NÖ Landesrechnungshof

Bericht 11/2004

IT-Sicherheit bei den Bezirkshauptmannschaften

St. Pölten, im Jänner 2005

NÖ Landesrechnungshof
3109 St. Pölten, Tor zum Landhaus
Wiener Straße 54 / Stg.A

Tel: (02742) 9005-12620
Fax: (02742) 9005-15740
E-Mail: post.lrh@noel.gv.at
Homepage: www.lrh-noe.at
DVR: 2107945

INHALTSVERZEICHNIS

ZUSAMMENFASSUNG

Das Ziel der Prüfung war es, einen Überblick über bestehende IT-Sicherheitseinrichtungen und –maßnahmen im Bereich der NÖ Bezirkshauptmannschaften zu vermitteln. Einen weiteren Schwerpunkt dieser Prüfungen bildete das Vorhandensein von Richtlinien und Dienstanweisungen sowie deren Einhaltung durch die Bediensteten der Bezirkshauptmannschaften. Die Überprüfung wurde vorrangig bei den einzelnen Bezirkshauptmannschaften vor Ort vorgenommen.
Es wurde eine sehr hoher Drucker- und Scanneranteil festgestellt. Dieser könnte durch gezielteren Einsatz effizienter gestaltet werden.

Trotz eines sehr hohen Engagements der IT-Koordinatoren sollte seitens der Abteilung Landesamtsdirektion-Informationstechnologie nicht auf die Vertiefung des vorhandenen Wissens und die Weiterbildung vergessen werden.

Obwohl positiv anzumerken ist, dass das Sicherheitsbewusstsein bei den Bediensteten eine positive Entwicklung erfahren hat, wurde festgestellt, dass einzelne Bedienstete von den bereits getroffenen Maßnahmen, in Richtlinien und Dienstanweisungen formuliert, nur sehr schwer zu überzeugen sind.

Die Absicherung der Server- und Verteilerräume ist sehr unterschiedlich und sollte auf einen einheitlichen Standard gebracht werden.

Die Passwortvielfalt stellt bei der Absicherung der Server gegen unbefugten Zugriff ebenso wie bei der Absicherung der verschiedenen Applikationen ein Problem dar.

Die Katastrophenvorsorge im IT-Bereich sollte ebenfalls in schriftlicher Form vorhanden sein und sollte im Katastrophenplan der Bezirkshauptmannschaft enthalten sein.

Die NÖ Landesregierung hat im wesentlichen zugesagt, den Empfehlungen und Beanstandungen des NÖ Landesrechnungshofes Rechnung zu tragen.

1 Prüfungsgegenstand

Der NÖ Landesrechnungshof (LRH) hat die IT-Sicherheitseinrichtungen und -maßnahmen im Bereich der Bezirkshauptmannschaften überprüft. Prüfungsschwerpunkt war das Vorhandensein von Sicherheitsmechanismen und die Einhaltung der geltenden Richtlinien und Dienstanweisungen über den Schutz EDV-mäßig verarbeiteter Daten.

2 Rechtliche Grundlagen

Für den Prüfungsgegenstand gelten die Bestimmungen des Datenschutzgesetzes 2000, BGBl I 1999/165, und des NÖ Datenschutzgesetzes, LGBl 0901.

Auf Grund der Verordnung über die Geschäftsordnung der NÖ Landesregierung ist Landeshauptmann Dr. Erwin Pröll für Angelegenheiten des Datenschutzes mit Ausnahme der Verwaltungsstrafverfahren und für Angelegenheiten der Informations- und Kommunikationstechnologie, zuständig.

Gemäß der Geschäftseinteilung des Amtes der NÖ Landesregierung nimmt die Aufgaben im Zusammenhang mit dem Datenschutz mit Ausnahme der Verwaltungsstrafverfahren und die Aufgaben der Informations- und Kommunikationstechnologie die Abteilung Landesamtsdirektion (LAD1) wahr, wobei innerhalb dieser der Fachbereich Verfassungsdienst (LAD1-VD) für die Angelegenheiten des Datenschutzes und der Fachbereich Informationstechnologie (LAD1-IT) für die Angelegenheiten der Informations- und Kommunikationstechnologie zuständig ist.

2.1 Dienstanweisung

Seitens der Abteilung Landesamtsdirektion-Informationstechnologie (LAD1-IT) wurde die Dienstanweisung, IT-Betrieb, 01-08/00-0160, herausgegeben, deren Ziel es ist, einen zweckmäßigen und einheitlichen Betrieb der Informationstechnologie in den Dienststellen (IT-Betrieb) zu gewährleisten. Diese Dienstanweisung ist auch auf den IT-Betrieb in den Bezirkshauptmannschaften anzuwenden.

3 Allgemeines

Die Bezirkshauptmannschaften sind seit Anfang der 80iger Jahre mit einem Netzwerk (token ring Verkabelung und Server) ausgestattet. Im Zuge von Neu- und Umbauten wurden ab den Jahren 1995/1996 die Bezirkshauptmannschaften sukzessive auf die neue Netzwerktechnologie Ethernet umgestellt. Seit 1998 sind die Bezirkshauptmannschaften mittels NÖWAN (Niederösterreichweites Netzwerk) mit dem Landhaus verbunden.

Die Prüfung der IT-Sicherheit bei den Bezirkshauptmannschaften erfolgte auch unter dem Aspekte der Personalausstattung und dienstrechtlicher Rahmenbedingungen.

Unabhängig von Anmerkungen zur Sicherheitsproblematik werden auch Anmerkungen zu der bei den Bezirkshauptmannschaften eingesetzten Hardware gemacht.

Es wird darauf hingewiesen, dass im Bericht verwendete geschlechtsspezifische Bezeichnungen grundsätzlich für Männer und Frauen gelten.

4 Personal

4.1 IT-Koordinator

Den IT-Koordinatoren kommt eine ganz wesentliche Rolle bei der IT-Sicherheit auf den Bezirkshauptmannschaften zu. Deshalb waren sie auch die Hauptansprechpartner dieser Prüfung.

Gemäß Dienstanweisung, IT-Betrieb, 01-08/00-0160, Punkt 13, ist für etwa 50 Arbeitsplätze ein IT-Koordinator zur Gänze zur Verfügung zu stellen. Die Stellvertretung ist im Abwesenheitsfall des IT-Koordinators sicherzustellen.

