Landtag
Nordrhein-Westfalen
17. Wahlperiode

Ausschussprotokoll
APr 17/1641
18.11.2021

Ausschuss für Digitalisierung und Innovation

59. Sitzung (öffentlich)

18. November 2021

Düsseldorf – Haus des Landtags

15:33 Uhr bis 16:48 Uhr

Vorsitz: Thorsten Schick (CDU)

Protokoll: Steffen Exner

Verhandlungspunkt:

Antrag
der Fraktion BÜNDNIS 90/DIE GRÜNEN
Drucksache 17/14260

– Anhörung von Sachverständigen *(s. Anlage)*

* * *

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

Antrag
der Fraktion BÜNDNIS 90/DIE GRÜNEN
Drucksache 17/14260

– Anhörung von Sachverständigen *(s. Anlage)*

Vorsitzender Thorsten Schick: Meine sehr geehrten Damen und Herren! Wir sind heute wieder in etwas kleinerer Runde zusammengekommen, aber ich sehe die anwesenden Landtagsabgeordneten und natürlich die Sachverständigen, die uns heute zur Verfügung stehen, sodass die wichtigste Expertise vorhanden ist.

Ich darf Sie alle sehr herzlich begrüßen. Noch ist es kein Jubiläum, sondern erst die 59. Sitzung des Ausschusses für Digitalisierung und Innovation. Ich begrüße die Vertreterinnen und Vertreter der Medien, sofern sie uns denn zugeschaltet sein sollten, sowie die sonstigen Zuschauerinnen und Zuschauer, den Sitzungsdokumentarischen Dienst und die Damen und Herren Sachverständigen.

Ich weise darauf hin, dass die Sitzung im Livestream übertragen wird.

Die Tagesordnung ist Ihnen mit der Nummer E 17/2097 – Neudruck – bekannt gegeben worden. Ich sehe keine Wortmeldungen zur Tagesordnung; dann ist dies unsere heutige Arbeitsgrundlage, und ich eröffne die Anhörung zum Antrag der Fraktion von Bündnis 90/Die Grünen. Der Antrag wurde uns am 2. Juli 2021 zur Federführung zugewiesen, mitberatend ist der Innenausschuss.

Ich möchte kurz auf das Tableau der heutigen Anhörung eingehen. Von IT.NRW ist Herr Dr. Weckendrup als Sachverständiger anwesend, vom Horst-Görtz-Institut für IT-Sicherheit von der Ruhr-Universität Bochum Herr Professor Dr. Borgolte, Herr Rundfeldt von der AG KRITIS und Herr Moayeri von der ComConsult GmbH. Herr Professor Dr. Engel vom KDN – Dachverbands kommunaler IT-Dienstleister ist uns per Video zugeschaltet. Ich freue mich, dass Sie dem Ausschuss heute zur Verfügung stehen.

Sie haben freundlicherweise Stellungnahmen erarbeitet, die den Abgeordneten vorab zugegangen sind. Eine Zusammenfassung der Stellungnahmen ist nicht vorgesehen, sondern die Abgeordneten haben die Möglichkeit, direkt mit Fragen an Sie einzusteigen. Wir beginnen mit Frau Brems von der antragstellenden Fraktion.

Wibke Brems (GRÜNE): Herzlichen Dank an die Sachverständigen, dass Sie uns heute Rede und Antwort stehen. – Ich möchte in der ersten Runde nur eine Frage stellen, und zwar an die AG KRITIS und an ComConsult. Die Frage klingt einfach, sie kann dann aber vielleicht umso umfangreicher beantwortet werden. Welche Anpassungen am Landesverwaltungsnetz erscheinen Ihnen vor dem Hintergrund der bekannten Gegebenheiten besonders notwendig?

Sven Werner Tritschler (AfD): Vielen Dank auch seitens der AfD-Fraktion für die Stellungnahmen.

Meine ersten Fragen richten sich an Herrn Dr. Weckendrup und an Herrn Rundfeldt. Wie würden Sie den Einsatz von Künstlicher Intelligenz bei der Sicherstellung von Resilienz bewerten? Ist so etwas bei IT.NRW schon im Einsatz? Können Sie dahin gehend schon Erfolge vermelden oder kennen Sie andere Best-Practice-Beispiele?

Dann möchte ich noch Herrn Rundfeldt im Speziellen eine Frage stellen. Welche anderen Möglichkeiten zur Sicherstellung von Resilienz können Sie neben klassischen Dingen wie Backups, Parallelsystemen und Redundanzen empfehlen?

Christina Kampmann (SPD): Herr Rundfeldt, ich habe auch eine Frage an Sie. Die AG KRITIS hat direkt viel zu tun. Das liegt wahrscheinlich an Ihrer wirklich sehr interessanten Stellungnahme. Darin schreiben Sie zum einen, dass es aus Ihrer Sicht mehr als überfällig ist, klare und verbindliche Regeln für Staat und Verwaltung zu schaffen. Uns würde interessieren, wie wesentliche Eckpunkte für solche Regeln und Standards aussehen könnten.

Sie sagen außerdem, dass der Zeitablauf nahelegt, dass Situationen wie diejenige, die Anlass für die Grünen war, diesen Antrag zu stellen, nicht ausreichend geübt und trainiert worden sind. Unsere Frage wäre, ob es entsprechende Übungen im Kontext anderer kritischer Infrastrukturen gibt und ob es Best Practices gibt, von denen wir lernen könnten.

Rainer Matheisen (FDP): Vielen Dank auch vonseiten der FDP-Fraktion für Ihre Stellungnahmen und dafür, dass Sie sich heute Zeit für uns nehmen.

Ich hätte in Bezug auf die Stellungnahme der AG KRITIS eine Frage, die ich aber an Herrn Dr. Weckendrup und Herrn Dr. Moayeri richten möchte. Wie bewerten Sie die in der Stellungnahme der AG KRITIS aufgestellten Forderungen, das Land solle eine Verwaltungsvorschrift erlassen, welche verbindliche Regelungen für kritische Infrastrukturen im Sektor „Staat und Verwaltung“ in NRW schafft?

Dr. Christian Untrieser (CDU): Wir schließen uns dem Dank für Ihre Anwesenheit und für Ihre Stellungnahmen an.

Ich möchte in der ersten Runde Herrn Dr. Weckendrup eine Frage stellen. Im Antrag der Grünen werden einige Maßnahmen aufgeführt. Könnten Sie uns erläutern, welche dieser Maßnahmen im Antrag der Grünen bei IT.NRW bereits umgesetzt sind bzw. der gängigen Praxis entsprechen?

Vorsitzender Thorsten Schick: Damit ist die erste Fragerunde abgeschlossen. Wir gehen bei den Antworten in der Reihenfolge des Tableaus vor, beginnend bei Herrn Dr. Weckendrup.

Dr. Dirk Weckendrup (IT.NRW): Ich beginne bei der Frage, welche Maßnahmen bereits umgesetzt worden sind. Wir haben natürlich auch aus diesem Fehler wieder lernen müssen. Jeder Fehler tut uns weh und ärgert uns; das ist keine Frage. Die Nacharbeit solcher Probleme ist aber Bestandteil der täglichen Routine.

Wir haben mehrere Maßnahmen umgesetzt, und zwar sowohl kurzfristige als auch langfristige. Kurzfristig haben wir mit den Herstellern gesprochen, insbesondere mit denen der problematischen Router in unserem Rechenzentrum. Entsprechende Software-Updates, die uns empfohlen worden sind, sind sofort eingespielt worden. Das ist gemeinsam mit dem Hersteller nicht nur auf der betroffenen Komponente, sondern auf allen Komponenten in unserem Landesverwaltungsnetz geschehen.

Wir haben darüber hinaus, um einen solchen Fehlerfall in Zukunft noch besser abfedern zu können, einen sogenannten Cold Standby, also ein identisches Gerät, danebengestellt. Falls ein solcher Cluster – es ist ja ein Verbund von zwei Systemen – tatsächlich nicht wieder in Betrieb zu nehmen ist, haben wir über einen solchen Cold Standby auf jeden Fall eine Möglichkeit, das Landesverwaltungsnetz und die darüber laufenden Dienste wieder in Betrieb zu nehmen.

