RECHNUNGSHOF
RHEINLAND-PFALZ

Auszug aus dem Jahresbericht 2022

Nr. 8 Einsatz von SAP-Systemen beim Landesbetrieb Liegenschafts- und Baubetreuung - sicherheitsrelevante Aktualisierungen unterblieben, Zuordnungen von Berechtigungen und Benutzerverwaltung waren 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. 8 Einsatz von SAP-Systemen beim Landesbetrieb Liegenschafts- und Baubetreuung - sicherheitsrelevante Aktualisierungen unterblieben, Zuordnungen von Berechtigungen und Benutzerverwaltung waren risikobehaftet -

Der Landesbetrieb Liegenschafts- und Baubetreuung setzt u. a. für seine Buchhaltung SAP-Systeme ein. Damit werden Auszahlungen von jährlich insgesamt 278 Mio. € veranlasst. Der Einsatz der SAP-Systeme genügte nicht allen Anforderungen an die IT-Sicherheit:

- **Das SAP-Basissystem war zuletzt 2015 aktualisiert worden. Seitdem waren sicherheitsrelevante Aktualisierungen unterblieben.**
- **Im Entwicklungssystem wurden unzulässigerweise Echtdaten aus dem Produktivsystem verwendet. Sie waren dadurch einem nicht berechtigten Personenkreis zugänglich.**
- **Ein verbindliches, den rechtlichen und fachlichen Anforderungen genügendes, aktuelles und vollständiges Berechtigungskonzept fehlte.**
- **Kritische Berechtigungen waren nicht vollständig identifiziert. Sie wurden zu häufig an Benutzer[1] vergeben. Die Benutzerverwaltung entsprach nicht allen Standards des Bundesamts für Sicherheit in der Informationstechnik.**
- **Die erforderliche Trennung von Benutzer- und Berechtigungsadministration war nicht eindeutig geregelt.**
- **Die Verschlüsselung von Benutzerpasswörtern entsprach nicht durchgehend dem aktuellen Stand der Technik.**
- **Die Überwachung der Aktivitäten von Benutzern mit kritischen Berechtigungen war unzureichend. Ein entsprechendes Protokollierungskonzept fehlte.**

1 Allgemeines

Nach der Organisationsverfügung für den Landesbetrieb Liegenschafts- und Baubetreuung (LBB) von 2019 ist dieser zuständig für die eigenverantwortliche Beschaffung, Bewirtschaftung und Verwertung der baulichen Infrastruktur der Landesbehörden und die Erfüllung der Bauaufgaben des Landes sowie des Bundes nach finanzwirtschaftlichen Grundsätzen.

Der LBB setzt u. a. für seine Buchhaltung, die Erstellung von Quartals- und Jahresabschlüssen nach dem Handelsgesetzbuch (HGB) und die Vorbereitung der täglichen Zahlläufe die Standardsoftware SAP ein. Im Jahr 2020 betrugen die Auszahlungen, z. B. an Architekturbüros oder Bauunternehmen, 278 Mio. €.

---

[1] Der technische Begriff „Benutzer“ bezeichnet das Konto einer Anwenderin oder eines Anwenders, die mit dem SAP-System arbeiten.

Der LBB ist für den fachlichen Betrieb und die Benutzerverwaltung der SAP-Systeme verantwortlich. Der technische Betrieb wird vom Landesbetrieb Daten und Information (LDI) sichergestellt, der in Abstimmung mit dem LBB u. a. für die Durchführung von Updates zuständig ist.

Der Rechnungshof hat den Einsatz der SAP-Systeme beim LBB geprüft. Ziel der Prüfung war es insbesondere festzustellen, ob

- die Systeme ausreichend abgesichert waren, um missbräuchliche Zahlungen und unberechtigte Datenzugriffe zu vermeiden,
- hierzu getroffene Maßnahmen entsprechend dokumentiert waren,
- in der Dokumentation beschriebene Maßnahmen umgesetzt waren und
- regelmäßige Auswertungen im System zur Erkennung risikobehafteter Ereignisse vorgenommen wurden.

Der Schwerpunkt der Prüfung lag auf dem Produktivsystem. Dort werden die sogenannten Echtdaten vorgehalten und verarbeitet. Dies sind z. B. alle Daten des Rechnungswesens sowie Adress- und Bankdaten einer Vielzahl von Unternehmen mit Vertragsbeziehungen zum LBB. Als Prüfungsmaßstab 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 SAP-Systeme nicht aktuell gehalten

