

22.06.2021

Antrag

der Fraktion BÜNDNIS 90/DIE GRÜNEN

Das Landesverwaltungsnetz weiterentwickeln, um der steigenden Bedeutung digitaler Verwaltungsprozesse gerecht zu bleiben

I. Ausgangslage:

Jedes Bundesland in Deutschland verfügt über ein Verwaltungsnetz. In Nordrhein-Westfalen (und Baden-Württemberg) wird dieses „Landesverwaltungsnetz“ genannt. Diese Netze sind jeweils ein vom Internet unabhängiges Intranet der Verwaltungen. Die Beschäftigten der Verwaltungen können darüber Videokonferenzen abhalten, Daten speichern und auf andere zugreifen, Formulare ausfüllen und viele weitere Vorgänge erledigen, ob in den Behörden und Einrichtungen oder vom Telearbeitsplatz aus. Diese Netze bilden so die grundlegende Infrastruktur für die digitale Verwaltungskommunikation im Land¹.

Das Landesverwaltungsnetz NRW besteht seit über 20 Jahren. Es wird vor allem vom Landesbetrieb IT.NRW bereitgestellt, der es als seine „wichtigste Infrastrukturleistung“ bezeichnet. „Diese Verbindung aller Behörden und Einrichtungen schafft die technische Basis für die Digitalisierung der Verwaltung in NRW“. Innerhalb des Landesverwaltungsnetzes bietet der Landesbetrieb weitere Infrastrukturleistungen an: Bereitstellung von Speicherplatz, regelmäßige Sicherungen und Langzeitspeicherung, Sekundärspeicher und Katastrophenfallsicherungen.²

Laut Bericht der Landesregierung vom 8. März 2021 (Vorlage 17/4780) ist „der Betrieb des Landesverwaltungsnetzes (LVN) (...) als hoheitliche Aufgabe dem Landesbetrieb IT.NRW sowie den Sondernetzbetreibern (Landesamt für Zentrale Polizeiliche Dienste, Rechenzentrum der Finanzverwaltung) übertragen. (...) Der Vorteil liegt in einem abgegrenzten technischen Rahmen, der unbeeinflusst von äußeren Einflüssen auch in Krisensituationen eine stabile und leistungsfähige Verwaltungsplattform bietet. Das Vorgehen hat sich in mehr als zwei Jahrzehnten als äußerst zuverlässig und flexibel skalierbar erwiesen“.

Das Landesverwaltungsnetz ist Teil der kritischen Infrastruktur des Landes, an den sich ohnehin hohe Anforderungen der Sicherheit und Funktionsfähigkeit stellen. Je mehr Verwaltungsprozesse digitalisiert werden, desto höher werden die Anforderungen.

In den nächsten Jahren werden entsprechend dem Onlinezugangsgesetz alle Verwaltungsleistungen des Bundes, der Länder und der Kommunen für Bürgerinnen und

¹ Die Kommunikation mit den Verwaltungsstrukturen von Bund, anderen Bundesländern und Kommunen erfolgt über das vom Landesnetz unabhängige Verbindungsnetz (vgl. Vorlage 17/4780).

² Vgl. <https://www.it.nrw/digitale-infrastruktur-fuer-das-land-nrw>

Bürger sowie Unternehmen online möglich sein – damit verknüpft auch die Leistungen der Europäischen Union und derjenigen EU-Staaten, die die technische Anbindung geschaffen haben. Hinzu kommen dafür notwendige, flankierende und weitere Digitalisierungsprozesse der Verwaltungen von Land, Kommunen und anderen öffentlichen Einrichtungen gemäß dem E-Government-Gesetz Nordrhein-Westfalen. Damit diese Leistungen verlässlich zur Verfügung stehen, werden unter anderem höchste Anforderungen bezüglich Verfügbarkeit und Stabilität, Übertragungsgeschwindigkeit und IT-Sicherheit an das Landesverwaltungsgesetz gestellt.

Am 20. April 2021 meldeten Nachrichtenagenturen und Medien, dass laut Landesbetrieb Information und Technik das Landesverwaltungsnetz seit dem Abend des Vortags erheblich gestört sei. Das Innenministerium, der für IT-Dienstleistungen zuständige Landesbetrieb IT.NRW und 30 Einrichtungen im Zuständigkeitsbereich des Justizministeriums hätten Probleme gehabt, auf Daten zuzugreifen oder online-Anwendungen auszuführen. Eine Analyse, welche Verfahren und Landesbehörden alle betroffen seien, gab es zu dem Zeitpunkt noch nicht. Auch sei noch nicht klar, in welchem Zuständigkeitsbereich genau die Störung läge. Laut Nachrichtenagenturen und Medien sei das Problem an einer wichtigen Telekommunikationsverbindung am Morgen des 21. April behoben worden. Das Landesverwaltungsnetz arbeite seitdem wieder störungsfrei.³

In der Fragestunde des Plenums am 28. April 2021 (Plenarprotokoll 17/125), anlässlich der Mündlichen Anfrage des Abgeordneten Matthi Bolte-Richter (Bündnis 90/Die Grünen), und zur Sitzung des Ausschusses für Digitalisierung und Innovation am 6. Mai 2021 (Vorlage 17/5168), anlässlich einer Berichts-anfrage der Fraktion Bündnis 90/Die Grünen, erläuterte der zuständige Minister Prof. Dr. Pinkwart einige Details zur Lage.

