NIEDERSÄCHSISCHER LANDTAG
18. WAHLPERIODE

N i e d e r s c h r i f t

über die 45. - öffentliche - Sitzung
des Ausschusses für Inneres und Sport
am 21. Februar 2019
Hannover, Landtagsgebäude

Tagesordnung: Seite:

Anwesend:

Ausschussmitglieder:

1. Abg. Thomas Adasch (CDU), Vorsitzender
2. Abg. Karsten Becker (SPD)
3. Abg. Dunja Kreiser (SPD)
4. Abg. Deniz Kurku (SPD)
5. Abg. Gerd Hujahn (i. V. d. Abg. Bernd Lynack) (SPD)
6. Abg. Sebastian Zinke (i. V. d. Abg. Doris Schröder-Köpf) (SPD)
7. Abg. Ulrich Watermann (SPD)
8. Abg. André Bock (CDU)
9. Abg. Rainer Fredermann (CDU)
10. Abg. Bernd-Carsten Hiebing (CDU)
11. Abg. Sebastian Lechner (CDU)
12. Abg. Uwe Schünemann (CDU)
13. Abg. Belit Onay (GRÜNE)
14. Abg. Jan-Christoph Oetjen (FDP)
15. Abg. Jens Ahrends (AfD)

Sitzungsdauer: 10.15 Uhr bis 12.33 Uhr.

Außerhalb der Tagesordnung:

Unterrichtungswunsch zum Thema „Rising Boys Hannover“

Abg. **Jan-Christoph Oetjen** (FDP) erinnerte an die Unterrichtung durch die Landesregierung über die Hintergründe und Ergebnisse der Hausdurchsuchungen bei Mitgliedern der Ultra-Gruppierung „Rising Boys Hannover“ am 14. Juni 2017, die der Innenausschuss der 17. Wahlperiode in seiner 123. Sitzung am 7. September 2017 entgegengenommen hatte. Er kündigte an, einen Antrag auf Fortsetzung der Unterrichtung - insbesondere mit Blick auf den Stand der damals eingeleiteten Ermittlungsverfahren - vorzulegen.

***

Tagesordnungspunkt 1:

Beschlussfassung über einen Antrag auf Unterrichtung durch die Landesregierung zum aktuellen Stand des Aufbaus eines Rechen- und Dienstleistungszentrums TKÜ

Der **Ausschuss** folgte dem Unterrichtungswunsch der FDP-Fraktion einstimmig und bat die Landesregierung um eine mündliche Unterrichtung.

***

Tagesordnungspunkt 2:

Entwurf eines Gesetzes zur Förderung und zum Schutz der digitalen Verwaltung in Niedersachsen und zur Änderung des Niedersächsischen Beamtengesetzes

Gesetzentwurf der Landesregierung - Drs. 18/1598

direkt überwiesen am 13.09.2018
federführend: AfluS
mitberatend: AfRuV; mitberatend gem. § 27 Abs. 4 Satz 1 GO LT: AfHuF

zuletzt beraten: 41. Sitzung am 17.01.2019

Anhörung

Arbeitsgemeinschaft der kommunalen Spitzenverbände Niedersachsens

Schriftliche Stellungnahme: Vorlage 6

Anwesend:

- *Beigeordneter **Thorsten Bullerdiek** (NSGB)*
- *Referatsleiter **Ulrich Mahner** (NST)*
- *Hauptgeschäftsführer Prof. **Dr. Hubert Meyer** (NLT)*
- *Referent **Manfred Malzahn** (NLT)*

Prof. **Dr. Hubert Meyer**: Die Digitalisierung ist ein Gemeinplatz und prägt inzwischen das Leben in der Gesellschaft und in der Verwaltung. Wir werden in den kommenden drei bis vier Jahren einen Quantensprung in der Umsetzung vollziehen müssen. Dazu dient auch dieses Gesetzgebungsvorhaben. Im Grundsatz ist es also sinnvoll und notwendig, dass das Land Niedersachsen diesen Gesetzentwurf vorlegt. Allerdings greift der Entwurf in der jetzigen Fassung vielfältig in die kommunale Organisationshoheit der Gemeinden, Städte und Landkreise ein.

Die Digitalisierung insgesamt und die Umsetzung des Onlinezugangsgesetzes (OZG) in Niedersachsen können nur gelingen, wenn das Land und die kommunalen Spitzenverbände auf Augenhöhe zusammenarbeiten und wir eine nachhaltige Finanzierung der Maßnahmen sichern. Beides ist leider nach unserer Einschätzung nicht der Fall, und wir halten es für fraglich, ob der Gesetzentwurf in der vorliegenden Form überhaupt umsetzbar ist.