SAP veröffentlicht regelmäßig sicherheitsrelevante Aktualisierungen für die SAP-Basissysteme und alle SAP-Module. Damit sollen bekannt gewordene Schwachstellen behoben und das System vor Gefährdungen geschützt werden. Die Aktualisierungen erfolgen u. a. durch sogenannte Support-Packages, die bereits installierte Softwareversionen erneuern, und „SAP-Sicherheitshinweise“, die einzelne Softwarefehler und Schwachstellen beheben. Letztere werden in der Regel monatlich veröffentlicht und von SAP mit einer Prioritätsstufe versehen. Nach den Standards des BSI müssen SAP-Sicherheitshinweise mit hoher Prioritätsstufe zeitnah angewendet werden. Ferner empfiehlt es, jährlich mindestens ein Support-Package einzuspielen.[2]

Das beim LBB eingesetzte SAP-Basissystem war zuletzt im Jahr 2015 aktualisiert worden. Seitdem waren sicherheitsrelevante Aktualisierungen unterblieben. Dadurch bestand das Risiko, dass Sicherheitslücken dazu genutzt werden, die SAP-Systeme zu manipulieren, vertrauliche Daten zu entwenden oder Geschäftsprozesse zu stören.

Der LBB hat mitgeteilt, die SAP-Systeme würden auf den neuesten Stand gebracht. Künftig würden Support-Packages in Abstimmung mit dem LDI im halbjährlichen Rhythmus eingespielt, bei sicherheitsrelevanten Packages geschehe dies unverzüglich.

2.2 Echtdaten unzulässig im Entwicklungssystem verwendet

Aufgrund der Komplexität der SAP-Systeme ist es erforderlich, regelmäßig Entwicklungen, kundenspezifische Einstellungen (sogenanntes Customizing) und Verfahrenstests vorzunehmen. Dabei darf der laufende Betrieb nicht beeinträchtigt werden. Der LBB setzt für diese Zwecke neben dem Produktivsystem für den laufenden Betrieb u. a. ein Entwicklungssystem ein.

---

[2] Vgl. BSI Umsetzungshinweise zum IT-Grundschutz-Kompendium 2019: Umsetzungshinweise zum Baustein APP.4.2 SAP-ERP-System APP.4.2.M10: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/Umsetzungshinweise_Kompendium_CD_2019.html?nn=12847.

Echtdaten aus dem Produktivsystem dürfen im Entwicklungssystem nicht genutzt werden, da dort regelmäßig ein größerer Personenkreis von externen Beschäftigten weitreichende Berechtigungen erhält. Dieser Personenkreis könnte damit uneingeschränkt auf die Daten aus dem Produktivsystem zugreifen.

Gleichwohl wurden im Entwicklungssystem des LBB in erheblichem Umfang Echtdaten aus dem Produktivsystem verwendet. Dabei handelte es sich z. B. um fast 30.000 Adressdaten sowie rund 40.000 Bankverbindungen von Unternehmen mit Vertragsbeziehungen zum LBB. Auf diese Daten konnten neben eigenen Bediensteten und denen des LDI auch externe Beschäftigte von SAP sowie Beraterfirmen zugreifen. Einige auch von Externen verwendete Benutzer verfügten über das Sammelprofil SAP_ALL. Diese umfassende, sogenannte kritische Berechtigung beinhaltet alle in einem SAP-System möglichen Berechtigungen.

Der LBB hat erklärt, der Kreis der im SAP-System eingesetzten externen Beschäftigten werde ausschließlich über Rahmenverträge des LDI beauftragt. Über die Verträge seien diese zur Verschwiegenheit verpflichtet. Weiter führt er an, der LDI werde eine Marktrecherche vornehmen, mit welchen Programmen die Echtdaten im Entwicklungssystem anonymisiert werden könnten und dennoch die erforderlichen Strukturen und Datenmengen für eine Test- und Entwicklungsumgebung zur Verfügung stünden. Nach Abschluss dieser Prüfung solle unter Kosten- und Nutzengesichtspunkten über das zukünftige Vorgehen entschieden werden.

Der Rechnungshof weist darauf hin, dass der Einsatz von Echtdaten aus dem Produktivsystem im Entwicklungssystem grundsätzlich weder erforderlich noch aus Datenschutzgründen zulässig ist. Vielmehr können dort reine Testdaten oder anonymisierte Daten verwendet werden. Bei einer Anonymisierung von Echtdaten muss eine Entschlüsselung durch Dritte ausgeschlossen sein. Allgemeine Verschwiegenheitserklärungen in Rahmenverträgen sind allein nicht ausreichend, um die Sicherheit dieser Daten zu gewährleisten.

2.3 Berechtigungskonzept nicht vollständig, verbindlich, nachvollziehbar und aktuell

Das Berechtigungskonzept stellt die elementare Sicherheitsfunktion in SAP-Systemen dar. Es muss die rechtlichen und organisatorischen Sicherheitsvorkehrungen des LBB technisch abbilden. Dementsprechend werden die Zugriffsregelungen für einzelne Benutzer oder Benutzergruppen auf das IT-System festgelegt. Das Berechtigungskonzept muss vollständig, verbindlich, nachvollziehbar und aktuell sein. Dadurch wird gewährleistet, dass in dem Konzept sämtliche erforderlichen Regelungen für eine wirksame Begrenzung der Zugriffsrechte festgelegt und diese für Dritte überprüfbar sind.

