Landtag von Baden-Württemberg **Drucksache 15 / 3550**

15. Wahlperiode **29. 05. 2013**

Mitteilung

der Landesregierung

Bericht der Landesregierung zu einem Beschluss des Landtags; hier: Denkschrift 2009 des Rechnungshofs zur Haushalts- und Wirtschaftsführung des Landes Baden-Württemberg – Beitrag Nr. 4: IuK-Ausfallvorsorge für Großschadensfälle

Landtagsbeschluss

Der Landtag hat am 21. Juli 2011 folgenden Beschluss gefasst (Drucksache 15/225 Abschnitt II):

Die Landesregierung zu ersuchen,

1. auf der Grundlage des Beschlusses vom 17. Dezember 2009 (Drucksache 14/5304, Abschnitt II)

a) in einem Ressort übergreifenden Konzept die IuK-Strukturen und Fachverfahren, die für die Daseinsvorsorge der Bevölkerung und die Sicherstellung der öffentlichen Ordnung erforderlich sind, verbindlich festzulegen,

b) für diese IuK-Infrastrukturen und Fachverfahren in dem Ressort übergreifenden Konzept zu prüfen, ob die Ausfallvorsorge bereits ausreichend ist, und gegebenenfalls notwendige Verbesserungen einschließlich der hierfür erforderlichen Kosten darzustellen;

2. auf der Grundlage des Ressort übergreifenden Konzepts im Jahr 2012 eine Ressort übergreifende Übung zur IuK-Ausfallvorsorge durchzuführen, in die die Ergebnisse der Länderübergreifenden Krisenmanagementübung 2011 (LÜKEX) zum Ausfallszenario bei IT- und Kommunikationssystemen einbezogen werden;

3. dem Landtag über das Veranlasste bis 1. Juni 2013 zu berichten.

Eingegangen: 29. 05. 2013 / Ausgegeben: 06. 06. 2013

Bericht

Mit Schreiben vom 23. Mai 2013 Nr. I-0451.1 berichtet das Staatsministerium wie folgt:

Zu Ziffer 1 a) und b):

Die Landesregierung hat zur IuK-Ausfallvorsorge zuletzt am 30. Juni 2010 berichtet. Dabei wurden den Abgeordneten als Verschlusssache eingestufte Tabellen zur Ausfallvorsorge für Großschadensereignisse übermittelt. Im Folgenden wird anstelle von IuK für Informations- und Kommunikationstechnik synonym auch der heute gebräuchlichere Oberbegriff IT verwendet.

Die IT-Strukturen der Landesverwaltung befinden sich gerade auf dem Prüfstand und werden, auch unter Wirtschaftlichkeitsaspekten, neu gestaltet. Dies betrifft auch die IT-Strukturen und Fachverfahren, die für die Daseinsvorsorge der Bevölkerung und die Sicherstellung der öffentlichen Ordnung erforderlich sind. Die Landesregierung hat das Innenministerium und das Ministerium für Finanzen und Wirtschaft beauftragt, ein Grobkonzept zur IT-Neuordnung zu erarbeiten und mit den Ressorts abzustimmen. Darauf sollen weitere Maßnahmen aufbauen. Dazu wird die Landesregierung separat berichten.

Zu Ziffer 2:

Zu verschiedenen kritischen oder wichtigen Verfahren sowie zur Basis-Infrastruktur wurden in der Landesverwaltung Notfallübungen durchgeführt und Maßnahmen umgesetzt.

So wurden beispielsweise zweimal pro Jahr im Ausfallrechenzentrum Oberreichenbach Notfallübungen der Ressorts Finanzen und Wirtschaft, Justiz und Ländlicher Raum durchgeführt. Bei der Polizei wurden Anwendungen auf Server-Cluster übertragen, deren Geräte auf die zwei Standorte Informatikzentrum Landesverwaltung Baden-Württemberg (IZLBW) und Landeskriminalamt verteilt sind, sodass die Funktionalität im Notfall auch bei Ausfall eines Standorts weiter gegeben ist. Ressort übergreifend wurden beispielsweise die Maßnahmen zur Ausfallsicherheit des Landesverwaltungsnetzes, des Outsourcings der Bürokommunikation und der Stromversorgung im Ressort übergreifend tätigen IZLBW durchgeführt.

Die Landesverwaltung hat inzwischen vor allem in den IT-Zentren Informatikzentrum Landesverwaltung Baden-Württemberg (IZLBW) sowie Landeszentrum für Datenverarbeitung (LZfD) eine Reihe von technischen Maßnahmen für die Ausfallvorsorge umgesetzt. Wesentliche Maßnahmen werden nachfolgend aufgeführt:

- Die Stromversorgung für die Maschinensäle des IZLBW wurde komplett erneuert. Alle Komponenten werden zweifach über getrennte Stromkreise mit Strom versorgt. Für die Stromversorgung wurden vom Energieversorger zwei getrennte Hauszuführungen über unterschiedliche Umspannwerke realisiert.