Auf der etwas längerfristigen Zeitschiene – wir sind es aber schon angegangen – wird auch die Architektur des Landesverwaltungsnetzes überprüft. Auch da haben wir nach diesen Erkenntnissen neue Ansätze gefunden, um eine bessere Resilienz, wenn ich diesen Begriff aufnehmen darf, dadurch zu erzeugen, dass wir den eigentlichen Core-Backbone des Landesverwaltungsnetzes von dem Bereich, der die Leitung bzw. die Verbindung zu den Behörden aufnimmt, trennen, um die Wechselwirkung, die uns da große Probleme bereitet hat, in Zukunft auseinanderzuziehen.

Der letzte Punkt – auch das haben wir adressiert –: Natürlich gehört immer dazu, wie die Prozesse gelaufen sind, wie die zeitliche Abfolge war, ob die richtigen Kolleginnen und Kollegen adressiert wurden, ob wir die richtige Unterstützung gehabt haben. Auch da gibt es kleinere Justierungen. Wir orientieren uns bei unseren Prozessen an der ITIL; das ist eine Sammlung von Best Practices, die bei uns gelebt werden. Auch da haben wir im Laufe dieses Vorgangs gemerkt, dass wir insbesondere bei der Information der Betroffenen manches noch zügiger hätten machen können. Wir haben dies in Absprache mit dem MWIDE letztendlich auch so umgesetzt.

Prof. Dr. Kevin Borgolte (Ruhr-Universität Bochum, Horst-Görtz-Institut für IT-Sicherheit): Zu der letzten Frage, die seitens der CDU gestellt wurde, kann ich eher weniger sagen, da ich das Landesverwaltungsnetz ja nicht selber betreibe.

(Dr. Christian Untrieser [CDU]: Nein, die war ja auch an den Kollegen!)

– Genau. Hinsichtlich der Frage der SPD zu Best Practices kann ich etwas sagen. Größere Firmen, die auf Cloud Infrastructure setzen – zum Beispiel Netflix – generieren selbst regelmäßige Ausfälle und nutzen diese. Da werden komplette Datacenters offline genommen, um solche Sachen zu üben. Für die kritische Infrastruktur ist so etwas natürlich nicht leicht umzusetzen. Dort ist es schwieriger, allerdings sollte auch dort so etwas geübt werden. Jeder übt einen Feueralarm, und genau dasselbe sollte

auch für die IT-Infrastruktur der Fall sein. Das heißt: Datacenters offline nehmen, Leitungen offline nehmen.

Generell ist es für mich schwierig, zu sagen, was genau vorgefallen ist. Meine Interpretation dessen, was öffentlich geworden ist, ist, dass ein Switch oder ein Router bei der Deutschen Telekom ausgefallen ist und danach das Border Gateway Protocol aufseiten des Landesverwaltungsnetzes gefailt hat. Interpretationsmäßig hilft es da natürlich, einen Cold Standby vor dem Switch zu haben, damit dieser nicht potenziell erst vom Hersteller angeliefert werden muss. Das fällt somit auch in den Bereich „Best Practices“.

Hinsichtlich der Frage der AfD: Künstliche Intelligenz würde ich persönlich in diesem Bereich nicht empfehlen, insbesondere weil bei vielen dieser Dinge einfach nicht interpretierbar ist, was wirklich passiert ist und inwieweit die Künstliche Intelligenz eventuell Entscheidungen getroffen hätte, die jemand, der wirklich Erfahrung mit dem System und Ahnung von dem Verwaltungsnetz hat, nicht getroffen hätte. Zum Teil könnte das zu noch schlimmeren Ausfällen führen. Deshalb würde ich persönlich empfehlen, einen weiten Bogen um Künstliche Intelligenz im Bereich der kritischen Infrastruktur zu machen. Das gilt vor allem noch derzeit. Das Forschungsfeld ist einfach nicht so weit ausgebaut, dass klar wäre, was man mit den Daten, die man potenziell gewinnen würde, machen könnte.

Johannes Rundfeldt (AG KRITIS): Danke für die an mich gestellten Fragen. Frau Brems, ich beginne mit Ihrer Frage, welche Anpassungen wir für besonders notwendig halten. – Nun, wir haben relativ wenige Informationen zu der genauen Netzstruktur. Herr Dr. Weckendrup kann das sicherlich im Detail besprechen. Wir sind hier jetzt allerdings nicht in einem technischen Meeting mit Ingenieuren des Unternehmens IT.NRW, sondern wir sind in einem politischen Rahmen. In diesem Rahmen möchte ich die Anpassungen, die an der IT-Infrastruktur des Landes NRW passieren müssen, diskutieren. Und da halten wir vor allen Dingen gesetzliche Anpassungen für notwendig.

Dieser Ausfall ist nur ein Symptom eines tiefer liegenden Problems. Über dieses tiefer liegende Problem möchte ich hier sprechen. Das Problem wird durch das unmittelbar bevorstehende Inkrafttreten des Onlinezugangsgesetzes brennend stärker. Damit ist der Bürger komplett abhängig von einer funktionierenden staatlichen digitalen Infrastruktur der Behörden und Ämter. Diese Infrastruktur darf daher nicht ausfallen, sie kann aber ausfallen. Es gibt dafür viele Auslöser: Wir hatten Überschwemmungen – zum Beispiel im Ahrtal –, wir hatten Ransomware in Mecklenburg-Vorpommern, wir hatten im Bundestag 2017 Spionage aus dem Ausland, wir haben Folgen und Schäden von Hackbacks in anderen Ländern beobachtet. Und allzeit beliebt ist das Thema der schlecht betriebenen oder schlecht gesicherten IT-Infrastruktur. Wenn diese Dinge ausfallen, dann ist die unmittelbare Auswirkung, dass die Bürgerinnen und der Staat nicht mehr handlungsfähig sind.

Außerhalb des Sektors „Staat und Verwaltung“ hat der Gesetzgeber dafür Gesetze erlassen, die sich zum Beispiel im BSI-Gesetz und in der Kritisverordnung wiederfinden. Anwendbar ist dies für privatwirtschaftliche Betreiber von Infrastruktur. In der Theorie

war 2016 auch mal vorgesehen, dass es etwas für den Sektor „Staat und Verwaltung“ geben sollte, und der Bund hat den UP Bund gegründet und damit seine Verantwortung erfüllt und eine Verordnung erlassen. Die 16 Länder haben dies unserer Kenntnis nach nicht getan. Da schließe ich das Land NRW ein.

Laut Gesetz müssen kritische Infrastrukturen nach dem Stand der Technik betrieben werden, und zwar in Bezug auf Vertraulichkeit, Integrität und Verfügbarkeit. Die Verfügbarkeit ist bei dem vorliegenden Sachverhalt im April 2021 nicht ausreichend bedient worden. Der Vorfall und der Ablauf des Vorfalls zeigen, dass dort eben nicht nach Stand der Technik gehandelt wurde; denn der Ausfall einer Leitung, eines Netzsegments, eines Routers darf eigentlich nicht dazu führen, dass ein Netz wegbricht.

Aus unserer Sicht ist das Landesverwaltungsnetz NRW klar eine kritische Infrastruktur im engeren Sinne. Der Ausfall hat gezeigt, dass das Schutzziel der Verfügbarkeit nicht erreicht wurde. Deswegen ist es aus unserer Sicht alternativlos, dass der Sektor „Staat und Verwaltung“ mindestens gleich hohen, wenn nicht sogar höheren Anforderungen genügt, als das BSI-Gesetz es nach den §§ 8a und 8b für private Betreiber vorgibt.

Wichtig ist dabei auch, dass IT-Sicherheit kein Wettbewerbsvorteil sein darf. Alle 16 Länder müssen im Einklang voranschreiten und es überall besser machen, als es jetzt gerade ist. Denn es gibt nur einen Cyberraum. Im Cyberraum gibt es keine Ländergrenzen oder Zuständigkeiten zwischen Bund und Ländern. Deswegen müssen alle 16 Länder und der Bund gemeinsam vorangehen.

