



Ministerium der Justiz Nordrhein-Westfalen, 40190 Düsseldorf

Seite 1 von 1

02.09.2024

Präsident des Landtags  
Nordrhein-Westfalen  
Herrn André Kuper MdL  
Platz des Landtags 1  
40221 Düsseldorf

Aktenzeichen  
1500-  
IT.94/Störungsmanagement  
bei Antwort bitte angeben

für die Mitglieder  
des Rechtsausschusses

Bearbeiter: Herr  
Dr. Höckelmann  
Telefon: 0211 8792-209

#### **44. Sitzung des Rechtsausschusses des Landtags Nordrhein-Westfalen am 04. September 2024**

Bericht zu „Großstörung im Rechenzentrum in Münster – kann die gesamte Justiz in NRW wirklich durch einen simplen Stromausfall lahmgelegt werden?“

#### **Anlage:**

- 1 Bericht -

Sehr geehrter Herr Landtagspräsident,

zur Information der Mitglieder des Rechtsausschusses übersende ich als Anlage einen öffentlichen Bericht zu dem oben genannten Berichtswunsch.

Mit freundlichen Grüßen

Dr. Benjamin Limbach

Dienstgebäude und  
Lieferanschrift:  
Martin-Luther-Platz 40  
40212 Düsseldorf  
Telefon: 0211 8792-0  
Telefax: 0211 8792-456  
poststelle@jm.nrw.de  
www.justiz.nrw





## Ministerium der Justiz des Landes Nordrhein-Westfalen

44. Sitzung des Rechtsausschusses  
des Landtags Nordrhein-Westfalen  
am 4. September 2024

Schriftlicher Bericht zu dem TOP  
„Großstörung im Rechenzentrum in Münster - kann die gesamte  
Justiz in NRW wirklich durch einen simplen Stromausfall lahm-  
gelegt werden?“

Mit dem Bericht der Landesregierung erfolgt die in dem Anmeldungsschreiben der FDP-Fraktion erbetene Unterrichtung zu dem vorbezeichneten Tagesordnungspunkt.

Am 16.08.2024 ereignete sich eine IT-Störung, die sich zwar flächendeckend in Nordrhein-Westfalen auf den justiz-internen IT-Betrieb aus der Zentralen IT-Betriebsstelle in Münster (ZBS) – bzw. die von dort zentral bereitgestellten Fachanwendungen – auswirkte, aber bei der nicht im Raum stand, dass die Störung über den Ereignistag hinaus andauern sollte und die schlussendlich auch in den Abend- bzw. Nachtstunden desselben Tages erfolgreich behoben wurde.

Die Gerichte waren am 16.08.2024 auf den üblichen Kommunikationswegen erreichbar. Elektronische Nachrichten konnten über das Elektronische Gerichts- und Verwaltungspostfach (EGVP) fristwährend eingereicht werden.

Am Ereignistag konnten die eingegangenen elektronischen Nachrichten lediglich nicht vom Intermediär abgeholt und justizseitig technisch verarbeitet werden. Noch am Freitagnachmittag wurde hierzu klarstellend – wie nachstehend noch ausgeführt wird – eine Meldung im Internetauftritt der Justiz NRW geschaltet. Unmittelbar nach dem Wiederanlauf der Systeme, ab 23:30 Uhr, wurden die eingegangenen Nachrichten sukzessive abgeholt und an die adressierten Gerichte geliefert.

Die justizseitige technische Verarbeitung sämtlicher am 16.08.2024 an die Justiz NRW versandten elektronischen Nachrichten wurde noch am Samstag, den 17.08.2024, erfolgreich abgeschlossen.

Die Nutzung des dienstlichen Endgeräts (PC, Laptop etc.) war nicht betroffen. Microsoft Office, Internet sowie der sogenannte digitale „Notfallkoffer“ standen lokal zur Verfügung. Outlook konnte mittels der Outlook-Web-App genutzt werden.

Alle Gerichte und Staatsanwaltschaften waren am 16.08.2024 stromversorgt. Daher lag kein Anwendungsfall des sog. 47er-Modells vor. Dieses Modell ist zur Aufrechterhaltung der rechtsstaatlichen Ordnung als vorbereitende Maßnahme der Notfallplanung für den Fall eines längerfristigen und flächendeckenden Stromausfalls etabliert. Es ermöglicht den Gerichten und Staatsanwaltschaften, bei einem anhaltenden Stromausfall auf die notstromversorgte Infrastruktur der Polizeidienststellen zurückgreifen zu können.

