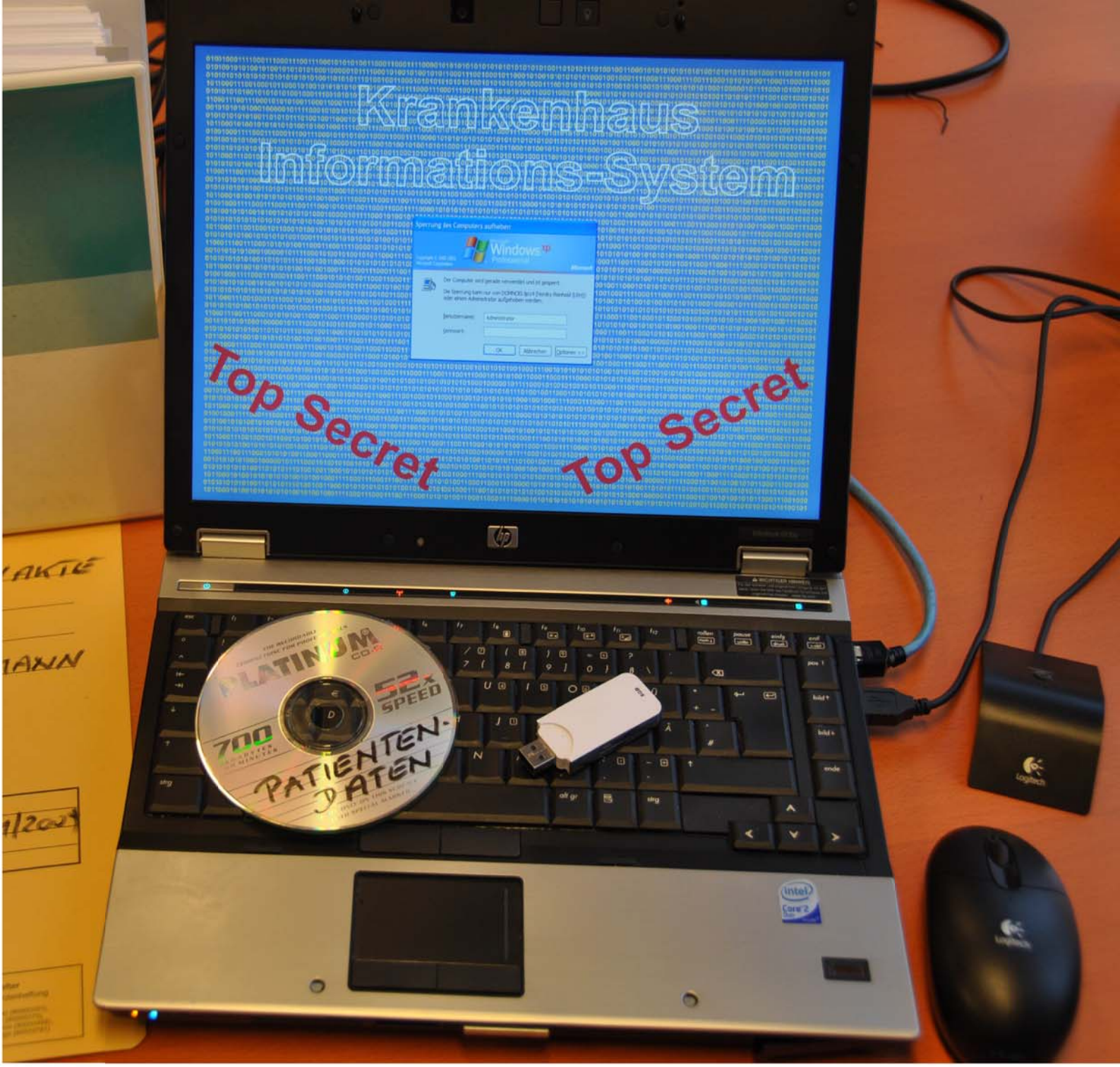

Landesrechnungshof
Niederösterreich

Datenschutz und Informationssicherheit in den NÖ Landeskliniken, Nachkontrolle

Bericht 1 | 2015

Impressum:
Medieninhaber, Hersteller und Herausgeber:
Landesrechnungshof Niederösterreich
A-3100 St. Pölten, Wienerstraße 54

Redaktion:
Landesrechnungshof Niederösterreich

Bildnachweis:
Landesrechnungshof Niederösterreich

Druck:
Amt der NÖ Landesregierung, Abteilung LAD3, Amtsdruckerei

Herausgegeben:
St. Pölten, im Jänner 2015

Im nebenstehenden QR-Code ist der Link zur Website des Landesrechnungshofs Niederösterreich eingebettet. Um die Adresse auszulesen, benötigen Sie ein Programm (App) für Ihr Mobiltelefon. Nachdem Sie es installiert haben, fotografieren Sie den Code. Das Programm übersetzt die URL und führt Sie auf unsere Website.

