Landesrechnungshof
Niederösterreich

Datenschutz und Informationssicherheit in den NÖ Landeskliniken

Bericht 3 | 2012

Datenschutz und Informationssicherheit in den NÖ Landeskliniken
Inhaltsverzeichnis

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.

1. Prüfungsgegenstand

Der Landesrechnungshof überprüfte den Datenschutz und die Informationssicherheit bei der NÖ Landeskliniken-Holding und den NÖ Landesklinken. Dazu wurden zehn NÖ Landeskliniken, je zwei pro Region nach Anzahl der Betten, Anzahl der Stationen sowie bestehende bzw. neu errichtete Infrastruktur, ausgewählt, welche in nachfolgender Grafik mit einem roten Punkte gekennzeichnet sind.

Abbildung 1: Standorte der NÖ Landeskliniken

Ziel der Querschnittsprüfung war, Möglichkeiten für weitere Vereinheitlichungen der in den Jahren 2004 bis 2008 mit den NÖ Krankenanstalten übernommenen inhomogenen Infrastruktur der Informations- und Kommunikationstechnologie sowie Verbesserungen für den Personaleinsatz aufzuzeigen. Außerdem sollten allfällige Sicherheitslücken erkannt und Vorschläge zur Behebung erarbeitet werden.

Daher wurden der aktuelle Stand des Datenschutzes und der Informationssicherheit, auf Grund der geltenden Gesetze, Normen, Best-Practice-Ansätze und Handlungsweisen bei den NÖ Landeskliniken überprüft.

Prüfungszeitraum waren die Jahre 2009 bis 2011, in welchem die wesentlichen für den Datenschutz und die Informationssicherheit in den NÖ Landeskliniken notwendigen Handlungsanweisungen erstellt wurden.

2. Begriffe

EDV bedeutet Elektronische Datenverarbeitung.

Datenschutz bezeichnet den Schutz des Einzelnen vor dem Missbrauch seiner personenbezogenen Daten. Der Zweck besteht darin, das Recht des Individuums auf informationelle Selbstbestimmung zu schützen. Jeder Mensch soll grundsätzlich selbst entscheiden können, für wen und zu welchem Zeitpunkt der notwendige Auszug aus seinen persönlichen Daten zugänglich sein soll. Der Datenschutz ist ein Grundrecht und unter anderem im Datenschutzgesetz des Bundes (DSG 2000), im NÖ Datenschutzgesetz, in der Vereinbarung zur Sicherstellung der Patientenrechte (Patientencharta), im Gesundheitstelematikgesetz und in der Gesundheitstelematikverordnung geregelt.

Informationssicherheit umfasst informationsverarbeitende und -speichernde Systeme, welche die Vertraulichkeit, Verfügbarkeit, Integrität und Authentizität sicher zu stellen haben. Informationssicherheit dient dem Schutz vor Gefahren bzw. Bedrohungen, der Vermeidung von Schäden und der Minimierung von Risiken. Dazu gibt es Qualitätsstandards und ergänzend gemeinsame Kriterien zur Evaluierung der Sicherheit von Informationstechnologie, wie zB Common Criteria. Informationssicherheit umfasst nicht nur die Sicherheit der Informationstechnologie-Systeme und der darin verarbeitenden und gespeicherten Daten, sondern auch jene von nicht elektronisch verarbeiteten und dokumentierten Informationen.

IKT steht für Informations- und Kommunikationstechnologie.

IT ist die Kurzform für Informationstechnologie.

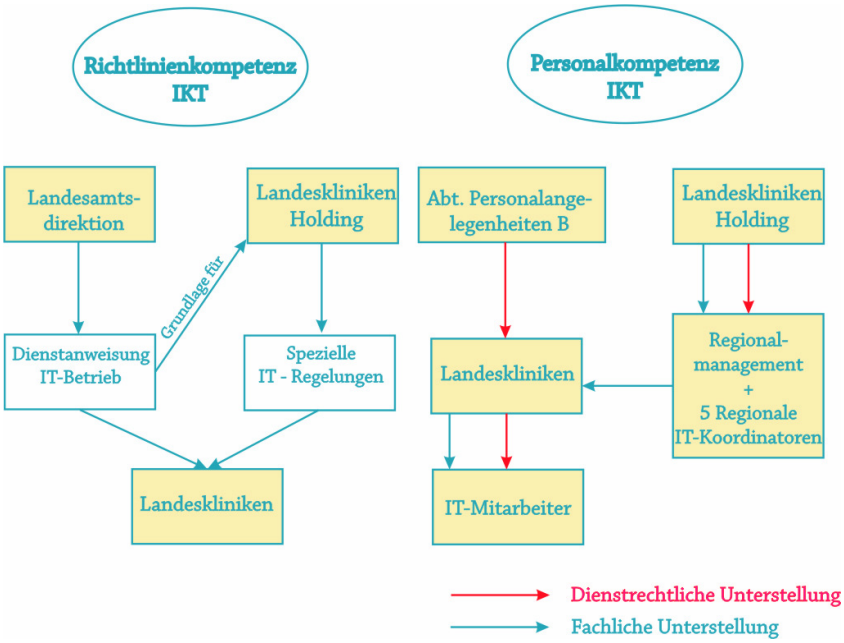
3. Aufgaben und Organisation

Auf Grund der Verordnung über die Geschäftsordnung der NÖ Landesregierung fielen die Aufgaben der Abteilung Landesamtsdirektion Informationstechnologie LAD1-IT in den Geschäftsbereich von Landeshauptmann Dr. Erwin Pröll, die Angelegenheiten der Landeskrankenanstalten in den Geschäftsbereich von Landeshauptmann-Stellvertreter Mag. Wolfgang Sobotka. Bei der NÖ Landeskliniken-Holding war der kaufmännische Geschäftsführer für die Angelegenheiten der Informations- und Kommunikationstechnologie verantwortlich.

Um Datenschutz und Informationssicherheit gewährleisten zu können, sind technische, fachliche sowie dienstrechtliche Maßnahmen erforderlich. In Bezug auf die NÖ Landeskliniken bestanden dafür unterschiedliche Zuständigkeiten, wobei die Richtlinienkompetenz und Personalkompetenz getrennt war.

Gemäß § 2 des Gesetzes über die Errichtung der NÖ Landeskliniken-Holding verblieb die Personalhoheit der Bediensteten der NÖ Landesklinken beim Amt der NÖ Landesregierung, während die Angelegenheiten der Informations- und Kommunikationstechnologie an die NÖ Landeskliniken-Holding übertragen wurden. Daraus folgten die nachstehenden Zuständigkeiten.