Kommen wir zum Thema „Verhältnismäßigkeit“. Der Staat macht den KRITIS-Betreibern hohe, strafbewehrte Auflagen in Bezug auf die Einhaltung der Schutzziele Verfügbarkeit, Integrität und Vertraulichkeit der Infrastrukturen, aber er sorgt im eigenen Haus, im eigenen Betrieb eben nicht dafür, das vergleichbar hohe Auflagen gelten. Das heißt, wir brauchen diese Umsetzung. Seit 2016 ist aus unserer Sicht überfällig, dass die 16 Bundesländer eine KRITIS-Gesetzgebung für den Sektor „Staat und Verwaltung“ erlassen.

Eventuell gibt es einzelne interne behördliche Vorschriften. Keinem unserer 42 Mitglieder, von denen mehrere sogar im Land NRW Informationssicherheits- oder Datenschutzbeauftragte sind, war eine solche Vorschrift aber bekannt; niemand konnte so etwas zitieren. Daraus schließen wir: Es gibt sie nicht, oder sie ist intransparent und hat keine verbindliche Wirkung für alle Behörden des Landes.

Diese Vorschriften zu schaffen, ist eine Aufgabe der Länder. Deswegen können wir nur an den Landtag appellieren, sich mit allen 16 Ländern zusammenzusetzen und verbindliche, rechtssichere, transparente gesetzliche Regelungen für den Sektor „Staat und Verwaltung“ zu schaffen.

Daraus folgt dann ein Umsetzungsaufwand, zum Beispiel für die Dienstleister des Landes NRW. Im Rahmen des Umsetzungsaufwands gibt es etablierte, definierte Prozesse, die in der Wirtschaft seit 2016 regelmäßig geübt werden. Dann sind die Netze auch in einem aktuellen Zustand.

Es ist nicht einmal so, dass da besonders viel neu geschaffen werden muss. Wir gehen davon aus, dass man große Mengen der Auflagen und Vorschriften aus dem Anhang 5 der Kritisverordnung, dem einschlägigen Anhang für Informations- und Kommunika-

tionsdienstleister, adaptieren und direkt weiterverwenden kann. Man müsste es nur tun, und dazu rufen wir auf.

Zur Frage der AfD zum Einsatz von KI, um mehr Resilienz zu erreichen: Wir als AG KRITIS können davon nur abraten. Die dafür verwendeten Gelder wären besser bei Brot-und-Butteraufgaben angelegt wie zum Beispiel bei der Vereinheitlichung von Übertragungswegen von Daten, der Schaffung von redundanten Infrastrukturen – wenn die eine ausfällt, kann man auf die andere umschalten – oder bei Krisenübungen.

Das erlaubt es mir, elegant zu der Frage von Frau Kampmann überzuleiten. Ja, Krisenübungen finden statt, und sie sind in der Privatwirtschaft regelmäßig anzutreffen. Es gibt Dienstleister, die sich darauf spezialisiert haben, Krisenübungen durchzuführen. Das wäre auch im Sektor „Staat und Verwaltung“ notwendig.

Die Behörden sind in sich hierarchischer organisiert als die Privatwirtschaft, und insbesondere mangelt es, wie wir an vielen Stellen beobachten durften, an einer Fehlerkultur. Eine Katastrophen- und Krisenübung bringt nur dann etwas, wenn sie wehtut. Das heißt, die Übung dient dem Zweck, Fehler in der Struktur der Behörden aufzudecken. So, wie Behörden in Deutschland im Regelfall ticken, sorgt das dafür, dass insbesondere in mittleren und höheren Führungsebenen empfindliche Karriereeinschränkungen der Beteiligten entstehen, wenn diese Fehler auftauchen.

Deswegen hat sich der Staat etwas ausgedacht, nämlich sogenannte Stabsrahmenübungen. Bei einer Stabsrahmenübung kommen die Beteiligten in einem Raum wie diesem hier zusammen und tun so, als würden sie eine Krise bewältigen, aber am Ende passiert nichts. Es wird keine Infrastruktur angefasst, kein Techniker wird informiert, es läuft keine Logistik an, keine Materialien werden von A nach B geschafft, keine Personen kommen zum Einsatz. Man stellt sich vor, dass das einfach alles genau so passiert, wie man es sich im Sitzungssaal ausdenkt. Das hat den Vorteil, dass dabei keine Fehler passieren oder aufgedeckt werden können. Damit kann man immer aus der Übung gehen und sagen: Das haben wir ja gut bewältigt.

Ein vielleicht bekanntes Beispiel für eine Stabsrahmenübungen ist die sogenannte LÜKEX-Übung, die alle zwei Jahre durch das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe zusammen mit dem BSI ausgerichtet wird. Sie wird auch nächstes Jahr wieder stattfinden. Wir als AG KRITIS können nur davon abraten, Stabsrahmenübungen als Übung zu betrachten. Denn dabei tauchen keine Fehler in der Struktur auf, die man dann beheben kann.

Daraus folgt: Fehlerkultur ist das Thema, das die Behörden vorrangig angehen müssen, bevor Übungen und Trainings wirklich Sinn machen. Es geht darum, eine Fehlerkultur zu schaffen, auf Augenhöhe miteinander zu sprechen, verschiedene Ebenen zusammenzuziehen, Austauschrunden zu schaffen. Denn die Missstände in der digitalen Infrastruktur sind auf den unteren Ebenen überall bekannt. Sie können jeden Admin fragen, was ihm wehtut, was ihn nervt, was nicht gut funktioniert. Aber diese Missstände werden unzureichend oder unvollständig in die oberen Hierarchieebenen kommuniziert. Denn natürlich befürchten die dort zuständigen Beamten eine Einschränkung ihrer Karrieremöglichkeiten in der Zukunft, wenn sie ehrlich kommunizieren. Es muss also ganz oben

angesetzt werden, damit die Fehlerkultur in den Behörden besser wird. Und dann habe ich auch Hoffnung, dass die Dinge besser werden könnten.

Kommen wir zu weiteren Maßnahmen, die wir in diesem Zusammenhang empfehlen. Insbesondere richtet sich dies an den Bund. Hier sind heute mehrere Vertreter von Parteien anwesend, die gerade einen Koalitionsvertrag verhandeln. Ihnen möchte ich mitgeben, dass Sie bitte die Unabhängigkeit des Bundesamts für Sicherheit in der Informationstechnik in den Koalitionsvertrag aufnehmen. Ich möchte Ihnen mitgeben, dass Sie sich für eine defensive IT-Sicherheitsstrategie einsetzen. Beide Aspekte sind im Übrigen Forderungen, die bereits Beschlusslage der FDP-Fraktion im Deutschen Bundestag sind. Ich möchte Ihnen mitgeben, dass Sie sich für die Rechtssicherheit von IT- und Sicherheitsforscherinnen einsetzen. Das ist ebenfalls Beschlusslage der FDP-Fraktion im Deutschen Bundestag. Und letztendlich kann ich nur den Aufruf wiederholen, für alle Behörden aller Bundesländer für verbindliche, transparente und gesetzliche Regelungen für den Einsatz von IT-Infrastruktur im Sektor „Staat und Verwaltung“ zu sorgen.

Dr. Behrooz Moayeri (ComConsult GmbH): An mich sind zwei Fragen gerichtet worden. Frau Brems, Sie haben die Frage gestellt, was die wichtigsten Anforderungen an die Weiterentwicklung des Landesverwaltungsnetzes sind. So habe ich es verstanden.

Aus meiner Sicht sind es vier Anforderungen: Leistungsfähigkeit, Sicherheit, Verfügbarkeit, Wirtschaftlichkeit. Da Herr Rundfeldt auf die politischen Aspekte eingegangen ist, möchte ich mich auf die Technik konzentrieren. Die Vorgaben stammen ja von der Politik. Was ist das zum Beispiel für eine Vorgabe, von diesen vier Zielen, die manchmal im Zielkonflikt stehen, das eine oder das andere Ziel zu favorisieren bzw. zu bevorzugen? Die Ziele „Wirtschaftlichkeit“, „Verfügbarkeit“, „Sicherheit“ und „Leistungsfähigkeit“ können durchaus im Zielkonflikt miteinander stehen.

Ich möchte auch ein bisschen davor warnen, dass vielleicht die Erwartungshaltung entsteht, dass, wenn die Politik etwas beschließt, dies automatisch auch umgesetzt ist. Es ist in der Technik wie auch in der Coronapandemie: Einige Dinge sind viel zu komplex, als dass man sie beherrschen könnte. Auch verbindliche Regelungen würden nicht weiterhelfen, Herr Matheisen, wenn man bestimmte äußere Bedingungen nicht beeinflussen kann.