Die vom LBB vorgelegten Unterlagen genügten diesen Anforderungen nicht. Zudem lag das „LBB SAP Berechtigungs- und Sicherheitskonzept“ lediglich als Entwurf mit Stand vom März 2013 vor. Ein Berechtigungskonzept für das zur Bewirtschaftung der Liegenschaften eingesetzte SAP-Modul RE-FX mit Stand vom Dezember 2017 enthielt lediglich Festlegungen für dieses Modul.

Der LBB hat mitgeteilt, dass der vorliegende Entwurf des „LBB SAP Berechtigungs- und Sicherheitskonzepts“ formal zwar nicht in Kraft gesetzt, jedoch in weiten Teilen faktisch umgesetzt und mit weiteren Verfahrenssicherungen versehen worden sei. Er hat zugesichert, das vorliegende Berechtigungs- und Sicherheitskonzept mit externer Unterstützung zu überarbeiten und den zwischenzeitlichen Weiterentwicklungen anzupassen. Es werde ein Zeitraum von zwölf Monaten für Entwicklung und Implementierung als realistisch angesehen und angestrebt.

2.4 Kritische Berechtigungen nicht immer identifiziert und zu häufig zugeordnet

2.4.1 Identifizierung kritischer Berechtigungen

Kritische Berechtigungen erlauben Operationen, die für die Systemsicherheit oder aus rechtlicher oder betriebswirtschaftlicher 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 risikobehafteter Prozesse im System oder Änderungen an allgemeinen Systemeinstellungen. Durch eine rechtswidrige Nutzung kann gegen das sogenannte Radierverbot gemäß § 239 Abs. 3 HGB verstoßen werden. Danach müssen ursprünglicher Inhalt und Änderungen von Aufzeichnungen der Buchführung feststellbar bleiben. Daher muss die Vergabe solcher Berechtigungen nach strengen Maßstäben erfolgen. Der LBB hat als Systembetreiber nach den Standards des BSI die kritischen Berechtigungen im SAP-System außerdem regelmäßig zu identifizieren, zu überprüfen und zu bewerten. Dies ist jeweils zu dokumentieren.

Im Entwurf des „LBB SAP Berechtigungs- und Sicherheitskonzepts“ waren über die standardmäßig vorhandenen kritischen Berechtigungen hinaus weitere kritische Berechtigungen eingerichtet. Diese waren weder identifiziert noch war deren Vergabe geregelt. Eine regelmäßige Überprüfung und Bewertung der Verwendung kritischer Berechtigungen war nicht dokumentiert. Die im SAP-System enthaltenen Funktionen zur notwendigen regelmäßigen Überwachung dieser kritischen Berechtigungen wurden nicht genutzt.

Der LBB hat erklärt, er werde das Thema in der Überarbeitung des Berechtigungs- und Sicherheitskonzepts mit behandeln.

2.4.2 Vergabe kritischer Berechtigungen

Das Sammelprofil SAP_ALL umfasst alle Berechtigungen im SAP-System. Damit können sämtliche Transaktionen und somit auch risikobehaftete Operationen ausgeführt werden. Eine Zuordnung des Sammelprofils im Produktivsystem ist nach den Vorgaben des BSI zu vermeiden. Nach den Empfehlungen von SAP und den Standards des BSI sollte es möglichst nur an Notfallbenutzer vergeben werden.[3]

Zum Zeitpunkt der Prüfung war das Sammelprofil SAP_ALL acht Benutzern zugeordnet. Auch weitere kritische Berechtigungen, wie das Sammelprofil SAP_NEW, das ebenfalls die Ausführung aller Transaktionen ermöglicht, wurden mehreren Benutzern zugeordnet. Es war nicht ersichtlich, inwieweit diese kritischen Berechtigungen für die Erledigung der Aufgaben erforderlich waren. Dadurch bestanden vermeidbare Sicherheitsrisiken.

Der LBB hat mitgeteilt, die Berechtigungsprofile SAP_ALL und SAP_NEW würden den Benutzern im Produktivsystem entzogen. Zukünftig werde dafür Sorge getragen, dass die Notwendigkeit für die Vergabe von kritischen Berechtigungen im Produktivsystem geprüft, hinreichend dokumentiert und auf ein Mindestmaß beschränkt werde.