- Die Abteilung Personalangelegenheiten B LAD2-B besorgte die Aufgaben der Personalverwaltung im Bereich der NÖ Landesklinken.
- Die Abteilung Landesamtsdirektion, Fachbereich Informationstechnologie LAD1-IT, erließ in Zusammenarbeit mit der NÖ Landeskliniken-Holding die generellen Dienstanweisungen mit Bezug auf Informations- und Kommunikationstechnologie für die NÖ Landeskliniken. Auf diese Weise wurde die Dienstanweisung „IT-Betrieb für Landeskliniken“ erlassen.
- Die NÖ Landeskliniken-Holding war für den Bereich Informations- und Kommunikationstechnologie und die Personalverwaltung der Bediensteten der NÖ Landeskliniken-Holding zuständig. Für den Bereich Informations- und Kommunikationstechnologie wurden folgende Aufgaben definiert:
  - Nutzung von Synergiepotenzialen im Verbund der 27 Standorte durch Konsolidierung der IKT-Landschaft
  - Sicherstellung der Effizienzpotentiale durch Unterstützung der Standardisierung betrieblicher Prozesse und Daten
  - Erhöhung der Qualität und Sicherheit im Betrieb der Informations- und Kommunikationstechnologie
  - Erlassung von speziellen Dienstanweisungen für die NÖ Landeskliniken-Holding.
- Die kollegiale Führung bzw. der kaufmännische Direktor in den NÖ Landeskliniken waren für die Umsetzung und Einhaltung der erlassen Vorschriften zuständig.



Wie die grafische Darstellung zeigt, sind in Bezug auf Datenschutz und Informationssicherheit mehrere Schnittstellen zu beachten, welche einen laufenden Koordinationsaufwand nach sich ziehen.

4. Rechtliche Grundlagen

Die NÖ Landeskliniken-Holding mit Sitz in St. Pölten übernahm mit August 2005 die Führung und den Betrieb der NÖ Landeskliniken. Mit dem Gesetz über die Errichtung der NÖ Landeskliniken-Holding wurde ihr der Betrieb der Informationstechnologie für die NÖ Landeskliniken und der NÖ Landeskliniken-Holding übertragen.

Für die Querschnittsprüfung waren folgende rechtliche Grundlagen und Qualitätsstandards maßgeblich:

Datenschutzgesetz (DSG 2000) und NÖ Datenschutzgesetz

In diesen Gesetzen, BGBl I 1999/165 und LGBl 0901-1, werden insbesondere auch die Rechte der Patienten auf den Schutz ihrer personenbezogenen sensiblen Daten geregelt.

Gesundheitstelematikgesetz

Dieses Bundesgesetz, BGBl I 2004/179, regelt unter anderem die Datensicherheit beim elektronischen Austausch von Gesundheitsdaten. Weiters wird verlangt, dass alle getroffenen Informationssicherheitsmaßnahmen nachvollziehbar zu dokumentieren sind.

Kranken und Kuranstaltengesetz und NÖ Krankenanstaltengesetz

Beide Gesetze, BGBl 1957/1 und LGBl 9440-31, legen unter anderem fest, dass Krankengeschichten mindestens 30 Jahre aufzubewahren sind, allenfalls in Mikrofilmen in doppelter Ausfertigung oder auf anderen gleichwertigen Informationsträgern, deren Lesbarkeit für den Aufbewahrungszeitraum gesichert sein muss. Für Röntgenbilder und andere Bestandteile von Krankengeschichten, deren Beweiskraft nicht 30 Jahre hindurch gegeben ist sowie bei ambulanter Behandlung kann durch die Landesgesetzgebung eine kürzere Aufbewahrungsfrist, mindestens jedoch zehn Jahre, vorgesehen werden. Auch in diesem Gesetz sind die Rechte des Patienten geregelt.

Gesetz über die Errichtung der NÖ Landeskliniken-Holding (NÖ LKH)

In diesem Landesgesetz, LGBl 9452-2, sind die Zuständigkeiten für die Personalhoheit und Betriebsorganisation festgelegt.

Bundesgesetz über die Verantwortlichkeit von Verbänden für Straftaten (Verbandsverantwortlichkeitsgesetz – VbVG)

Dieses Bundesgesetz, BGBl I Nr. 2005/151, regelt, unter welchen Voraussetzungen Verbände für Straftaten verantwortlich sind und wie sie sanktioniert werden sowie das Verfahren, nach dem die Verantwortlichkeit festgestellt und Sanktionen auferlegt werden. Entscheidungsträger im Sinne dieses Gesetzes sind unter anderem Geschäftsführer, Vorstandsmitglieder und Prokuristen oder wer aufgrund organschaftlicher oder rechtsgeschäftlicher Vertretungsmacht in vergleichbarer Weise dazu befugt ist, den Verband nach außen zu vertreten.

Interne Regelungen

Außerdem gelten im Zusammenhang mit Datenschutz und Informationssicherheit bei der NÖ Landeskliniken-Holding und den NÖ Landeskliniken folgende interne Regelungen:

- Die generelle Dienstanweisung „IT-Betrieb für Landeskliniken“ für das Personal der NÖ Landeskliniken
- Die Richtlinie „Informationssicherheit, Richtlinie für Benutzer der Holding Zentrale“ für das eigen Personal der NÖ Landeskliniken-Holding

- Zusätzlich wurden folgende Richtlinien erlassen:
  - Richtlinie „IKT-Infrastruktur – Konfigurationsvorgaben IT-Benutzer- und IT-Gerätenamen
  - Richtlinie „IKT-Infrastruktur – Standard-Software“
  - Richtlinie „Errichtung von IKT-Infrastruktur in den NÖ Landeskliniken (WEISSBUCH-IKT)
  - Richtlinie „Informationssicherheit – IS Organisation“
  - Richtlinie „Informationssicherheit – Sofort-Maßnahmen per 1.3.2009“

Qualitätsstandards und Best-Practice-Ansätze

Außerdem waren folgende Qualitätsstandards und Best-Practice-Ansätze anzuwenden:

- Die Normenreihe ISO/IEC 2700*, im speziellen ISO/IEC 27002 Informationstechnik – IT-Sicherheitsverfahren – Leitfaden für das Informationssicherheits-Management. Dieser internationale Standard beinhaltet Kontrollmechanismen für die Informationssicherheit.
- Die Normenreihe ISO/IEC 13335, für Vorgangsweisen zum Managen und Planen von Konzepten und Modellen der IT-Sicherheit. Im Weiteren werden auch die Auswahl der Sicherheitsmaßnahmen und der Management Guide für Netzwerksicherheit behandelt.
- Das Österreichische Informationssicherheitshandbuch des Bundeskanzleramtes orientierte sich an den normativen Vorgaben der ISO/IEC Normen 27001 / 27002 und verwandter Standards sowie den sehr detaillierten Leitfäden und Handbüchern zur Informationssicherheit, beispielsweise den Grundschutzstandards und -bausteinen des Bundesamtes für Sicherheit in der Informationstechnologie der Bundesrepublik Deutschland. Einerseits ist es im Stil einer Vorschrift formuliert, um notwendige Überlegungen und Maßnahmen klar und unzweifelhaft darzustellen, andererseits bietet es eine Auswahl an Möglichkeiten und Entscheidungskriterien für die Implementierung in der Praxis. Dabei wurde allerdings auf die gebotene Kompaktheit geachtet. (Siehe www.sicherheitshandbuch.gv.at)
- COBIT (Control Objectives for Information and Related Technology) ist ein international anerkannte Handlungsrahmen zur IT-Governance. Die Aufgaben der Informationstechnologie werden in Prozesse und Kontrollziele gegliedert. Dabei wird nicht vorrangig definiert wie die Anforderungen umzusetzen sind, sondern welche umzusetzen sind.

