



HESSISCHER LANDTAG

25. 10. 2024

Kleine Anfrage

Oliver Stirböck (Freie Demokraten) vom 19.06.2024

Ausfälle von Rechenzentren und deren Auswirkungen

und

Antwort

Ministerin für Digitalisierung und Innovation

Vorbemerkung Fragesteller:

Am 14. Mai 2024 kam es im Landkreis Fulda zu einem signifikanten Ausfall des Internets, der viele Bürger, Unternehmen und öffentliche Einrichtungen beeinträchtigte und etwa dreieinhalb Stunden andauerte. Dieser Vorfall wurde durch einen Stromausfall in einem Frankfurter Rechenzentrum am Frankfurter Osthafen ausgelöst. Ursache war laut Medienberichten die Unterbrechung der Energieversorgung im Rechenzentrum. Generatoren sind nicht sofort angesprungen, was zu einem Verlust der kritischen Lasten und einem Ausfall der IT-Infrastruktur führte. Der Ausfall hatte spürbare Auswirkungen auf die öffentlichen Dienste und das tägliche Leben. Schulen und zahlreiche Arbeitsplätze, insbesondere im Home-Office, waren betroffen. Bürgerdienste, wie die Online-Terminvergabe, waren vorübergehend nicht erreichbar, was zu zahlreichen Anrufen bei den Behörden führte. Des Weiteren war es nicht möglich, Zahlungen per EC-Karte durchzuführen. Interessanterweise waren nicht alle Dienste gleich betroffen. Einige kommunale Anwendungen, die direkte Verbindungen zu anderen Rechenzentren hatten, funktionierten weiterhin ohne Unterbrechung, während andere ohne diese redundanten Verbindungen ausfielen. Der Vorfall zeigt die Bedeutung einer robusten und redundanten digitalen Infrastruktur und offenbart die Abhängigkeit von zentralisierten Diensten in einer vernetzten Gesellschaft. Es ist daher dringend notwendig vorhandene Notfallpläne und die Infrastruktursicherheit zu verbessern, um in ähnlichen Fällen künftig schneller darauf reagieren zu können.

Vorbemerkung Ministerin für Digitalisierung und Innovation:

Die Verwaltung des Landkreises Fulda verfügt über zwei angemietete Leitungen, die über einen Provider ins Kreishaus führen und damit über eine Redundanz, die sie mit den Rechenzentren verbindet. Am 14. Mai 2024 war nach dem Ausfall einer der beiden Leitungen der Redundanzweg über die zweite Leitung bis zum Provider verfügbar; dieser wiederum hatte jedoch auf einem Verbindungsweg ins Rechenzentrum Frankfurt ebenfalls einen technischen Defekt. Aufgrund dieses Defektes vom Provider zum Rechenzentrum gab es letztlich auf der Gesamtstrecke eine „Lücke“, was zu dem angesprochenen Ausfall von Internetdiensten führte. Anzumerken ist jedoch, dass die kommunalen Anwendungen der ekom21 (kommunales IT-Dienstleistungsunternehmen) in dem betreffenden Zeitraum weiterhin durch die Verwaltung genutzt werden konnten.

Diese Vorbemerkungen vorangestellt, beantworte ich die Kleine Anfrage im Einvernehmen mit dem Minister des Innern, für Sicherheit und Heimatschutz wie folgt:

Frage 1 Welche Informationen liegen der Landesregierung bezgl. der Ursachen und Auswirkungen des Internetausfalls in Hessen vor?

Der Landesregierung liegen über die der Presseberichterstattung sowie der Vorbemerkung zu entnehmenden Informationen hinaus keine weiteren vor.

Frage 2 Wie oft kam es in den letzten fünf Jahren nach Informationen der Landesregierung zu ähnlichen Ereignissen?

Die Landesregierung führt über derartige Ereignisse keine gesonderten Erhebungen. In einer Befragung des amerikanischen Uptime-Institutes gaben mehr als die Hälfte der beteiligten Rechenzentrumsbetreiber (55 Prozent) an, in den vergangenen drei Jahren einen Ausfall erlitten zu haben. Nur einer von zehn Ausfällen sei hierbei als schwerwiegend oder kritisch eingeordnet worden. Die Ursache lag in der Mehrzahl der Fälle im Bereich der Stromversorgung.