2.5 Benutzerverwaltung genügte nicht den Anforderungen

Zu ausgewählten sicherheitsrelevanten Bereichen der Benutzerverwaltung im Produktivsystem hat der Rechnungshof Folgendes festgestellt:

- SAP-Standardbenutzer, die bei der Installation von SAP automatisch angelegt werden und die häufig über umfangreiche Berechtigungen verfügen, waren

---

[3] Vgl. SAP-Dokumentation Berechtigungsprofil SAP_ALL: https://help.sap.com/saphelp_dm40/helpdata/de/78/7a553efd234644e10000000a114084/frameset.htm.

nicht immer wie erforderlich gesperrt oder nicht den Anforderungen entsprechend konfiguriert worden. Auch wurden ihre Aktivitäten nicht wie vorgeschrieben protokolliert.[4]

- Bei zeitlich befristeten Benutzern wurden nach Ablauf der vorgesehenen Nutzungsdauer die zugewiesenen Berechtigungen nicht entfernt.
- Inaktive Benutzer, die über einen längeren Zeitraum nicht mehr im SAP-System angemeldet waren, wurden nicht immer gesperrt.
- In einigen Fällen konnten sich mit einer Benutzerkennung mehrere natürliche Personen gleichzeitig anmelden. Dadurch war eine eindeutige Zuordnung der Aktivitäten im System nicht sichergestellt.

Der LBB hat erklärt, in Abstimmung mit dem LDI werde den Empfehlungen des Rechnungshofs bei den Standardbenutzern entsprochen. Mit der Überarbeitung des Berechtigungs- und Sicherheitskonzepts werde der Umgang mit abgelaufenen und inaktiven Benutzern geregelt. Ferner sei der LDI beauftragt worden, Mehrfachanmeldungen mit einer Benutzerkennung systemseitig zu unterbinden.

2.6 Weitere Mängel

Weiterer Verbesserungsbedarf bestand in folgenden Bereichen:

- Die notwendige Trennung von Benutzer- und Berechtigungsadministration war nicht eindeutig geregelt.
- Die zur Speicherung der Benutzerpasswörter eingesetzte Verschlüsselungstechnik entsprach nicht immer dem aktuellen Stand der Technik. Die Passwörter waren teilweise nur mit einem veralteten, leicht zu entschlüsselnden Algorithmus gesichert.
- Die Aktivitäten von Benutzern mit kritischen Berechtigungen wurden nicht gesondert protokolliert und überwacht. Es fehlte ein Protokollierungskonzept, das Art und Umfang der vorgenommenen Protokollierungen umfassend regelt.

Der LBB hat mitgeteilt, er werde die Funktionstrennung zwischen Benutzer- und Berechtigungsadministration bei der Überarbeitung des Berechtigungs- und Sicherheitskonzepts behandeln und die Dokumentation nachschärfen. Das vom Rechnungshof aufgezeigte Problem hinsichtlich der Verschlüsselung der Passwörter werde derzeit durch den LDI überprüft und in Abstimmung mit dem LBB beseitigt. Die Empfehlungen bezüglich der Protokollierung von Benutzern mit kritischen Berechtigungen würden umgesetzt. Ein entsprechendes Protokollierungskonzept werde erarbeitet.

3 Folgerungen

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

Der Rechnungshof hatte gefordert,

a) die SAP-Systeme des Landesbetriebs Liegenschafts- und Baubetreuung auf einen aktuellen Stand zu bringen und zukünftig sicherzustellen, dass sicherheitsrelevante Aktualisierungen regelmäßig durchgeführt werden,

b) im Entwicklungssystem keine Echtdaten aus dem Produktivsystem zu verwenden,

c) ein vollständiges, verbindliches und nachvollziehbares Berechtigungskonzept zu erstellen und aktuell zu halten,

---

[4] Dies betraf insbesondere die Standardbenutzer SAP*, DDIC, SAPCPIC, TMSADM und WF-Batch.

d) kritische Berechtigungen vollständig zu identifizieren, regelmäßig zu überprüfen und zu bewerten und dies zu dokumentieren, die Zuordnung kritischer Berechtigungen zu regeln und deren Vergabe auf den für die Aufgabenerledigung erforderlichen Umfang zu begrenzen,

e) automatisch im System angelegte Standardbenutzer abzusichern, Berechtigungen bei abgelaufenen Benutzern zu entfernen, inaktive Benutzer zu sperren sowie Mehrfachanmeldungen zu unterbinden,

f) die Trennung von Benutzer- und Berechtigungsadministration im Berechtigungskonzept eindeutig zu regeln,

g) die Passwörter der Benutzer entsprechend dem aktuellen Stand der Technik zu verschlüsseln,

h) Aktivitäten der Benutzer mit kritischen Berechtigungen zu überwachen und ein Protokollierungskonzept zu erstellen.

3.2 Folgende Forderung ist nicht erledigt:

Der Rechnungshof hat gefordert, über die Ergebnisse der eingeleiteten Maßnahmen zu Nr. 3.1 zu berichten.