Die folgende Tabelle soll einen Überblick darüber geben, wie viele Arbeitsstationen bei den einzelnen Bezirkshauptmannschaften zu betreuen sind und wie viele IT-Koordinatoren in welchem Ausmaß beschäftigt sind:

Bezirkshaupt-mannschaft	Anzahl der Arbeits-stationen (inkl. Note-books) der BH	Anzahl der Arbeits-stationen (inkl. Note-books) externer Dienststellen die betreut werden	Gesamt-anzahl	IT-Koord.	Besch. Ausm. in %
Amstetten	147	19	166	1 B 1 C	100 100
Baden	191	6	197	1 C 2 VB-d	100 100
Bruck/Leitha	91	9	100	1 C 1 C	100 50
Gänserndorf	143	14	157	1 C 1C	100 80
Gmünd	101	8	109	1 C 1 C	100 75
Hollabrunn	118	3	121	1 B 2 C	100 100
Horn	92	24	116	1 C	100
Korneuburg	132	19	151	1 C 1 C	100 75
Krems/Donau	126	6	132	2 C	100
Lilienfeld	70	3	73	1 B 1 C	Fachgebietsleiter Bürodirektor-Stv.
Melk	124	8	132	2 C	100
Mistelbach	125	17	142	1 C 1 C	100 75
Mödling	175	40	215	1 B 1 C	100 100
Neunkirchen	135	6	141	2 C	100
Scheibbs	67	4	71	1 C 1 C	100 50
St. Pölten	141	5	146	1 C 1 C	100 80
Tulln	124	4	128	1 C 1 C 1 C	100 100 37,5
Waidhofen/Thaya	84	4	88	1 C 1 C	100 50
Wr. Neustadt	139	40	179	2 C	100
Wien Umgebung	186	4	190	1 B 1 C	100 100
Zwettl	107	14	121	2 C	100

Aus der vorstehenden Zusammenstellung ist zu entnehmen, dass die Koordinatoren aller Bezirkshauptmannschaften mehr als den von LAD1-IT vorgegebenen Richtwert von 50 Arbeitsplätzen zu betreuen haben. In der ursprünglichen bis Jänner 2004 geltenden Dienstanweisung der LAD1-IT war der Richtwert für die von einem IT-Koordinator zu betreuenden Arbeitsstationen mit 100 festgelegt. Bei der Überprüfung der Bezirkshauptmannschaften konnte der Eindruck gewonnen werden, dass sich der Arbeitsumfang für die IT-Koordinatoren nicht in dem Ausmaß erhöht hat, in dem der Richtwert herabgesetzt wurde.

Ergebnis 1
Der Richtwert hinsichtlich der von einem IT-Koordinator zu betreuenden Arbeitsplätzen sollte neu überdacht werden.

Stellungnahme der NÖ Landesregierung:

Eine fixe Zahl der von einem IT-Koordinator zu betreuenden Arbeitsplätze, die allen Situationen gerecht wird, kann nicht exakt angegeben werden. Dazu ist die Aufgabenvielfalt der IT-Koordinatoren zu groß und von Dienststelle zu Dienststelle zu verschieden. Die in der Dienstanweisung IT-Betrieb angeführte Zahl ist ein Richtwert (wie auch im Bericht des LRH angeführt), der für alle Abteilungen des Landes und auch für alle Bezirkshauptmannschaften gilt. Sie wird vor allem auch bei der Berechnung der quantitativen Höhe der IT-Koordinatoren-Zulage heran gezogen. Die tatsächliche Zahl der Benutzer, die ein IT-Koordinator betreuen kann, liegt zwischen 50 und 100 und kann nur individuell in jeder Dienststelle festgelegt werden. Bei den Bezirkshauptmannschaften ist aus Sicht der Abt. LAD1-IT davon auszugehen, dass die Zahl näher bei 50 liegen wird. Gerade in BH's sind besonders viele Anwendungen zu betreuen. Es werden laufend neue Anwendungen in Betrieb genommen bzw. wesentliche Erweiterungen durchgeführt (2004: Anlagen, Jagd, teilw. LAKIS, Änderungen bei Gewerbe, Fremdenpolizei). Die Anwendungen laufen auf den unterschiedlichsten technischen Systemen, die jeweils hohes und verschiedenes Know How erfordern und die Fehlerdiagnose erschweren (lokale Anwendungen, Anwendungen auf den BH-Servern, NÖ-zentrale Anwendungen, Bundes-Anwendungen, Großrechner-Anwendungen, Windows-Anwendungen, Magic-Anwendungen, Web-Anwendungen, Linux-Anwendungen).

NÖ Landesrechnungshof:

Die Stellungnahme wird zur Kenntnis genommen.

Im Zuge der Überprüfung war eine unterschiedliche Personalausstattung, bezogen auf Quantität als auch auf Qualität, bei den Bezirkshauptmannschaften festzustellen. Manche IT-Koordinatoren bzw. Stellvertreter sind nicht nur für diesen Bereich tätig sondern haben noch andere Aufgaben als Sachbearbeiter bis hin zum Sachgebietsleiter zu erfüllen. Ein besonderes Beispiel dafür ist die Bezirkshauptmannschaft Lilienfeld, da der IT-Koordinator auch die Funktion eines Fachgebietsleiters und der IT-Koordinator-

stellvertreter auch die Funktion eines Bürodirektor Stellvertreters bekleidet. Die zusätzlichen Funktionen beanspruchen die IT-Koordinatoren in unterschiedlichem Ausmaß, sodass eine prozentmäßige Darstellung der Koordinatorentätigkeit gar nicht möglich ist. Diese Konstruktion führt dazu, dass entweder ein Bereich nicht in ausreichendem Ausmaß abgedeckt wird oder die betroffenen Kollegen durch erhöhte Mehrdienstleistung das Manko ausgleichen müssen. Aus arbeitstechnischer Sicht wäre es sicher sinnvoll, wenn zumindest ein IT-Koordinator zu 100 % für IT-Tätigkeiten eingesetzt würde. Die Stellvertretung ist – wie im Erlass vorgesehen - innerhalb der Dienststelle zu regeln.

Es ist aufgefallen, dass der größte Teil der IT-Betreuung der in den Bezirkshauptmannschaften eingerichteten Außenstellen zentraler Dienststellen nicht durch die IT-Koordinatoren der jeweiligen Abteilung sondern durch die IT-Koordinatoren der Bezirkshauptmannschaften vor Ort wahrgenommen wird. Diese auch nach Ansicht des LRH sinnvolle Hilfestellung sollte auch arbeitsmäßig den IT-Koordinatoren der Bezirkshauptmannschaften zugerechnet werden.

