Datenschutz und Informationssicherheit in den NÖ Landeskliniken Zusammenfassung

Der Landesrechnungshof überprüfte den Datenschutz und die Informationssicherheit bei der NÖ Landeskliniken-Holding. Dazu wurden zehn NÖ Landeskliniken, je zwei pro Region, ausgewählt.

Ziel war, weitere Möglichkeiten zur Vereinheitlichung der Infrastruktur für Informations- und Kommunikationstechnologie sowie Verbesserungen für die Personalplanung aufzuzeigen. Außerdem sollten allfällige Sicherheitslücken erkannt und Vorschläge zur Behebung erarbeitet werden.

In ihrer Stellungnahme sagte die NÖ Landesregierung die Umsetzung aller 16 Empfehlungen zu. In der NÖ Landeskliniken-Holding werden demnach eine unternehmensweite Risikoanalyse und eine umfassende Sicherheitspolitik etabliert. Außerdem wird die heterogene IKT-Landschaft schrittweise weiter konsolidiert. Erhebliche Einsparungen konnten demnach bereits bei den Lizenzmodellen realisiert werden.

Um Datenschutz und Informationssicherheit gewährleisten zu können, sind technische, fachliche sowie dienstrechtliche Grundlagen und Maßnahmen erforderlich.

Positiv festgestellt wurde, dass die NÖ Landeskliniken-Holding eine Risikoanalyse für einzelne Bereiche erstellt hatte und in Projekten daran arbeitete, die inhomogene Hard- und Softwarelandschaft zu konsolidieren.

Risikoanalyse und Sicherheitspolitik

Die Risikoanalyse und die Projekte bezogen sich schwerpunktmäßig auf die Informations- und Kommunikationstechnologie und umfassten nicht alle Vermögenswerte und Geschäftsbereiche. Daher waren die Risiken für die gesamte NÖ Landeskliniken-Holding zu bewerten und daraus eine unternehmensweite Sicherheitspolitik mit erforderlichen Maßnahmen zu entwickeln und umzusetzen.

Personalbedarf

Dabei war zu beachten, dass die Personalhoheit für die Bediensteten der NÖ Landeskliniken beim Amt der NÖ Landesregierung verblieb, während die Angelegenheiten der Informations- und Kommunikationstechnologie der NÖ Landeskliniken-Holding übertragen wurden.

Personalausstattung

Die personelle Ausstattung mit Mitarbeitern für Informations- und Kommunikationstechnologie an den 27 Standorten betrug 2 bis 18,5 Vollzeitäquivalente und war damit sehr unterschiedlich. Diese Mitarbeiter hatten gemäß ihrer Stellenbeschreibungen die sichere elektronische Datenverarbeitung zu gewährleisten. Ihre Aufgaben waren teilweise umfassend „für alles zuständig" und teilweise sehr detailliert festgelegt.

Konsolidierung

Die Konsolidierung der Hard- und Softwarelandschaft war weiter voranzutreiben. Dafür waren jedoch deren Vermögenswerte (Hard- und Software, Daten) vollständig zu erfassen und auf dem aktuellen Stand zu halten. So kann auch der Personalbedarf besser ermittelt und der Sach- und Personalaufwand, zum Beispiel für Lizenzen, Aus- und Weiterbildung oder Betreuung der Nutzer, verringert werden. In diesem Zusammenhang sollten für die Mitarbeiter im Bereich Informations- und Kommunikationstechnologie auch standardisierte Stellenbeschreibungen und ein verbindliches Aus- und Weiterbildungskonzept erstellt werden.

Außerdem waren die Dokumentationen der Hard- und Softwarelandschaft, der Infrastruktur und der Berechtigungsvergaben zu standardisieren.

Sicherheitsrisiken

Sicherheitsrisiken bestanden in Serverräumen, in denen leicht brennbare Materialen (zB Papier) gelagert, flüssigkeitsführende Leitungen verlegt oder wie in einem Fall die zwei zentralen Netzwerkverteilerpunkte (CORE-Switches) im selben Raum aufgebaut waren.

Auch bei der Vergabe von Berechtigungen für das Zugreifen ins und das Arbeiten im Netzwerk sowie der Datenrücksicherung von den Sicherungsbändern erwartete der Landesrechnungshof noch Verbesserungen. Ein hohes Risiko stellten so genannte Gruppenuser dar, die für mehrere Benutzer angelegt wurden, sodass nicht nachvollzogen werden konnte, wer Änderungen in Systemen und Datenbanken durchführte.