Insbesondere kritisieren wir, dass es an einer verfassungsrechtlich geforderten verlässlichen Kostenfolgenabschätzung fehlt. Auf der Bundesebene gibt es bekanntlich Streit darüber, ob durch das OZG Konnexität ausgelöst worden ist oder nicht. Wir haben in unserer schriftlichen Stellungnahme darauf hingewiesen, was die Bundesvereinigung der kommunalen Spitzenverbände hierzu Ende Januar 2018 vorgetragen hat. Ich möchte das nicht im Einzelnen vorlesen, aber ich möchte aus der Antwort des Bundesinnenministeriums vom 9. Februar 2018 zitieren. Dort heißt es:

> „Bezüglich Ihrer Ausführungen zum Anwendungsbereich des OZG auf Kommunen möchte ich darauf hinweisen, dass sowohl die Gesetzesbegründung zu Art. 91c Abs. 5 GG als auch die Begründung zum OZG die Kommunen ausdrücklich in den Anwendungsbereich einbeziehen. Das OZG verpflichtet die Kommunen direkt, soweit sie Bundesgesetze vollziehen. Soweit darüber hinaus auch die Erfüllung kommunaler Selbstverwaltungsaufgaben betroffen ist, sind die Länder verpflichtet, die Vorgaben des OZG in ihren E-Government-Gesetzen entsprechend umzusetzen.“

Wir bitten nachdrücklich darum, dass diese Einschätzung des Bundes auch im Land Niedersachsen entsprechend umgesetzt wird. Unter diesen Umständen können wir es nur schwer nachvollziehen und werten es auch als einen deutlichen Wertungswiderspruch, wenn es auf der einen Seite auf Seite 29 unten in der Gesetzesbegründung heißt:

> „Die Landesregierung erwartet ebenfalls hohe Kosten im kommunalen Bereich und plant Schritte zur finanziellen Unterstützung der Kommunen bei der Umsetzung des ‚OZG-Handlungsplans’.“

und wenige Zeilen später dezidiert in Abrede gestellt wird, dass die Kosten, die den Kommunen entstehen, überhaupt die Erheblichkeitsschwelle gemäß der Konnexitätsregelung des Landes erreichen. Das ist ein Widerspruch, den wir nicht erklären können und der aus unserer Sicht die Problematik verdeutlicht.

Wir fordern eine solide Finanzierung, eine solide Projektstruktur, die auch den Aufwand der Verbände und ihrer Geschäftsstellen einrechnet, und einen partnerschaftlichen Umgang auf Augenhöhe.

Dies ist uns als Vorbemerkung zum Gesetzgebungsvorhaben insgesamt wichtig.

Zu den einzelnen Themen will ich nun nur punktuell Stellung nehmen. Unsere ausführliche schriftliche Stellungnahme liegt Ihnen vor.

Aus unserer Sicht stellt der OZG-Handlungsplan eine gute Grundlage für den weiteren Ausbau der digitalen Verwaltung in Niedersachsen dar. Nach unserer Einschätzung werden die Kommunen die ersten Ansprechpartner der Bürgerinnen und Bürger bei der Digitalisierung der Verwaltung sein, weil sie einen Großteil der Dienstleistungen anbieten, die vor Ort in Anspruch genommen werden.

Artikel 1 - Niedersächsisches Gesetz über digitale Verwaltung und Informationssicherheit (NDIG)

Zweiter Teil - Digitale Verwaltung

§ 3 - Geltungsbereich

Ich weise darauf hin, dass es Besonderheiten für die Mitgliedsgemeinden von Samtgemeinden gibt. Dazu wird Kollege Bullerdiek im Anschluss noch gesondert vortragen. Im Übrigen werden dort einzelne Bereich aus der Verwaltung herausgenommen. Das erscheint uns zum Teil wenig überzeugend. Wir haben darauf hingewiesen, dass wir schwer nachvollziehen können, warum es z. B. eine Ausnahmeregelung für Schulen gibt.

Manches scheint mir auch inkonsequent. Ich will ein Beispiel, das wir nicht in der schriftlichen Stellungnahme erwähnt haben, nennen.

Nach § 3 Abs. 3 Nr. 10 des Entwurfs sind Zweckverbände ausgenommen. Unsere Mitglieder übernehmen aber auch Aufgaben, die generell durch die Kommunen selbst wahrgenommen werden, teilweise in Form von Zweckverbänden. Als Beispiel will ich für den Landkreisbereich das Veterinäramt JadeWeser nennen, das für drei Landkreise und eine kreisfreie Stadt die Aufgaben der Lebensmittel- und Veterinärüberwachung wahrnimmt. In diesem Fall ist folglich die Lebensmittel- und Veterinärüberwachung ausgenommen. In allen anderen Fällen wird der Bereich hingegen vom Anwendungsbereich erfasst. Das scheint nicht sonderlich konsequent.

§ 4 - Elektronischer Zugang zur Verwaltung

Wir gehen davon aus, dass die Kosten für die notwendige Infrastruktur, die personellen Mehraufwendungen und die laufende Unterhaltung vom Land ermittelt und getragen werden.

§ 5 - Elektronische Informationen und Verwaltungsportal

Ich will darauf hinweisen, dass die Qualität der Daten im sogenannten BUS erheblich verbessert werden muss. Darauf wird der NSGB noch gesondert eingehen.