Landesrechnungshof
Niederösterreich

Datenschutz und Informationssicherheit in den NÖ Landeskliniken Nachkontrolle

Bericht 1/ 2015

Datenschutz und Informationssicherheit in den NÖ Landeskliniken, Nachkontrolle
Inhaltsverzeichnis

Datenschutz und Informationssicherheit in den NÖ Landeskliniken, Nachkontrolle Zusammenfassung

Die Nachkontrolle zum Bericht 3/2012 „Datenschutz und Informationssicherheit in den NÖ Landeskliniken“ ergab, dass von den 16 Empfehlungen aus diesem Bericht sechs ganz, sechs teilweise und vier nicht umgesetzt wurden. Die NÖ Landeskliniken-Holding und die NÖ Landeskliniken haben den Empfehlungen damit zu 56 Prozent entsprochen.

Die NÖ Landeskliniken-Holding konnte damit Einsparungen von 1,20 Millionen Euro pro Jahr bei den Softwarelizenz- und Wartungskosten sowie bei der Hardwarebeschaffung erreichen und die personelle und betriebliche Sicherheit verbessern. Außerdem wurden Gruppenuser auf Applikationsebene abgeschafft und Zugriffe mit Hilfe einer Berechtigungsmatrix für einzelne Benutzer festgelegt.

Durch die Abteilung Informations- und Kommunikationstechnologie wurden Einzelmaßnahmen auf Basis der durchgeführten Risikoanalyse verabschiedet. Die zugesagte unternehmensweite Risikoanalyse und Sicherheitspolitik sowie die Gefahren- und Notfallhandbücher konnten jedoch nicht abgeschlossen werden.

Statt das Programm zur Verwaltung der Hard- und Softwareausstattung wie zugesagt fortzuführen, wurde ein neues Projekt zur Verwaltung der Vermögenswerte gestartet. Die NÖ Landeskliniken übermittelten daher weiterhin quartalsweise die Daten der Vermögenswerte mittels Excel-Tabellen an die NÖ Landeskliniken-Holding.

Die NÖ Landesregierung sagte in ihrer Stellungnahme vom 30. September 2014 die Umsetzung der Empfehlungen zu.

1. Prüfungsgegenstand

Der Landesrechnungshof überprüfte die Umsetzung seiner 16 Empfehlungen aus dem Bericht 3/2012 „Datenschutz und Informationssicherheit in den NÖ Landeskliniken“ bei der NÖ Landeskliniken-Holding und fünf NÖ Landeskliniken, die nach den Kriterien neue Projekte, Neubau sowie nach den Stellungnahmen zu den Empfehlungen aus dem Vorbericht ausgewählt wurden.

Der NÖ Landtag hatte diesen Bericht am 10. Mai 2012 mit der Aufforderung zur Kenntnis genommen, dass den im Bericht dargelegten Auffassungen des Rechnungshofausschusses entsprochen wird.

Ziel der Nachkontrolle war es, den NÖ Landtag über den Stand der Umsetzung der sowohl organisatorischen als auch technischen Empfehlungen zu informieren.

Der Landesrechnungshof stellte daher die Ergebnisse aus dem Bericht „Datenschutz und Informationssicherheit in den NÖ Landeskliniken“ mit dem jeweiligen Umsetzungsstand zum 31. Mai 2014 dar.

Zum Zeitpunkt der Nachkontrolle waren von 16 Empfehlungen aus diesem Bericht sechs ganz, sechs teilweise und vier nicht umgesetzt. Die NÖ Landeskliniken-Holding und die NÖ Landeskliniken entsprachen den Empfehlungen somit zu rund 56 Prozent.

Um die Übersichtlichkeit zu erhöhen und die Lesbarkeit zu vereinfachen, wurden personenbezogene Bezeichnungen im Bericht grundsätzlich nur in einer Geschlechtsform verwendet und umfassten Männer und Frauen.

