

19. Wahlperiode

Schriftliche Anfrage

des Abgeordneten Marc Vallendar (AfD)

vom 12. Juni 2023 (Eingang beim Abgeordnetenhaus am 13. Juni 2023)

zum Thema:

Betrieb der Landes-IT bei disruptiven Ereignissen im Internet

und **Antwort** vom 27. Juni 2023 (Eingang beim Abgeordnetenhaus am 29. Juni 2023)

Der Regierende Bürgermeister von Berlin
Senatskanzlei

Herrn Abgeordneten Marc Vallendar (AfD)
über
die Präsidentin des Abgeordnetenhauses von Berlin

über Senatskanzlei - G Sen -

Antwort
auf die Schriftliche Anfrage Nr. 19/15793
vom 12. Juni 2023
über Betrieb der Landes-IT bei disruptiven Ereignissen im Internet

Im Namen des Senats von Berlin beantworte ich Ihre Schriftliche Anfrage wie folgt:

Vorbemerkung des Abgeordneten:

Das Internet ist ein weltumspannendes Netz, innerhalb dessen sowohl Basisdienste wie auch anwendungsspezifische Dienste Kommunikation durchführen.

Auf der Ebene der Basisdienste sind beispielsweise der Nameservice (DNS), das Netzwerk-Zeitprotokoll (NTP) besonders zu erwähnen. Auf der Ebene anwendungsspezifischer Dienste ergeben sich logische Kommunikations- bzw. Datenflüsse aus den konkreten Anwendungen, z. B. bei einer PKW-Anmeldung in einem Berliner Amt die Kommunikation mit Servern beim Kraftfahrtbundesamt. Erwähnenswert ist auch, dass vielerorts auf chiffrierte und mit digitalen Signaturen versehene Kommunikation gesetzt wird. Die Überprüfung digitaler Signaturen erfordert zwecks Sicherstellung der Authentizität eines Kommunikationspartners regelmäßig die Prüfung digitaler Zertifikate, wobei wiederum oft auf Daten von anderen Internet-Teilnehmersystemen zurückgegriffen werden muss.

Sind Teile des Internet nicht verfügbar, kann das auch bei der Durchführung lokaler Kommunikationen bzw. Bearbeitung rein lokaler Vorgänge unter Umständen zu empfindlichen Störungen kommen. Diese können sich

ergeben z. B. durch teilweise Dysfunktionalität von oben bereits genannten Basisdiensten wie dem Nameservice (DNS), Ausfall der Netzzeit (NTP), Nichtprüfbarkeit von digitalen Signaturen (z. B. SSL/TLS-Zertifikate), Nichterreichbarkeit von Kommunikations-Gegenstellen im Fachverfahrensbereich etc.

Teilausfälle des Internet werden insbesondere vor dem Hintergrund der Energieknappheit wahrscheinlicher. Auf Bundesebene wurden bereits Vorbereitungen getroffen, bei Strommangel ggf. mit rollierenden Stromnetz-Abschaltungen ("Brownouts") zu reagieren. Solche Situationen können dazu führen, dass das eigentlich zusammenhängende Internet in einzelne Teilnetze "zerfallen" kann, zum Beispiel wenn Übertragungswege oder sogar ganze Rechenzentren zeitweilig mangels elektrischer Energie vom Netz gehen müssen.

Auch wenn typischerweise zentrale IT-Infrastrukturen über Redundanzkonzepte inklusive Notversorgung verfügen, gibt es rein statistisch immer wieder Probleme bezogen auf die reale Nutzbarkeit der theoretisch bestehenden Rückfallebenen. Wir haben ja z. B. vor kurzem noch in der Charité gesehen, dass auch Notstromkonzepte nicht immer komplikationsfrei greifen. Vergleichbares kann auch in Rechenzentren passieren, bzw. es hat derartige Negativ-Vorfälle bereits gegeben, z. B. vor wenigen Jahren in einem Rechenzentrum in Oberhausen, wo das IP-Routing nach Wiederaufschalten des Netzstroms zunächst ausgefallen ist, oder auch bei einem Rechenzentrum in Berlin-Tempelhof, welches ebenfalls über Notstrom verfügte, wo es aber bei der Rückkehr zu regulärem Netzstrom-Betrieb zu einem Komplettausfall des Rechenzentrums für etliche Stunden kam.

Man sollte insofern davon ausgehen, dass beim Eintreten insbesondere einer Notwendigkeit für geplante Stromabschaltungen auch im Bereich des Internet-Betriebes mit Kollateralschäden zu rechnen ist.