Seitens der Koordinatoren war ein Mangel an Aus- und Weiterbildungsangeboten beim Amt der NÖ Landesregierung festzustellen. Manche sind ein halbes Jahr in dieser Funktion tätig und haben noch immer keinen Betriebssystem- und Novellkurs absolviert. Da es die personelle Situation erfordert, werden von diesen Personen aber bereits User administriert. Dass es dadurch zu teilweisen Fehldefinitionen sowohl im Sicherheitsbereich (Passwort und dessen Änderungsaufforderung) als auch bei den Zugriffsdefinitionen kommen kann, ist auf Grund des oben beschriebenen Sachverhalts kaum vermeidbar.

Die IT-Koordinatoren zeigen ein sehr hohes Engagement und bilden sich durch Selbststudium fort. Weiters wird angeregt, die teilweise nur jährlichen Treffen zwischen den IT-Koordinatoren und der zentralen Abteilung LAD1-IT in kürzeren Abständen abzuhalten, um den Erfahrungsaustausch und die Weitergabe von Informationen aus erster Hand zielgerichteter gestalten zu können. Die vorhandenen Medien (E-Mail; Troubleticket mittels Remedy) sind zwar gut und die Reaktionen zufrieden stellend, jedoch können komplexere Themen, die in mehreren Bezirkshauptmannschaften auftreten, nicht erschöpfend genug behandelt werden.

Ergebnis 2
Um einen ordnungsgemäßen Dienstbetrieb sicherzustellen, ist dafür Sorge zu tragen, dass alle IT-Koordinatoren auf dem gleichen Grundwissen aufbauen können. Durch Workshops und andere Weiterbildungsmaßnahmen sollte das Wissen gesichert und ausgebaut werden. Außerdem sollte sichergestellt werden, dass zumindest ein IT-Koordinator zur Gänze für Koordinatorentätigkeiten eingesetzt wird.

Stellungnahme der NÖ Landesregierung:

Die Schulung der IT-Koordinatoren wird durch die LAD1-IT Benutzerunterstützung durchgeführt. Alle der Abt. LAD1-IT gemeldeten IT-Koordinatoren werden zu den folgenden Schulungen einberufen: IT Grundschulung, Novell-Kurs, XP-Kurs. Diese Kurse finden im Schulungsraum in St. Pölten statt. Aus Wirtschaft-

lichkeitsgründen (die Kurse werden zum Teil von Firmen gehalten) ist es aber nicht möglich, jeden IT-Koordinator sofort nach seiner Ernennung zu einer Schulung einzuberufen, sondern erst dann, wenn ein gesamter Kurs (10 Schulungsplätze) voll ist. Das kann im Einzelfall bis zu einem halben Jahr dauern.

In den letzten Jahren wurden bereits verstärkt Weiterbildungsmaßnahmen für IT-Koordinatoren durchgeführt. Für die BH IT-Koordinatoren wird mindestens einmal jährlich eine Informationsveranstaltung abgehalten. Weiters gibt es Workshops an denen alle IT-Koordinatoren teilnehmen können (derzeit 1-2 Themen pro Jahr). Dieses System der Weiterbildungsmaßnahmen wird weiter ausgebaut werden.

Seit September 2004 sind darüber hinaus zwei Mitarbeiter der Benutzerunterstützung als primäre Ansprechpartner und Betreuer für die Bezirkshauptmannschaften definiert. Nach der Einarbeitung dieser Mitarbeiter sollen alle neu ernannten BH IT-Koordinatoren gleich nach ihrer Ernennung eine erste Grundeinschulung erhalten, um alle laufenden Arbeiten durchführen zu können. Weiters ist eine persönliche Unterstützung auf Anforderung in der Anfangsphase auf der jeweiligen BH vor Ort möglich.

Es wird bei kleinen Dienststellen nicht als sinnvoll angesehen, dass ein Koordinator zur Gänze für diese Aufgabe eingesetzt wird. Dies hätte den Nachteil, dass bei Abwesenheit dieses einen Mitarbeiters (Urlaub, Krankheit, ...) eine Vertretung kaum eingearbeitet wäre und daher nur bedingt ihrer Aufgabe nachkommen könnte.

NÖ Landesrechnungshof:

Die Stellungnahme wird teilweise zur Kenntnis genommen. Der LRH hat sich bei der gegenständlichen Prüfung vor allem mit der Situation der IT Koordinatoren an den Bezirkshauptmannschaften auseinandergesetzt. Unter Anwendung der Vorgaben seitens der Abt. LAD1-IT, wie viele Arbeitsstationen von einem IT-Koordinator zu betreuen sind, ergibt es sich, dass selbst für die kleinste Bezirkshauptmannschaft mehr als ein IT-Koordinator erforderlich ist. In diesem Fall erachtet es der LRH für zweckmäßiger, wenn ein IT-Koordinator von anderen Aufgaben der Verwaltung (vor allem von solchen mit Parteienverkehr) zur Gänze entbunden wird, um eine optimale IT-Betreuung zu garantieren. Selbstverständlich muss der IT-Koordinator – schon im eigenen Interesse – dafür sorgen, dass auch sein Vertreter die Aufgaben im Vertretungsfall erfüllen kann.

4.1.1 Stellenbeschreibung IT-Koordinator

Die von der Abteilung LAD1-IT ausgearbeitete und der Dienstanweisung, IT-Betrieb, 01-08/00-0160, als Beilage angeschlossene Stellenbeschreibung geht sehr ins Detail, da nur die Beschreibung des Aufgabenbereiches allein zwei DIN A4 Seiten beträgt. Im Zuge des Projektes Bezirkshauptmannschaft – NEU wurde von der Arbeitsgruppe „IT-Angelegenheiten der Bezirkshauptmannschaften“, eine neue Stellenbeschreibung im Einvernehmen mit der Abteilung Landesamtsdirektion erstellt, die den Aufgabenbe-

reich des IT-Koordinators weiter gefasst darstellt, sodass sie einen größeren Interpretationsspielraum hinsichtlich der tatsächlichen Aufgaben des IT-Koordinators zulässt.