2. Risikobewertung

In Ergebnis 1 wurde folgende Empfehlung festgehalten:

„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.“

Die Empfehlung des Landesrechnungshofs wurde teilweise umgesetzt.

Die NÖ Landesregierung hielt in ihrer Stellungnahme vom 22. November 2011 fest, dass die Etablierung einer unternehmensweiten Risikoanalyse noch im Laufe des kommenden Jahres auch nach Maßgabe der organisatorischen und budgetären Rahmenbedingungen fertiggestellt werde.

Der Landesrechnungshof stellte nunmehr fest, dass die NÖ Landeskliniken-Holding im Jahr 2013 die Stabsstelle „Ressourcen- und Risikomanagement“ eingerichtet hatte. Gleichzeitig wechselte die Leitung der Abteilung „Informations- und Kommunikationstechnologie“.

Die Abteilung Informations- und Kommunikationstechnologie verabschiedete Einzelmaßnahmen auf Basis der durchgeführten Risikoanalyse, die für das Jahr 2012 zugesagte Fertigstellung der unternehmensweiten Risikoanalyse erfolgte jedoch nicht.

Der Landesrechnungshof bekräftigte, dass die Risiken der Informationstechnologie nur einen Bereich des Gesamtrisikos darstellen und die unternehmensweite Risikoanalyse daher ehestmöglich abzuschließen ist.

Stellungnahme der NÖ Landesregierung:

Nach Freigabe der personellen Ressourcen wird 2015 der Aufbau eines holdingweiten Risikomanagements fortgeführt werden. Dabei sollen die bereits bestehenden Teile eines Risikomanagementsystems (z.B. Gefahrenabwehrhandbuch, CIRS, etc.) in einem Gesamtsystem integriert und organisatorisch in der Holding-Organisation verankert werden.

Äußerung des Landesrechnungshofs Niederösterreich:

Die Stellungnahme wurde zur Kenntnis genommen.

3. IT-Sicherheitspolitik

In Ergebnis 2 wurde folgende Empfehlung festgehalten:

„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.“

Die Empfehlung des Landesrechnungshofs wurde nicht umgesetzt.

Die NÖ Landesregierung hatte in ihrer Stellungnahme mitgeteilt, dass im Zuge der Etablierung der unternehmensweiten Risikoanalyse auch eine unternehmensweite Sicherheitspolitik erarbeitet wird.

Der Landesrechnungshof stellte nunmehr fest, dass die zuletzt im Jahr 2007 aktualisierte „IKT-Sicherheitspolitik“ der NÖ Landeskliniken-Holding nach

wie vor nicht in eine generelle verbindliche Sicherheitspolitik des Unternehmens eingebettet war, weil die unternehmensweite Risikoanalyse nicht fertiggestellt wurde.

Der Landesrechnungshof bekräftigte seine Empfehlung.

Stellungnahme der NÖ Landesregierung:

Eine Einbindung der bestehenden IKT-Sicherheitspolitik wird im Zuge der Entwicklung einer Gesamt-Unternehmensrisikopolitik erfolgen.

Äußerung des Landesrechnungshofs Niederösterreich:

Die Stellungnahme wurde zur Kenntnis genommen.

4. Verwaltung der Vermögenswerte

In Ergebnis 3 wurde folgende Empfehlung festgehalten:

„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."

Die Empfehlung des Landesrechnungshofs wurde nicht umgesetzt.

Die NÖ Landesregierung hatte in ihrer Stellungnahme mitgeteilt, dass bereits ein Programm zur Verwaltung der Hard- und Softwarelandschaft angeschafft und mit Basisdaten befüllt wurde. Die Kommunikation an die NÖ Landeskliniken und der Rollout sollte samt Benutzerschulung 2012 umgesetzt werden.

Der Landesrechnungshof stellte dazu fest, dass Basisdaten der Hard- und Softwarelandschaft der NÖ Landeskliniken-Holding in das Programm zur Verwaltung der Vermögenswerte (Asset-Management-System) aufgenommen wurde.

Die Abteilung Informations- und Kommunikationstechnologie der NÖ Landeskliniken-Holding attestierte diesem Programm im laufenden Betrieb jedoch mangelnde Flexibilität bzw. Funktionalität im Bereich des Lizenzmanagements und verlängerte die Softwarelizenz im Jahr 2014 nicht mehr.