Demnach wurde das Problem am 19. April von den automatischen Überwachungssystemen erkannt. Insgesamt wären 47 angemietete Netzwerkleitungen gestört gewesen. Diese Störung hätte zu einem Fehler in einer zentralen Netzwerkkomponente bei IT.NRW geführt. Das Redundanzsystem hätte in Folge der Leitungsstörung eine Fehlfunktion gehabt, die zu Folgestörungen geführt habe, auch wenn die genaue Ursache nicht abschließend festgestellt werden konnte. Daher hätten 40 der 371 angeschlossenen Einrichtungen und Behörden teilweise oder gänzlich nicht auf das Landesverwaltungsnetz zugreifen können. Betroffen wären zwei Bezirksregierungen, der Bau- und Liegenschaftsbetrieb sowie weitere Landesbetriebe, mehrere Hochschulen und Studierendenwerke, das Justizministerium und mehrere Gerichte. Die Verbindung zum Internet und Dienste wie E-Mails, Videokonferenzen und Fernzugriff aus dem Homeoffice seien teilweise gestört gewesen. Dies hätte zu einer indirekten Störung geführt, bei der eine größere Zahl von Meldungen von Coronafallzahlen letztlich mit Verzug übermittelt wurde.

Störungen dieser Größenordnung seien sehr selten. Die detaillierte Analyse der Störungen wäre zu den Berichtszeitpunkten noch nicht abgeschlossen gewesen. Dazu gehörten Überprüfungen der Redundanzmechanismen und der organisatorischen Abläufe bei IT.NRW zur Fehleranalyse und -behebung sowie Informationsweitergabe. Aufgefallen sei, dass ein Teil der dezentralen Redundanzsysteme von Ministerien und Behörden funktioniert habe, ein anderer Teil nicht. So hätten drei Ministerien sofort auf Richtfunkssysteme umschalten können, während dies beim Justizministerium nicht automatisch funktioniert habe. Dem würde nachgegangen und Verbesserungen in Aussicht gestellt. Die zuvor fehlerhafte Netzwerkkomponente werde bereits umgebaut und erhalte eine neue Software.

³ Vgl. bspw. <https://www.zeit.de/news/2021-04/20/stoerungen-nrw-corona-daten-am-dienstag-unvollstaendig> und <https://www.zeit.de/news/2021-04/21/nach-stoerung-system-neustart-im-landesverwaltungsnetz>.

Der Einsatz und die Funktionsfähigkeit von Redundanzen spielt auch im Zusammenhang mit IT-Sicherheit eine Rolle. Laut Bericht der Landesregierung „Informationssicherheit in der Landesverwaltung NRW – Sicherheit der IT-Systeme“ vom 8. März 2021 (Vorlage 17/4780) ist „nach Einschätzung des Bundesamtes für Sicherheit in der Informationstechnik (BSI) und des landeseigenen Computer Emergency Response Teams (CERT NRW) die Gefährdungslage als „Hoch“ einzuschätzen. Das bedeutet, dass jederzeit mit wirkungsvollen Cyberangriffen auf die staatlichen Institutionen und Einrichtungen des Landes zu rechnen ist. (...) Meist gelingt eine Verhinderung oder eine Abschwächung (Mitigation) des Angriffs. Für den Fall des Versagens aller Maßnahmen sind Notfallkonzepte erforderlich, die die zügige Wiederherstellung des ungestörten Betriebszustands ermöglichen“. Weiter heißt es: „Trotz aller zentralen Maßnahmen gelangt Schadsoftware in das Landesverwaltungsnetz (LVN). (...) In einem solchen Fall werden lokale Maßnahmen in den Behörden aktiv, um eine Infektion zu stoppen und Schäden zu verhindern oder jedenfalls zu begrenzen“.

Der Leiter des Hochschulrechenzentrums an der Goethe-Universität Frankfurt und der Informationssicherheits-Koordinator der Fraunhofer-Gesellschaft führen in einem Beitrag zur IT-Sicherheit von wissenschaftlichen Einrichtungen an, dass „sichergestellt sein [muss], dass kritische Systeme so redundant betrieben werden, dass sie im Angriffsfall möglichst ohne Unterbrechung weiterlaufen können“⁴. Für die staatsunmittelbare Verwaltung gilt die Erfordernis umso mehr, dass kritische Systeme auch im Fall eines Cyberangriffs so gut wie möglich weiterlaufen müssen.

