RECHNUNGSHOF
RHEINLAND-PFALZ

Auszug aus dem Jahresbericht 2011

Nr. 11 Landesamt für Soziales, Jugend und Versorgung
- Mängel bei dem IT-Einsatz und der IT-Sicherheit -

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. 11 Landesamt für Soziales, Jugend und Versorgung - Mängel bei dem IT-Einsatz und der IT-Sicherheit -

Im Geschäftsbereich des Landesamts werden zahlreiche Server-, Speicher- und Drucksysteme betrieben. Bei einer Vereinheitlichung, Zusammenführung und Virtualisierung der Server- und Speichersysteme genügen 20 anstelle der bisher eingesetzten 79 Server. Hierdurch können einmalig Ausgaben von 70.000 € für Ersatzbeschaffungen sowie Energie- und Personalkosten von 100.000 € jährlich vermieden werden. Die Druckkosten können um bis zu 30 % gesenkt werden, wenn ein leistungsfähiges Drucksystem eingerichtet wird.

Das Landesamt mietete Telefonanlagen ohne vorherige Ermittlung der wirtschaftlichsten Beschaffungsart. Durch den Erwerb vergleichbarer Anlagen hätten die Ausgaben um 200.000 € verringert werden können.

Ein den Anforderungen genügendes IT-Sicherheitskonzept fehlte. IT-Sicherheit und Datenschutz waren nicht hinreichend gewährleistet.

1 Allgemeines

Dem Landesamt für Soziales, Jugend und Versorgung sind u. a. die Ämter für soziale Angelegenheiten und die Landesschulen für sinnesbehinderte Menschen nachgeordnet. Im Geschäftsbereich des Landesamts werden an neun Standorten IT-Systeme zur Unterstützung der Aufgabenerledigung betrieben. Die einzelnen Standorte sind über leistungsfähige Netzwerkverbindungen miteinander verknüpft. Diese wurden vom Landesbetrieb Daten und Information (LDI) bereitgestellt. In das Netzwerk sind etwa 1.000 Arbeitsplatzrechner eingebunden.

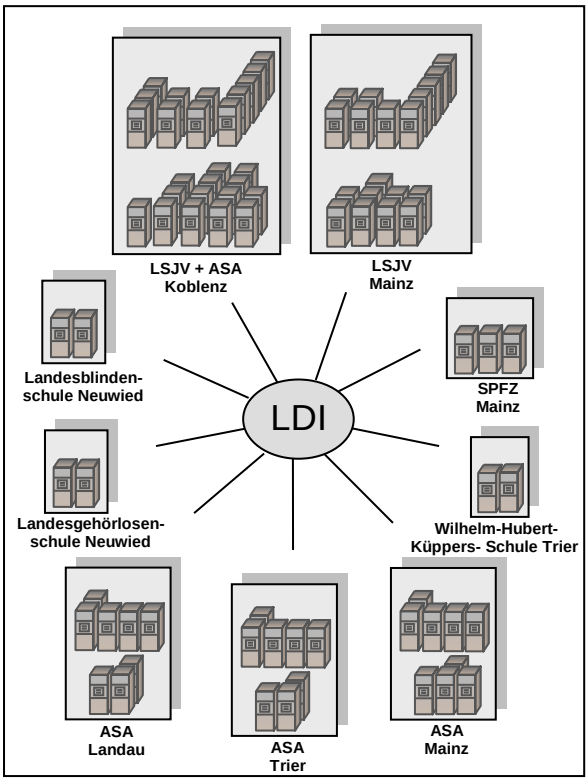
Der Rechnungshof hat in ausgewählten Bereichen den IT-Einsatz geprüft. Insbesondere wurde untersucht, ob hierbei wirtschaftlich verfahren wurde und die Sicherheit des IT-Einsatzes gewährleistet war.

2 Wesentliche Prüfungsergebnisse

2.1 Ungenutzte Möglichkeiten zur Verbesserung der IT-Infrastruktur

An den neun Standorten wurden insgesamt 79 Server und zehn Systeme zur Datensicherung (Backup) eingesetzt, um die für den IT-Betrieb erforderliche Rechenleistung und Speicherkapazität bereitzustellen. Die folgende Abbildung zeigt die Verteilung der Server- und Speichersysteme:

IT-Infrastruktur im Geschäftsbereich des Landesamts - Stand: 30. Juni 2009



Die Abbildung zeigt die IT-Infrastruktur des Landesamts und dessen nachgeordneter Einrichtungen. An neun Standorten wurden zahlreiche Server- und Speichersysteme vorgehalten.