Für den fünfjährigen Einsatz des Programms fielen Lizenz- und Wartungskosten von 33.852,00 Euro an. Parallel dazu führten die IKT-Koordinatoren der einzelnen NÖ Landeskliniken weiterhin Excel-Tabellen mit Hard- und Soft-

wareausstattung, die einen aktuellen Versionsstand der Software auswiesen, welche sie quartalsweise an die NÖ Landeskliniken-Holding übermittelten.

In diesen Excel-Tabellen fehlten jedoch wesentliche kaufmännische und vertragliche Informationen, ob zum Beispiel für ein Gerät zu einem bestimmten Zeitpunkt noch Garantieansprüche geltend gemacht werden konnten.

Die Abteilung Informations- und Kommunikationstechnologie legte am 21. April 2014 einen Antrag zu einem Projekt vor, mit dem die Hard- und Softwareausstattung mit einem neu anzuschaffenden Programm datenbankbasiert erfasst werden sollte, um die Ausstattung aktuell abzubilden und daraus Kennzahlen zum Beispiel zu Anzahl, Produkttypen und Versionsständen zu ermitteln.

Dazu sollte eine Marktanalyse bis Ende 2014 klären, welche verfügbaren Softwarelösungen für den Einsatz geeignet wären. Dafür waren vorläufige Beratungskosten von 37.800,00 Euro budgetiert.

Der Landesrechnungshof bekräftigte seine Empfehlung und regte an, die Stabstelle Landesamtsdirektion Informationstechnologie anzusprechen, um von deren Know-How im Bereich der Hard- und Softwareverwaltung profitieren zu können.

Stellungnahme der NÖ Landesregierung:

Die NÖ Landeskliniken-Holding wird versuchen, bestehende Erfahrungswerte hinsichtlich der Hard- und Softwareverwaltung aus anderen Landesbereichen bei der Umsetzung zu berücksichtigen.

Äußerung des Landesrechnungshofs Niederösterreich:

Die Stellungnahme wurde zur Kenntnis genommen.

5. Personelle Sicherheit

5.1 Stellenbeschreibungen

In Ergebnis 4 wurde folgende Empfehlung festgehalten:

„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.“

Die Empfehlung des Landesrechnungshofs wurde teilweise umgesetzt.

Die NÖ Landesregierung hatte in ihrer Stellungnahme ausgeführt, dass die NÖ Landeskliniken-Holding erst seit 2008 an einer IKT-Strategie zur Konsolidierung der sehr zersplitterten IKT-Landschaft arbeiten konnte. Sie hatte weiters mitgeteilt, dass diese Konsolidierung kontinuierlich voran schreitet, ein Konzept zur Konsolidierung vorliegt, das die Aufstockung der Ressourcen durch eine strategische Kooperation vorsieht, was vor allem durch so genannte Customer Competence Centers (CCC) für ausgewählte IKT-Services erreicht werden sollte.

Der Landesrechnungshof stellte nunmehr fest, dass die NÖ Landeskliniken-Holding im Bereich der Hardware PCs, Laptops und Drucker zentral einkaufte und den NÖ Landeskliniken dafür ein Bestellportal zur Verfügung stellte, das ab 2012 im Vollbetrieb war.

Im Bereich Software hatte die NÖ Landeskliniken-Holding im Jahr 2013 mit der Anbindung der ersten NÖ Landeskliniken an ein zentrales Laborinformationssystem (LIS) begonnen. Die NÖ Landeskliniken-Holding gab an, dass bis Ende 2017 alle NÖ Landeskliniken mit dem neuen System ausgestattet sein sollten.

Die in der Stellungnahme der NÖ Landesregierung angeführte strategische Kooperation umfasste zwölf Projekte, wovon acht bereits abgewickelt wurden. Vier Projekte liefen noch, wobei eines Ende 2014 beendet werden sollte.

Außerdem erstellte die NÖ Landeskliniken-Holding standardisierte Stellenbeschreibungen für die Leiter der Bereiche IKT in den NÖ Landeskliniken. Die Erstellung von Stellenbeschreibungen für die IKT-Mitarbeiter blieb den einzelnen NÖ Landeskliniken überlassen. Ein verbindliches Aus- und Weiterbildungskonzept fehlte nach wie vor.

Der Landesrechnungshof anerkannte die Bemühungen zur Konsolidierung der zersplitterten Hard- und Softwarelandschaft und bekräftigte seine Empfehlung, diese Konsolidierung konsequent voran zu treiben.