II. Der Landtag stellt fest:

- Das Landesverwaltungsnetz ist Teil der kritischen Infrastruktur, an den sich ohnehin hohe Anforderungen der Sicherheit und Funktionsfähigkeit stellen. Je wichtiger digitale Verwaltungsprozesse werden, desto höher werden die Anforderungen. Manchmal sind Störungen unvermeidbar, aber weitgehend können sie durch professionelles und kontinuierlich geschultes Personal, aktuell gehaltene Technik und strukturierte Sicherheitsprozesse verhindert werden.
- Dabei kann und muss aus Problemen und Fehlern gelernt werden. Eine Analyse der genaueren Gründe, die zu einer Störung geführt haben, und die Suche nach Lösungen für ein stabileres und sichereres Landesverwaltungsnetz müssen auf einer sachlichen Ebene geführt werden. Eine sachgerechte Weiterentwicklung des Landesverwaltungsnetzes und der damit verbundenen Prozesse und Kapazitäten muss unter Einbeziehung von IT-Expertinnen und -Experten erfolgen und darf keine rein politische Debatte sein.
- IT-Sicherheit und -Redundanz müssen nicht nur erkauf und installiert werden, sie müssen auch eingeübt und dauerhaft aufrecht erhalten werden. Regelmäßige Tests und Übungen sind wichtig, damit ein Problem bei auftretender Krise kleingehalten werden kann und die zuständigen Stellen in der Krise schnell wieder vor die Lage kommen, statt durch sie getrieben zu werden. Dazu gehört eine konstruktive und offene Feedback-Kultur. Nur so kann eine Diskrepanz zwischen technisch theoretischer und funktionaler Redundanz ausgeschlossen werden.
- Es ist selbstverständlich, dass eine Weiterentwicklung des Landesverwaltungsnetzes Zeit, Ressourcen und erfahrenes Personal benötigt.

III. Der Landtag beschließt:

1. Die Landesregierung wird gebeten, dem Landtag eine detaillierte Analyse der Störung am Landesverwaltungsnetz vom 19. bis 21. April 2021 vorzulegen und konkrete

⁴ Vgl. <https://www.forschung-und-lehre.de/management/wie-it-sicherheit-an-hochschulen-gelingt-3292/>

Lösungsvorschläge aufzuzeigen, mit denen die spezifische Störung künftig bestmöglich vermieden werden kann, und welche Maßnahmen gegebenenfalls bereits umgesetzt wurden.

2. Die Landesregierung wird gebeten, zur Weiterentwicklung von Sicherheit und Funktionsfähigkeit des Landesverwaltungsnetzes zu prüfen und entsprechende Maßnahmen vorzunehmen:
 - a. Wie Auswirkungen durch Ausfälle von angemieteten Netzwerkleitungen möglichst vermieden werden können.
 - b. Welche Möglichkeiten es gibt, das Information Security Management System und das Business Continuity Management zu verbessern.
 - c. Wie die Reaktionszeit für künftige Störungen verbessert werden kann. Dazu gehören eine Überprüfung der Besetzung des Notbetriebs, des Systems für Störmeldungen, des Providermanagements sowie der Prozesse und Verträge mit den Dienstleistern.
 - d. Ob ein Mangel an Ressourcen jedweder Art an neuralgischen Stellen mögliche Probleme und Ausfälle provoziert.
 - e. An welchen Stellen zusätzliche Redundanzen aufgebaut oder bestehende weiterentwickelt bzw. ersetzt werden müssen und wie funktional mehr dezentrale Redundanzen sein können.
 - f. Ob künftig häufiger nach Systemaufbau, -erweiterungen oder -änderungen harte Redundanztests und darüber hinaus auch regelmäßige Redundanztests durchgeführt werden müssen.
 - g. Inwiefern auch an indirekt betroffenen Systemteilen Verbesserungen sinnvoll oder notwendig sind.
 - h. Welches Verbesserungspotenzial es bei der Feedback-Kultur in der Landesverwaltung gibt.
3. Die Landesregierung wird darüber hinaus gebeten, zu prüfen, bei welchen Prozessen der Landesverwaltung, oder solchen zwischen kommunaler und Landesebene, eine automatische Datenübertragung via Software-Schnittstellen sinnvollerweise die händische Übertragung per E-Mail oder Webportal ersetzen kann, und entsprechende Maßnahmen vorzunehmen.

Josefine Paul
Verena Schäffer
Mehrdad Mostofizadeh
Matthi Bolte-Richter

und Fraktion