- ITIL (Information Technology Infrastructure Library) ist eine Sammlung von Best-Practices, welche eine mögliche Umsetzung eines IT-Servicemanagements beschreiben und international als De-facto-Standard hierfür gelten. Es werden die für den Betrieb einer IT-Infrastruktur notwendigen Prozesse, die Aufbauorganisation und die Werkzeuge beschrieben.

5. Risikobewertung

Um Datenschutz und Informationssicherheit gewährleisten zu können, sind die verschiedenen Risiken zu bewerten.

„Risikobewertungen sollten die Risiken gegen die Kriterien für Risikoakzeptanz und für die Organisation relevanten Ziele identifizieren, quantifizieren und priorisieren. Die Ergebnisse sollten die angemessenen Handlungen des Managements und die Prioritäten für das Managen von Informationssicherheits-Risiken und für das Implementieren der zum Schutz gegen diese Risiken ausgewählten Maßnahmen lenken und bestimmen. Der Prozess des Bewertens der Risiken und des Auswählens der Maßnahmen muss möglicherweise mehrfach durchgeführt werden, um unterschiedliche Teile der Organisation oder einzelne Informationssysteme abzudecken.“
(ÖNorm ISO/IEC 27002)

Die NÖ Landeskliniken-Holding und die NÖ Landesklinken betrieben auf Grund der früheren unterschiedlichen Trägerschaften teilweise noch eine sehr inhomogene Informations- und Kommunikationstechnologie Landschaft. In dieser Landschaft standen verschiedene Hardware, Software, Netzwerkkomponenten und Telekommunikationseinrichtungen im Einsatz, wobei die Hard- und Software nach Medizinprodukten und Nicht-Medizinprodukte zu unterscheiden war.

Mit 1. Jänner 2006 verpflichtete auch das Verbandsveranwortlichkeitsgesetz dazu, Fehlerquellen im Betrieb aufzuspüren und in einem weiteren Schritt technische, organisatorische, personelle und andere Maßnahmen festzulegen, um strafrechtliche Folgen zu vermieden.

Auf Basis dieses Gesetzes führte die NÖ Landeskliniken-Holding eine Risikoanalyse im Bereich der Informationstechnologie durch, bei der Gefährdungen oder Bedrohungen, wie zB die Aufrechterhaltung der Einsatzfähigkeit, die Vermeidung von Störungen der Abläufe und Prozesse, die Kriminalitätsvorbeugung sowie Notfall- und Krisenmanagement als Risiken erkannt wurden.

Parallel dazu wurden verschiedenen Sicherheitszonen, wie zB Öffentlicher Bereich, Kontrollierter Bereich, Sicherheitsbereich und Medizinischer Bereich identifiziert. In weiterer Folge wurden risikosenkende Maßnahmen erarbeitet und mit Checklisten ergänzt. Der übergebene Bearbeitungstand dieses Sicherheitskonzepts war mit 10. August 2010 datiert.

Dieses Sicherheitskonzept wurde jedoch von der Holdingleitung nicht verabschiedet und war dadurch auch in den NÖ Landeskliniken nicht bekannt.

Der Landesrechnungshof wies weiters darauf hin, dass das Risiko der Informationstechnologie nur einen Bereich des Gesamtrisikos abdeckt. Die Risikoanalyse der Informationstechnologie ist daher in eine, alle Bereiche umfassende, Risikoanalyse einzubetten. Dies ist als Grundlage für eine unternehmensweite Sicherheitspolitik erforderlich.

Ergebnis 1
Die NÖ Landeskliniken-Holding hat die Risikoanalyse für alle Bereiche zu ergänzen, die Ergebnisse zusammenzufassen, daraus Maßnahmen abzuleiten und in Kraft zu setzen, welche die Grundlage für die Sicherheitspolitik bilden.

Stellungnahme der NÖ Landesregierung:

Die Etablierung einer unternehmensweiten Risikoanalyse ist seit 2008 in Umsetzung. Eine Zusammenfassung bzw. Fertigstellung erfolgt noch im Laufe des kommenden Jahres auch nach Maßgabe der organisatorischen und budgetären Rahmenbedingungen.

Äußerung des Landesrechnungshofs Niederösterreich:

Die Stellungnahme wurde zur Kenntnis genommen.

Im Jahr 2009 hatte die NÖ Landeskliniken-Holding ein Wirtschaftsprüfungs- und Beratungsunternehmen mit einer Risikoanalyse bei den NÖ Landeskliniken beauftragt. Schwerpunkte waren Physische Zutrittssicherheit, Physische Sicherheit und Leistungsfähigkeit sowie Reserven der Serverräume und der Netzwerkanbindungen (LAN/WAN). Weiters wurden Dokumentation und Organisation von Systemen und Notfall-/Katastrophenfallplanung auf deren Vollständigkeit überprüft.

Außerdem untersuchte ein Wirtschaftsprüfer im Jahr 2009 die Informationstechnologie zur Beurteilung des Risikos mit Schwerpunkt Zugriffsrechte für Programme, Nachvollziehbarkeit von Datenänderungen und Notfallpläne. Diese Überprüfung beschränkte sich auf ausgesuchte Themenbereiche innerhalb eines festgelegten Rotationsplans. Der Wirtschaftsprüfer wies im Rahmen der Abschlussprüfung zum IT-Risiko zusammenfassend darauf hin, dass die Ordnungsmäßigkeit im Bereich der Berechtigungsvergaben nicht gegeben war. Die beiden Aufträge bildeten die Basis für die Konsolidierung der unterschiedlichen Sicherheitslandschaften im Bereich der NÖ Landeskliniken.

Der Landesrechnungshof hat diese Überprüfungen mit den ergänzenden Erhebungen für die in diesem Bericht gemachten Feststellungen einbezogen.