Stellungnahme der NÖ Landesregierung:

Der Empfehlung des Landesrechnungshofes wird nachgekommen werden. Die Bemühungen zur Konsolidierung der unterschiedlichen Hard- und Softwaresysteme werden weiter vorangetrieben. Darauf aufbauend, können in weiterer Folge sukzessive die Stellenanforderungen und damit auch die Stellenbeschreibungen standardisiert werden.

Äußerung des Landesrechnungshofs Niederösterreich:

Die Stellungnahme wurde zur Kenntnis genommen.

5.2 Zugriffsberechtigungen

In Ergebnis 5 wurde folgende Empfehlung festgehalten:

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

Die Empfehlung des Landesrechnungshofs wurde umgesetzt.

Die NÖ Landesregierung hatte in ihrer Stellungnahme mitgeteilt, dass ein entsprechendes Maßnahmenpaket für eine standardisierte Verwaltung von IKT-Zugangsrechten bereits in wenigen Wochen fertiggestellt wird.

Der Landesrechnungshof stellte bei den fünf überprüften Standorten fest, dass die Gruppenuser auf Applikationsebene abgeschafft wurden. Mit einer Berechtigungsmatrix wurden in den NÖ Landeskliniken die Zugriffe auf die einzelnen Anwendungen (Applikationen) auf Mitarbeitergruppenebene festgelegt.

In Ergebnis 6 wurde folgende Empfehlung festgehalten:

„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."

Die Empfehlung des Landesrechnungshofs wurde umgesetzt.

Wie die NÖ Landesregierung in ihrer Stellungnahme ausgeführt hatte, sollte die empfohlene Analyse der Softwarelandschaft Mitte Dezember 2011 fertig gestellt werden. Außerdem bestanden mit der Dienstanweisung IT-Betrieb für Landeskliniken, 01-08/00-0161, vom 19. August 2011 bezüglich der Verwendung von Internet und E-Mail einheitliche Regelungen, deren Einhaltung von der NÖ Landeskliniken-Holding überprüft wird.

Der Landesrechnungshof stellte dazu fest, dass die Analyse in der Berechtigungsmatrix mündete, die in den NÖ Landeskliniken die Verwendung von Internet und E-Mail sowie Zugriffe auf die einzelnen Anwendungen auf Mitarbeitergruppenebene festlegte.

In Ergebnis 7 wurde folgende Empfehlung festgehalten:

„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."

Die Empfehlung des Landesrechnungshofs wurde teilweise umgesetzt.

Die NÖ Landesregierung hatte in ihrer Stellungnahme betont, dass grundsätzlich jeglicher Versand von patientenbezogenen Daten per E-Mail gesetzlich untersagt war. Weiters hatte sie zugesagt, die organisatorischen Auswirkungen einer Deaktivierung der Versandfunktion von Funktions- und Gruppenmailboxen zu überprüfen.

Der Landesrechnungshof stellt dazu fest, dass die NÖ Landeskliniken-Holding keine Änderungen vorgenommen hatte, weil Mitteilungen über die jeweilige Gruppenmailbox auch jene Mitarbeiter erreichten, die über kein eigenes Postfach verfügten. Andererseits diente die Gruppenmailbox dazu, Antworten auf externe Anfragen im Namen der Abteilung zu versenden, was hauptsächlich über das jeweilige Sekretariat des Primariats erfolgte.

Der Landesrechnungshof anerkannte, dass ein Landesklinikum die E-Mail Gruppenpostfächer abschaffte und allgemeine Informationen, die auch für Mitarbeiter ohne eigenen Computerzugang bestimmt waren, auf anderen Kommunikationswegen verbreitete.

Der Landesrechnungshof bekräftigte seine Empfehlung, dass E-Mail-Ausgänge nur mittels Identifikation (Username) und Authentifizierung (Passwort) möglich sind, sodass aus Gruppenmailboxen keine E-Mails unautorisiert verschickt werden können.

Stellungnahme der NÖ Landesregierung:

Der Empfehlung des Landesrechnungshofes wird gefolgt werden. Die Anzahl der vorhandenen E-Mail Sammelbenutzer wurde bereits drastisch reduziert. In jenen Fällen, bei denen E-Mail-Sammelbenutzer erforderlich sein sollten, wird die NÖ Landeskliniken-Holding sicherstellen, dass diese nur für eingehende E-Mails verwendet werden können. Die Versandfunktion von diesen Sammelbenutzern wird deaktiviert werden.