Der Betrieb der Server- und Speichersysteme war nicht wirtschaftlich:

- In vielen Fällen stellten die Server nur einen bzw. wenige Dienste (wie z. B. Datenbank, E-Mail und Ablage) zur Verfügung. Dadurch waren deren Rechen- und Speicherkapazitäten bei Weitem nicht ausgelastet.
- Gleichartige Anwendungen und Dienste waren auf mehreren Servern und an unterschiedlichen Standorten installiert. Dadurch mussten die für den Betrieb erforderlichen Ressourcen mehrfach vorgehalten werden.
- Bei den Speichersystemen handelte es sich zumeist um lokale Festplattenspeicher, die direkt mit einem Server verbunden waren. Dadurch konnte die Auslastung der einzelnen Speichersysteme nicht zentral festgestellt werden. Auch eine dynamische und flexible Zuweisung von Speicherkapazität war nicht möglich. Wurde z. B. mehr Speicherplatz benötigt oder traten technische Probleme auf, musste die Festplatte "vor Ort" bei dem betroffenen Server ausgetauscht werden.

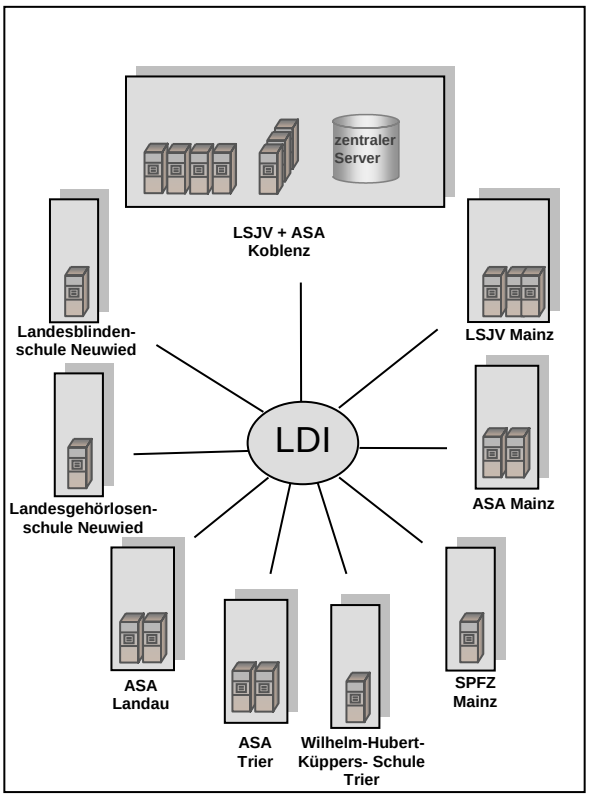
Ein wirtschaftlicherer IT-Einsatz lässt sich durch eine Erhöhung der Zahl der Dienste und Anwendungen, die pro Server bereitgestellt werden, erreichen. Dadurch steigt die Auslastung der einzelnen Geräte und die Zahl der Server kann verringert werden. Außerdem sollten bisher dezentral betriebene Server und Anwendungen an möglichst wenigen Standorten auf wenigen Geräten konzentriert werden (physische Konsolidierung). Über die bestehenden Netzwerkverbindungen ist der Datenaustausch mit hohen Übertragungskapazitäten sichergestellt.

Allein bei Nutzung dieser Verbesserungsmöglichkeiten kann die Zahl der Server auf 40 vermindert werden.

Weitere Rationalisierungsvorteile werden durch eine Virtualisierung erzielt. Hierbei werden auf einem leistungsfähigen Server mit Hilfe einer speziellen Software mehrere virtuelle Server gleichzeitig und vollständig unabhängig voneinander eingerichtet. Dazu werden Hardware, Betriebssystem und Anwendungen eines einzelnen

Servers als Einheit aufgefasst und als virtueller Server nachgebildet. Werden mehrere virtuelle Server auf einem physischen System betrieben, ist eine weitere Reduzierung auf nur noch 20 Server möglich. Die verbleibenden Serversysteme können, wie die folgende Abbildung verdeutlicht, weitgehend an einem Standort zentralisiert werden:

Verbesserung der IT-Infrastruktur bei Virtualisierung



Die Abbildung verdeutlicht, dass bei einer Virtualisierung gegenüber dem Ist-Zustand erhebliche Rationalisierungsvorteile erzielt werden können. Die Zahl der Server kann um 59 auf 20 verringert werden.

Durch Konsolidierung und Virtualisierung können bei der Hard- und Software im Vergleich zur anstehenden Ersatzbeschaffung der derzeit betriebenen Systeme einmalig Ausgaben von rund 70.000 € vermieden werden. Zudem können durch geringere Energiekosten und einen verringerten Administrationsaufwand Einsparungen von rund 100.000 € jährlich erreicht werden.