Zwischen den beiden Stellenbeschreibungen bestehen dienstrechtliche Unterschiede. Die Stellenbeschreibung der Abteilung LAD1-IT sieht vor, dass der IT-Koordinator in disziplinären Fragen dem jeweiligen **Dienststellenleiter** und in Fachfragen der LAD1-IT Leitung der Anwendungsentwicklung oder Leitung der Benutzerunterstützung unterstellt ist.

In der von der Arbeitsgruppe „IT-Angelegenheiten der Bezirkshauptmannschaften" erarbeiteten Stellenbeschreibung ist hingegen die Stelle nicht dem Bezirkshauptmann als Dienststellenleiter direkt sondern dem **Stabsstellenleiter** (= Bürodirektor) unterstellt, „bei fachlichen Komponenten und Fragen sind die Vorgaben und Anordnungen der Abteilung LAD1-IT einzuhalten".

In einigen Bezirkshauptmannschaften wurde die neue Stellenbeschreibung bereits in Kraft gesetzt. Bei den Restlichen gilt nach wie vor die Stellbeschreibung gem. Dienstanweisung.

Ergebnis 3
Auf Grund der Aufgabenstellung der Bezirkshauptmannschaften wurde eine neue Stellenbeschreibung im Einvernehmen mit der Abteilung Landesamtsdirektion entwickelt. Diese ist einheitlich in allen Bezirkshauptmannschaften in Kraft zu setzen.

Stellungnahme der NÖ Landesregierung:

Die neue einheitliche Stellenbeschreibung für IT-Koordinatoren auf den Bezirkshauptmannschaften ist seit Einführung der BH-Neu mit 1.1.2004 in Kraft und bei einem Großteil der Bezirkshauptmannschaften bereits umgesetzt. Jene Bezirkshauptmannschaften, bei denen diese Stellenbeschreibung noch nicht in Kraft gesetzt wurde, haben damit bis zum Vorliegen von einheitlichen Stellenbeschreibungen für alle Stellen in sämtlichen Fachgebieten zugewartet.
Bei den restlichen Bezirkshauptmannschaften ist die Umsetzung im Gange.

NÖ Landesrechnungshof:

Die Stellungnahme wird zur Kenntnis genommen.

4.2 Anwender

Das Sicherheitsverständnis der Anwender ist im Allgemeinen als gut zu bezeichnen. Gemäß Punkt. 2 der Dienstanweisung, IT-Betrieb, 01-08/00-0160, ist „… Jede Benutzerin und jeder Benutzer verpflichtet vorzusorgen, dass während des Betriebes der Arbeitsplatzcomputer sowie bei jedem Verlassen des Arbeitsplatzes weder dienstfremde Personen noch nicht berechtigte Bedienstete in ein Programm bzw. in Daten Einsicht nehmen können (z.B. durch Versperren oder softwaremäßige Tastatursperren). Weiters ist jede Mitarbeiterin und jeder Mitarbeiter verpflichtet, alle jeweils notwendigen Maß-

nahmen zur Verhinderung von Datenmanipulationen durch dienstfremde Personen oder nicht berechtigte Bedienstete zu treffen. Erforderlichenfalls hat die Benutzerin bzw. der Benutzer aus dem laufenden Programm auszusteigen und die Verbindung zum Netzwerk bzw. zum Zentralrechner zu beenden. …“

Die bei der Windows XP Umstellung installierten Bildschirmschonereinstellungen, welche nach zehn Minuten Leerlauf den Zugriff auf den PC sperren, dürfen keine Ausrede der Bediensteten für etwaige Missachtung geltender Vorschriften sein.

Im Zuge der Überprüfung einer Bezirkshauptmannschaft konnte festgestellt werden, dass die eindringlichen Anweisungen des Dienststellenleiters und der IT-Koordinatoren von einigen Mitarbeitern nach wie vor nicht beachtet werden. Der nicht amtsbekannte Prüfer des LRH konnte ungehindert auf einen unbesetzten und nicht versperrten Computerarbeitsplatz im Bürgerbüro zugehen, den Bildschirminhalt lesen und durch klicken mit der Maus auch in anderen Programmen personenbezogene Daten abrufen. Am Rande sei noch die Bemerkung erlaubt, dass zu diesem Zeitpunkt keine Parteien anwesend waren.

Das Versperren des Arbeitsplatzes, das vor allem den unbefugten Zugriff auf personenbezogene Daten verhindern soll, dient auch dem Selbstschutz für den einzelnen Bediensteten. Sollten Daten ungerechtfertigt von einer „offenen Arbeitsstation“ weitergeleitet oder gelöscht werden, so ist jener Benutzer haftbar, der angemeldet war und den PC unversperrt hinterlassen hat

Ergebnis 4
Die geltenden Vorschriften sind in regelmäßigen Abständen allen Bediensteten nachweislich zur Kenntnis zu bringen. Bei wiederholter Missachtung der Anweisungen sind disziplinäre Maßnahmen zu ergreifen.

Stellungnahme der NÖ Landesregierung:

Die Dienstanweisung bezüglich des IT-Betriebes wurde jedem Benutzer und jeder Benutzerin zur Kenntnis gebracht. Die beobachteten Mängel und Missstände werden zum Anlass genommen, diese Anweisung neuerlich den Mitarbeitern und Mitarbeiterinnen in Erinnerung zu rufen.

NÖ Landesrechnungshof:

Die Stellungnahme wird zur Kenntnis genommen.

5 Hardwareausstattung am Arbeitsplatz

Die vorgefundene Arbeitsplatzausstattung kann durchwegs als gut und ausreichend bezeichnet werden, es ist jedoch generell die sehr hohe Anzahl an Druckern aufgefallen. Durch zweckmäßige Verwendung von so genannten JetDirect (Netzwerkkarte für Drucker) könnte ein Drucker durch mehrere Mitarbeiter gemeinsam genutzt werden. Der Wegfall von Druckern würde eine budgetäre Entlastung bedeuten und auch den Administrationsaufwand für die IT-Koordinatoren verringern. Wie die unten stehende Tabelle

zeigt, wurde diese Überlegung bei einigen Bezirkshauptmannschaften bereits umgesetzt.