Die NÖ Landeskliniken-Holding arbeitete in Projekten daran, die Konsolidierung der inhomogenen Informations- und Kommunikationslandschaft in den NÖ Landeskliniken herbeizuführen.

6. IT-Sicherheitspolitik

Nach ISO/IEC 27002 umfasst die IT-Sicherheitspolitik Ziele und Richtlinien der Sicherheit für die Informationstechnologie. Diese beschreiben das gewünschte Verhalten der Mitarbeiter und bilden eine Arbeitsgrundlage in allen Bereichen eines Unternehmens. Basis der IT-Sicherheitspolitik ist eine umfassende Risikoanalyse.

Die NÖ Landeskliniken-Holding erarbeitete eine Sicherheitspolitik für die Informations- und Kommunikationstechnologie, welche auch für die NÖ Landeskliniken im Jahr 2005 verbindlich erklärt wurde. Diese Sicherheitspolitik für die Informations- und Kommunikationstechnologie war jedoch nicht in eine generelle verbindliche Sicherheitspolitik des Unternehmens eingebettet, daher fehlte ihr eine wesentliche Grundlage.

Der Landesrechnungshof empfahl daher, eine generelle Sicherheitspolitik zu entwickeln und die bestehende Sicherheitspolitik Informations- und Kommunikationstechnologie darauf abzustimmen.

Ergebnis 2
Die NÖ Landeskliniken-Holding soll eine unternehmensweite Sicherheitspolitik entwickeln und für verbindlich erklären. Die Sicherheitspolitik für die Informations- und Kommunikationstechnologie ist auf die Gesamtpolitik abzustimmen.

Stellungnahme der NÖ Landesregierung:

Die Erarbeitung einer alle Bereiche umfassenden Sicherheitspolitik erfolgt auch im Zuge der Etablierung der unternehmensweiten Risikoanalyse (siehe auch Stellungnahme zu Ergebnis 1).

Äußerung des Landesrechnungshofs Niederösterreich:

Die Stellungnahme wurde zur Kenntnis genommen.

7. Verwaltung der Vermögenswerte

Für einen wirksamen Datenschutz und für eine effektive Informationssicherheit sind alle Vermögenswerte zu erfassen und auf dem aktuellen Stand zu halten. Dabei sind folgende Anforderungen zu berücksichtigen:

„Die Organisation sollte alle Vermögenswerte identifizieren und deren Wichtigkeit dokumentieren. Die Bestandsliste der Vermögenswerte sollte alle Informationen enthalten, die im Falle einer Katastrophe für die entsprechende Wiederherstellung erforderlich sind; dazu gehören: Art des Vermögenswerts, Format, Standort, Informationen zum Backup, Lizenzinformationen und Buchwert. Diese Bestandsliste sollte keine unnötigen Duplikate anderer Bestandslisten enthalten; es sollte jedoch sichergestellt werden, dass ihre Inhalte abgeglichen sind.

Darüber hinaus sollten für alle Vermögenswerte das Eigentum und die Informationsklassifizierung vereinbart und dokumentiert werden. Auf der Grundlage der Wichtigkeit des Vermögenswerts, seines Buchwerts und seiner Sicherheitsklassifizierung sollten angemessene Schutzniveaus identifiziert werden, die der Wichtigkeit der Vermögenswerte entsprechen." (siehe ÖNorm ISO/IEC 27002)

Neben der bestehenden Hardware sind auch alle eingesetzten Softwarepakete (zB Systemsoftware, Anwendungssoftware) samt den dazugehörigen Datenbanksystemen zu erfassen. Das ermöglicht eine genaue Risikoanalyse und bietet einen Überblick, um mögliche Einsparungen (zB bei Lizenzen, Softwareeinkauf) und Synergieeffekte erkennen und ausschöpfen zu können. Ein weiterer Nutzen besteht darin, dass die genaue Erfassung der Vermögenswerte einen strategischen Austausch von Hard- und Softwareprodukten ermöglicht. Auch darin liegen Einsparungspotenziale.

Die NÖ Landeskliniken-Holding verfügte über ein Asset-Management-System (Programm zum Verwalten der Vermögenswerte) mit Trouble-Ticket-Management. Das Trouble-Ticket-Management diente der Erfassung von Problemmeldungen und deren Lösungen. Diese beiden Systeme umfassten einen Teil

der in der NÖ Landeskliniken-Holding und in den NÖ Landeskliniken eingesetzten Hard- und Software. Eine vollständige Erfassung der Hard- und Softwarelandschaft fehlte.

Der Landesrechnungshof stellte fest, dass lediglich einer von fünf regionalen IT-Koordinatoren eine Softwareliste mit genauem Versionsstand führte.

Ergebnis 3
Die NÖ Landeskliniken-Holding hat so rasch als möglich die gesamte Hard- und Softwarelandschaft in ihr Programm zur Verwaltung der Vermögenswerte (Asset-Management-System) aufzunehmen.

Stellungnahme der NÖ Landesregierung:

Ein Programm zur Verwaltung der Hard- und Softwarelandschaft wurde bereits angeschafft und mit Basisdaten befüllt. Die Kommunikation an die Kliniken und der Rollout samt Benutzerschulung wird 2012 umgesetzt werden.

Äußerung des Landesrechnungshofs Niederösterreich:

Die Stellungnahme wurde zur Kenntnis genommen.

8. Personelle Sicherheit

Eine wesentliche Rolle und Verantwortung kommt bei Datenschutz und Informationssicherheit den Mitarbeitern zu.

Die Personelle Sicherheit bezweckt, *"dass Mitarbeiter, Auftragnehmer und Dritte ihre Verantwortlichkeiten verstehen und für die vorgesehenen Rollen geeignet sind und die Risiken durch Diebstahl, Betrug oder Missbrauch von Einrichtungen verringern. Sicherheitsbezogene Verantwortlichkeiten sollten vor Beginn des Beschäftigungsverhältnisses in entsprechenden Stellenbeschreibungen und in Beschäftigungsbedingungen angesprochen werden. Alle Benutzer von Einrichtungen zur Informationsverarbeitung, d. h. die eigenen Mitarbeiter, Auftragnehmer und Dritte sollten eine Vereinbarung über ihre Sicherheitsrollen und -verantwortlichkeiten unterzeichnen."* (ÖNorm ISO/IEC 27002)

Im Hinblick auf die Entwicklungen im Bereich der Informationstechnologie empfahl der Landesrechnungshof, die Aus- und Weiterbildungsmaßnahmen für die Mitarbeiter der Informations- und Kommunikationstechnologie verbindlich vorzusehen.