1. Wurde im Bereich der Landes-IT das Szenario evaluiert, dass zwar hier in Berlin (und Umland) die Stromversorgung und auch die Kommunikationsinfrastruktur einwandfrei funktioniert, aber Teile des Internet über längere Zeit nicht erreichbar sind?

Zu 1.:

Die Stromversorgung einschließlich des Betriebes der kritischen Kommunikationsinfrastruktur ist Bestandteil des Krisen-/ Notfallmanagements des Landes Berlin, einschließlich der dafür notwendigen Werkzeuge. Die Leitlinie zum IKT-Notfallmanagement (IKT-NotfallM-LL) ist das zentrale Strategiedokument des IKT-Notfallmanagements der Berliner Verwaltung. In dem Dokument werden der Stellenwert und die übergeordneten landesweiten Ziele des IKT-Notfallmanagements sowie dessen grundsätzliche Ausrichtung zusammengefasst. Des Weiteren wird der Rahmen für die Konzeption, den Aufbau und die Aufrechterhaltung des IKT-Notfallmanagements festgelegt. Die Leitlinie definiert auch wesentliche Begriffe, Rollen und Tätigkeiten. Die Stromversorgung und die Kommunikationsinfrastruktur, die durch das ITDZ Berlin für das Land Berlin betrieben wird, wurde im Rahmen der BSI-Zertifizierung positiv auditiert. Dieses Audit ist Bestandteil der gültigen BSI-IGZ-0471-2021 (gültig bis zum 07.07.2024).

2. Arbeitet die Landes-IT unter Nutzung lokaler Nameserver (DNS-Server), die als "Caching Nameserver" auch für die Fachverfahrensserver und Arbeitsplatzrechner fungieren, oder erfolgen Nameserver-Anfragen der Fachverfahrensserver und Arbeitsplatzrechner direkt durch (ggf. iterierende) DNS-Anfragen an entfernte Systeme?

Zu 2.:

Die IKT-Architektur des Landes Berlin in der jeweils gültigen Fassung legt den Einsatz von DNS-Servern im Land Berlin fest. Im Rahmen des E-Government-Gesetzes Berlin (EGovG Bln) ist die Methodik des BSI IT-Grundschutz-Kompendiums anzuwenden. Die Anforderungen aus dem Kompendium in der aktuellen Fassung an einen DNS-Server (APP.3.6) werden im ITDZ Berlin umgesetzt und wurden im Rahmen der BSI-Zertifizierung positiv auditiert. Dieses Audit ist Bestandteil der gültigen BSI-IGZ-0471-2021 (gültig bis zum 07.07.2024).

3. Ist für den Dienst "Netzwerk-Systemzeit" (Protokoll NTP) ein lokaler Server (z. B. beim ITDZ) verfügbar? Oder greifen Fachverfahrensserver und Arbeitsplatzrechner direkt auf einen oder mehrere entfernte NTP-Server zu? Falls Zugriff auf externe Dienste: Wie verhalten sich die betroffenen NTP-Clients, wenn der Dienst "Netzwerk-Systemzeit" nicht verfügbar ist?

Zu 3.:

Die IKT-Architektur des Landes Berlin in der jeweils gültigen Fassung legt den Einsatz von NTP-Servern im Land Berlin fest. Im Rahmen des E-Government-Gesetzes Berlin ist die Methodik des BSI IT-Grundschutz-Kompendiums anzuwenden. Die Anforderungen aus dem Kompendium in der aktuellen Fassung an einen NTP-Server werden im ITDZ Berlin umgesetzt und wurden im Rahmen der BSI-Zertifizierung positiv auditiert. Dieses Audit ist Bestandteil der gültigen BSI-IGZ-0471-2021 (gültig bis zum 07.07.2024).

4. Themenfeld Kryptographie und SSL/TLS-Zertifikate: Sind die für die Kommunikation zwischen Server- und Clientsystemen innerhalb der Berliner-Landes-IT noch prüfbar, wenn größere Teile des Internet aufgrund einer irgendwie gearteten Störung nicht erreichbar sind? Können die Zertifikate dennoch überprüft werden? Oder wird die Kryptographie dann zum "Showstopper" für die Kommunikation zwischen Servern und Clients innerhalb der Berliner Landes-IT?