Bezirkshauptmannschaft	Anzahl der Arbeitsstationen (inkl. Notebooks) der BH	Drucker
Amstetten	147	141
Baden	191	153
Bruck/Leitha	91	51
Gänserndorf	143	150
Gmünd	101	91
Hollabrunn	118	111
Horn	92	93
Korneuburg	132	103
Krems/Donau	126	75
Lilienfeld	70	73
Melk	124	90
Mistelbach	125	110
Mödling	175	147
Neunkirchen	135	79
Scheibbs	67	70
St. Pölten	141	121
Tulln	124	120
Waidhofen/Thaya	84	88
Wr. Neustadt	139	129
Wien Umgebung	186	136
Zwettl	107	82

Besonders auffällig war die zumeist mehr als reichliche Ausstattung der Bürgerbüros, wobei vor allem die Anzahl der Scanner (wie aus der unten angeführten Tabelle ersichtlich) in einzelnen Bezirkshauptmannschaften (teilweise je Bürgerbüroarbeitsplatz ein Scanner) zu beanstanden ist. Bei der Prüfung war nur ein sehr geringer Einsatz der Scanner festzustellen. Die Scanner, die einen Anschaffungswert von durchschnittlich € 700 haben und für die Stapelverarbeitung mehrseitiger Dokumente ausgerüstet sind, sind für die derzeit damit ausgeführten Arbeiten überdimensioniert, was jedoch auf technischen Vorgaben des Ministeriums für die künftige Ausstellung des Personalausweises (Passbild muss dafür elektronisch gespeichert sein) zurückzuführen ist.

Bezirkshaupt-mannschaft	Anzahl Scanner (ausgen. Bür-gerbüro)	Anzahl Scanner im Bürgerbüro	Anzahl der Arbeitsplätze im Bürgerbüro
Amstetten	4	4	8
Baden	9	8	8
Bruck/Leitha	3	3	5
Gänserndorf	1	5	11
Gmünd	7	1	5
Hollabrunn	1	2	6
Horn	8	2	4
Korneuburg	5	3	7
Krems/Donau	10	4	7
Lilienfeld	1	1	4
Melk	4	6	6
Mistelbach	2	5	8
Mödling	4	5	8
Neunkirchen	5	2	7
Scheibbs	2	2	5
St. Pölten	2	3	9
Tulln	3	3	6
Waidhofen/Thaya	3	3	4
Wr. Neustadt	10	5	7
Wien Umgebung	4	8	15
Zwettl	6	7	7

Ergebnis 5
Es sollte neu überdacht werden, ob eine so hohe Anzahl an Druckern und Scannern in jeder Bezirkshauptmannschaft wirklich notwendig ist.

Stellungnahme der NÖ Landesregierung:

Da auf jedem Arbeitsplatz eines Bürgerbüros alle Anliegen und Leistungen für die Bürger erbracht werden sollen, ist eine umfangreiche Ausstattung für jeden Arbeitsplatz zwingend erforderlich. Die Geräte, insbesondere Scanner und Drucker sind entsprechend den Vorgaben des BMI anzuschaffen, das auch die entsprechende Software zur Verfügung stellt. Würden diese Vorgaben nicht eingehalten, bestünde die Gefahr, dass die Software nicht ordnungsgemäß funktioniert bzw. die Qualitäts- und Sicherheitsanforderungen nicht erfüllt werden könnten. In einigen Fällen war es auf Grund der räumlichen Situation trotzdem möglich, Einsparungen zu machen, womit sich unterschiedliche Zahlen in den Bürgerbüros erklären.

Es gibt bereits generelle Überlegungen (nicht nur für BH's), wie eine Reduzierung der Drucker erreicht werden kann (Einsatz von Abteilungs-, Gang- bzw. Stockwerksdruckern).

NÖ Landesrechnungshof:

Die Stellungnahme wird zur Kenntnis genommen.

6 Sicherung der Serverdaten

Die Sicherung der gespeicherten Daten des Fileservers und des Exchangeservers (E-Mail Server) erfolgt bei allen Bezirkshauptmannschaften gemäß Dienstanweisung durch eine tägliche Vollsicherung. Die Verwahrung der Sicherungsbänder wird unterschiedlich gehandhabt. So war festzustellen, dass die Sicherungsbänder bei mehreren Bezirkshauptmannschaften direkt im Serverraum aufbewahrt werden. Dies ist aus Sicherheitsgründen nicht empfehlenswert, da im Brandfall im Serverraum auch die Sicherungsbänder vernichtet würden. Die Verwahrung in einem feuersicheren Schrank würde einen guten Schutz für die Sicherungsbänder bringen. In jeder Dienststelle wird zumindest einmal wöchentlich eine Vollsicherung entweder in einem Bankschließfach bzw. in einem externen Gebäude der Bezirkshauptmannschaft in einem Tresor oder feuersicheren Schrank hinterlegt.

Ergebnis 6

Die Verwahrung der Sicherungsbänder im Serverraum bei Auslagerung von nur einer Vollsicherung pro Woche wird als unzureichend erachtet, da im Schadensfall die Sicherung von eventuell 4 bis 5 Werktagen verloren gehen würde. Dies würde ein Aufarbeiten der verloren gegangenen Daten erforderlich machen. Die Sicherungsbänder sollten zumindest in einem anderen Raum in einem anderen Stockwerk, idealer Weise in einem feuersicheren Schrank, versperrt aufbewahrt werden.

Stellungnahme der NÖ Landesregierung:

Die momentan gelebte Vorgangsweise bezüglich der Verwaltung bzw. Auslagerung der Sicherungsbestände beruht auf dem Ergebnis der IT-Sicherheitsanalyse 2002, die dem Rechnungshof im Zuge der Prüfung zur Verfügung gestellt wurde. Auf Basis dieser Sicherheitsstudie wurden den BH´s Vorgaben für die ordnungsgemäße Auslagerung gemacht.

Es ist geplant, im Jahre 2005 die Services (File-/Printservices und Mail) von den 21 Bezirkshauptmannschaften zentral nach St. Pölten zu verlegen. Dadurch werden auf den Bezirkshauptmannschaften keine Sicherungen mehr vor Ort durchgeführt, sondern die Daten werden entsprechend den hohen Qualitätsanforderungen gespeichert, die derzeit für das Amt implementiert werden.

Zwischenzeitlich wird folgende Variante angedacht werden: Aus Zeitgründen bzw. wegen der großen Datenmengen ist die Erstellung von zwei Sicherungsbändern (eines für Lagerung in der BH, eines für Auslagerung) nur am Wochenende möglich. Das Originalband der jeweiligen letzten täglichen Sicherung könnte aber sofort ausgelagert werden.
Der Ankaufes von feuerfesten Datensicherungsschränken für alle 21 BH´s erscheint für die noch zu verbleibende Zeit (bis zur Serverkonsolidierung) aus Kostengründen nicht gerechtfertigt.