Statistische Daten über die Aufhebung von Sitzungsterminen liegen dem Ministerium der Justiz nicht vor. Insofern kann aber auch auf die nachstehend dargestellten „Vorsorgeinstrumente“ verwiesen werden, die gerade für die Fälle einer Rechenzentrumsstörung insbesondere die Aufrechterhaltung des Sitzungsbetriebs gewährleisten sollen.

In den meisten Gerichten besteht so etwa die Möglichkeit, auf ausgewählte Akten auch bei einem Ausfall des Rechenzentrums zuzugreifen (sogenanntes „eAkten Caching“).

Von den insgesamt 193 zentralisierten Gerichten (151 Gerichte der ordentlichen Gerichtsbarkeit, 33 Arbeitsgerichte und 9 Sozialgerichte) haben derzeit 188 ein aktives eAkten Caching. Die Verwaltungs- und Finanzgerichte verfügen derzeit zwar noch nicht über das eAkten-Caching, allerdings wird dort stattdessen eine sogenannte „PDF-Gesamtkarte“ für den Notfall vorgehalten, auf die die zuständigen Mitarbeiterinnen und Mitarbeiter Zugriff haben. Diese PDF-Akten werden fortlaufend aktualisiert.

Soweit Akten lokal vorgehalten werden, erfolgt die Auswahl der Akten für das Caching wie folgt: Alle Akten, für die innerhalb der nächsten 14 Tage eine Aufgabe in der eAkte fällig wird, werden automatisch 14 Tage vor und bis zu 21 Tage nach Fälligkeit lokal vorgehalten. Hiervon erfasst sind auch Akten, die für einen Sitzungstermin auf Wiedervorlage gesetzt werden. Darüber hinaus können Justizangehörige Akten manuell zu einem gewünschten Zeitpunkt für das Caching auswählen. Diese stehen dann bei Bedarf ebenfalls lokal zur Verfügung.

Das lokale Vorhalten elektronischer Akten ist wesentlicher Bestandteil des umfassenden und mit den Gremien sowie dem Geschäftsbereich abgestimmten Notfallhandbuchs „Notfallmanagement elektronische Akte (e-Akte)“, welches in regelmäßigen Abständen aktualisiert wird. Die grundlegenden Informationen zum Notfallmanagement können justizintern diesem Notfallhandbuch entnommen werden. Ziel des Cachings ist es, präventive und reaktive Maßnahmen zu ergreifen, um den Zugriff gegen unvorhergesehene Ausfälle zu sichern bzw. Ausfallzeiten zu reduzieren.

Die Einrichtung des Cachings wird durch das umfassende technische Konzept „Einrichtung des eAkten-Cachings“ beschrieben. Der organisatorische Umgang mit dem eAkten-Caching wird ergänzend im justizinternen Konzept „Das Caching elektronisch geführter Akten als Teil des Notfallkonzeptes“ dargestellt. Die Nutzung des eAkten-Cachings wird den Anwenderinnen und Anwendern durch eine detaillierte Anwenderinformation vermittelt. Beide Dokumente stehen den Justizbehörden zur Verfügung.

Der sogenannte digitale „Notfallkoffer“ hält in den Behörden relevante Formularsammlungen dezentral vor, die im Falle eines flächendeckenden Stromausfalls oder eines Ausfalls des Rechenzentrums den Mitarbeiterinnen und Mitarbeitern – auf dem jeweiligen Arbeitsplatzdesktop – lokal zur Verfügung stehen und mit Microsoft Office bearbeitet werden können. Hierdurch wird insbesondere der Sitzungsdienst durch Formularvorhaltung gesichert.

Ursächlich für die Betriebsstörung am 16.08.2024 in der durch den Zentralen IT-Dienstleister der Justiz NRW (ITD) betriebenen ZBS war die Unterbrechung der Stromzufuhr an die Infrastruktur der ZBS in der Nacht zuvor.