Das Landesamt hat erklärt, bei der Ablösung und Zusammenführung von Serversystemen im Rahmen einer Konsolidierung oder Virtualisierung müssten auch Sicherheitskriterien und Betriebsempfehlungen der Hersteller beachtet und Administratoren in den neuen Techniken ausgebildet werden. Eine detaillierte Betrachtung sei unerlässlich, um die sinnvollen und wirtschaftlichen Möglichkeiten genauer abschätzen zu können. Das Landesamt werde die Empfehlungen als mittel- bzw. langfristige Ausrichtung einplanen und einzelne Serversysteme nach und nach virtualisieren oder zusammenführen.

Der Rechnungshof merkt hierzu an, dass eine lediglich mittel- oder langfristige Umstellung der IT-Infrastruktur zu vermeidbaren Kosten führt. Daher sollten bereits die anstehenden Ersatzbeschaffungen zum Anlass genommen werden, die aufgezeigten Verbesserungsmöglichkeiten zeitnah zu nutzen.

2.2 Unwirtschaftlicher Einsatz von Drucksystemen

Von 2004 bis Mitte 2009 wurden für den Kauf von rund 700 Druckern und für Verbrauchsmaterial (Tintenpatronen, Tonerkartuschen) 470.000 € aufgewendet. Insgesamt wurden zur Zeit der Erhebungen des Rechnungshofs im Geschäftsbereich des Landesamts rund 770 Drucker betrieben. Es waren 20 verschiedene Druckermodelle im Einsatz. Dabei handelte es sich zumeist um nicht netzwerkfähige Arbeitsplatzdrucker.

Der Betrieb dieser Drucksysteme war nicht wirtschaftlich:

- Da die Arbeitsplatzdrucker nicht in ein Netzwerk eingebunden waren, konnte das Landesamt die Auslastung der einzelnen Drucker weder feststellen noch steuern.
- Durch den Kauf zahlreicher kleiner und unterschiedlicher Drucker entstanden vergleichsweise hohe Beschaffungskosten.
- Für die unterschiedlichen Modelle musste jeweils das passende Verbrauchsmaterial beschafft und verwaltet werden.
- Die Betreuung einer Vielzahl von Arbeitsplatzdruckern erforderte einen hohen Administrationsaufwand.

Durch den Einsatz eines leistungsfähigen netzwerk-basierten Drucksystems können die Druckkosten (Gesamtkosten einschließlich Kauf/Miete/Leasing, Verbrauchsmaterial und Administration) um bis zu 30 % gesenkt werden.

Das Landesamt hat erklärt, das Druckkonzept im Gesamtgeschäftsbereich werde überarbeitet. Hauptziel sei die Umstellung auf einheitliche monochrome Etagendrucksysteme. Einzelplatzdrucker würden nur noch in begründeten Ausnahmefällen zugelassen. Als Sofortmaßnahme, bis das Gesamtkonzept vorliege, seien bereits mehrere Einzelplatzdrucksysteme durch netzwerkfähige Drucksysteme ersetzt worden.

2.3 Gemietete Telefonanlagen zu teuer

Für die Miete der Telefonanlage für das Dienstgebäude des Landesamts in Mainz und der technisch mit ihr gekoppelten Anlage des Sozialpädagogischen Fortbildungszentrums zahlte das Landesamt 2004 bis 2009 insgesamt rund 310.000 €. Vor der Vergabe der Leistungen hatte das Landesamt die wirtschaftlichste Beschaffungsart nicht ermittelt. Die Leistungen waren auch nicht im Wettbewerb vergeben worden.

Für den Kauf und die Wartung vergleichbarer Anlagen an den Standorten Koblenz und Landau fielen im gleichen Zeitraum Ausgaben von nur 103.000 € und 111.000 € an. Die Miete war damit fast drei Mal so teuer wie ein Kauf.

Das Landesamt hat erklärt, die Mietverträge würden gekündigt und die gemieteten Telefonanlagen noch im Jahr 2010 durch neue Anlagen abgelöst, die über den Rahmenvertrag des Landes beschafft werden sollten. Der Gesamtpreis belaufe sich auf dem Niveau des Kaufpreises der anderen Anlagen.

2.4 IT-Sicherheit und Datenschutz nicht gewährleistet

Beim Landesamt fehlte ein umfassendes IT-Sicherheitskonzept, das die aus einer Risiko- und Schutzbedarfsanalyse abgeleiteten Maßnahmen zur Gewährleistung der IT-Sicherheit enthält. Auch Regelungen zu technischen und organisatorischen Sicherheitsmaßnahmen und zu derem Zusammenwirken waren nicht oder nicht ausreichend vorhanden. Mängel bestanden insbesondere in folgenden Bereichen:

- Serverräume waren nicht ausreichend klimatisiert, Brandschutztüren fehlten.
- Die unterbrechungsfreie Stromversorgung der Server war nicht ausreichend dimensioniert oder funktionierte nicht.