Ich habe jetzt etwas von regelmäßigen Übungen gehört – nicht nur kalte Übungen, sondern auch warme Übungen. Ja, das ist eine tolle Sache. Ich möchte aber darauf hinweisen, dass das einen Mehraufwand, mehr Personalaufwand bedeutet.

Es gibt eine Randbedingung, an der Sie nichts ändern können: Wo kommen die Fachkräfte her, die die schönen Beschlüsse der Politik umsetzen sollen? Sie stehen als öffentliche Verwaltung mit der Wirtschaft im Wettbewerb um die Fachkräfte. Auch da muss sich etwas ändern. Die öffentliche Verwaltung muss im „war for talent“ – das ist ein unschöner Ausdruck – wettbewerbsfähiger werden. Der Markt ist leergefegt. Die Wirtschaft kann Ihnen ein Lied davon singen. Die Frage ist: Wie können Sie Fachkräfte für das Landesverwaltungsnetz bzw. für die öffentliche Verwaltung gewinnen und im Wettbewerb mit der Wirtschaft diesbezüglich bestehen?

Die anderen Aspekte habe ich in meiner Stellungnahme aufgeführt, auf welche ich hier verweisen möchte.

Angesichts der sehr ausführlichen Stellungnahme des Ministers bei der letzten Anhörung, die jetzt im Web veröffentlicht ist, habe ich nicht den Eindruck, Herr Rundfeldt, dass hier die Transparenz das Problem ist. Es ist sehr transparent. Ich konnte anhand öffentlicher Dokumente vieles ablesen. Aber was ich nicht ablesen kann, ist, ob diese vielleicht verspätete Reaktion technisch begründet war oder auf einer Präferenz gründete. Wie ich den Minister im Protokoll verstanden habe, stand man, da die Mehrheit der Landesverwaltung weiterarbeiten konnte, vor der Entscheidung, ob man eine Unterbrechung für alle riskiert, um eine Unterbrechung für einige zu beheben. Wann gehen wir dieses Risiko ein?

Das wurde in den frühen Morgenstunden des dritten Tages beschlossen, was natürlich darauf hindeutet, dass hier kein Rund-um-die-Uhr-Betrieb gemacht wird. Auch das ist etwas, was man beschließen kann, was man aber vielleicht doch nicht umsetzen kann, weil man nicht die Personalkapazitäten dafür hat.

Alles Weitere habe ich in meiner Stellungnahme ausgeführt.

Vorsitzender Thorsten Schick: Das ist gut; denn Stellungnahmen sollen auch intensiv studiert werden. Zwischendurch mal darauf zu verweisen, schärft den Blick für das, was wir schon auf dem Papier haben.

Wir würden dann in die zweite Fragerunde einsteigen. Frau Brems war die erste Person, die sich gemeldet hat. Es folgen Frau Kampmann, Herr Dr. Untrieser und Herr Matheisen.

Wibke Brems (GRÜNE): Herzlichen Dank für die Antworten in der ersten Runde. Ich habe nun zunächst zwei Fragen an Herrn Dr. Weckendrup.

Vorhin ist in zwei Äußerungen auf die Übungen hingewiesen worden. Mich würde interessieren, was Sie dazu sagen können, wie oft und in welcher Form Übungen – ob kalt oder warm – bei Ihnen im Haus, auch mit anderen zusammen, gemacht werden.

Die zweite Frage: Sie haben in Ihrer Stellungnahme Bedarfe angedeutet, um den Anforderungen der fortschreitenden Digitalisierung dauerhaft gerecht werden zu können. Handelt es sich dabei um allgemeinen Mehrbedarf in allen Bereichen, oder gibt es spezielle Bereiche, worauf dies zutrifft?

Dann habe ich noch eine Frage an Herrn Rundfeldt. Sie beschreiben es in Ihrer Stellungnahme und sind eben auch kurz darauf eingegangen, mir ist aber noch nicht klar, was es genau bedeutet, dass das Land mit seinen eigenen Standards unterhalb dessen liege, was der Staat den privaten Unternehmen vorschreibt. Vielleicht könnten Sie das noch erläutern oder ein Beispiel dafür bringen. Und welche Schlussfolgerungen ziehen Sie daraus?

Christina Kampmann (SPD): Es ist deutlich geworden, wie wichtig es ist, dass gerade mit der Umsetzung des OZG dieser Teil der kritischer Infrastruktur tatsächlich so weit

gestärkt wird, wie es möglich ist. Mein Fragen richten sich daher ebenfalls an Herrn Dr. Weckendrup. Sie gehen in dieselbe Richtung wie die Fragen von Frau Brems.

Wir haben jetzt sehr viel über Übungen diskutiert, die das Ganze vielleicht in einem weiteren Fall oder in anderen Fällen verhindern könnten. Es wurde eine mögliche andere Fehlerkultur angesprochen, ebenso wie das Fachkräfteproblem. Mich würde interessieren, was aus Ihrer Sicht notwendig wäre, damit Sie nicht nur kalte, sondern auch warme oder praktische Übungen so durchführen können, dass dies für die Stabilität des Landesverwaltungsnetzes hilfreich wäre.

Die zweite Frage bezieht sich auf das, was von der AG KRITIS gerade gesagt wurde. Sie haben gesagt, dass das Ganze durchaus auch auf tief liegende Missstände in der Digitalisierung der Landesbehörden hindeuten kann. Sie haben gesagt, dass kritische Infrastrukturen nach dem Stand der Technik betrieben werden müssten. Sie haben aus Ihrer Sicht Indikatoren angeführt, warum dies nicht der Fall ist. Herr Dr. Weckendrup, dazu würde mich Ihre Meinung interessieren; denn dass es auf dem Stand der Technik ist, ist essenziell für das Funktionieren des Landesverwaltungsnetzes.

Dr. Christian Untrieser (CDU): Ich möchte Herrn Professor Engel um eine Einordnung bitten. In der ersten Runde und auch in der Stellungnahme hat der geschätzte Herr Rundfeldt die Lage doch relativ kritisch eingeschätzt. Ich meine das aber positiv. Wir freuen uns, dass Sie da sind, und wir wollen hier ja auch etwas lernen. Aber Sie haben die Lage eben insgesamt relativ kritisch eingeschätzt. Herr Professor Engel, wie bewerten Sie es? Auf welchem Stand der Technik ist die Landesverwaltung? Nach welchen Zertifizierungen arbeitet man? Wie würden Sie die Lage insgesamt einschätzen? Vielleicht könnten Sie sich da auch etwas auf Herrn Rundfeldt beziehen.

Rainer Matheisen (FDP): Ich habe festgestellt, dass sowohl die Kollegin Kampmann mit ihren Fragen an Herrn Dr. Weckendrup als auch Herr Dr. Untrieser meine Fragen vorweggenommen haben. Von daher verzichte ich auf weiteren Fragen.

Vorsitzender Thorsten Schick: Dass die vorangegangenen Fragen und Anmerkungen in ähnliche Stoßrichtungen gingen, zeigt ja nur, Herr Matheisen, wie zielgerichtet wir hier Befragungen durchführen. – Herr Professor Engel hat am längsten gewartet, und daher schlage ich vor, dass er in der zweiten Fragerunde mit seinen Antworten beginnt.

Prof. Dr. Andreas Engel (KDN – Dachverband kommunaler IT-Dienstleister *[per Video zugeschaltet]***):** Ich will das Thema gerne aus der Sicht eines kommunalen IT-Dienstleisters aufgreifen. So sehr ich die AG KRITIS auch schätze, hat Herr Rundfeldt nach meinem Geschmack im Zusammenhang mit diesem Störfall etwas häufig von Missständen gesprochen. Ich habe das nicht so bewertet und auch nicht so gesehen. Denn obwohl ich mich nur auf die vorliegenden veröffentlichten Landtagsdrucksachen stützen kann, muss ich doch sagen, dass der Störfall nachvollziehbar und plausibel beschrieben worden ist und auch die eingeleiteten Maßnahmen zur Störungsbehebung aus meiner Sicht durchaus angemessen und geeignet waren.