NÖ Landesrechnungshof:

Die Stellungnahme wird teilweise zur Kenntnis genommen. Da die angeführte Sicherheitsstudie nicht Gegenstand der Prüfung war, wurde auf deren Ergebnisse auch im Bericht nicht eingegangen. Es wird jedoch darauf verwiesen, dass beispielsweise auf Seite 48 der zitierten Studie unter dem Punkt Datensicherung wörtlich ausgeführt wird: „Ein Auslagerung der Datensicherung in **einen anderen Brandabschnitt** als die Sicherungshardware wäre empfehlenswert."
Es wir erwartet, dass das Originalband der jeweiligen letzten täglichen Sicherung ab sofort ausgelagert wird.

7 Zutrittssicherheit

7.1 Gebäude

Die Koordination der sicherheitstechnischen Ausstattungen der einzelnen Bezirkshauptmannschaften ist als unzureichend anzusehen. So wurden zur sicheren Verwahrung streng verrechenbarer Drucksorten die ersten Alarmanlagen angeschafft. Aus aktuellem Anlass (Vorfall in der Bezirkshauptmannschaft Wr. Neustadt) wurden die Alarmanlagen um Alarmtaster erweitert und die Zutrittssicherung in die Gebäude (auch hier ebenfalls nicht einheitlich) geregelt. Bei der Zutrittssicherung in die Amtsgebäude ist anzumerken, dass manche Bezirkshauptmannschaften außerhalb der Amtsstunden nur durch Anmeldung beim im Eingangsbereich situierten Telefonisten und vorheriger Rücksprache mit dem Sachbearbeiter durch Parteien betreten werden können. Bei den meisten Bezirkshauptmannschaften ist jedoch ein ungehinderter Zutritt möglich.

7.2 Serverräume

Die EDV-technische Ausstattung der Server- und Stockwerksverteilerräume ist einheitlich, wenn auch in manchen Bezirkshauptmannschaften etwas überdimensioniert. Manche Serverräume werden zusätzlich noch als Lagerraum für nicht EDV-taugliche Komponenten verwendet (Blumenkisten, Luster, Bilder, etc.). Die Lagerung derartiger Gegenstände in Serverräumen ist zu unterlassen, da sich damit auch zwangsläufig der Personenkreis vergrößert, der Zutritt zu diesen Räumlichkeiten hat. Es sollte darauf geachtet werden, dass die Serverräume nicht von außen eingesehen oder als solche (zB durch

Beschriftung) erkannt werden können. Dies gilt analog für die Stockwerksverteilerräume.

Der Kreis der Zutrittsberechtigten zu den Server- und Stockwerksverteilerräumen ist möglichst klein zu halten und das in der Dienstanweisung, IT-Betrieb, 01-08/00-0160, geforderte Besucherbuch, das nur bei einigen Bezirkshauptmannschaften existiert, zu führen. Das Besucherbuch dient vor allem den Zutrittsberechtigten als Selbstschutz, um später nachvollziehen zu können, welche betriebsfremden Personen den Serverraum betreten haben. Prinzipiell sollte nicht zutrittsberechtigten Personen nur im Einvernehmen mit dem IT-Koordinator oder dessen Stellvertreter Zutritt zu den Serverräumen gewährt werden.

Ergebnis 7
Der Zutritt von nicht berechtigten Personen zu den Serverräumen ist nur im Beisein eines Zutrittsberechtigten gestattet und auf jeden Fall im Besucherbuch zu dokumentieren. Bezirkshauptmannschaften, die noch kein Besucherbuch führen, haben umgehend eines anzulegen.

Stellungnahme der NÖ Landesregierung:

Die Bereitstellung der notwendigen Raumstruktur für die Errichtung einheitlicher EDV-Zentralen bzw. EDV-Stockwerksverteilerräume konnte nur in Abstimmung mit dem Bürodirektor und je nach der zur Verfügung stehenden Baustruktur in Abstimmung mit dem Architekten bzw. Haustechnikplaner erreicht werden. Daher kann die Größe der EDV-Zentralen bzw. EDV-Verteilerräume differieren.

Es wird künftig darauf geachtet werden, dass die Serverräume nicht von außen eingesehen oder als solche erkannt werden können.

Das in der Dienstanweisung für den IT-Betrieb geforderte Besucherbuch wird aus gegebenem Anlass den einzelnen Bezirkshauptmannschaften in Erinnerung gerufen und, sofern noch nicht erfolgt, umgehend aufgelegt werden.

NÖ Landesrechnungshof:

Die Stellungnahme wird zur Kenntnis genommen.

Für die Alarmsicherung sind die Abteilung Allgemeine Verwaltungsangelegenheiten (LAD3) und die Abteilung LAD1-IT in beratender Funktion zuständig. Die Verrechnung der Alarmsicherung erfolgt über die Abteilung Landesamtsdirektion-Rechnungsgruppe (LAD1-RG). Vor ca. 15 Jahren wurde die Firma Alarm und Raumschutz durch Ausschreibung als Bestbieter ermittelt. Sie hatte den Auftrag Alarmanlagen als Einbruchschutz und für die Verwahrung der streng verrechenbaren Drucksorten in definierten Räumlichkeiten einzurichten. Im Zuge der internen Vernetzung der einzelnen Bezirkshauptmannschaften wurden dann Serverräume und Verteilerräume geschaffen. Welche Maßnahmen für die Absicherung dieser Räumlichkeiten gesetzt wurden, lag im Ermessen des jeweiligen Bürodirektors und IT-Koordinators.

Hinsichtlich der Absicherung der Serverräume gegen unbefugten Zutritt wurden bisher keine Standards vorgegeben. Dadurch ist eine vielfältige Landschaft an Absicherungsmaßnahmen entstanden. So kommt es vor, dass Serverräume mit Alarmanlagen (Chip oder durch Eingabe eines Zahlencodes), Bewegungsmelder im Raum und durch Glasbruchsensoren an den Fenstern, andere aber nur durch ein einfaches Schloss abgesichert sind, zu dem mehrere Personen (nicht nur IT-Koordinator, Stellvertreter und Bürodirektor) einen Schlüssel haben. Auch hier wären einheitliche Vorgaben sehr sinnvoll gewesen.