Zu 4.:

Die landesweite Public Key Infrastructure/ Certification Authority (PKI/CA) ist Teil der Leitlinie zur Informationssicherheit der Landesverwaltung des Landes Berlin (InfoSic-LL) und der Leitlinie zum IKT-Notfallmanagement. Die vom ITDZ Berlin betriebene PKI/CA ist abgesichert gemäß BSI IT-Grundschutz-Kompendium und wurde im Rahmen der BSI-

Zertifizierung positiv auditiert. Dieses Audit ist Bestandteil der gültigen BSI-IGZ-0471-2021 (gültig bis zum 07.07.2024).

5. Themenfeld "Schwarzstart der Landes-IT nach Stromausfall": Ist es (unter Berücksichtigung der in Punkten 2-4 angesprochenen Herausforderungen) möglich, die Berliner Landes-IT nach einem Stromausfall, gleichzeitig noch nicht oder nicht vollständig zugreifbarem überregionalem Internet wieder hochzufahren? Falls nein: Bitte erläutern Sie die möglichen Probleme, die beim Wiederanlaufen entstehen würden.

Zu 5.:

Der Wiederanlauf von der Berliner Landes-IT ist Bestandteil des Krisen-/ Notfallmanagements des Landes Berlin, einschließlich der dafür notwendigen Werkzeuge. Für alle kritischen Komponenten der ITDZ Berlin betriebenen Infrastruktur liegen Wiederanlaufpläne vor. Ein übergreifender Wiederanlaufplan sichert zudem einen koordinierten und abgestimmten Wiederanlauf nach einem Schwarzstart.

6. Themenfeld Netzwerk-Dateisysteme: Nutzen Server der Berliner Landes-IT, oder Arbeitsplätze in den Einzelbehörden, Dienste wie z. B. Netzwerk-Dateisysteme via NFS oder vergleichbare Protokolle, um auf Dateisysteme von Servern außerhalb des Bundeslandes Berlin zuzugreifen?

Zu 6.:

Nein.

7. Themenfeld Netzwerk-Dateisysteme, Teil 2: Wurde bei der Konzeption von Netzwerk-Dateisystemnutzung (NFS oder andere Verfahren) darauf geachtet, zirkuläre Abhängigkeiten zu vermeiden, die einen "Schwarzstart" erschweren oder verunmöglichen würden? (Diese Frage bezieht sich ausdrücklich nicht nur auf gebietskörperübergreifende Nutzung von Netzwerk-Dateisystemen, sondern auch auf Netzwerk-Dateisysteme innerhalb der Berliner Server- und Client-Landschaft).

Zu 7.:

Der Wiederanlauf von der Berliner Landes-IT ist Bestandteil des Krisen-/ Notfallmanagements des Landes Berlin, einschließlich der dafür notwendigen Werkzeuge. Für alle kritischen Komponenten der ITDZ Berlin betriebenen Infrastruktur liegen Wiederanlaufpläne vor. Ein übergreifender Wiederanlaufplan sichert zudem einen koordinierten und abgestimmten Wiederanlauf nach einem Schwarzstart. Die vom ITDZ Berlin betriebene Speichersysteme sind abgesichert gemäß BSI IT-Grundschutz-Kompendium und wurden im Rahmen der BSI-Zertifizierung positiv auditiert. Dieses Audit ist Bestandteil der gültigen BSI-IGZ-0471-2021 (gültig bis zum 07.07.2024).

8. Gebietskörperschaftsübergreifende Fachverfahren: Die Kommunikation zwischen Fachverfahren kann ja grundsätzlich sowohl asynchron ("store and forward") wie auch synchron (direkter Kommunikationskanal, z. B. via TCP-Verbindung) erfolgen. Welche IKT-Fachverfahren sind zwingend auf direkte, synchrone Kommunikation angewiesen? Bitte zählen Sie die Fachverfahren in zwei Übersichten auf: einmal bezogen auf diejenigen Fachverfahren, die seitens Verwaltungs-Mitarbeitern genutzt werden, und zum anderen bezogen auf diejenigen Fachverfahren, die seitens der Bürger online im Sinne von OZG-Serviceangeboten genutzt werden.

Zu 8.:

IT-Fachverfahren werden grundsätzlich durch Mitarbeiterinnen und Mitarbeiter der Verwaltung genutzt. Eine direkte Nutzung durch Bürgerinnen, Bürger oder Unternehmen ist nicht vorgesehen. Dem Senat liegen keine Informationen vor, welche IT-Fachverfahren synchrone oder asynchrone Kommunikationsmethoden verwenden.