8.1 Stellenbeschreibungen

Bei den NÖ Landeskliniken waren an den 27 Standorten rund 100 Personen für Informations- und Kommunikationstechnologie im Einsatz. Dieser Bereich war dem Kaufmännischen Direktor unterstellt. Die personelle Ausstattung mit Mitarbeitern für Informationstechnologie (IT-Mitarbeiter) war sehr unterschiedlich und reichte von 2 bis 18,5 Vollzeitäquivalenten.

Nach ihrer Stellenbeschreibung hatten diese IT-Mitarbeiter die Sicherheit des täglichen EDV-Betriebes sicherzustellen sowie die Einführung einer einerseits möglichst konformen und andererseits möglichst an die Benutzerbedürfnisse angepassten, zeitgemäßen EDV-Struktur sowohl im Hardwarebereich (Netzwerk, Server, Arbeitsplätze) als auch im Softwarebereich (Server- und PC-Betriebssysteme, Bürokommunikation, Krankenhausinformationssystem) zu gewährleisten. Die Aufgaben und Verantwortlichkeiten waren teilweise umfassend „für alles zuständig“ und teilweise sehr detailliert festgelegt.

Außerdem bestand bei den NÖ Landeskliniken für die Berechnung des Mitarbeiterschlüssels für Personal der Informations- und Kommunikationstechnologie keine Maßzahl, wie dies beim Amt der NÖ Landesregierung mit einem IT-Koordinator für rund 50 Arbeitsplätze in der Vorschrift „IT-Betrieb“ geregelt ist. Der Personalbedarf richtete sich nach der vorhandenen Infrastruktur. Standardisierte Stellenbeschreibungen fehlten.

Der Landesrechnungshof empfahl, die Konsolidierung und Standardisierung von Hard- und Softwarelandschaft schrittweise voranzutreiben und die Stellenbeschreibungen für die Mitarbeiter der Informations- und Kommunikationstechnologie zu standardisieren. Damit kann auch der diesbezügliche Personalbedarf ermittelt und der Sach- und Personalaufwand (zB Lizenzkosten, Aus- und Weiterbildung, Betreuungsaufwand) verringert werden.

Die NÖ Landeskliniken-Holding hat auf Grundlage der IKT-Risikoanalyse und der IKT-Sicherheitspolitik unter der Berücksichtigung der Sparsamkeit, Wirtschaftlichkeit und Zweckmäßigkeit ein Gesamtkonzept zu erstellen, welches auf den Versorgungsauftrag abgestimmt ist.

Ergebnis 4
Die NÖ Landeskliniken-Holding hat ein Gesamtkonzept für die Konsolidierung der Informations- und Kommunikationstechnologie zu erstellen, welches auf den Versorgungsauftrag abgestimmt ist. In weiterer Folge sind die Stellenbeschreibungen zu standardisieren.

Stellungnahme der NÖ Landesregierung:

Vor dem Jahr 2008 war die IT-Landschaft durch die 22 unterschiedlichen Rechtsträger und vor allem durch viele unterschiedliche Programme und Anbieter sehr zersplittert.
Die NÖ Landeskliniken-Holding konnte daher erst seit 2008 an einer IKT-Strategie, die die Konsolidierung der IKT-Landschaft als zentralen Fokus hat, arbeiten.
Die angesprochene Konsolidierung schreitet kontinuierlich voran. Ein Konzept zur Konsolidierung liegt vor und sieht die Aufstockung der Ressourcen durch eine strategische Kooperation mit der Oberösterreichischen Gesundheits- und Spitals- AG (Gespag) vor. Dies soll vor allem durch Schaffung von so genannten Customer Competence Centers (CCC) für ausgewählte IKT-Services erreicht werden.

Äußerung des Landesrechnungshofs Niederösterreich:

Die Stellungnahme wurde zur Kenntnis genommen.

8.2 Zugriffsberechtigungen

Der Landesrechnungshof überprüfte die Festlegungen von Rollen und die Vergabe von Berechtigungen für die Benutzer bzw. User.

Um die Vermögenswerte, wie hier Patientendaten, vor unberechtigtem Zugriff, unberechtigter Weitergabe, Änderung und Vernichtung zu schützen, sind standardisierte Abläufe für die Festlegung von Rollen und die Vergabe von Berechtigungen verbindlich festzulegen.

Die für die Informationstechnologie Verantwortlichen in den NÖ Landeskliniken vergaben und kontrollierten monatlich die Berechtigungen im System auf Basis einer Personenstandsliste.

Dafür bestanden zwei Vorgehensweisen. Zum einen wurden neu aufgenommene Mitarbeiter als Benutzer bzw. User angelegt und mit Passwörtern ausgestattet, wenn die Personalstelle dies telefonisch meldete. Die zweite und etwas sicherere Methode war, dass der neu aufgenommene Mitarbeiter mit Hilfe eines Laufzettels auch beim IT-Mitarbeiter bzw. IT-Verantwortlichen vorstellig wurde und dort die Berechtigungen und das Passwort bzw. die Passwörter erhielt.

Die Rollen und Berechtigungen (zB medizinisches Personal) wurden auf Grund der Berufsgruppe funktionell und nicht auf Grund der individuellen Aufgabenstellungen vergeben. Da diese nicht schriftlich dokumentiert wurden, blieben einmal vergebene Rechte bei Wechsel oder Austritt eines Mitarbeiters erhalten.

Der Landesrechnungshof regte an, die Rollen und Berechtigungen anhand eines standardisierten Formulars, welches der Abteilungs- bzw. Stationsleiter ausfüllt, zu vergeben und schriftlich zu dokumentieren. Die Beurteilung welche Berechtigungen für wen erforderlich sind, sollte nicht allein den IT-Verantwortlichen überlassen bleiben. Auf diese Weise ist auch eine Kontrolle jederzeit möglich.

Ergebnis 5
Die NÖ Landeskliniken-Holding hat in den NÖ Landesklinken die Vergabe von Rollen und Berechtigungen zu standardisieren und eine nachvollziehbare Dokumentation einzuführen.

Stellungnahme der NÖ Landesregierung:

Ein entsprechendes Maßnahmenpaket für eine standardisierte Verwaltung von IKT-Zugangsrechten wurde bereits seit langem beauftragt und es wird die Fertigstellung in wenigen Wochen erfolgen.

Äußerung des Landesrechnungshofs Niederösterreich:

Die Stellungnahme wurde zur Kenntnis genommen.

Es gab persönliche Berechtigungen und Berechtigungen für Personengruppen, die so genannten Gruppenuser.

Die persönlichen Berechtigungen sind an eine Person gebunden. Diese war mit Benutzer bzw. Username und Passwort ausgestattet und konnte somit in jedem System protokolliert werden. Damit waren alle Eingaben und Änderungen, die diese Person durchführt im jeweiligen System nachvollziehbar.