Ergebnis 8
Für die Absicherung der Server- und Verteilerräume gegen unbefugten Zutritt sollten einheitliche Standards definiert werden, da die Absicherung dieser Räume nicht im Ermessen einzelner Bediensteter vor Ort liegen kann.

Stellungnahme der NÖ Landesregierung:

Die Alarmsicherung ist nicht einheitlich geregelt, da die unterschiedlichsten Zutrittssysteme (Blockschloss, Motorzylinder, Chipschlösser) an den Standorten der 21 Bezirkshauptmannschaften bereits vorhanden waren und die Realisierung nicht zum selben Zeitpunkt erfolgte.

Da die meisten EDV-Verteilerräume nicht gesichert waren, wurden Anpassungen an die Alarmanlagen (Erweiterung der Raumsicherungen) durch die Abteilung Landesamtsdirektion/Rechnungsgruppe veranlasst. Eine generelle Vereinheitlichung war aus budgetären Gründen bisher nicht möglich.

NÖ Landesrechnungshof:

Die Stellungnahme wird zur Kenntnis genommen.

Bei der Begehung der Serverräumlichkeiten ist aufgefallen, dass keine Einheitlichkeit bei der Unterbringung der Schaltschränke der Firma NÖKOM gegeben ist. In einigen Bezirkshauptmannschaften sind die Schaltschränke im Serverraum untergebracht. Diese Situation ist aus sicherheitstechnischen und organisatorischen Gründen nicht zufriedenstellend, da die Firma NÖKOM die Schaltschränke auch als Verteiler für andere Institutionen ausbaut und bereits Firmen über diese Schaltschränke angebunden hat. Befinden sich also die angeführten Schaltschränke im Serverraum, so muss auch am Samstag, Sonntag und an Feiertagen der Zugang zu den Schaltschränken gewährleistet sein. In diesem Zusammenhang ist die Bezirkshauptmannschaft Krems hervorzuheben, die für die Anlagen der Firma NÖKOM einen eigenen Raum zur Verfügung gestellt hat, der von der Gebäudeaußenseite betreten werden kann. Dadurch kann die Firma, ohne dass sie den Bürotrakt betritt, jederzeit ihre Komponenten warten.

Ergebnis 9
In Zukunft ist bei Neu-, Zu- oder Umbauten darauf zu achten, dass der Serverraum separat abgesichert ist und die Anlagen von Firmen (wie zB NÖKOM), die diese auch außerhalb der Amtsstunden betreuen müssen, in einem eigenen Raum situiert sind.

Stellungnahme der NÖ Landesregierung:

Für den zentralen Standort der NÖKOM - Komponenten in der EDV-Zentrale spricht die Notwendigkeit, dass im Fehlerfall (24 Stunden-Service) der kontrollierte Zutritt zu den Komponenten möglich sein muss. Wegen der hohen Verflechtung der IT-Komponenten mit den NÖKOM-Anbindungen wäre die Aufteilung auf zwei Räume eher nicht sinnvoll. Weiters wird angemerkt, dass außerhalb der Amtsstunden der Zutritt nur nach Ausweisleistung beim örtlichen Sicherheitsdienst (Gendarmerie bzw. Polizei) möglich ist.

NÖ Landesrechnungshof:

Die Stellungnahme wird teilweise zur Kenntnis genommen. Laut Auskunft der IT-Koordinatoren liegen für einige Bezirkshauptmannschaften keine Schlüssel bei den örtlichen Sicherheitsdiensten. In diesen Fällen muss die Bezirkshauptmannschaft für die Zugänglichkeit zu den Räumlichkeiten sorgen. Auch hier wäre eine einheitliche Vorgangsweise anzudenken.

8 Zugriffssicherheiten

Die Server der Bezirkshauptmannschaften besitzen zum Teil gleiche Passwörter oder Passwörter die aus der regionalen Lage leicht abwandelbar sind. Es ist verständlich, dass auf Grund der Anzahl der Server nicht jeder mit einem individuellen Passwort abgesichert wird. Gerade hier sollte auf jeden Fall gewährleistet sein, dass alle Vorgänge und Transaktionen protokolliert und nachvollziehbar sind.

Die Aktualität der Benutzer in der Benutzerverwaltung hat in den einzelnen Bezirkshauptmannschaften sehr unterschiedliche Qualität. Benutzer, welche versetzt oder in Pension sind, wurden weder gelöscht noch gesperrt. Auch User-ID's (Benutzernamen) ohne Passwort wurden gefunden. Solche User sollte es in einem System gar nicht erst geben. Sollten User ohne Passwort dennoch gebraucht werden, so sind diese, sobald sie nicht mehr benötigt werden, mit einem Passwort zu versehen oder zu sperren.

Derzeit benötigt man fast für jede zugewiesene Applikation ein Passwort. Die Termine für die Passwortänderungen sind nicht synchron und so müssen sich die Mitarbeiter auf den Bezirkshauptmannschaften oftmals mehrere Passwörter mit unterschiedlichem Ablaufdatum merken. Die Gefahr ist daher sehr groß, dass Passwörter notiert und eventuell auch noch an allgemein zugänglichen Stellen hinterlegt werden. Daher wäre es überlegenswert, ob auf Grund der vielfältigen Hard- und Softwarelandschaft und der damit verbundenen Passwortvielfalt, ein so genanntes Secure Identity Management mit zentra-

ler Benutzerdatenverwaltung, welches dezentral über Systemgrenzen hinweg nutzbar ist, eine wesentliche Erleichterung in der Passwort- und Berechtigungsverwaltung mit sich bringen würde. Grundgedanke eines solchen Managementsystems ist es, dem Benutzer je nach Dienstzuteilung Applikationen und Berechtigungen zuzuweisen. Durch einmalige Eingabe von Benutzername und Passwort werden alle Berechtigungen geladen und man braucht bei den einzelnen Applikationen kein Passwort mehr eingeben.

Ergebnis 10
Auf die Aktualität der definierten Benutzer ist besonders Wert zu legen, da hier durch unachtsamen Umgang sehr große Sicherheitslücken entstehen können. Die geltenden Vorschriften sind zu beachten und stichprobenweise durch die zuständigen Benutzerunterstützer der Abteilung Landesamtsdirektion-Informationstechnologie zu überprüfen.
Die Einrichtung eines Secure Identity Managements mit zentraler Benutzerdatenverwaltung sollte überlegt werden.