Nach meiner Einschätzung ist es allenfalls ein mittlerer Störfall gewesen, auch wenn man die Zeiten betrachtet. Er ist am 19. nach Dienstschluss aufgetreten. Die Monitoringsysteme des Landesbetriebs IT.NRW haben den Störfall entdeckt. Das ist schon mal ganz wichtig. Es gab auch noch eine Meldung aus dem Justizministerium. Dann ist nach meiner Wahrnehmung direkt mit der Störungsanalyse und -behebung begonnen worden, und der externe Dienstleister ist einbezogen worden. Am Vormittag des nächsten Tages war das Störungsbild klar, und es waren auch die Maßnahmen identifiziert, die dann umgesetzt werden sollten.

Wenn dann IT.NRW in Abstimmung mit dem Digitalministerium entschieden hat, den Neustart des Netzes in die frühen Morgenstunden des nächsten Tages zu verschieben, dann ist das eine Güterabwägung, die ich auch nachvollziehen kann; denn es waren ja nur etwa 10 % der Behörden betroffen, und mit dem Neustart des Landesverwaltungsnetzes wären alle Behörden im Tagesbetrieb betroffen gewesen. Ich finde, das hat sich alles noch im Rahmen gehalten.

Natürlich muss man aus dem Störfall lernen. Das hat Herr Dr. Weckendrup auch gesagt, und das hat IT.NRW offensichtlich auch getan. Herr Dr. Weckendrup hat die Maßnahmen schon erläutert.

Was die allgemeine Bewertung des Sicherheitsmanagements und des Betriebsmanagements bei IT.NRW angeht, kann ich mir natürlich als kommunaler IT-Dienstleister nicht ein abschließendes Urteil erlauben, indem ich in den Betrieb reinschaue und feststelle, wie der Betrieb bzw. das Betriebsmanagement organisiert ist. Aber man kann es im Internet recherchieren: Der Landesbetrieb IT.NRW ist nach ISO 27001 – BSI-Grundschutz – vom Bundesamt für Sicherheit in der Informationstechnik zertifiziert. In diesem Zertifikat ist ein hoher Sicherheitsstandard bestätigt worden.

Die Zertifizierung nach BSI-Grundschutz ist eine Maßnahme, die auch für die privaten IT-Dienstleister aus den KRITIS-Branchen hinsichtlich der Herangehensweise und auch hinsichtlich der Orientierung an ISO-Standards gefordert und umgesetzt wird, teilweise auch nur mit Teilen des Maßnahmenkatalogs „BSI-Grundschutz“. Ich muss hier schon auch einmal feststellen, dass der Betrieb IT.NRW durchaus hohe Anforderungen an das Sicherheitsmanagement erfüllt und eine Zertifizierung mitbringt, die schließlich bei der Umsetzung der NIS-Richtlinie – das ist ja die EU-Richtlinie, über die wir hier im KRITIS-Umfeld reden – eine geeignete und auskömmliche Maßnahme ist.

Im Übrigen ist es ja so: Diese NIS-Richtlinie, die EU-Richtlinie, stammt aus 2016. Es heißt, dass eine Novellierung dieser Richtlinie Ende dieses Jahres noch kommen soll, spätestens Anfang des nächsten Jahres. Dann sind sowohl Bund als auch Länder aufgefordert, innerhalb von 18 Monaten eine Umsetzungsplanung für die EU-Richtlinie vorzulegen. Das wäre ja dann genau diese gesetzliche Maßnahme, die Bund und Länder umsetzen müssten, damit dann auch die Forderungen und Kriterien an das Sicherheitsmanagement von öffentlichen IT-Dienstleistern definiert sind.

Johannes Rundfeldt (AG KRITIS): Frau Brems fragte, wie es sein kann, dass das Land hinter dem zurückbleibt, was der Staat den privaten Betreibern vorgibt, und was ich damit meine. Mit der IT-Sicherheitsgesetzgebung – IT-Sicherheitsgesetz 1.0 von

2016 –, die die Umsetzung der eben erwähnten NIS-Richtlinie darstellt, hat der Staat Vorgaben für zu dem Zeitpunkt neun KRITIS-Sektoren gemacht. Von diesen neun KRITIS-Sektoren wurde allerdings lediglich für sieben eine Verordnung geschaffen; die Kritisverordnung. Die beiden Sektoren „Kultur und Medien“ und „Staat und Verwaltung“ sind nicht berücksichtigt worden. Für diese gibt es unserer Kenntnis nach keine Kritisverordnung oder ein vergleichbares Äquivalent.

Wir stehen kurz vor der Umsetzung der NIS-2-Richtlinie. Aus unserer Sicht ist es so, dass die NIS-Richtlinie für den Sektor „Staat und Verwaltung“ nicht umgesetzt worden ist. Sonst gäbe es dazu ein öffentlich einsehbares Gesetz oder eine Vorschrift, die dies darlegt. Das halten wir für einen großen Missstand in der politischen Struktur der Bundesländer.

Es ist nicht so, dass es ausreichen würde, die NIS- oder die NIS-2-Richtlinie umzusetzen; denn daneben gibt es auch noch die RCE-Direktive, die sich mit kritischen Infrastrukturen befasst und die auch dem Sektor „Staat und Verwaltung“ konkrete Pflichten auferlegt. Auch diese müsste umgesetzt worden sein, sie ist aber in den Bundesländern bisher nicht umgesetzt worden.

Wenn wir zu den Kommunen schauen, dann stellen wir fest, dass es äußerst uneinheitlich geregelt ist. Beispielsweise betreibt das Äquivalent von IT.NRW in Hessen – dort gibt es auch einen Dienstleister, dessen Name mir gerade entfallen ist; er lässt sich aber sicherlich herausfinden – das Landes-CERT für Hessen. Dieses Computer Emergency Response Team ist zuständig für die Kommunen und für die Landesbehörden. In NRW ist dem nicht so. Das Landes-CERT, das von dem Arbeitgeber IT.NRW betrieben wird, ist eben nicht automatisch zuständig für die Kommunen, sondern es ist nur dann zuständig, wenn die Kommunen monatlich einen gewissen Obolus an den Dienstleister entrichten.

Das empfinde ich persönlich als einen unglaublichen Missstand; denn wenn wir schon den Fachkräftemangel, den Herr Moayeri treffend beschrieben hat, feststellen, dann kann die Antwort doch nicht lauten: Wir haben hier Ressourcen, aber wir geben sie euch nicht, weil ihr nicht genug bezahlt. – Das ist innerhalb des Staats. Das ist „rechte Tasche, linke Tasche“. Es ist nicht so, dass diese Gelder nicht vorhanden wären oder umgeschichtet werden müssten. Das meine ich mit einer Vereinheitlichung zwischen den 16 Bundesländern, die dringend notwendig ist.

Um noch einmal zu der Frage von Frau Brems zurückzukehren: Der Sektor „Staat und Verwaltung“ hat diese Vorschriften in dieser Form nicht erlassen. Es gibt keine Vorschrift, aus der ersichtlich ist, welche Infrastrukturen oder welche Infrastrukturkomponenten, welche Anlagenteile besonders kritisch sind. Zum Beispiel in Anhang 5 – IKT – Abschnitt drei in der Kritisverordnung finden sich Tabellen, in denen gesagt wird: Ein Rechenzentrum mit 25.000 Maschinen gilt als KRITIS. Solche konkreten Vorgaben, was KRITIS im Sektor „Staat und Verwaltung“ ist, brauchen wir.

Hinten heraus kann man dann als umsetzendes Mittel bzw. als Werkzeug eine ISO-27001-Zertifizierung, einen Grundschutz oder ein Baukastensystem nehmen. Das hat die Wirtschaft seit 2016 geübt. Es gibt zig Dienstleister, die anbieten, dies für einen KRITIS-Betreiber umzusetzen.

Ich kann nur an den Staat appellieren, für die Länder eine Umsetzung dieser Art zu machen. Dann klappt es auch mit der NIS-2- und der RCE-Richtlinie, die im nächsten Jahr kommen wird.

Dr. Dirk Weckendrup (IT.NRW): Ich möchte zunächst gerne auf einen Impuls von Ihnen, Frau Kampmann, reagieren. Auch Sie haben von Missständen gesprochen und nach dem Stand der Technik gefragt.