  Entsprechendes gilt für das LZfD.

- Sollte die Stromversorgung des Energieversorgers ausfallen, kann der Betrieb des IZLBW durch leistungsfähige und redundant auslegte Diesel-Aggregate auch über einen längeren Zeitraum hin aufrechterhalten werden. Die Funktionsfähigkeit der Notstromversorgung wird monatlich durch Testläufe der Diesel-Aggregate überprüft. Im Jahr 2011 haben sich die Notsysteme zur Stromversorgung bei einem Stromausfall des Energieversorgers bewährt.

  Entsprechendes gilt für das LZfD.

- Wichtige Netzzugänge sind ebenfalls doppelt ausgelegt. Die Spanne reicht hierbei von doppelten Hauseinführungen in den Rechenzentren und großen Behörden (z. B. Ministerien oder Regierungspräsidien) bis hin zu Netzkopplungen etwa mit dem Koppelnetz der deutschen Verwaltung (Deutschland Online Infrastruktur) an zwei getrennten Standorten. Teilweise sind parallel Netzanbindungen über Glasfaser und Richtfunk realisiert worden. Im Jahr 2012 hat sich die doppelte Anbindung des Innenministeriums bei einem Netzausfall bewährt.

- Das Wissenschaftsnetz BelWü als Netzalternative für Ausfallsituationen (Backup-Verbindungen) im Landesverwaltungsnetz (LVN) wurde ebenfalls erfolgreich getestet und ist in die Planungen zur Ausfallsicherheit einbezogen.

- Das Glasfasernetz zur breitbandigen Vernetzung der großen Behördenzentren ist vielfach als Ringstruktur realisiert worden, wodurch sich Unterbrechungen einer Strecke kompensieren lassen. So wurden im Jahr 2012 und 2013 beispielsweise alle vier Regierungspräsidien redundant über getrennte Hauseinführungen an diese Ringstrukturen angeschlossen.

- Die Anbindung des LVN ans Internet erfolgt über BelWü. Zur Ausfallvorsorge erfolgt dies über getrennte Hauseinführungen in das IZLBW sowie über unterschiedliche Wegeführung.

- Alle zentralen Komponenten zur Kommunikation innerhalb des LVN und in andere Netze sind redundant ausgelegt (z. B. zentrale Firewall- und E-Mail-Systeme). Dies gilt gleichermaßen für alle zentralen Komponenten zur Benutzerverwaltung und zur Anmeldung der Benutzer an Fachverfahren und Anwendungen (z. B. Active Directory).

- Für kritische Verfahren und Kommunikationsdienste hat das IZLBW den Aufbau von Speicher- und Datensicherungssystemen an einem Standort außerhalb des eigenen Gebäudes begonnen (z. B. Datenspiegelung für die E-Mail-Systeme und Auslagerung von Backupdaten). Dabei wird darauf geachtet, den Freiraum für künftige Beschlüsse der Landesregierung zur IT-Bündelung nicht einzuengen. Auch das LZfD spiegelt Daten an einen anderen Standort oder lagert Daten aus.

- Darüber hinaus hat das IZLBW damit begonnen, angelehnt an den Standard 100-4 des Bundesamts für Sicherheit in der Informationstechnik (BSI) für die Ausfallvorsorge und das Notfallmanagement für sich als Rechenzentrum sowie die von ihm bereit gestellte und betriebene behördenübergreifende Infrastruktur eine Notfallorganisation aufzubauen und eine Gesamtkonzeption für Ausfallvorsorge und Notfallmanagement zu erstellen.

  Im Vorgriff auf dieses umfangreiche und komplexe Projekt hat das IZLBW 2011 einen sogenannten Betriebsleiter vom Dienst eingerichtet, der bei außergewöhnlichen Betriebsstörungen kurzfristig eine Task Force einberuft, die eine koordinierte und priorisierte Wiederherstellung des Normalbetriebs sicherstellt. Das Verfahren wurde inzwischen mit Kunden des IZLBW geübt und hat sich auch bei echten Störfällen bewährt.

  Entsprechendes gilt für das LZfD.

Auch beim BK-Outsourcing der Landesverwaltung, das derzeit rund 14.000 Bildschirmarbeitsplätze umfasst (Justiz flächendeckend im Land, das Wissenschaftsministerium und das Integrationsministerium) sind Maßnahmen zur Ausfallvorsorge umgesetzt worden, die den hardware-technischen Ausfall von zwei Hostrechnern ohne Performanceeinbußen überbrücken und die die Wiederherstellung der Daten auch bei großflächigen Ausfällen gewährleisten:

- Das Rechenzentrum des Auftragnehmers verfügt über eine redundante Auslegung der Strom-, Wasser-, Klimaversorgung sowie eine unterbrechungsfreie Stromversorgung und eine automatische Branderkennung bzw. Brandmeldung.