Für solch einen Fall gibt es technische Vorsorgeeinrichtungen, die die Stromversorgung bei Störungen übernehmen sollen. Sie werden der Justiz NRW durch den Landesbetrieb für Information und Technik IT.NRW bzw. die Eigentümerin der Rechenzentrumsimmobilie (Westfälisch-Lippische Vermögensverwaltungsgesellschaft mbH - WLW) zur Verfügung gestellt.

Leistungen der Haustechnik einschließlich der (Not-)Stromversorgung werden im Rahmen einer vertraglichen Vereinbarung von IT.NRW bezogen. Einzeln ausgewiesene Kostenpositionen für die Sicherstellung einer Notstromversorgung für das Rechenzentrum der Justiz NRW sind nicht bei der Haushaltsveranschlagung für das Jahr 2025 berücksichtigt, diese sind Teil der Nebenkosten.

Die Stromversorgung der ZBS (beide Rechnersäle) wird aus zwei Quellen gesichert, aus dem öffentlichen Stromnetz und einer Netzersatzanlage (NEA). Falls der Strom aus dem Stromnetz ausfällt oder eine Störung vermutet wird, schaltet die NEA prophylaktisch ein. Während die NEA (Diesel) hochfährt, übernehmen Batterien (Unterbrechungsfreie Stromversorgung – USV) die Stromversorgung.

Die Komponenten der Stromversorgung werden durch ein elektromechanisches Schaltsystem gesteuert. In diesem System lag jedoch ein Defekt vor: Ein Akku, der dieses System autark mit Strom versorgen soll, war beschädigt. Dieser Defekt ist im Rahmen eines Funktionstests der Anlage durch die WLW am 05.08.2024 nicht zutage getreten.

Wegen des funktionslosen Schaltersystems waren im Rechnersaal Nord weder die Zuleitung der öffentlich Energie-(Netz-)versorgung noch die Zuleitung der NEA geschaltet, wodurch keine Stromversorgung bestand und der Rechnersaal Nord nur temporär über die USV versorgt worden war und sodann stromlos fiel. Es kam daher nicht zur automatisierten Umschaltung, sondern zu einem regelwidrigen Abriss der Stromversorgung im Rechnersaal Nord. Im Rechnersaal Süd war der Schalter für die Zuleitung der NEA geöffnet, und der Schalter für das öffentliche Stromnetz war in einer Zwischenposition hängen geblieben.

Unmittelbar nach Unterrichtung durch IT.NRW trat der ITD noch in den frühen Morgenstunden des 16.08.2024 entsprechend dem dortigen Incident-Management umgehend in die Störungsanalyse und -behebung sowie den intensiven Austausch mit IT.NRW – unter enger Einbeziehung der Gebäudeeigentümerin WLW – betreffend die Wiederherstellung der Stromversorgung der Rechenzentrumsinfrastruktur ein. Mit Rücksicht auf die prognostische Störungsbehebung noch am Ereignistag wurde kein gesonderter Krisenstab eingerichtet.

Der alleinige Betrieb aus dem Rechnersaal Süd war nicht möglich, weil noch die Umsetzung einer Empfehlung der Firma Fujitsu Technology Solutions (FTS) hinsichtlich

einer von der Unterbrechung der Stromzufuhr unabhängigen Storage-Problematik abhängig war. Diese Maßnahme hatte bis dato zwar keine Auswirkungen für die Anwenderinnen und Anwender gezeitigt, allerdings ergab der unmittelbare und intensive Austausch des ITD mit FTS, dass von dort eindringlich empfohlen wurde, zunächst den Rechnersaal Nord geordnet wieder hoch zu fahren.

Ein ungeordnetes Herunterfahren birgt stets die Gefahr physikalischer Schäden an der Hardware. Daher war eine sorgfältige Prüfung des Zustandes der Hardware nötig. Zudem musste sichergestellt sein, dass alle Datenbestände konsistent und auf dem aktuellen Stand waren. Diese Umstände wirkten sich auf die Dauer der Entstörung aus. Erst nach erfolgreichem Ausschluss von Hardwaredefekten sowie eines inkonsistenten Datenbestandes konnten die vorbereiteten Wiederanlaufpläne ausgeführt werden.

Der ursächliche Akku in der Schalteranlage wurde noch in den Morgenstunden des 16.08.2024 ausgetauscht. Um 12:30 Uhr konnte dann durch IT.NRW bestätigt werden, dass die Stromversorgung auch im Falle voller Last bei Wiederanlaufen der Systeme gewährleistet sei, sodass sukzessiv der Wiederanlauf der Systeme vorgenommen werden konnte.