Frage 3 Welche präventiven Schritte will die Landesregierung ergreifen, um solche Ausfälle zu verhindern?

Die Landesregierung verfügt weder über die finanziellen Mittel noch über die gesetzlichen bzw. technischen Möglichkeiten, derartige Ausfälle in Zukunft verhindern zu können. Dies liegt vorrangig in der Zuständigkeit der Telekommunikationsunternehmen, der Rechenzentrumsbetreiber sowie anderer, vorrangig privatwirtschaftlicher Akteurinnen und Akteure. Gleichwohl können die verschiedenen Ebenen von EU, Bund und Ländern Regelungen treffen, welche einen Beitrag zu einer resilienten IT-Infrastruktur leisten.

Frage 4 Wie bewertete die Landesregierung die Kommunikationsstrategie der beteiligten Akteure mit Bürgern und Unternehmen während des Internetausfalls?

Die Landesregierung hat keine Kenntnisse darüber, welche Kommunikationsstrategien die einzelnen Akteurinnen und Akteure für solche Fälle konzipiert haben bzw. verfolgen. Eine solche Strategie muss in jedem Falle dazu beitragen, sehr rasch Klarheit über Ursachen, Auswirkungen sowie die voraussichtliche zeitliche Dauer breit zu vermitteln. Dies ist ein entscheidender Beitrag dafür, dass die zuständigen Institutionen und Ansprechpartner schnell Gegenmaßnahmen ergreifen können.

Frage 5 Welche Schritte unternimmt die Regierung, um sicherzustellen, dass Rechenzentren als Teil der kritischen Infrastruktur besser geschützt sind?

Der Schutz von Rechenzentren erfolgt regelmäßig nach einem multidimensionalen Ansatz auf Grundlage einer ausführlichen Risikoanalyse, welcher z. B. physische Barrieren gegen das unbefugte Eindringen, aber auch bauliche und weitere technische Maßnahmen wie Brandmelde- und Löschtechnik, Sicherheits- und Zutrittssysteme oder die Energieversorgung umfasst, bspw. die Installation eines Überspannungsschutzes und einer entsprechenden Notstromversorgung. Eine Handlungsnotwendigkeit i. e. S. besteht in diesem Feld für die Landesregierung — mit Ausnahme der landeseigenen Rechenzentren — nicht.

Dem Schutz der (Grund-)Versorgung vor Ausfällen, der Krisenvorsorge und der Krisenbewältigung kommt in der Landesregierung hohe Bedeutung zu. Primär sind die Betreiber der Kritischen Infrastruktur (KRITIS) für die Erbringung der Infrastrukturleistungen zuständig und verantwortlich. Der Landesregierung ist es aber auch ein besonderes Anliegen, einen Beitrag zu leisten, die bestmöglichen Bedingungen für den Erhalt der Funktions- und Versorgungsfähigkeit der KRITIS in Hessen zu gewährleisten. Hierzu stehen die einzelnen, für die jeweiligen KRITIS-Bereiche zuständigen Ressorts in regelmäßigem Austausch mit den KRITIS-Betreibern und deren Branchenvertretungen.

Um über eine einheitliche Informationsbasis zur Sicherstellung der Funktionsfähigkeit und Versorgungssicherheit der KRITIS zu verfügen, wird die KRITIS-Lageentwicklung kontinuierlich bewertet und hinsichtlich zukünftiger Veränderungen prognostiziert. Die Landesverwaltung erstellt hierzu regelmäßig ein Lagebild-KRITIS, in das auch Informationen der KRITIS-Betreiber einfließen.

Der Sektor „Informationstechnik und Telekommunikation“ bildet einen von insgesamt elf Sektoren der KRITIS in Hessen. Mit Blick auf den Schutz der KRITIS „Rechenzentrum“ ist anzumerken, dass ein erheblicher Teil der Rechenzentren in Hessen nicht nur für die Versorgungssicherheit in Hessen, sondern auch deutschlandweit und mitunter international eine wesentliche Schlüssel-funktion einnehmen. So betreiben mehrere global agierende Konzerne rund um den Internetknoten Frankfurt am Main Rechenzentren. Daher stimmt sich die Landesregierung auch eng mit dem Bund bei der Koordination der notwendigen Maßnahmen zum Schutz dieser KRITIS ab.

Frage 6 In welcher Weise stellt die Landesregierung sicher, dass diesbezügliche Notfallpläne aktuell und praktikabel sind?

