgang mit diesen,
- ein Notfallbenutzerkonzept sowie
- die Festlegung interner Kontrollprozesse.

Es muss sichergestellt sein, dass das Berechtigungskonzept vollständig, nachvollziehbar und aktuell ist. Dadurch wird gewährleistet, dass in dem Konzept sämtliche erforderlichen Regelungen für eine wirksame Begrenzung der Zugriffsrechte festgelegt und diese für Dritte überprüfbar sind.

---

[2] IPEMA®-Reisekostenportal wurde bis Ende 2020 sukzessive bei den Dienststellen des Landes eingeführt.

[3] IPEMA® beinhaltet mehrere einzelne SAP-Systeme. Dazu zählen auch Entwicklungs-, Qualitätssicherungs- und Referenzsysteme.

Das vom Landesamt vorgelegte Berechtigungskonzept, das aus einem Rahmenkonzept sowie weiteren Dokumenten bestand, genügte den Anforderungen an die Vollständigkeit, die Nachvollziehbarkeit und die Aktualität nicht. Beispielsweise waren in der Änderungshistorie nicht alle Versionen des Rahmenkonzepts aufgeführt und über sechs Jahre keine Aktualisierung dokumentiert. Getroffene Festlegungen waren nicht vollständig in IPEMA® umgesetzt und risikobehaftete Sachverhalte teilweise nicht eindeutig geregelt.

Das Landesamt hat mitgeteilt, bis Ende 2020 werde ein neues Berechtigungskonzept vorgelegt, welches die rechtlichen Vorgaben, die Empfehlungen des BSI und die Anregungen des Rechnungshofs berücksichtige.

2.2 Kritische Berechtigungen bedürfen der Überprüfung

2.2.1 Identifizierung

Kritische Berechtigungen erlauben Operationen, die für die Systemsicherheit oder aus rechtlicher oder haushaltswirtschaftlicher Sicht erhebliche Risiken bergen. Hierzu gehören z. B. Zugriffe auf personenbezogene Daten, das Ändern oder Löschen von Daten und Protokollierungen, die alleinige und unkontrollierte Ausführung kritischer Prozesse im System oder Änderungen an allgemeinen Systemeinstellungen.

Daher muss die Vergabe solcher Berechtigungen nach strengen Maßstäben erfolgen. Nach den Standards des BSI hat das Landesamt als Systembetreiber von IPEMA® die kritischen Berechtigungen im SAP-System regelmäßig zu identifizieren, zu überprüfen und zu bewerten.

Das Landesamt hatte nur wenige kritische Berechtigungen in IPEMA® identifiziert und deren Einsatz im Berechtigungskonzept geregelt. Es hatte keinen umfassenden Überblick, welchen Benutzern kritische Berechtigungen zugeordnet waren und welche konkreten Risiken dadurch bestanden. Die in SAP-Systemen standardmäßig enthaltenen Funktionen zur Identifizierung, Überprüfung und Bewertung kritischer Berechtigungen wurden nicht genutzt.

Das Landesamt hat erklärt, die kritischen Berechtigungen und deren Vergabe würden geprüft und gegebenenfalls entfernt. Darüber hinaus werde eine turnusmäßige Überprüfung installiert. Die Nutzung vorhandener Funktionen werde geprüft.

2.2.2 Vergabe der Berechtigungen

Das Sammelprofil SAP_ALL umfasst alle Berechtigungen im SAP-System. Damit können sämtliche Transaktionen und somit auch risikobehaftete Operationen ausgeführt werden. Die Vergabe des Sammelprofils ist daher auf Einzelfälle zu beschränken. Außerdem ist eine Zuordnung des Sammelprofils im Produktivsystem nach den Umsetzungshinweisen des BSI zu vermeiden. Danach und gemäß den Empfehlungen von SAP sollte es möglichst nur an Notfallbenutzer vergeben werden.[4] Auch im Rahmenkonzept des Landesamts war geregelt, dass das Sammelprofil dem Notfallbenutzer vorbehalten sein sollte.

Mit diesen Hinweisen und Vorgaben war es nicht vereinbar, dass das Sammelprofil seit der Einrichtung von IPEMA® im Jahr 2010 bis einschließlich Februar 2020 in 658 Fällen temporär an Benutzer vergeben worden war. Die mit vergleichbar umfassenden Berechtigungen versehene Rolle ZSAP_ALL wurde in 1.633 Fällen zeitlich befristet Benutzern zugeordnet. Bei der Vergabe weiterer kritischer Berechtigungen, die zum Teil durch das BSI als „hochkritisch“ eingestuft waren, war nicht immer ersichtlich, inwieweit sie für die Erledigung der Aufgaben benötigt wurden.