Äußerung des Landesrechnungshofs Niederösterreich:

Die Stellungnahme wurde zur Kenntnis genommen.

In Ergebnis 8 wurde folgende Empfehlung festgehalten:

„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."

Die Empfehlung des Landesrechnungshofs wurde umgesetzt.

Die NÖ Landesregierung hatte in ihrer Stellungnahme mitgeteilt, dass die Harmonisierung der Benutzeranlage aufgrund der unterschiedlichen medizinisch-pflegerischen Prozesse noch nicht möglich war und die Harmonisierung der Lizenzmodelle kontinuierlich fortgeführt wird, was erhebliche Einsparungen gegenüber der Situation vor 2008 brachte. Im Jahr 2010 wurden beispielsweise Campuslizenzen für OP-Dokumentationssysteme, HL7-Schnittstellen verschiedener Systemlieferanten, etc. beschafft.

Der Landesrechnungshof stellte anhand der im Jahr 2013 eingeführten Berechtigungsmatrix für alle Mitarbeiter der NÖ Landeskliniken fest, dass die Berechtigungen sowie die daraus abgeleiteten Lizenzen effizient verwaltet wurden. Die Berechtigungsmatrix bildete auch die Grundlage für Software-Audits der Hersteller, also Soll-Ist-Vergleiche der vertraglich vereinbarten Softwarelizenzen mit den tatsächlich genutzten durch die Hersteller.

Die NÖ Landeskliniken-Holding gab an, dass durch diese Effizienzmaßnahmen jährliche Einsparungen bei Softwarelizenzkosten, Softwarewartungskosten und Hardwarebeschaffung von rund 1,20 Millionen Euro erzielt werden konnten.

Einsparungen pro Jahr in Euro	
Softwarelizenzen und Wartung	520.000,00
Hardware (PC, Monitore, Notebooks)	300.000,00
Drucker	400.000,00

5.3 Passworteinstellungen

In Ergebnis 9 wurde folgende Empfehlung festgehalten:

„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."

Die Empfehlung des Landesrechnungshofs wurde teilweise umgesetzt.

Die NÖ Landesregierung hatte in ihrer Stellungnahme mitgeteilt, dass ein Maßnahmenpaket im Sinne der Empfehlung beauftragt und eine Passwortrichtlinie an die NÖ Landeskliniken zur Umsetzung übermittelt wurden. Dazu hatte sie angemerkt, dass ein verpflichtender Passwortwechsel erst nach den notwendigen Prozess- bzw. Organisationsänderungen vorgesehen und bei Neubeschaffung von Software die Single-Sign-On Funktionalität berücksichtigt werden.

Der Landesrechnungshof stellte nunmehr fest, dass die Gruppenuser der vier Krankenhausinformationssysteme (KIS) abgeschafft wurden. Die Passwortrichtlinie konnte jedoch wegen der vier unterschiedlichen Softwarelösungen nicht umgesetzt werden.

Der Landesrechnungshof anerkannte die getroffenen Maßnahmen und empfahl, die Authentifizierung in der Zielelandkarte und im Maßnahmenplan der Abteilung Informations- und Kommunikationstechnologie vorrangig zu berücksichtigen.

Stellungnahme der NÖ Landesregierung:

Der Empfehlung des Landesrechnungshofes wird nachgekommen werden. Aktuell wird in drei Pilotkliniken das Fingerprint-Authentifizierungssystem getestet. Ein holdingweites Konzept zur Umsetzung an allen NÖ Landeskliniken ist in Ausarbeitung.

Äußerung des Landesrechnungshofs Niederösterreich:

Die Stellungnahme wurde zur Kenntnis genommen.

6. 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.

6.1 Katastrophen- und Notfallmanagement

In Ergebnis 10 wurde folgende Empfehlung festgehalten:

„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."

Die Empfehlung des Landesrechnungshofs wurde nicht umgesetzt.

Wie in der Stellungnahme der NÖ Landesregierung zugesagt, wurde mit der Umsetzung eines entsprechenden Maßnahmenpakets begonnen.

Die dem Landesrechnungshof vorgelegten Gefahren- und Notfallhandbücher von fünf Klinikstandorten enthielten Maßnahmen für das Verhalten im Krisenfall für bestimmte Bereiche (zum Beispiel Brandschutz, Pandemie, Sprechfunk), beinhalteten jedoch keine spezifischen Maßnahmen für die Informations- und Kommunikationstechnologie.