Die Landesregierung verfügt weder über die finanziellen Kapazitäten noch die personellen Möglichkeiten, Beratungsleistungen für private Rechenzentrumsbetreiber im Hinblick auf Notfallpläne zu erbringen. Dies ist nach Auffassung der Landesregierung auch nicht erforderlich, da Betreiber im Regelfall u. a. über entsprechende Notfallpläne, ein Business Continuity Management System (BCMS) oder ein Informations-Sicherheitsmanagement-System (ISMS) verfügen.

Frage 7 Inwieweit sind Redundanzen in der Stromversorgung für kritische Einrichtungen wie Rechenzentren vorgeschrieben?

In rechtlicher Hinsicht wird beim KRITIS-Schutz in Deutschland der Ansatz verfolgt, die Regulierung von Schutzvorkehrungen, Krisenvorbereitungsmaßnahmen und Krisenreaktionsmechanismen innerhalb des für die einzelne KRITIS-Branche einschlägigen Fachrechtes zu realisieren. Daher existiert in Deutschland kein zentrales KRITIS-Gesetz, sondern der KRITIS-Schutz ist integraler Bestandteil der sektor- bzw. branchenspezifischen Regulierung. Hierdurch ist es möglich, den zwischen den einzelnen KRITIS-Bereichen unterschiedlichen Eigenschaften, Bedingungen und Leistungsstrukturen gerecht zu werden.

Für die Mehrheit der KRITIS-Bereiche existieren keine dezidierten Anforderungen an Redundanzen der Stromversorgung. In einigen KRITIS-Bereichen haben Betreiber aus Eigenantrieb heraus und freiwillig Notstromausstattungen eingerichtet. Vereinzelt werden in bestimmten KRITIS-Bereichen Notstromvorrichtungen staatlicherseits gefördert.

Gemäß § 8a Abs. 1 Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSIG) vom 14. August 2009 (BGBl. I S. 2821), zuletzt geändert durch Art. 12 des Gesetzes zur Regelung des Datenschutzes und des Schutzes der Privatsphäre in der Telekommunikation und bei Telemedien vom 23. Juni 2021 (BGBl. I S. 1982), sind Betreiber Kritischer Infrastrukturen verpflichtet, angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen maßgeblich sind. Dabei soll der Stand der Technik eingehalten werden. Organisatorische und technische Vorkehrungen sind angemessen, wenn der dafür erforderliche Aufwand nicht außer Verhältnis zu den Folgen eines Ausfalls oder einer Beeinträchtigung der betroffenen Kritischen Infrastruktur steht. Der Nachweis für die Erfüllung der Anforderungen kann von den betroffenen Betreibern durch Sicherheitsaudits, Prüfungen oder Zertifizierungen erfolgen (§ 8a Abs. 3 Satz 2 BSIG).

Die Abgrenzung des Geltungsbereiches erfolgt hierbei entlang der Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSIG (BSI-KritisV). Für den Geltungsbereich des Telekommunikationsgesetzes (TKG) formulieren § 165 ff. TKG ebenfalls Sicherheitsanforderungen.

Betreiber Kritischer Infrastrukturen und ihre Branchenverbände können auch branchenspezifische Sicherheitsstandards zur Gewährleistung der Anforderungen vorschlagen, wobei das Bundesamt für Sicherheit in der Informationstechnik (BSI) auf Antrag feststellt, ob diese geeignet sind, die entsprechenden Anforderungen zu gewährleisten (§ 8a Abs. 2 Satz 1 und 2 BSIG). Für den hier angesprochenen Bereich existiert ein branchenspezifischer Sicherheitsstandard (B3S) für Housing, Hosting und Content Delivery Netzwerke. Darin sind auch Handlungsempfehlungen zur Vorfallerkennung und -bearbeitung oder Energieversorgung enthalten, z. B. zu Netzersatzanlagen oder dem Aufbau der Energieverteilung.

Mit dem geplanten Gesetz zur Umsetzung der Richtlinie des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie) und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung (NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz) sind Präzisierungen, Ausweitungen und Umgliederungen der entsprechenden gesetzlichen Bestimmungen zu erwarten.