9. Digitale Bürgerdienste/OZG-Serviceangebote: Ist bei Nichterreichbarkeit des Querschnittsdienstes "Identifikation" eine Rückfallebene dahingehend vorgesehen, dass Anträge zwar nicht direkt authentifiziert, aber zumindest erst einmal vorläufig entgegengenommen werden?

Zu 9.:

Bei Nichterreichbarkeit des Querschnittsdienstes "Identifikation" besteht gemäß §4 Abs. 7 EGovG Bln die Möglichkeit einen Antrag über einen anderen Kommunikationsweg (z. B. in schriftlicher Form) zu stellen.

10. In Ergänzung zu Frage 8: Welche IKT-Fachverfahren im Land Berlin nutzen das OSC-Protokoll in der Betriebsart "synchrone Übertragung"? Welche dieser IKT-Fachverfahren sind bei Nichtverfügbarkeit synchroner Kommunikation in der Lage, automatisch auf asynchrone Kommunikation (über die elektronische "Poststelle") zu wechseln im Sinne einer Rückfallebene?

Zu 10.:

Dem Senat liegen dazu keine Informationen vor.

11. In Ergänzung zu Fragen 8 und 10 weiterhin: Welche IKT-Fachverfahren nutzen für gebietskörperübergreifende Kommunikation andere Kommunikationsprotokolle als OSCI und realisieren dabei eine synchrone Kommunikation?

Zu 11.:

Dem Senat liegen dazu keine Informationen vor.

12. Ist im Falle einer Abtrennung der Berliner Landes-IT vom weltweiten Internet, aber weiterhin bestehenden örtlichen Kommunikationskanälen eine landesinterne Behördenkommunikation (mittels E-Mail, eBPF etc.) weiterhin möglich? Oder fallen Berlin-intern die digitalen Kommunikationsdienste aus, auch wenn auf IP-Ebene noch Erreichbarkeit zwischen Servern und Clients besteht?

Zu 12.:

Das Berliner Landesnetz als Multi-Service-Netzwerk (BeLa-MSN) verbindet auf der landeseigenen LWL-Infrastruktur verschiedene Behörden-Standorte miteinander sowie diese mit den Rechenzentren des ITDZ Berlin. Somit ist eine Sprach- und Datenkommunikation (z.B. E-Mail landesintern) innerhalb des Berliner Landesnetzes auch dann gewährleistet, wenn das Internet einmal ausfallen sollte. Die Verbindung zu externen Netzwerken ist ausschließlich über den Sicherheitsbereich „Externe Kommunikation“ zulässig. In den Rechenzentren des ITDZ Berlin werden die IKT-Dienste und Services für das BeLa bereitgestellt. Unter den beschriebenen Voraussetzungen ist eine Berlin-interne Kommunikation weder über das elektronisches Behördenpostfach (eBPF) bzw. ein besonderes elektronisches Behördenpostfach (beBPo) möglich, da für die Prüfung von Signaturen bzw. Zertifikaten von sicheren elektronischen Identitäten im Kommunikationsablauf, welche nicht im ITDZ-Trustcenter ausgestellt wurden, ein Internetzugang für die prüfenden Instanzen notwendig ist.

13. Bestehen seitens des Senates Planungen, im Rahmen einer koordinierten Übung einen Internet-Teilausfall und das Verhalten des Berliner-Landes-IT zu erproben? Oder ist dies sogar bereits geschehen, und falls ja, mit welchem Ergebnis?

Zu 13.:

Einmal jährlich wird im Land Berlin eine übergreifende IKT-Notfallübung durchgeführt. Diese adressiert auch verschiedene Ausfallszenarien. Von einer näheren Beschreibung der untersuchten Ausfallszenarien und einer Auflistung der ermittelten Ergebnisse im

Rahmen der IKT-Notfallübung wird, mit Blick auf die Sensibilität dieser Informationen und zum Schutz der IKT-Sicherheit im Land Berlin, zur Wahrung der Vertraulichkeit abgesehen.

14. Gibt es aus früheren Internet-Störungen bereits Erkenntnisse, welche Server oder Dienste sich ggf. als problemträchtig erweisen? Falls ja: Bitte beschreiben Sie stichwortartig, was vorgefallen ist, welche Art von Problemen entstanden sind, und welche Reaktionen darauf erfolgten.

Zu 14.:

Dem Senat liegen dazu keine Informationen vor.

Berlin, den 27. Juni 2023

Der Regierende Bürgermeister von Berlin
In Vertretung

Martina Klement
Staatssekretärin für Digitalisierung
und Verwaltungsmodernisierung / CDO