Die NÖ Landeskliniken-Holding gab dazu an, dass das übergreifende Risikomanagement von der Abteilung Informations- und Kommunikationstechnologie im dritten Quartal 2014 mit der Stabsstelle Ressourcen- und Risikomanagement und der Abteilung Bau und Facility Management in Angriff genommen wird.

Der Landesrechnungshof wies darauf hin, dass sich die – in den Gefahren- und Notfallhandbüchern angeführten – technischen Störungen wie zum Beispiel ein Stromausfall auf die Informations- und Kommunikationstechnologie auswirken. Wegen der Wechselwirkungen muss eine Koordination vorgesehen werden, welches ein bereichsübergreifendes Konzept erstellt und im Anlassfall umsetzt.

Der Landesrechnungshof bekräftigte dazu seine Empfehlungen.

Stellungnahme der NÖ Landesregierung:

Im Zuge der Erarbeitung eines unternehmensweiten Risikomanagements und der damit zusammenhängenden Sicherheitspolitik wird auch der geforderte IKT-Notfallplan erstellt werden.

Äußerung des Landesrechnungshofs Niederösterreich:

Die Stellungnahme wurde zur Kenntnis genommen.

6.2 Serverräume

In Ergebnis 11 wurde folgende Empfehlung festgehalten:

„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."

Die Empfehlung des Landesrechnungshofs wurde umgesetzt.

Die NÖ Landesregierung hatte in ihrer Stellungnahme mitgeteilt, dass die Führung von Besucherlogbüchern in die Richtlinien zum IT-Betrieb der NÖ Landesklinken aufgenommen wurde und von den NÖ Landeskliniken umgesetzt wird.

Der Landesrechnungshof stellte dazu fest, dass für die überprüften zehn Serverräume jeweils Besucherlogbücher in Form von Zutrittslisten geführt wurden, die den Zutritt und das Verlassen von Personen dokumentierten. In einem Landesklinikum wurde im Zuge des Neubaus zudem eine technische Lösung in Form eines elektronischen Zutrittssystems vorbereitet, das zukünftig alle Zutritte personenbezogen protokollieren sollte.

In Ergebnis 12 wurde folgende Empfehlung festgehalten:

„Serverräume sind nicht als Lagerräume zu verwenden."

Die Empfehlung des Landesrechnungshofs wurde umgesetzt.

Die NÖ Landesregierung hatte in ihrer Stellungnahme zugesagt dass die Anforderungen an Serverräume, welche zum Beispiel Themen wie "Führen eines Besucherlogbuches", "Verwendungsverbot als Lagerraum", "Terminierung von flüssigkeitsführenden Leitungen" etc. entsprechend regeln, in die Richtlinien eingearbeitet werden.

Wie der Landesrechnungshof feststellte, wurde seine Empfehlung in der Dienstanweisung IT-Betrieb für Landeskliniken, 01-08/00-0161, vom 19. August 2011 ergänzt. Die im Zuge der Nachkontrolle überprüften zehn Serverräume waren frei von Lagermaterial.

In Ergebnis 13 wurde folgende Empfehlung festgehalten:

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

Die Empfehlung des Landesrechnungshofs wurde teilweise umgesetzt.

Die NÖ Landesregierung hatte in ihrer Stellungnahme zugesagt, dass die Anforderungen an Serverräume, welche zum Beispiel Themen wie "Führen eines Besucherlogbuches", "Verwendungsverbot als Lagerraum", "Terminie-

rung von flüssigkeitsführenden Leitungen" etc. entsprechend regeln, in die zu Ergebnis 11 angeführten Richtlinien eingearbeitet werden.

Der Landesrechnungshof fand jedoch in einem neu errichteten Serverraum terminierende flüssigkeitsführende Leitungen vor, weil darin installierte Klimaaggregate die Kühlung über Kaltwasserzufuhr und Warmwasserableitung regelten, obwohl gemäß Anhang zum Weißbuch - IKT-Betriebsräume in einem Serverraum das Terminieren oder die Durchführung von flüssigkeits- bzw. gasführenden Leitungen untersagt waren.

Der Landesrechnungshof bekräftigte seine Empfehlung, wonach bei Um- und Neubauten darauf Bedacht zu nehmen ist, dass keine flüssigkeits- bzw. gasführenden Leitungen in Serverräumen terminieren oder durch Serverräume durchführen dürfen.