Gruppenuser stellen ein Risiko dar, weil der Username im System protokolliert wird, aber nicht nachvollziehbar ist, wer Eingaben bzw. Änderungen durchgeführt hat. Gruppenuser wurden auf den so genannten Stations-PCs in den NÖ Landeskliniken eingesetzt, um den Zeitaufwand für das ständiges An- und Abmelden an den Programmen und Systemen zu ersparen.

Der Landesrechnungshof empfahl, die Verwendung von Gruppenusern auf die Anmeldung an das Betriebssystem zu beschränken. An den einzelnen Spezialsystemen (zB Krankenhausinformationssystem, Laborinformationssystem, Radiologieinformationssystem) sollten sich die Mitarbeiter jedoch mit Username und Passwort anmelden.

Weiters empfahl der Landesrechnungshof, die Softwarelandschaft auf den Stationen so zu gestalten, dass dadurch zeitsparendes Arbeiten möglich ist, ohne den Datenschutz und die Informationssicherheit zu vernachlässigen.

Ergebnis 6
Die NÖ Landeskliniken-Holding hat die Softwarelandschaft dahingehend zu analysieren, dass unter Einhaltung von Datenschutz und Informationssicherheit ein effizientes Arbeiten auf den Stationen möglich ist.

Stellungnahme der NÖ Landesregierung:
Die geforderte Analysetätigkeit ist bereits angelaufen und soll Mitte Dezember 2011 fertig gestellt werden.
Laut Dienstanweisung IT-Betrieb für Landeskliniken, 01-08/00-0161 vom 19.8.2011 obliegt es der Dienststellenleitung in ihrer alleinigen Verantwortung, den Zugang zu Internet und E-Mail für Klinikmitarbeiter festzulegen. Weiters enthält dieser Normerlass Regelungen bezüglich Nutzungsbestimmungen von Internet und E-Mail.
Es sind somit bezüglich der Verwendung von Internet und E-Mail einheitliche Regelungen vorhanden, die seitens der NÖ Landeskliniken-Holding auf ihre Einhaltung überprüft werden.

Äußerung des Landesrechnungshofs Niederösterreich:
Die Stellungnahme wurde zur Kenntnis genommen.

Einen weiteren Schwerpunkt der Überprüfung bildete die Verwendung von Internet und E-Mail bei den NÖ Landeskliniken. Auch dafür fehlten einheitliche Regelungen. Grundsätzlich wurde bei den überprüften NÖ Landeskliniken bei Vergabe von persönlichen Benutzer- bzw. Usernamen und Passwort auch eine E-Mail-Adresse mit eingerichtet. Diese konnte nur verwendet werden, wenn sich der Mitarbeiter auch persönlich am Betriebssystem anmeldete.

In manchen NÖ Landeskliniken waren auch E-Mail-Adressen bei den so genannten Gruppenusern eingerichtet. Dies bedeutete, dass nicht festgestellt werden konnte, wer eine E-Mail versendet hatte.

Der Landesrechnungshof wies darauf hin, dass damit Patientendaten nicht nachvollziehbar verschickt werden konnten, was datenschutzrechtlich bedenklich ist.

Ergebnis 7
E-Mail Zugänge sind nur im Zusammenhang mit persönlichem Benutzer- bzw. Usernamen und Passwort zu vergeben. Noch vorhandene E-Mail Zugänge bei Gruppenusern sind umgehend zu deaktivieren.

Stellungnahme der NÖ Landesregierung:

Grundsätzlich ist jeglicher Versand von patientenbezogenen Daten per E-Mail gesetzlich untersagt. Die organisatorischen Auswirkungen der vom NÖ Landesrechnungshof geforderten Deaktivierung der Versandfunktion von Funktions- und Gruppenmailboxen wird überprüft.

Äußerung des Landesrechnungshofs Niederösterreich:

Die Stellungnahme wurde zur Kenntnis genommen.

Der Landesrechnungshof überprüfte auch das Anlegen von Benutzern bzw. Usern in Betriebssystemen und in Anwendungen stichprobenartig, weil das je nach bestehendem Vertrag Kosten verursacht. Neben Unternehmenslizenzen, bei denen die Anzahl der Benutzer bzw. User keine Rolle spielte, lagen auch Lizenzsysteme vor, die jeden einzelnen User verrechneten. Manche dieser Lizenzmodelle unterschieden weiters, welche User mit welchen Berechtigungen (Lesen, Ändern, Administrator) im System angelegt werden. Dabei war darauf zu achten, dass nur die notwendigen User angelegt werden, um Lizenzgebühren zu vermeiden.

Der Landesrechnungshof stellte fest, dass das Anlegen von Benutzern bzw. Usern unterschiedlich gehandhabt wurde. Die Bandbreite bewegte sich zwischen 50 % und 100 % der jeweils Beschäftigten. Daher regte der Landesrechnungshof an, die Lizenzmodelle zu evaluieren, um bei den Lizenzen und in der Verwaltung von Benutzerberechtigungen Kosten einzusparen.

Ergebnis 8
Die Anlage von Benutzern bzw. Usern ist dahingehend zu evaluieren, ob bei den Lizenzen und bei der Verwaltung der Berechtigungen Kosten eingespart werden können. Dabei ist auch zu prüfen, welches Lizenzmodell das kostengünstigste ist.

Stellungnahme der NÖ Landesregierung:

Die Harmonisierung der Benutzeranlage ist aufgrund der unterschiedlich gelebten medizinisch-pflegerischen Prozesse noch nicht möglich. Die Harmonisierung der Lizenzmodelle hat in vielen Bereichen bereits stattgefunden und wird kontinuierlich fortgeführt.

Die genannten Maßnahmen brachten für die Betriebsführung erhebliche Einsparungen gegenüber der Situation vor 2008.

Im Jahr 2010 wurden beispielsweise Campuslizenzen für OP-Dokumentationssysteme, HL7-Schnittstellen verschiedener Systemlieferanten, etc. beschafft. Bei sämtlichen Neubeschaffungen von Software wird holdingweit das wirtschaftlichste und am besten geeignete Lizenzmodell beauftragt werden.

Äußerung des Landesrechnungshofs Niederösterreich:

Die Stellungnahme wurde zur Kenntnis genommen.

8.3 Passworteinstellungen

Das Wirtschaftsprüfungsunternehmen hielt in seinem Bericht fest, dass sehr viele Benutzer in einem System oder in Anwendungen weit reichende Berechtigungen hatten und die Passwörter nicht regelmäßig geändert werden mussten. Dies galt auch für die Gruppenuser und persönliche Zugänge.

Die IT-Mitarbeiter und die regionalen IT-Koordinatoren begründeten dies damit, dass bei einem Passwortwechsel die Weitergabe des neuen Passworts im Zuge des Dienstwechsels bei Gruppenusern nicht lückenlos erfolgen wird. Damit entsteht für die IT-Mitarbeiter ein zusätzlicher Aufwand, um die dazugehörigen Zugänge frei zu schalten bzw. die Passwörter zurück zu setzen.

