Kurzübersicht
Markthallen München
SAP-Sicherheit

Überblick zum Prüfungsgegenstand

Die Markthallen München (MHM) sind ein Eigenbetrieb nach Art. 88 der Gemeindeordnung für den Freistaat Bayern mit eigenständiger Buchführung. Die MHM betreiben ein eigenes SAP-System, das auf Servern von IT@M läuft und im Auftrag von den MHM von IT@M administriert wird.

Zielsetzung der Prüfung

Ziel der Prüfung war es, die Ordnungsmäßigkeit des SAP-Systems der Markthallen München sicherzustellen und die einschlägigen Datenschutz- und Datensicherheitsbestimmungen einzuhalten.

Prüfungsergebnisse (Zusammenfassung)

- Kritische RFC-Berechtigungen wurden zu großzügig vergeben.
- Dialogbenutzer können als Referenzbenutzer zugeordnet werden.
- Kritische und selbst erstellte Tabellen sind nicht ausreichend vor manuellen Änderungen geschützt.
- Nicht alle für die Rechnungslegung oder die Systemsicherheit relevanten Tabellenänderungen werden protokolliert.
- Importe von Tabelleninhalten können nicht über Protokolle nachvollzogen werden.
- Zwei Benutzer haben das Recht zum Löschen der Tabellenänderungsprotokolle.
- Die Berechtigung, die System- und die Mandantenänderbarkeit einzustellen, war zu großzügig vergeben.
- Vier Benutzer haben volle Zugriffsrechte zum Customizing im Produktivmandanten.
- Fünf Benutzer besitzen im Produktivsystem das Zugriffsrecht Programme mit Replace-Möglichkeit zu debuggen.
- 29 Dialogbenutzer können Programme zum Löschen von Programmversionen nutzen.
- Zwei Benutzer besitzen die Berechtigung, Transaktionen anzulegen oder zu ändern.
- Selbst erstellte Transaktionen sind zumeist nicht durch Berechtigungsobjekte geschützt.
- Vier Personen, die nicht für die Benutzer- und Berechtigungsverwaltung zuständig sind, haben uneingeschränkte Rechte für die Benutzerverwaltung.

Empfehlungen auf der Basis der Prüfungsergebnisse (Zusammenfassung)

- Kritische RFC-Berechtigungen sind auf das zwingend erforderliche Maß zu begrenzen
- Das System ist so zu konfigurieren, dass nur Referenzbenutzer als Referenz zugeordnet werden können.
- Die Berechtigungen zum Ändern von Tabellen sind auf das zwingend erforderliche Maß zu begrenzen. Weiterhin sind selbst entwickelte Tabellen dem Risiko entsprechend zu schützen.
- Bei allen Tabellen, die für die Rechnungslegung oder die Systemsicherheit relevant sind, ist das Protokollkennzeichen zu setzen. Selbst erstellte Tabellen sollten grundsätzlich protokolliert werden.
- Die Protokollierung für Importe von Tabelleninhalten ist zu aktivieren.
- Das Recht zum Löschen der Tabellenänderungsprotokolle darf nicht vergeben werden.
- Die Berechtigung zur Einstellung der System- und Mandantenänderbarkeit sollte nur der Notfallbenutzer haben.
- Die Customizingrechte sind einzuschränken.
- Das Recht, Programme mit Replace-Möglichkeit zu debuggen, darf im Produktivsystem nicht vergeben werden.

- Die Programme zum Löschen von Programmversionen sind durch das Zuordnen einer entsprechenden Berechtigungsgruppe so zu schützen, dass diese weder im Produktivsystem, noch im Entwicklungssystem ausgeführt werden können.
- Die Berechtigung Transaktionen anzulegen oder zu ändern sollte im Produktivsystem nur der Notfallbenutzer haben.
- Selbst erstellte Transaktionen sollten grundsätzlich durch Berechtigungsobjekte geschützt werden.
- Die Berechtigungen zur Benutzer- und Berechtigungsverwaltung sollten auf das zwingend notwendige Maß eingeschränkt werden.

Stellungnahme der geprüften Organisationseinheiten (Zusammenfassung)

Die geprüften Dienststellen erklärten ihr Einverständnis mit den Prüfungsergebnissen. Die Empfehlungen wurden zum größten Teil bereits umgesetzt oder werden demnächst umgesetzt.

Der Rechnungsprüfungsausschuss übernimmt die Prüfungsergebnisse und trägt die Empfehlungen des Revisionsamts mit.