- Verfügbarkeitsanforderungen für die Server waren nicht bestimmt. Die Verfügbarkeit der Server war nicht durch entsprechende Wartungsvereinbarungen sichergestellt.
- Funktionen und Verantwortlichkeiten bei der Systembetreuung und der Verfahrensentwicklung waren nicht eindeutig festgelegt. Regelungen für die sichere Nutzung der IT-Systeme durch die Mitarbeiter des Landesamts fehlten.
- Die Vergabe von Zugriffsrechten im Netzwerk des Landesamts war nicht einheitlich geregelt und wurde nicht ausreichend dokumentiert.
- Personenbezogene Daten waren nicht ausreichend geschützt. Mitarbeiter hatten Zugriff auf Datenbankdateien, in denen personenbezogene Daten gespeichert waren. Diese konnten kopiert und gelesen werden, ohne dass dies protokolliert wurde.
- Durch die private Internet- und E-Mail-Nutzung stieg die Gefahr des Befalls der IT-Systeme durch Dateien mit Schadfunktionen. Regelungen zum Verhalten beim Auftreten solcher Dateien fehlten.
- Es gab kein einheitliches Verfahren zur Datensicherung. Datensicherungsbänder wurden nicht oder in zu langen Intervallen ausgelagert.

Das Landesamt hat erklärt, die bisher bereits angewendeten Sicherheitsrichtlinien würden in das geforderte IT-Sicherheitskonzept aufgenommen. Das Sicherheitskonzept werde verfeinert und auf der Grundlage der Empfehlungen des Bundesamts für die Sicherheit in der Informationstechnik ausformuliert und fortgeschrieben. Festgestellte Mängel bei der IT-Sicherheit seien behoben worden oder würden behoben. Bezüglich des Zugriffs auf personenbezogene Daten in Datenbankdateien werde von neuen Lösungen abgesehen.

Der Rechnungshof weist darauf hin, dass bei der Verarbeitung von personenbezogenen Daten die innerbehördliche Organisation so zu gestalten ist, dass diese Daten nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können[1]. Dies schließt auch bereits bestehende Verfahren ein.

2.5 Softwareentwicklung nicht zweckmäßig organisiert

Im Geschäftsbereich des Landesamts wurden vielfach Datenbankanwendungen entwickelt. Zur Organisation wurde u. a. Folgendes festgestellt:

- Fachliche Anforderungen an die zu programmierenden Verfahren waren nicht schriftlich festgehalten.
- Einheitliche Vorgaben für die Programmierung (Programmierrichtlinien) fehlten.
- Die Wirtschaftlichkeit der Eigenprogrammierung wurde nicht geprüft.
- Der Einsatz der Programmierer wurde nicht zentral gesteuert. Eine fachliche und zeitliche Koordinierung der Entwicklungsarbeiten fand nicht statt.

Das Landesamt hat erklärt, es habe ein Antragsformular für Programmieraufträge und Programmänderungen entworfen, das bereits eingesetzt werde. Bestehende Vorgaben für die Programmierung seien in einen ersten Entwurf für Programmierrichtlinien zusammengeführt worden. Dieser werde verbindlich eingesetzt. Die fachliche und zeitliche Steuerung der Entwicklungsarbeiten werde im Zuge der neuen Aufgabenverteilung mit definiert. Weiterhin würden Konzepte zu Codeverwaltungs-, Aufgabenverwaltungs- und Dokumentationssystemen erarbeitet, die eine bessere Projektsteuerung ermöglichten.

---

[1] § 9 Abs. 2 Landesdatenschutzgesetz (LDSG) vom 5. Juli 1994 (GVBl. S. 293), zuletzt geändert durch Gesetz vom 17. Juni 2008 (GVBl. S. 99), BS 204-1.

3 Folgerungen

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

Der Rechnungshof hatte gefordert,

a) einen wirtschaftlicheren Einsatz von Drucksystemen sicherzustellen,

b) die Mietverträge für die Telefonanlagen in Mainz rechtzeitig zu kündigen und bei der Ersatzbeschaffung die Nutzung der Rahmenverträge des Landes zu prüfen,

c) Mängel bei der IT-Sicherheit zu beheben,

d) ein den Anforderungen genügendes umfassendes IT-Sicherheitskonzept zu erstellen und umzusetzen,

e) die Entwicklung von Datenbankanwendungen wirksam zu steuern und Entwicklungskapazitäten zu nutzen.

3.2 Folgende Forderungen sind nicht erledigt:

Der Rechnungshof hat gefordert,

a) Server- und Speichersysteme im Geschäftsbereich des Landesamts möglichst bald zu konsolidieren und zu virtualisieren,

b) sicherzustellen, dass personenbezogene Daten nicht unbefugt kopiert, verändert oder entfernt und gelesen werden können,

c) über das Ergebnis der eingeleiteten Maßnahmen zu Nr. 3.1 Buchstaben a und d zu berichten.