Ich möchte aus meiner Position darauf hinweisen, dass ich glaube, dass wir ein sehr, sehr hoch qualifiziertes Team bei IT.NRW für den Aufbau, die Verwaltung und die Konzeption unseres Landesverwaltungsnetzes haben, das mit viel Engagement bis spät in die Nacht hinein – die Zeiten sind dem Bericht zu entnehmen – an der Fehlerbehebung gearbeitet hat.

Wir haben für die Behörden im Land ein abgestuftes Dienstleistungsangebot, das sich nicht nur auf die Bandbreite, also darauf, wie viel Verkehr genutzt wird, beschränkt, sondern eben auch auf die Verfügbarkeit abzielt. Wenn eine Behörde für sich in Anspruch nimmt, dauerhaft höhere Verfügbarkeiten in einem SLA von uns garantiert haben zu wollen, so ist dies jederzeit möglich. Wir können zweite Leitungen dazubuchen und Ähnliches. Die Ministerien haben beispielsweise genau das für sich in Anspruch genommen. Jede Behörde kann uns also beauftragen, sowohl die Bandbreite als auch die Verfügbarkeit zu erhöhen.

Noch ein Aspekt hinsichtlich des Stands der Technik ist, dass wir regelmäßig unsere Dienstleistungen, die wir in Anspruch nehmen, ausschreiben. Wir suchen immer wieder Partner für die Erbringung dieser der Leitungsinfrastruktur zugrunde liegenden Dienstleistungen. Auch da werden die zugesagten Verfügbarkeit sowie die entsprechenden Reaktionszeiten, die wir mit unseren Dienstleistern vereinbaren, mit jeder Ausschreibung besser. Insofern würde ich mich in der Tat gerne Herrn Professor Dr. Engel anschließen: Hier von Missständen zu reden, finde ich nicht angemessen.

Gleichwohl – das habe ich gerade schon gesagt – ärgert natürlich jeder Fehler. Aber ein Bagger, der eine Leitung durchtrennt, ist erst einmal ein Problem, auf das wir persönlich keinen Einfluss haben; denn das war die Ursache dieses Themas. Insofern bin ich der Meinung, dass unser Team zusammen mit dem externen Dienstleister, mit der Telekom, diese Fehler, diese Krisensituation im Rahmen der Möglichkeiten abgearbeitet hat.

Das Thema „Fehlerkultur“ wurde bereits angesprochen. Klar, zu jedem Fehler gehört, daraus etwas zu lernen. Ich habe es bereits ausgeführt: Das haben wir getan. Dazu stehen wir, und das gehört dazu. Es ist nicht so, wie Herr Rundfeldt ausgeführt hat, dass ich beim Adressieren eines Fehlers in meinem Team Sorge hätte oder damit rechnen müsste, dass ich die nächste Beförderung nicht bekomme. Diese Zeit haben wir, denke ich, zumindest in unseren Teams weit hinter uns gelassen.

Ich würde gerne noch etwas zu dem Fragenkomplex der Übungen sagen. Ich gebe zu, dass Übungen immer zwei Seiten mit sich bringen. Einerseits möchte man aus einer Übung etwas lernen. Man möchte sehen, ob Redundanzmechanismen und Ähnliches greifen. Damit verbunden ist aber immer auch die Gefahr, dass Sie das, was Sie eigent-

lich schützen wollen, nämlich die Verfügbarkeit der Services bei den Kunden, also bei unseren Behörden, ganz bewusst beeinträchtigen. Sie gehen einfach ein hohes Risiko ein. Wenn Sie so einen Fehler finden, bedeutet dies: Da fällt irgendetwas aus.

Insofern ist die Anzahl dieser wirklich aktiven Übungen nicht so hoch. Wir nehmen regelmäßig an den LÜKEX-Übungen teil, wir haben einen IT-Notfallbeauftragten, wir haben – auch das ist bereits ausgeführt worden – entsprechende BSI-Konzepte, die wir umsetzen. Wenn wir an diesen Clustern arbeiten, sind die regelmäßigen Updates jedes Mal ein Test der Verfügbarkeiten. Denn man nimmt Teile dieses Clusters außer Betrieb, und der andere Teil muss die Verfügbarkeit sicherstellen. Wenn neue Updates eingespielt werden, spielen wir diese natürlich, wie es weltweit Standard ist, nicht als erstes in die Produktionssysteme ein, sondern in die Testsysteme, um zu sehen, wie dort die Reaktion ausfällt. Funktioniert das alles?

Ja, Übungen sind wichtig. Eine gute Vorbereitung von Veränderungen entsprechender Prozesse ist nach meiner Erfahrung aber mindestens genauso wichtig.

Dann richtete sich eine Frage darauf, welche Bedarfe wir hinsichtlich der Digitalisierung sehen. Das ist eine nicht so leicht zu beantwortende Frage. Wenn Sie nach dem Bedarf für Digitalisierung fragen, fragen Sie aus meiner Sicht die komplette Leistungskette ab. Wenn Sie eine Leistung vom Arbeitsplatz bis hin zum Bürger erbringen wollen, müssen Sie alle Glieder dieser Kette betrachten. Das LVN ist davon ohne Zweifel ein ganz besonders wichtiges. Im Grunde müssen Sie aber die gesamte Leistungskette sehen.

Das LVN spielt in der Tat eine besondere Rolle. Deswegen erfolgt auch diese sehr intensive und konzentrierte Weiterentwicklung des Netzes. Gemeinsam mit dem MWIDE sind wir jedes Jahr dabei, es bedarfsgerecht weiterzuentwickeln, um speziell dem Vernetzungsaspekt innerhalb der Landesverwaltung ausreichend Rechnung zu tragen.

Vorsitzender Thorsten Schick: Damit sind die Fragen der zweiten Runde beantwortet. Herr Dr. Untrieser und Frau Brems haben sich noch zu einer dritten Fragerunde gemeldet.

Dr. Christian Untrieser (CDU): Ich würde gerne noch einmal Herrn Rundfeldt ansprechen. Ich habe Ihre Stellungnahme mit großem Interesse gelesen. Wenn ich es richtig verstanden habe, dann stören Sie sich daran, das für Staat und Verwaltung – als einer dieser KRITIS-Sektoren – nicht explizit genannt wird, dass der Staat da etwas tun muss. Das war der Vorwurf.

Nun habe ich aber gerade gelernt, dass das Land bzw. IT.NRW nach ISO 27001 zertifiziert ist. Ich meine, in Ihrem letzten Beitrag haben Sie gesagt, dass dies durchaus ein probates Mittel wäre: Wenn man diese Zertifizierung nach ISO 27001 hat, dann ist man zumindest auch auf dem aktuellen Stand und ordentlich geschützt.

Damit ich es richtig verstehe: Sie hätten zwar lieber die gesetzliche Verpflichtung, aber so, wie es derzeit aufseiten des Landes geregelt ist, ist es vom Stand der Technik her auch in Ordnung? Habe ich das so richtig verstanden?

Ich habe dann noch eine Frage an die gesamte Runde. Wir haben schon über Nordrhein-Westfalen und über verschiedene Bundesländer gesprochen. Falls sich jemand berufen fühlt, es zu beantworten: Gibt es andere Bundesländer, die es eventuell anders – besser oder schlechter – machen als Nordrhein-Westfalen? Wie ist Nordrhein-Westfalen im Bundesländervergleich aufgestellt?

Wibke Brems (GRÜNE): Wenn ich es gerade richtig verstanden habe, ging es bei IT.NRW darum, dass das Einspielen von Updates quasi auch eine Art Übung ist. Weil ich in diesem Bereich einfach nicht so tief drin bin und um es technisch nachzuvollziehen, würde ich gern Herrn Moayeri und Herrn Rundfeldt fragen, ob dies aus Ihrer Sicht wirklich ausreichend ist, wenn man doch sagt, man bräuchte eigentlich bestimmte Übungen. Ist das in solchen Fällen wirklich ausreichend, oder müsste man damit andere Dinge verbinden? Oder bräuchte man noch ganz andere Übungen?

Vorsitzender Thorsten Schick: Wir beginnen die dritte Antwortrunde bei Herrn Moayeri und gehen dann in umgekehrter Reihenfolge zur ersten Runde vor.