---

[4] https://help.sap.com/saphelp_dm40/helpdata/de/78/7a553efd234644e10000000a114084/frameset.htm (abgerufen am 1. Oktober 2020).

Das Landesamt hat mitgeteilt, die vorhandenen Sammelprofil-Vergaben würden geprüft und gegebenenfalls entfernt. Die Rolle ZSAP_ALL werde inhaltlich überprüft, um festzustellen, ob sie weiter beschränkt werden könne. Die Vergabe weiterer kritischer Berechtigungen werde überprüft und gegebenenfalls angepasst.

2.3 Fehlende Trennung der Benutzer- und Berechtigungsverwaltung

Benutzer- und Berechtigungsadministratoren haben unterschiedliche Verantwortlichkeiten und müssen aus Gründen der Systemsicherheit nach den Standards des BSI getrennte Berechtigungen haben. Kann eine Person zum Beispiel neue Benutzer und auch Berechtigungen, z. B. Rollen anlegen, besteht die Gefahr von Missbrauch. Kann diese Funktionstrennung aus zwingenden organisatorischen Gründen nicht gewährleistet werden, müssen regelmäßige kompensierende Kontrollen z. B. nach dem Vieraugenprinzip vorgenommen werden, um die Benutzer- und Berechtigungsverwaltung zu überwachen.

Im IPEMA®-Service-Center, das beim Landesamt für den Anwendungsbetrieb von IPEMA® zuständig ist, war die erforderliche Funktionstrennung nicht sichergestellt. Notwendige kompensierende Kontrollen unterblieben.

Das Landesamt hat erklärt, eine Trennung zwischen Benutzer- und Berechtigungsverwaltung sei in dem Berechtigungsteam mit drei Vollzeitkräften aufgrund der Vielfältigkeit der Aufgaben und im Hinblick auf eine geregelte Vertretungssituation derzeit nicht möglich. Dies gelte auch für die Einführung eines permanenten Vieraugenprinzips bei gleichbleibender Personalstärke. Künftig solle es den IPEMA® verwendenden Dienststellen ermöglicht werden, den Benutzern über die Zuweisung von Rollen Berechtigungen zuzuordnen. Das Berechtigungsteam werde dann insbesondere im Fehlerfall Benutzer überprüfen und korrigieren. Technisch sei das Team weiterhin in der Lage, all diese Bereiche zu bearbeiten. Es werde geprüft, ob die geplante Verfahrensumstellung Kapazitäten im Berechtigungsteam freisetze, die zugunsten einer Funktionstrennung eingesetzt werden könnten. Darüber hinaus würden Möglichkeiten für kompensierende Kontrollen geprüft.

Hierzu weist der Rechnungshof darauf hin, dass auch mit der beabsichtigten Verfahrensumstellung die gebotene Systemsicherheit nicht gewährleistet werden kann. Die Bediensteten des Berechtigungsteams werden weiterhin über Berechtigungen zur Benutzer- und Berechtigungsadministration verfügen. Daher sollten möglichst bald geeignete kompensierende Kontrollen eingeführt werden.

2.4 Einrichtung von Benutzerkonten für mehrere Personen problematisch

In SAP-Systemen können Benutzerkonten eingerichtet werden, die von mehreren Personen nutzbar sind. Von diesen sogenannten Sammelbenutzern durchgeführte Änderungen am System können nicht zweifelsfrei einer konkreten Person zugeordnet werden. Die Verwendung der Sammelbenutzer muss deshalb im Berechtigungskonzept dokumentiert und geregelt sein. Ihnen dürfen nur die für die jeweilige Aufgabe benötigten Berechtigungen zugeordnet werden. Ferner müssen sie einer verstärkten Kontrolle unterliegen.

In IPEMA® waren Sammelbenutzer z. B. zur Systempflege oder für die Anwenderbetreuung eingerichtet. Auf diese Benutzerkonten hatten jeweils bis zu vier Bedienstete Zugriff. Ihnen waren zeitweise weitreichende kritische Berechtigungen wie das Sammelprofil SAP_ALL zugeordnet.