Ein weiterer Grund lag darin, dass für jede einzelne Anwendung Passwörter eingerichtet waren, deren Änderung sich nicht synchron schalten ließ. Da die Stations-PCs nicht jeden Tag herunterzufahren sind und dadurch die Computer oft mehrere Wochen durchlaufen, greift ein erzwungener Passwortwechsel kaum.

Im Hinblick auf den gebotenen Datenschutz sind in den NÖ Landeskliniken die Passwörter in regelmäßigen Abständen zu ändern. Da eine Vielfalt an klinischen Anwendungen besteht, wäre es wirtschaftlich und zweckmäßig, die Anmeldung an die Kliniksysteme schrittweise über Single-Sign-On (Einmal Authentifizierung) zu realisieren. Single-Sign-On bietet den Vorteil, dass sich jeder Mitarbeiter nur einmal mit einem Usernamen und einem Passwort anmelden muss und dadurch in die verschiedenen Anwendungen ohne neuerliche Anmeldung einsteigen kann. Bei der Beschaffung von Software sollte diese Anforderung als Muss-Kriterium in die Ausschreibungen aufgenommen werden.

Ergebnis 9
Passwörter sind in regelmäßigen Abständen zu ändern. Im Sinne von Datenschutz und Informationssicherheit ist die Authentifizierung der Benutzer bzw. User bei der Anmeldung an Systeme und Anwendungen auf Single-Sign-On (Einmal Authentifizierung) schrittweise umzustellen. Diese Anforderung sollte bei der Beschaffung von Software berücksichtigt werden.

Stellungnahme der NÖ Landesregierung:

Ein entsprechendes Maßnahmenpaket im Sinne der Empfehlung wurde bereits beauftragt. Eine verbindliche Passwortrichtlinie wurde an die Kliniken zur Umsetzung übermittelt. Angemerkt sei, dass aufgrund der derzeit noch vorhandenen Gruppenuser die Richtlinie noch keinen verpflichtenden Passwortwechsel regeln kann. Die organisatorischen Auswirkungen hierzu werden zurzeit analysiert. Nach der Einführung der notwendigen Prozess- bzw. Organisationsänderungen ist ein verpflichtender Passwortwechsel vorgesehen.

Bei der Neubeschaffung von Software wird bereits die angesprochene Single-Sign-On Funktionalität berücksichtigt.

Äußerung des Landesrechnungshofs Niederösterreich:

Die Stellungnahme wurde zur Kenntnis genommen.

9. Betriebliche Sicherheit

Für den laufenden Betrieb und den Betrieb nach einem Ereignis sind jene Maßnahmen zu ergreifen, welche im Katastrophenfall einen definierten „geordneten Mindestbetrieb" gewährleisten.

9.1 Katastrophen- und Notfallmanagement

Im Jahr 2009 wurde festgestellt, dass ein umfassender Notfallplan für alle Landeskliniken fehlte. Bei den einzelnen Landeskliniken waren zur Überbrückung von Ausfällen einzelner Rechenzentren teilweise interne, aber nicht vollständige Notfallpläne vorhanden. Damit kann in einem Notfall die Wiederherstellung innerhalb der geschäftskritischen Zeit jedoch nicht gewährleistet werden. Die jeweilige geschäftskritische Zeit ist in der Risikoanalyse zu definieren.

Der Landesrechnungshof stellte beispielsweise bei den NÖ Landeskliniken fest, dass Notstromvorkehrungen zur Überbrückung von Stromausfällen im Bereich der Serverräume nur teilweise vorhanden waren.

Der vom Wirtschaftsprüfer empfohlene umfassende Notfallplan lag noch nicht vor. Daher fehlte weiterhin die Grundlage für die Bewältigung von Notfällen im IT-Bereich.

Für die Umsetzung der im Notfallplan zu dokumentierenden Szenarien sind Verantwortliche festzulegen. Außerdem sind die Wirkungsweisen der Szenarien durch regelmäßige Tests zu überprüfen. Aus den Tests gewonnene Erkenntnisse sind im Anschluss in die Dokumentation einzuarbeiten. Dadurch entsteht ein kontinuierlicher Verbesserungsprozess.

Ergebnis 10
Die NÖ Landesklinken-Holding hat für den Bereich der NÖ Landeskliniken einen umfassenden Notfallplan zu entwickeln, um im Fall eines Ereignisses die Wiederherstellung von kritischen Geschäftsprozessen innerhalb der definierten Zeiträume gewährleisten zu können.

Stellungnahme der NÖ Landesregierung:

Mit der Umsetzung eines entsprechenden Maßnahmenpaketes wurde begonnen.

Äußerung des Landesrechnungshofs Niederösterreich:

Die Stellungnahme wurde zur Kenntnis genommen.

9.2 Serverräume

Der Landesrechnungshof überprüfte auch Serverräume. Dabei fiel ihm auf, dass nur bei einer Klinik ein Besucherbuch vorhanden war, obwohl dies die Dienstanweisung „IT-Betrieb“ für die NÖ Landesklinken unter Punkt 6.3 „Zutritt zu Räumen mit Netzwerkrechnern“ vorschreibt.

Ergebnis 11
Die NÖ Landeskliniken haben gemäß Dienstanweisung ein Besucherbuch in Serverräumen aufzulegen und damit das Betreten und Verlassen dieser Räume von Personen ohne Zutrittsberechtigung lückenlos zu dokumentieren.

Stellungnahme der NÖ Landesregierung:

Die empfohlenen Richtlinien wurden erarbeitet und werden diese von den Kliniken bereits umgesetzt. Die verpflichtende Führung von Besucherlogbüchern wurde dabei aufgenommen.

Äußerung des Landesrechnungshofs Niederösterreich:

Die Stellungnahme wurde zur Kenntnis genommen.

Weiters stellte der Landesrechnungshof fest, dass die Serverräume auch zusätzlich als Lagerräume verwendet wurden. Besonders kritisch war, dass in einigen Serverräumen auch leicht brennbare Materialien, wie zB Papier und Verpackungskartons, gelagert wurden.

Ergebnis 12
Serverräume sind nicht als Lagerräume zu verwenden.

Stellungnahme der NÖ Landesregierung:

Die Anforderungen an Serverräume, welche z.B. Themen wie "Führen eines Besucherlogbuches", "Verwendungsverbot als Lagerraum", "Terminierung von Flüssigkeitsführenden Leitungen" etc. entsprechend regeln, wurden in die zu Ergebnis 11 angeführten Richtlinien eingearbeitet.