Besonders für den weiteren Wiederanlaufprozess war dann wiederum, dass die vorhandenen Wiederanlaufskripte und Pläne mit Rücksicht auf den harten Stromabriss anzupassen waren. Eine vorherige Übung dieses Szenarios war nicht möglich gewesen, weil mit der abrupten Abschaltung des Rechenzentrums ohne Herunterfahren von Systemen stets ein hohes Risiko von Hardwaredefekten verbunden ist.

Die manuellen Arbeiten, im Wesentlichen das manuelle Starten und Prüfen von einzelnen Systemen, konnten in großen Teilen in den späten Abend- und Nachtstunden des 16.08.2024 abgeschlossen werden. Im Anschluss erfolgten Funktionstests und Testanmeldungen, sodass gegen 01:00 Uhr am 17.08.2024 der zentralisierte Arbeitsplatz grundsätzlich wieder freigegeben wurde.

Zur Optimierung der vorhandenen Ausfallsicherheit und weiteren Härtung der Energieinfrastruktur der ZBS steht der ITD bereits im intensiven Austausch mit IT.NRW und der Gebäudeeigentümerin WLV. Insbesondere prüft IT.NRW in Abstimmung mit der WLV, ob die betreffende Schalteranlage an die USV-Batterien als hochsicheres System angeschlossen werden könnte.

Zum Schutz der zentralen IT-Infrastruktur der Justiz NRW sind umfangreiche technische wie organisatorische Maßnahmen getroffen, die für alle zentralisierten Gerichte und Behörden gleichermaßen greifen. Beispielhaft sind betreffend die Rechenzentrums-Infrastruktur und Redundanz folgende Maßnahmen zu nennen:

Das Rechenzentrum Münster besteht aus zwei Rechenzentrumsabschnitten (Nord und Süd) im selben Gebäude, die brandschutztechnisch voneinander getrennt sind.

Ergänzend hierzu ist in ca. 100 km Luftlinie vom Standort Münster entfernt ein georedundantes Rechenzentrum eingerichtet.

Die infrastrukturelle Sicherung erfolgt u.a. mit USV, NEA, Einbruchmeldeanlage (EMA), (Video-)Überwachungsanlage, Vereinzelnungsanlage sowie infrastrukturellen Redundanzen (Server, Storage, Netzwerk etc.).

Alle relevanten IT-Komponenten werden mittels Status-Monitoring kontinuierlich überwacht. Die zuständigen Teams werden bei kritischen Systemzuständen oder Ausfall einzelner Komponenten automatisch benachrichtigt, um die Störung umgehend beseitigen zu können.

Das Rechenzentrum konnte im Jahr 2021 erstmalig nach ISO 27001 zertifiziert und im Jahr 2024 erfolgreich (re-)zertifiziert werden. Die jährlichen Überwachungsaudits wurden ausnahmslos erfolgreich abgeschlossen.

Der ITD hat ein Notfall-Management-System auf Basis des BSI-Standards 200-4 etabliert. Notfallstabs-Übungen sowie technische Notfallübungen werden geplant durchgeführt.

Obgleich Justizeinrichtungen nur zu den kritischen Einrichtungen im Sinne der nationalen Strategie zum Schutz Kritischer Infrastrukturen (KRITIS-Strategie) gehören, jedoch nicht dem BSI-Gesetz und der darauf aufbauenden KRITIS-VO unterliegen und daher erweiterte gesetzliche Vorgaben zum Schutz von Justizeinrichtungen nicht bestehen, ist der Schutz der Funktionsfähigkeit aller Justizeinrichtungen sowie des Ministeriums der Justiz von zentraler Bedeutung.