Des Weiteren ist das sog. IT-Grundschutz-Kompendium des BSI zu erwähnen, das nach eigenen Angaben Themen und Entwicklungen in der Informationssicherheit behandelt und hieraus praktische Sicherheitsempfehlungen ableitet. In dem entsprechenden Abschnitt werden der Einsatz einer unterbrechungsfreien Stromversorgung (USV), deren ausreichend Dimensionierung sowie ihre regelmäßige Wartung als zwingend bewertet.

Das BSI hat zudem im vergangenen Jahr Handlungsempfehlungen zu baulich-technischen Maßnahmen für Rechenzentren mit erhöhtem Verfügbarkeitsbedarf („RZ-Verfügbarkeitsmaßnahmen“) veröffentlicht, die ausdrücklich auch auf Aspekte wie Netzersatzanlagen und USV eingehen.

Jenseits der unmittelbaren gesetzlichen Anforderungen bestehen für Betreiber auch vielfältige Auditierungs- und Zertifizierungsmöglichkeiten (z. B. DIN EN 50600, DIN EN 62040 oder ISO 27001), um die technischen Gegebenheiten entlang der spezifischen Voraussetzungen der jeweiligen Norm objektiv zu dokumentieren und gegenüber Kundenanforderungen transparent zu machen.

Frage 8 Welche Unterstützung bietet die Landesregierung Bildungseinrichtungen und Behörden, um Ausfallzeiten zu minimieren?

Die Ursachen für solche Vorkommnisse entziehen sich im Regelfall dem Verantwortungsbereich der Landesregierung wie auch dem der Bildungseinrichtungen und Behörden. Dies gilt gleichermaßen für Bemühungen der Beseitigung dieser Ursachen zwecks Verkürzung der Ausfallzeiten. Daher werden keine gesonderten Unterstützungsleistungen vorgesehen. Der Umgang liegt in der Eigenverantwortung der Netzdienstleistungen oder ähnlich nutzenden Stelle. Für etwaige Fälle sind, soweit erforderlich, dort eigene Vorkehrungen und Konzepte auszuarbeiten.

Frage 9. Welche Schätzungen gibt es zu den wirtschaftlichen Auswirkungen solcher Ausfälle?

Aussagen hierzu sind aufgrund der Komplexität des Untersuchungsgegenstandes nur schwierig möglich. So ging z. B. die Schätzung eines mittlerweile nicht mehr am Markt tätigen VPN-Anbieters (virtual private network) bereits vor einigen Jahren davon aus, dass ein 24-stündiger totaler Internetausfall weltweit Umsatzausfälle von ca. 43 Mrd. US-Dollar verursachen könnte. Auf Deutschland würden demnach rund 1,5 Mrd. US-Dollar entfallen. Im Hinblick auf die wachsende Verflechtung globaler Daten- und Warenströme ist, trotz eines steigenden Risikobewusstseins für die Belastbarkeit von Lieferketten und vor dem Hintergrund der globalen politischen Lage, davon auszugehen, dass dieser Wert mittlerweile deutlich höher liegen dürfte.

Frage 10 Welche konkreten Maßnahmen ergreift die Landesregierung, um die Mitarbeiterinnen und Mitarbeiter im Landesdienst bezgl. des Umgangs mit solchen Ausfällen zu schulen?

Für schwerwiegende ressortübergreifende IT-Sicherheitsvorfälle, z. B. durch Ausfälle im Rechenzentrum, wurde in der hessischen Landesverwaltung das IT-Krisenmanagement etabliert und IT-Krisenmanager in den Ressorts benannt. Die Strukturen wurden im Rahmen der Länderübergreifenden Krisenmanagementübung (LÜKEX) 2023 getestet und werden derzeit evaluiert — konkret wurde auch die Bewältigung von (Teil-) Ausfällen von Rechenzentren und die damit verbundenen Maßnahmen zum geordneten Wiederanlaufen der Systeme trainiert.

Im Rahmen des IT-Notfallmanagements bzw. IT-Krisenmanagements finden im Ministerium des Innern, für Sicherheit und Heimatschutz regelmäßig Übungen und Workshops statt. Die mit IT-Sicherheitsvorfällen befassten Mitarbeiterinnen und Mitarbeiter werden praxisnah auch im Umgang mit Ausfällen im Rechenzentrum geschult, so fand bspw. ein „Stromausfall-Workshop“ statt.

Wiesbaden, 18. Oktober 2024

In Vertretung:
Stefan Sauer