Dr. Behrooz Moayeri (ComConsult GmbH): Herr Dr. Untrieser, Sie haben gefragt, wie NRW im Vergleich zu anderen Bundesländern dasteht. Wir beraten einige der Bundesländer, und das, was am 19., 20. und 21. April passiert ist, also dieser teilweise Ausfall des Landesverwaltungsnetzes, ist durchaus keine Seltenheit. Ich kann bei solchen Ausfällen, die auf Landesebene, auf Ebene der kommunalen Rechenzentren oder auf Ebene der Bundeseinrichtungen passieren, nicht sagen, dass NRW im Vergleich zu anderen öffentlichen Verwaltungen schlechter oder besser dasteht.

Auch kann ich nicht den Eindruck bestätigen, dass die Wirtschaft weiter sei als die öffentliche Verwaltung, wie heute sehr gelobt wurde. Ich bin seit über 30 Jahren immer wieder auch in solchen Krisenstäben eingeweiht und eingebunden. Troubleshooting ist sozusagen mein Hobby. Überall dort, wo Dinge wirklich sehr schnell entschieden werden müssen, bin ich auch als Techniker immer wieder gefragt. Mein Eindruck ist nicht, dass die Netze der öffentlichen Verwaltung diesbezüglich wesentlich schlechter dastehen als die Netze der Wirtschaft.

Ich habe vorhin von den Zielkonflikten gesprochen. Die größten Baustellen der öffentlichen Verwaltung, die ich im Moment sehe, finden sich nicht im Bereich der Netze, die auch mal durch einen Bagger, wie Herr Dr. Weckendrup sagte, in Mitleidenschaft gezogen werden können, sondern beispielsweise der weiße Fleck, den Sie jetzt seit Tagen beim RKI sehen, betrifft eine Kommune, die offensichtlich keine funktionierende Datensicherung hatte. Da sind die größten Gefahren, und da sind die größten Baustellen und der feuchte Keller bei der öffentlichen Verwaltung. Also: Funktioniert die Datensicherung? Wie reagiert man auf solche Angriffe – Ransomware, Verschlüsselung usw.? Viele Krankenhäuser waren in letzter Zeit davon betroffen, beispielsweise auch hier in Düsseldorf.

Die Netze und das, was im April passiert ist, machen den geringsten Teil der Ausfälle aus, die wir im Moment feststellen. Das gilt insbesondere für die öffentliche Verwaltung, die öffentlichkeitswirksam von denjenigen ausgeschlachtet wird, die solche Angriffe

auch durchführen. Ich kann nicht sagen, dass die Trägernetze die größten Probleme verursachen. Es sind eher andere Dinge, die aber natürlich ebenfalls von Standards wie ISO 27001 adressiert werden.

Was die Übungen betrifft, muss man erst einmal die redundanten Strukturen schaffen, die man in solchen Übungen dann auch testet. Die zweite Voraussetzung ist, dass man die Personalkapazität hat, um solche Übungen zu realisieren. Wenn man sich – zum Beispiel aus Wirtschaftlichkeitsgründen – dafür entscheidet, auf die Redundanz zu verzichten, dann kann man auch keine warme Übung daran ausprobieren. Gegen kalte Übungen, wie Sie sie erwähnt haben, Herr Rundfeldt, spricht nichts. Prozesse müssen geübt werden. Aber da würde ich genauso wie die Techniker auch die Politik mit einbeziehen; denn in solchen Dingen – die Erfahrung habe ich gemacht – werden einige Entscheidungen politisch getroffen. Der Inhalt der Stellungnahme des Ministers gibt her, dass es auch eine politische Entscheidung war, diese 10 % der Landesverwaltung erst in den frühen Morgenstunden des dritten Tages lauffähig zu machen.

Johannes Rundfeldt (AG KRITIS): Die ISO 27001 ist ein Baukastensystem. Bevor man damit sinnvoll eine Verbesserung des Status quo erreichen kann – Gleiches gilt für den IT-Grundschutz vom BSI –, braucht es eine Schutzbedarfsanalyse. Herr Dr. Weckendrup hat es gerade schon gesagt: Es gibt Behörden, welche die relevante Leitung bestellt haben, andere haben das nicht getan.

Das erfolgt also zuerst. Wir müssen zuerst die Schutzbedarfsanalyse machen und feststellen, ob die Konsequenz eines Ausfalls einer Faser wäre, dass eine Behörde offline ist. Wenn es sich dabei um eine kritische Infrastruktur handelt, kommt die Schutzbedarfsanalyse zu dem Ergebnis, dass wir eine redundante Leitung vorhalten müssen. Und dann kann man sich aus dem Grundschutz oder aus dem Katalog nach ISO 27001 die Maßnahmen zusammenbasteln: Wie machen wir es mit der zweiten Faser, mit der Redundanz?

Es ist also nicht so, dass ISO 27001 oder IT-Grundschutz konkret vorgeben, was man machen muss, um sicher zu sein, sondern da werden Prozesse beschrieben. Die Vorgaben, die eine Behörde oder ein Stromnetzbetreiber oder ein Flughafenbetreiber erfüllen muss, müssen gesetzlicher Natur sein. Und die gibt es so nicht.

Es gibt beispielsweise im Anhang 2 – Verkehr – eine Vorschrift für bestimmte Flughäfen, dass deren Stromversorgung redundant ausgelegt werden muss. Sie muss also zweimal vorhanden sein. Wenn nun eines der beiden Stromnetze ausfällt, darf der Flughafen nicht mehr betrieben werden, weil die Stromversorgung nicht mehr redundant ist. Wenn wir also von einer redundanten Stromversorgung sprechen und dann eine Übung machen oder etwas wegen einer Wartung abschalten wollen, dann sind wir bei zwei plus eins, also bei drei Stromleitungen, die wir zum Flughafen bauen müssen. Bremen hatte da mal so ein Szenario.

Was hier beschrieben wird – dass wir, wenn wir daran üben, möglicherweise die Redundanz nicht mehr erfüllen –, ist richtig. Dann muss man in der Schutzbedarfsanalyse feststellen, dass wir eben drei Anbindungen pro Behörde brauchen. Und auch das ist noch konservativ und völlig in Ordnung. Dann macht man eine per Laserlink, eine per

60-Gigahertz-Richtfunkstrecke und eine per Faser im Boden. Nur eines dieser drei Dinge kann vom Bagger zerstört werden. Trotzdem ist der redundante Betrieb selbst dann, wenn eine alte, kaputte Mikrowelle einer Anwohnerin noch den 60-Gigahertz-Link stört – auch das wäre möglich; die Bundesnetzagentur braucht zwei Stunden, bis sie da ist und es behoben hat –, noch sichergestellt; denn dann ist der Laserlink noch da.

Auf diesem Niveau müssen wir denken; denn es geht hier nicht darum, dass es mal eine Stunde oder einen Tag ausfallen kann. Es geht hier um kritische Infrastrukturen, also Infrastrukturen, bei deren Ausfall erhebliche Einschränkungen des Gemeinwesens zu befürchten sind.

Bei Infrastrukturen, die weniger als 500.000 Menschen versorgen, ist alles verhandelbar. Das ist nicht KRITIS. Aber Infrastrukturen, die mehr als 500.000 Menschen versorgen, müssen so gebaut sein, dass sie nicht ausfallen können, weil bei der Schutzbedarfsanalyse bereits so geplant wurde, dass das nicht passieren kann. Und wenn diese Planung erfolgt ist, kann man sich aus dem Baukastensystem des BSI und der ISO-Normen das zusammensuchen, was man braucht, um die gesetzlichen Pflichten zu erfüllen. Dieses Fundament – was müssen wir pro Behörde eigentlich machen? – ist von den 16 Landesregierungen in Deutschland so nicht gebaut worden. Das ist ein Missstand, den wir bemängeln.

Ich möchte kurz noch etwas zu Herrn Moayeri sagen. Bei meinen Aussagen zur Transparenz habe ich mich auf die gesetzlichen Vorgaben bezogen, nicht auf die Einlassungen des Ministers. Die waren in dieser Sitzung in der Tat vorbildlich transparent. Das haben wir auch festgestellt. Aber es geht darum, dass es nicht reicht, dass es eine kleine Vorschrift in einer Behörde gibt, die irgendwo irgendein ISB mal erlassen hat – „so machen wir das jetzt“ –, sondern es geht darum, dass es für alle Behörden einheitliche Vorschriften gibt, damit Herr Dr. Weckendrup sagen kann: Alle unsere Kunden brauchen zwei Leitungen – oder in manchen Szenarien auch drei –, und dann läuft das auch.