Stellungnahme der NÖ Landesregierung:

Die Empfehlung des Landesrechnungshofes wird in das Weißbuch für IKT-Betriebsräume für Neu- und Umbauten aufgenommen.

Äußerung des Landesrechnungshofs Niederösterreich:

Die Stellungnahme wurde zur Kenntnis genommen.

In Ergebnis 14 wurde folgende Empfehlung festgehalten:

„Zentrale Verteiler bzw. CORE-Switches sind jeweils in eigenen Serverräumen zu betreiben. Aus sicherheitstechnischen Überlegungen ist eine getrennte Aufstellung in verschiedenen Brandabschnitten vorzunehmen."

Die Empfehlung des Landesrechnungshofs wurde teilweise umgesetzt.

Die NÖ Landesregierung hatte in ihrer Stellungnahme mitgeteilt, dass sich lediglich in einem Klinikum die beiden CORE-Switches in ein und demselben Raum befanden, wobei die geforderte getrennte Aufstellung auch in diesem Klinikum erfolgen wird.

Der Landesrechnungshof überzeugte sich davon, dass die CORE-Switches (Zentraler Netzwerkknoten) in einem Landesklinikum tatsächlich räumlich getrennt wurden, stellte jedoch bei einem anderen Klinikum fest, dass dort die beiden CORE-Switches in ein und demselben Raum untergebracht waren.

Der Landesrechnungshof bekräftigte seine Empfehlung, die CORE-Switches in allen NÖ Landeskliniken räumlich zu trennen.

Stellungnahme der NÖ Landesregierung:

Der Empfehlung des Landesrechnungshofes wird nachgekommen werden.

Äußerung des Landesrechnungshofs Niederösterreich:

Die Stellungnahme wurde zur Kenntnis genommen.

6.3 Datensicherung

In Ergebnis 15 wurde folgende Empfehlung festgehalten:

„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."

Die Empfehlung des Landesrechnungshofs wurde umgesetzt.

Die NÖ Landesregierung hatte in ihrer Stellungnahme mitgeteilt, dass an einer Vereinheitlichung der regelmäßigen testweisen Rücksicherung gearbeitet wird.

Der Landesrechnungshof stellte nunmehr fest, dass die fünf im Zuge der Nachkontrolle überprüften NÖ Landeskliniken die Zeitfenster während der monatlichen Wartungen auch dazu nutzten, die Rücksicherung auf Dateiebene auf ihre vorgesehen Funktionalität zu überprüfen.

7. Dokumentation

In Ergebnis 16 wurde folgende Empfehlung festgehalten:

„Eine ordnungsmäßige Dokumentation ist durch zentrale Vorgaben sicherzustellen."

Die Empfehlung des Landesrechnungshofs wurde nicht umgesetzt.

Die NÖ Landesregierung hatte in ihrer Stellungnahme ausgeführt, dass in dem zu Ergebnis 3 bereits beschriebenen Managementsystem auch die zentralen Vorgaben einer ordnungsgemäßen Dokumentation Eingang finden werden.

Da noch kein Programm zur Erfassung der Hard- und Software und der Lizenzdaten eingeführt wurde, gab es noch keine einheitliche Dokumentationsvorlage für Rechenzentren und Serverräume bei den NÖ Landeskliniken, sondern lediglich dezentrale Dokumentationen. Anhand der einheitlich erfassten Assets wird es der NÖ Landeskliniken-Holding künftig möglich sein zu entscheiden, welche Hard- und Softwarekomponenten zentral wirtschaftlicher zu betreiben sind.

Der Landesrechnungshof bekräftigte seine Empfehlung, eine ordnungsgemäße Dokumentation für die gesamte Hard- und Softwarelandschaft in einem Assetmanagementsystem zentral sicherzustellen.

Stellungnahme der NÖ Landesregierung:

Die NÖ Landeskliniken-Holding wird, wie im Ergebnis 3 formuliert, die Empfehlung des Landesrechnungshofes umsetzen.

Äußerung des Landesrechnungshofs Niederösterreich:

Die Stellungnahme wurde zur Kenntnis genommen.

St. Pölten, im Jänner 2015

Die Landesrechnungshofdirektorin

Dr. Edith Goldeband

Tor zum Landhaus · Wiener Str. 54/A · 3109 St.Pölten
T +43 2742 9005 126 20 · F +43 2742 9005 157 40
post.lrh@noel.gv.at · www.lrh-noe.at