Äußerung des Landesrechnungshofs Niederösterreich:

Die Stellungnahme wurde zur Kenntnis genommen.

Ein weiteres hohes Risiko stellten Wasser- bzw. Abwasserleitungen dar, welche teilweise gebündelt durch den Serverraum führten. Die Servereinheiten wurden in solchen Fällen mit so genannten Tropftassen geschützt. Diese schützen jedoch bei einem Rohrbruch nur sehr begrenzt. Diese Situation war nicht nur in älteren Serverräumen, sondern auch in einem neueren Serverraum vorzufinden, obwohl dies gemäß „Weissbuch-IKT“ Punkt 2.1.2-02 untersagt und für Ausschreibungen als „MUSS“ Kriterium gekennzeichnet war.

Der Landesrechnungshof wies darauf hin, dass die Sicherheitsmängel bei zukünftigen Umbauarbeiten zu beheben sind. Bei Neubauten ist von vornherein darauf zu achten.

Ergebnis 13
Flüssigkeitsführende Leitungen sind nicht durch Serverräume zu führen oder dort zu terminieren. Dies ist bei Um- und Neubauten zu berücksichtigen.

Stellungnahme der NÖ Landesregierung:

Die Anforderungen an Serverräume, welche z.B. Themen wie "Führen eines Besucherlogbuches", "Verwendungsverbot als Lagerraum", "Terminierung von Flüssigkeitsführenden Leitungen" etc. entsprechend regeln, wurden in die zu Ergebnis 11 angeführten Richtlinien eingearbeitet.

Äußerung des Landesrechnungshofs Niederösterreich:

Die Stellungnahme wurde zur Kenntnis genommen.

Alle NÖ Landesklinken sind mit Datenleitungen, von zwei physisch getrennten Anschlusspunkten aus, an das landesweite Netzwerk der NÖ Landeskliniken-Holding (NÖMED-WAN) angeschlossen. Die Anbindung der NÖ Landeskliniken erfolgte über eigene zentrale Verteiler, die so genannten CORE-Switches. Die hausinterne Verkabelung führte von hier aus zu den jeweiligen Endpunkten. Die NÖ Landeskliniken-Holding betrieb über diese Leitungen zentrale Dienste, wie zB E-Mail. Einige NÖ Landeskliniken waren über diese Leitungen mit einem externen Rechenzentrum verbunden, bei dem unter anderem ein Krankenhaus-Informationssystem betrieben wurde.

Der Landesrechnungshof bemerkte in einer Landesklinik kritisch, dass beide zentralen Verteiler bzw. CORE-Switches in einem Serverraum standen. Dies stellte ein hohes Risiko dar, weil im Schadensfall (zB Wassereinbruch oder Brand) beide ausfallen und die Verbindung zu den zentral geführten Diensten und Komponenten nicht mehr gegeben ist. Auch dieser Fall zeigte wie wichtig eine unternehmensweite Risikoanalyse und ein entsprechender Notfallplan sind.

Ergebnis 14
Zentrale Verteiler bzw. CORE-Switches sind jeweils in eignen Serverräumen zu betreiben. Aus sicherheitstechnischen Überlegungen ist eine getrennte Aufstellung in verschiedenen Brandabschnitten vorzunehmen.

Stellungnahme der NÖ Landesregierung:

Lediglich in einem Klinikum befinden sich die beiden Core-Switches in ein und demselben Raum. Aufgrund des geplanten Bauprojektes und aus Kostengründen wurde bisher von einer Verlegung Abstand genommen. Nach Abschluss der Bauarbeiten wird die geforderte getrennte Aufstellung auch in diesem Klinikum erfolgen.

Äußerung des Landesrechnungshofs Niederösterreich:

Die Stellungnahme wurde zur Kenntnis genommen.

9.3 Datensicherung

Die Datensicherung bei den NÖ Landeskliniken erfolgte zum Großteil vor Ort. Dabei konnte positiv festgestellt werden, dass die Umrüstung auf ein einheitliches Sicherungskonzept zum überwiegenden Teil bereits abgeschlossen war.

In einer der überprüften NÖ Landeskliniken wurden die Sicherungskopien in einem Safe im gleichen Brandabschnitt aufbewahrt, wo auch der Bandroboter stand.

Eine Datenrücksicherung von den Sicherungsbändern wurde nur teilweise durchgeführt. Daher empfahl der Landesrechnungshof auch hier eine zentrale Vorgabe für alle NÖ Landskliniken, dass in regelmäßigen Abständen eine Rücksicherung von einzelnen Dateien dokumentiert erfolgt. Damit kann das Risiko eines Datenverlustes gesenkt werden.

Ergebnis 15
Um das Risiko des Datenverlustes zu senken, ist eine Rücksicherung einzelner Dateien von verschiedenen Sicherungsbändern in regelmäßigen Abständen durchzuführen. Diese Maßnahme ist nachvollziehbar zu dokumentieren.

Stellungnahme der NÖ Landesregierung:

An einer Vereinheitlichung der regelmäßigen testweisen Rücksicherung wird gearbeitet.

Äußerung des Landesrechnungshofs Niederösterreich:

Die Stellungnahme wurde zur Kenntnis genommen.

10. Dokumentation

Der Wirtschaftprüfer bemängelte die Dokumentation der NÖ Landeskliniken in den Jahren 2008 und 2009, weil diese unterschiedlich oder nicht vorhanden war.

Wie der Landesrechnungshof bereits in einigen anderen Punkten festhielt, fehlten mangels Risikobewertung, unternehmensweiter Sicherheitspolitik und vollständiger Verwaltung der Vermögenswerte, auch zentrale Vorgaben für alle NÖ Landeskliniken. Diese sind so zu gestalten, dass sämtliche Rechenzentren unabhängig von ihren Hard- und Softwarekomponenten einheitlich dokumentiert werden können. In diesem Zusammenhang wäre auch zu überlegen, welche Hard- oder Softwarekomponenten zentral wirtschaftlicher zu betreiben sind. Der Landesrechnungshof wies darauf hin, dass dadurch auch Aufgaben von der NÖ Landeskliniken-Holding übernommen und damit die IT-Mitarbeiter in den NÖ Landeskliniken entlastet werden.

Ergebnis 16
Eine ordnungsmäßige Dokumentation ist durch zentrale Vorgaben sicherzustellen.

Stellungnahme der NÖ Landesregierung:

In dem zu Ergebnis 3 bereits beschriebenen Managementsystem werden auch die zentralen Vorgaben einer ordnungsgemäßen Dokumentation Eingang finden.

Äußerung des Landesrechnungshofs Niederösterreich:

Die Stellungnahme wurde zur Kenntnis genommen.

St. Pölten, im Jänner 2012

Die Landesrechnungshofdirektorin

Dr. Edith Goldeband