Prof. Dr. Andreas Engel (KDN – Dachverband kommunaler IT-Dienstleister *[per Video zugeschaltet]***):** Ich möchte gerne noch auf zwei Punkte eingehen. Ich kann mir keinen Vergleich der Sicherheitsniveaus und -standards zwischen den Bundesländern erlauben. Ich kann nur darauf hinweisen, dass die für die öffentliche Verwaltung maßgebliche Zertifizierung ISO 27001 und der BSI-Grundschutz im Internet öffentlich zugänglich sind. Alle IT-Dienstleister der Privatwirtschaft und der öffentlichen Verwaltung, die nach diesem Standard zertifiziert sind, können dort eingesehen werden. Und wenn ich mich recht erinnere, haben längst nicht alle Bundesländer mit ihrem IT-Dienstleister eine solche Zertifizierung.

Ich will noch einen Aspekt erwähnen, der in einem Nebensatz angesprochen wurde: die kommunalen Zuständigkeiten. Es war die Rede davon, dass die Hessische Zentrale für Datenverarbeitung – das Pendant zu IT.NRW – auch die Zuständigkeit für kommunale IT hat. Wir legen als kommunale IT-Dienstleister schon Wert darauf, dass wir die Sicherheit in eigener Verantwortung haben, genauso wie wir kommunale IT-Dienstleistungen in eigener Verantwortung betreiben.

Ich möchte aber darauf hinweisen, dass es gerade Mitte des Jahres, im Juni, hier im Ausschuss eine Anhörung zum Thema „Aufbau eines zentralen Kommunal-CERT“ gab, in der wir die Sachlage und auch die Zusammenarbeit zwischen Land und Kommunen ausführlich erörtert haben. Ich habe die Gelegenheit gehabt, zu erläutern, dass die Zusammenarbeit zwischen der IT des Landes und kommunaler IT sich gerade beim Thema „IT-Sicherheit“ sehr positiv entwickelt hat. Es gibt eine sehr enge Zusammenarbeit. Das CERT NRW teilt alle vorliegenden Warn- und Informationsmeldungen mit den kommunalen Stellen. Das CERT ist … *(akustisch unverständlich)* Kommunen und für die angeschlossenen CERT-Verbünde. Und perspektivisch ist uns in Aussicht gestellt worden, dass das Computer Emergency Response Team des Landes zur lokalen Unterstützung herangezogen werden kann, wenn es in Kommunen zu Sicherheitsvorfällen kommt.

Ich finde, hier im Land haben wir eine hohe Aufmerksamkeit für das Thema „IT-Sicherheit“, und wir setzen durchaus den Gedanken um, dass die Sicherheit und das Sicherheitsmanagement nicht an Behördenzuständigkeiten enden, sondern dass wir im Land eine gemeinsame Managementstruktur aufbauen und pflegen wollen.

Prof. Dr. Kevin Borgolte (Ruhr-Universität Bochum, Horst-Görtz-Institut für IT-Sicherheit): Zu der Frage von Herrn Dr. Untrieser kann ich persönlich nichts sagen. Mir ist nicht bekannt, wie die anderen Bundesländer ihre IT-Sicherheit, also auch Redundanz, implementiert haben und umsetzen.

Zu der Frage von Frau Brems kann ich mich den Punkten von Herrn Rundfeldt größtenteils anschließen, insbesondere dahin gehend, dass warme Übungen im KRITIS-Bereich einfach notwendig sind. Man kann einfach nicht sagen, dass eine kalte Übung hinreichend ist. Man landet dann sehr schnell an dem Punkt, dass es in der kalten Übung so aussieht, als würde alles funktionieren und als würde man die richtigen Entscheidungen treffen. Man kann zurückrudern und sagen: „Dann machen wir es eben doch anders“, was bei einer warmen Übung einfach nicht möglich ist. Aus dem Ausfall, der potenziell innerhalb von 30 Minuten hätte behoben werden können, werden dann schnell mal zwei oder drei Tage, weil an einem Punkt eine falsche Entscheidung getroffen worden ist.

Dr. Dirk Weckendrup (IT.NRW): Auch ich kann zum Ländervergleich nicht umfassend Auskunft geben. Wir stehen natürlich in Kontakt mit einigen Ländern, die ähnliche Netze betreiben wie wir, teilweise mit veränderten Leistungsschnitten. Das heißt: Das, was wir machen, ist teilweise in anderen Ländern outgesourct. Die Ansprüche an die Netze sind aber sehr vergleichbar.

Ich würde gerne noch auf einen Hinweis von Ihnen, Herr Rundfeldt, reagieren. Sie haben im Zusammenhang mit kritischen Infrastrukturen ausgeführt, dass diese so gebaut werden müssen, dass sie nicht ausfallen können. Da entsteht für mich ein Eindruck, den ich gerne einmal kommentieren würde.

Ich glaube, dass das im IT-Umfeld so einfach gar nicht möglich ist. Es geht meiner Meinung nach nicht. Wenn Sie zum Beispiel doppelt so viel Geld einsetzen, dann bekommen Sie doppelt so hohe Verfügbarkeit. Damit kommen sie aber nie auf null. Wenn

Sie immer mehr Redundanz hinzufügen, fügen Sie leider – das ist nämlich das Problem – auch immer mehr Komplexität hinzu, und die müssen Sie beherrschen. Sie haben eine immer höhere Anfälligkeit für Fehler und Ähnliches.

Insofern gilt es immer, einen Schieberegler zwischen dem Aufwand, den man in Redundanz steckt, und den damit erzielten Effekten auf die Verfügbarkeit zu tarieren. Mehr Geld allein hilft nicht. Man muss genau schauen, was in der jeweiligen Situation wirklich am zielführendsten für die dann maximal zu erreichende Verfügbarkeit ist.

Vorsitzender Thorsten Schick: Ich bedanke mich bei den Sachverständigen für Ihre Expertise und dafür, dass Sie den Weg hierhin gefunden haben. Danke auch an Herrn Professor Engel, der uns zugeschaltet ist.

Das Protokoll der heutigen Veranstaltung wird auf der Internetseite des Ausschusses bzw. des Landtags abrufbar sein. Sicherlich ist das für Sie genauso interessant wie für die Mitglieder des Ausschusses, die es als Grundlage für die weitere Beratung nutzen.

Ich wünsche Ihnen einen guten Heimweg.

Um 17:00 Uhr geht es für uns weiter mit der 60. Sitzung. Sie sind eingeladen, dieser Sitzung noch beizuwohnen, das ist aber natürlich keine Pflicht.

Ich schließe die Anhörung und hoffe, dass wir pünktlich um 17:00 Uhr mit der nächsten Ausschusssitzung beginnen können.

gez. Thorsten Schick
Vorsitzender

Anlage
15.12.2021/20.12.2021
10

Stand: 18.11.2021

Anhörung von Sachverständigen
Sitzung des Ausschusses für Digitalisierung und Innovation

Das Landesverwaltungsnetz weiterentwickeln, um der steigenden Bedeutung digitaler Verwaltungsprozesse gerecht zu bleiben
Antrag der Fraktion BÜNDNIS 90/DIE GRÜNEN, Drucksache 17/14260

am 18. November 2021
15.30 Uhr bis 17.00 Uhr, **Raum E 3 A 02**

Tableau

eingeladen	Teilnehmer/innen	Stellung-nahme
Information und Technik Nordrhein-Westfalen (IT.NRW) Düsseldorf	**Dr. Dirk Weckendrup**	**17/4534**
Ruhr-Universität Bochum Horst-Görtz-Institut für IT-Sicherheit Bochum	**Professor Dr. Kevin Borgolte**	./.
KDN – Dachverband kommunaler IT-Dienstleis-ter Professor Dr. Andreas Engel Geschäftsführer Siegburg	**Professor Dr. Andreas Engel** *- per Video zugeschaltet -*	./.
AG KRITIS Wipperfürth	**Johannes Rundfeldt**	**17/4496**
ComConsult GmbH Dr. Behrooz Moayeri Aachen	**Dr. Behrooz Moayeri**	**17/4516**

***