Stellungnahme der NÖ Landesregierung:

Die Abteilung LAD1-IT erhält seit 2003 von der Abteilung Personalangelegenheiten monatlich eine Liste der Mitarbeiter, die versetzt oder pensioniert wurden bzw. das Dienstverhältnis zum Land gelöst haben. Diese Liste wird von Mitarbeitern der Abteilung LAD1-IT kontrolliert und nach Rücksprache mit dem IT-Koordinator werden jene User, die noch nicht gesperrt bzw. gelöscht sind, entsprechend deaktiviert. In den Schreiben der Abteilung Personalangelegenheiten an die Dienststellen anlässlich des Ausscheidens eines Mitarbeiters wird darauf hingewiesen, dass das Outlook Postfach und der elektronische Schreibtisch (Lakis) zu bereinigen sind und die User-ID zu deaktivieren ist. Dies hat schon bei Antritt eines allfälligen Resturlaubs und nicht erst mit der tatsächlichen Pensionierung zu erfolgen. Eine stichprobenweise Kontrolle auf User ohne Passwort, User, die schon länger nicht mehr im System waren oder sonstige nicht zuordenbare User gibt es derzeit nicht. Die Abteilung LAD1-IT hat keinen Zugriff auf die Personaldaten, um zu prüfen ob ein Benutzer noch aktiver Bediensteter ist, pensioniert oder versetzt wurde. Selbst wenn ein Zugriff auf die Personaldaten möglich wäre, kann zentral nie jemand über Antritt eines allfälligen Resturlaubes oder allfällige unverzüglich zu setzende Maßnahmen Bescheid wissen. Eine dezentralisierte Userverwaltung ist daher auch aus diesem Grund die sinnvollste Variante. Ein Single Login ist für einige Anwendungen (Abteilung Wohnungsförderung) bereits im Einsatz. Beim eingesetzten Produkt Secure Login (passt am besten zu Novell) gibt es aber noch technische Probleme, sodass derzeit noch viele Bereiche - auch die Bezirkshauptmannschaften - fehlen. An einer Lösung wird seit längerem ohne durchschlagenden Erfolg gearbeitet. Mittlerweile gibt es aber von Sicherheitsexperten Warnungen vor derartigen Systemen, da dann eben alle Anwendungen offen sind, sobald eine Sperre überwunden ist. Möglicherweise ist eine sinnvolle Lösung daher erst mit Einsatz von Signaturkarten und eventuell biometrischen Merkmalen möglich. Zu diesem Thema wurde eine Arbeitsgruppe, beste-

hend aus Mitarbeitern der Abteilungen Landesamtsdirektion, Personalangelegenheiten und Gebäudeverwaltung sowie der Zentralpersonalvertretung eingesetzt.

NÖ Landesrechnungshof:

Die Stellungnahme wird teilweise zur Kenntnis genommen. Die Userverwaltung ist entsprechend den Vorgaben der Abteilung LAD1-IT vom jeweiligen IT-Koordinator durchzuführen, die Einhaltung dieser Vorgaben sollte jedoch durch die zuständigen Mitarbeiter der Abteilung LAD1-IT zumindest stichprobenweise überprüft werden.

9 Katastrophenvorsorge

In den Bezirkshauptmannschaften sind für den IT-Bereich keine schriftlichen Aufzeichnungen zur Katastrophenvorsorge vorhanden. Hier wäre es zielführend, zu definieren, welche Bereiche der IT-Landschaft in einem Katastrophenfall einsatzbereit sein müssen. Eine separate Stromversorgung mit eigenen Notstromleitungen wäre sicherlich nutzbringend.

Es wäre überlegenswert, zwischen den Bezirkshauptmannschaften und den zentralen Abteilungen ein Positionspapier zu verabschieden, in dem festgehalten wird, wer die jeweiligen Ansprechpersonen in einem IT-Katastrophenfall sind und welche Person, in einer vorgegebenen Reihenfolge, definierte Prozesse bzw. Handlungen auslöst. An Hand dieses Positionspapiers sollte fallweise auch eine Katastrophenübung durchgeführt werden.

Auch bei Ausfall einer größeren Anzahl von PC's sollte gewährleistet sein, dass der Betrieb in einer Bezirkshauptmannschaft nicht zusammenbricht. Daher wäre es sinnvoll, sich auch mit dem Thema der Verfügbarkeit von Hard- und Software auseinander zu setzen. Überlegungen, wie zB „… Wie lange kann ein Sachgebiet ohne IT-Infrastruktur seine Aufgaben ordnungsgemäß wahrnehmen? …" sollten hier einfließen. In diesem Zusammenhang wäre auch die Aufnahme der auf jedem Arbeitsplatz installierten Software für die Arbeit des IT-Koordinators hilfreich, um etwaige Nachinstallationen gleich vor Inbetriebnahme am jeweiligen Einsatzort durchführen zu können. Auch bei der Auflistung der Software kann es im Katastrophenfall nützlich sein, wenn eine Prioritätenreihung der Verfügbarkeit definiert ist. Mit diesen Themen haben sich zwar alle IT-Koordinatoren mehr oder weniger auseinander gesetzt, aber es gibt keine schriftliche Dokumentation.

Die Hoffnung, dass eine IT-Katastrophe nie eintreten wird, enthebt niemanden der Verantwortung sich damit aktiv auseinander zu setzen und die Verantwortlichen darauf aufmerksam zu machen. Die angestellten Überlegungen sollten niedergeschrieben und allen Bediensteten zugänglich gemacht werden, um im Ernstfall allen Bediensteten die Möglichkeit zu geben, den Schaden so gering wie möglich zu halten.

Ergebnis 11
Katastrophenvorsorge für die IT-Landschaft ist genauso wichtig, wie in den bereits definierten Bereichen und sollte Inhalt der bestehenden Katastrophenpläne sein.

Stellungnahme der NÖ Landesregierung:

Dem Thema der Katastrophenvorsorge für BH's wird große Bedeutung zugemessen. Entsprechende Aktivitäten wurden gesetzt. Wie vom NÖ Landesrechnungshof angemerkt, ist dies keinesfalls primär ein IT-Thema. Dass die bisherigen Aktivitäten erfolgreich waren, zeigt die Betriebsaufnahme auf der BH Tulln innerhalb von weniger als 12 Stunden nach ‚Brand aus'.

NÖ Landesrechnungshof:

Die Stellungnahme wird zur Kenntnis genommen.

St. Pölten, im Jänner 2005
Der Landesrechnungshofdirektor
Dr. Walter Schoiber