Es wird ein ressortweites Informationssicherheitsmanagement nach dem IT-Grundsicherungsstandard des BSI etabliert, dessen Strukturen sich aus der Leitlinie ergeben, die ihrerseits auf einer ressortübergreifenden Leitlinie beruht. Im Rahmen der Umsetzung der Vorgaben der BSI werden – in Abhängigkeit des jeweiligen Schutzbedarfs – zahlreiche Maßnahmen vor allem technischer, organisatorischer und baulicher Art umgesetzt, die teilweise behördenübergreifend identisch, zum Teil aber auch behörden-spezifisch sind. Der IT-Grundsicherungsstandard zielt auf den umfassenden Schutz aller Informationen einer Organisation, egal ob sie digital vorliegen und worauf die Gefährdungen beruhen. So werden neben klassischen „IT-Gefahren“ auch Naturgefahren wie Erdbeben, Überschwemmungen etc. in den Blick genommen. Gerade im Hinblick auf die Sicherung der dezentralen IT-Infrastrukturkomponenten werden derzeit flächendeckend Verbesserungspotenziale abgefragt und umgesetzt.

Die landes- bzw. justizinterne Meldung von Sicherheitsvorfällen oder Notfällen ist seitens des Landes NRW über die „Richtlinie Definition Informationssicherheitsvorfall NRW“ und die „Richtlinie zum zentralen Meldewesen Informationssicherheit NRW“ verbindlich geregelt und wird durch das Ministerium der Justiz NRW in der „Richtlinie



Definition Informationssicherheitsvorfall Justiz NRW“ und in der „Richtlinie Meldewege Justiz NRW“ konkretisiert.

Darüber hinaus ist im Rahmen des Notfallmanagements für den ITD und für das Oberlandesgericht Köln u.a. geregelt, dass „Verlautbarungen gegenüber der Öffentlichkeit und Presse durch die Leitung des Notfallstabes bzw. nur in Abstimmung mit dieser festgelegt werden“. Damit wird für das OLG Köln eine „einheitliche, sachlich richtige und widerspruchsfreie Kommunikation“ gegenüber öffentlichen Stellen gewährleistet. Innerhalb des OLG Köln übernimmt das Pressedezernat die Kommunikation in Richtung der Medien.

Unmittelbar nach Bekanntwerden der eigenständigen Startseiten-Meldung des OVG NRW im Internet wurde noch am Ereignistag um 14:44 Uhr eine klarstellende Veröffentlichung auf der Web-Seite der Justiz NRW im Internet mit dem Inhalt geschaltet, dass elektronische Nachrichten zwar fristwährend eingehen, aber justizseitig gegenwärtig nicht verarbeitet werden können. Mit Rücksicht auf die justizinterne Freigabe des zentralisierten Arbeitsplatzes am 17.08.2024 um ca. 01:00 Uhr wurde diese Meldung noch am selben Tage zurückgezogen. Der zunächst abweichende Text auf der Seite des OVG beruhte auf technischen Problemen beim Hochladen der korrekten Störungsmeldung.

Die Meldung über die Wiederaufnahme des Regelbetriebes im Justizrechenzentrum wurde am 19.08.2024 um 9:29 Uhr geschaltet, nachdem gesichert war, dass das Gesamtsystem wieder funktionierte.

Bereits unmittelbar am Ereignistag informierte der ITD frühzeitig vor Dienstbeginn um 06:34 Uhr per ITD-Aktuell-Meldung an alle Verwaltungspostfächer und alle Anwenderinnen und Anwender unmittelbar und sodann fortlaufend über den Störungsstatus.

Das Ministerbüro war nicht nur über das Vorliegen der Störung und auch über die im Laufe des Tages andauernden Einschränkungen fortlaufend informiert, sondern – insbesondere dann als sich abzeichnete, dass justizseitig EGVP-Eingänge vorübergehend nicht bearbeitet werden konnten – in die Abstimmung zur Veröffentlichung seitens des Ministeriums eingebunden.

Unabhängig vom 16.08.2024 ist justizintern eine Störungshistorie betreffend aktuelle und archivierte EGVP-Störungsmeldungen eingerichtet, um insbesondere mögliche Ersatzeinreichungskonstellationen ex post effektiv nachvollziehen zu können. Weiter besteht über den Internetauftritt des EGVP die Möglichkeit, sich über aktuelle Störungen informiert zu halten sowie hierzu einen Newsletter zu abonnieren.

Eine Information der Oppositionsmitglieder des Rechtsausschusses sowie der regierungstragenden Fraktionen und Mitglieder des Rechtsausschusses erschien mit Blick auf die Prognose zur Störungsbehebung noch am Ereignistag sowie insbesondere die

oben dargestellten Vorsorgeinstrumente zur Gewährleistung des Dienstbetriebes und insbesondere des Sitzungsdienstes nicht angezeigt.