- Die Applikationen sind im Rechenzentrum auf einer virtualisierten Plattform mit zwölf Hostrechnern verteilt über zwei Brandabschnitte betrieben.

- Die Datenbanken und die Fileservices für die geschäftskritischen Anwendungen sind redundant über zwei Brandabschnitte gespiegelt.

- Die Datensicherung auf Band erfolgt auf ein zweites Rechenzentrum.

- Der Zugang erfolgt redundant über beide Rechenzentren.

Für den sicheren Betrieb des elektronischen Grundbuchs beim IZLBW im Auftrag der Justiz wurden die Vorgaben und Maßnahmen zur Ausfallvorsorge im Jahr 2012 im Rahmen von Notfallübungen auf ihre Belastbarkeit und Tauglichkeit überprüft:

- Serverwiederherstellung

  Es wurden 5 Serversysteme der Integrationsumgebung, darunter auch die beiden Datenbankserver des RAC-Clusters wiederhergestellt.

- Wiederherstellung der Produktiv-Datenbanken

  Die produktiven Datenbanken wurden zweimal in der Referenzumgebung wiederhergestellt.

- SAN-Speicher Spiegelungstest

  In der Referenzumgebung wurde ein Umschalttest auf das Spiegel-Speichersystem und ein Rückschalttest auf das Original-Speichersystem durchgeführt.

Die Tests belegen, dass die im Rechenzentrum betriebenen Verfahren zur Sicherung und Wiederherstellung von Servern, Datenbanken und Speichern des Elektronischen Grundbuchs in hohem Maße verlässlich sind.

Bei den Justizvollzugsanstalten ist inzwischen die hohe Verfügbarkeit der IT-Verfahren – notwendigerweise in einem 7 d x 24 h-Betrieb – für die sichere Abwicklung der Aufgaben (z. B. auch Verwaltung der Besuche und der Entlassungen bzw. Verschubungen von Gefangenen) unabdingbar geworden.

Um diese Anforderung wirtschaftlich umzusetzen, sind folgende zusätzlichen Maßnahmen im Rahmen des BK-Outsourcing Projektes der Justiz umgesetzt:

- Bereithaltung von jederzeit verfügbaren Ersatzgeräten (Hot Standby-Geräte) an strategisch wichtigen Stellen wie z. B. Torwache oder Sicherheitszentrale,

- Notstromversorgung vor Ort,

- automatische Erstellung und Übermittlung (regelmäßig nachts) von Notfalllisten im Format PDF auf die lokalen Festplatten der o. g. Hot Standby-Geräte. Diese Notfalllisten enthalten alle für einen geordneten Betrieb relevanten Daten der Justizvollzugsanstalt und deren Insassen. Die Übermittlung der Notfalllisten wird protokolliert, die Protokolle gehen per E-Mail an eine Koordinierungs-Stelle der Justiz. Diese Koordinierungs-Stelle kontrolliert und überwacht die Protokolle, Abweichungen werden je nach Fehlerfall an die betroffene Justizvollzugsanstalt und den Auftragnehmer gemeldet,

- pro angefangene 50 Arbeitsplätze je Lokation wird zum raschen Austausch auch außerhalb der normalen Arbeitszeiten ein Bildschirmarbeitsplatz (Monitor, Desktop, Notebook, Drucker) vor Ort auf Lager vorgehalten. Diese können im Bedarfsfall durch festgelegte Funktionsträger in der Justizvollzugsanstalt unverzüglich in Betrieb genommen werden.

Die Tauglichkeit dieser Maßnahmen wurde – unfreiwillig – im Zuge großflächiger Netzausfälle durch Bau- bzw. Elektroarbeiten bestätigt.

Mit diesen Maßnahmen in unterschiedlichen Bereichen der Landesverwaltung sind die wesentlichen auch in den unter Nr. 1 genannten Tabellen angesprochenen Komponenten der Basis-Infrastruktur abgedeckt. Für die IT-Fachverfahren wird im Zuge der IT-Neuordnung in den Jahren 2014 ff. eine neue Bewertung anstehen.

Die Landesverwaltung hat außerdem mit einer Rahmenleitungsgruppe an der Länderübergreifenden Krisenmanagementübung LÜKEX 2011 teilgenommen und ausgewählte Unternehmen der Kritischen Infrastruktur (KRITIS) dabei eingebunden. Eine wichtige Erkenntnis aus dieser Übung ist, dass die Verzahnung zwischen IT und Katastrophenschutz zunehmend an Bedeutung gewinnt. Hierzu gehört auch die Sensibilisierung und der Erfahrungsaustausch zu Fragen der IT-Sicherheit mit Unternehmen der Kritischen Infrastruktur. Zu diesem Themenkomplex wurde in der Länderoffenen AG Cybersicherheit des Arbeitskreises II der Innenministerkonferenz ein Leitfaden entwickelt, der jetzt bei gemeinsamen Gesprächen von Katastrophenschutz und IT-Sicherheitsbeauftragten mit den Unternehmen zum Einsatz kommen soll.