Das Berechtigungskonzept enthielt keine Regelungen zu Sammelbenutzern. Es war auch nicht ersichtlich, ob die Sammelbenutzer zur Erfüllung ihrer Aufgaben derart weitreichende Berechtigungen benötigten. Eine vollständige Kontrolle der Aktivitäten erfolgte nicht. Die Kennwörter wurden nur alle drei Monate geändert. In diesem Zeitraum konnten sich Bedienstete noch am System anmelden, auch wenn sie die umfassenden Berechtigungen nicht mehr für ihre Tätigkeit benötigten.

Das Landesamt hat mitgeteilt, Sammelbenutzer würden künftig im Berechtigungskonzept geregelt und ihre Aktivitäten gesondert protokolliert. Die Hinweise des Rechnungshofs zur Kennwortvergabe und zur eindeutigen Zuordnung zu einer natürlichen Person würden berücksichtigt, ihre Umsetzung geprüft.

2.5 Weitere Mängel

Weiterer Verbesserungsbedarf bestand in folgenden Bereichen:

- Das Landesamt nahm keine regelmäßige und systematische Prüfung vor, um festzustellen, welche Berechtigungen nicht mehr benötigt werden und den Benutzern entzogen werden können.
- Wesentliche Änderungen in IPEMA® waren nicht immer durch das hierfür eingerichtete Ticketsystem dokumentiert. Dies betraf z. B. die Systemwartung oder umfangreiche Programmänderungen[5].
- Kritische Berechtigungen wurden teilweise ohne Antrag vergeben. Beim Anlegen von Benutzern und der Zuordnung von Berechtigungen war nicht ersichtlich, auf welcher konkreten Anforderung die Änderung im System beruhte.
- Die Aktivitäten von Benutzern mit kritischen Berechtigungen wurden in IPEMA® nicht gesondert protokolliert und überwacht. Es fehlte ein Protokollierungskonzept, das Art und Umfang der vorgenommenen Protokollierungen umfassend darstellte.
- Die in IPEMA® für die Speicherung der Passwörter der Benutzer eingesetzte Verschlüsselungstechnik entsprach nicht dem aktuellen, in SAP-Systemen verfügbaren Stand der Technik. Die Kennwörter der IPEMA®-Benutzer waren nur mit einem veralteten, leicht zu entschlüsselnden Algorithmus gesichert.

Das Landesamt hat erklärt, es werde einen Turnus festlegen und mit der Planung der nächsten Bereinigung nicht benötigter Berechtigungen beginnen. Künftig würden auch bei wiederkehrenden Tätigkeiten, wie z. B. bei Wartung, Tickets angelegt. Mit dem Update des Solutionmanagers könne die Neuanlage von Benutzerkennungen und die Zuordnung von Berechtigungen dokumentiert werden. Die Aktivitäten von Benutzern mit kritischen Berechtigungen würden überwacht. Ein Protokollierungskonzept, in dem auch die regelmäßige Auswertung der Protokollierungen zu regeln sei, werde erstellt. Bezüglich der Feststellungen zur Kennwortverschlüsselung sei der Sachverhalt geprüft und zur Umsetzung an den Landesbetrieb Daten und Information weitergegeben worden.

3 Folgerungen

3.1 Zu den nachstehenden Forderungen wurden die gebotenen Folgerungen bereits gezogen oder eingeleitet:

Der Rechnungshof hatte gefordert,

a) für IPEMA® ein nachvollziehbares und vollständiges Berechtigungskonzept zu erstellen und dieses regelmäßig zu aktualisieren,

b) die kritischen Berechtigungen vollständig zu identifizieren, regelmäßig zu überprüfen und zu bewerten, die Zuordnung kritischer Berechtigungen zu regeln und deren Vergabe auf den für die Aufgabenerledigung erforderlichen Umfang zu begrenzen,

c) Benutzerkonten möglichst nur für einzelne Bedienstete einzurichten und Aktivitäten von Sammelbenutzern zu protokollieren und zu überwachen,

d) nicht benötigte Berechtigungen regelmäßig zu entfernen,

e) wesentliche Änderungen in IPEMA® vollständig zu dokumentieren,

---

[5] Sogenannte Releasewechsel.

f) Aktivitäten der Benutzer mit kritischen Berechtigungen zu überwachen und ein Protokollierungskonzept zu erstellen,

g) die Kennwörter der Benutzer entsprechend dem aktuellen Stand der Technik zu verschlüsseln.

3.2 Folgende Forderungen sind nicht erledigt:

Der Rechnungshof hat gefordert,

a) die Trennung von Benutzer- und Berechtigungsadministration sicherzustellen oder kompensierende Kontrollen einzuführen,

b) über die Ergebnisse der eingeleiteten Maßnahmen zu Nr. 3.1 zu berichten.