§ 6 - Elektronische Bezahlmöglichkeiten und Rechnungen

Wir würden es als vorteilhaft empfinden und empfehlen es, den verwaltungsrechtlichen und den vergaberechtlichen Regelungsgehalt dieser Norm im Interesse der Normenklarheit in zwei Vorschriften aufzuteilen.

§ 7 - Nachweise

Wir haben registriert, dass im Rahmen des entsprechenden Gesetzgebungsvorhabens in der vergangenen Legislaturperiode - das nicht zu Ende geführt wurde - davon ausgegangen wurde, dass für die Speicherung und den Abruf von Einwilligungen ein IT-Verfahren erforderlich sei, das sinnvollerweise mit dem Servicekonto Basisdienst verbunden sein müsse. Für uns ist nicht ersichtlich, warum die Einschätzung, die damals vertreten wurde, jetzt nicht mehr gelten soll.

§ 9 - Georeferenzierung

Ich mache darauf aufmerksam, dass die Kommunen einen überwiegenden Anteil von Registern im übertragenen Wirkungskreis führen und insoweit auch die Frage der Konnexität zu betrachten ist.

Der nach § 12 Abs. 1 zur Verfügung zu stellende Basisdienst muss nach unserer Auffassung online und kostenfrei zur Verfügung gestellt werden und aus verschlüsselten Adressinformationen sowie aus unverschlüsselten Lagebezeichnungen die benötigten Koordinaten zurückgeben.

§ 11 - Übertragen und Vernichten von Dokumenten in Papierform

Die geplante Schaffung einer Rechtsgrundlage für das Übertragen von Dokumenten in die elektronische Form und die anschließende Vernich-

tung des Originals begrüßen wir ausdrücklich. Bei der zu erarbeitenden Handreichung bieten wir ausdrücklich unsere Mitarbeit an.

§ 12 - Basisdienste

Der § 12 des Entwurfs sollte aus unserer Sicht insgesamt einen höheren Verbindlichkeitsgrad erhalten. Das Ziel, das verfolgt wird, nämlich aufeinander abgestimmte Basisdienste und IT-Architekturvorgaben zu erhalten, verlangt im Wesentlichen standardisierte Prozesse. Wir haben in den vergangenen Jahren die Erfahrung gemacht, dass die Nutzung von Basisdiensten des Landes durch Kommunen eine eher problematische Angelegenheit darstellt. Diese Dienste werden seit Jahren angeboten, allerdings fehlt es bis heute an verlässlichen, marktüblichen Qualitätsstandards, an Service- und an Nutzungsregelungen. Wir erinnern daran, dass es seit nunmehr anderthalb Jahren die Zusage für Leistungsbeschreibungen und Preise für die Nutzung gibt. Sie liegen uns bis heute nicht vor.

Dritter Teil - Informationssicherheit

Erster Abschnitt - Gewährleistung der Informationssicherheit

§ 15 - Sicherheitsverbund, Verpflichtung zu Sicherheitsmaßnahmen

So sehr wir die in den Grundsätzen der Informationssicherheit zum Ausdruck kommende Regelung begrüßen, so wird sie doch in der praktischen Umsetzung problematisch sein. Denn für den Bereich des Landes wird zwar sehr ausführlich dargestellt, welche Maßnahmen zur Gewährleistung der Informationssicherheit getroffen werden sollen, aber gerade mit Rücksicht auf die sehr heterogene Behördenstruktur im kommunalen Bereich muss sichergestellt werden, dass das einheitliche Sicherheitsniveau mit einem vertretbaren Aufwand von allen Behörden gleichermaßen erreicht werden kann.

Zweiter Abschnitt - Einsatz von Systemen zur Erkennung und Abwehr von Gefahren für die IT-Sicherheit

§ 27 - Übermittlung personenbezogener Daten

Ich will darauf hinweisen, dass ausweislich der Gesetzesbegründung der vorliegende Gesetzentwurf auch der Umsetzung des OZG dient. Insofern regen wir an, die im OZG enthaltenen Übergangsfristen auch in das NDIG zu übernehmen.

Artikel 2 - Änderung des Niedersächsischen Beamtengesetzes

Wir finden es gut und notwendig, dass man für die Umstellung auf die elektronische Aktenführung, insbesondere für Personalakten, auch auf nicht zur Verwaltung rechnende Personalressourcen zurückgreifen darf - insbesondere also auf spezialisierte private Dienstleister. Das muss aber wirklich zweifelsfrei und in allen Fällen ermöglicht werden, um den knappen Ressourcen in der kommunalen Verwaltung Rechnung zu tragen.

Fazit

Zusammenfassend darf ich feststellen, dass es ein Gesetzgebungsvorhaben ist, das viele einzelne, sehr technisch anmutende Umsetzungsfragen enthält, die wir möglicherweise nicht in allen Einzelheiten überblicken. Für mich selbst muss ich jedenfalls sagen, dass ich das nicht in allen Einzelheiten überblicke. Wir glauben aber, dass wir uns diesen Herausforderungen stellen müssen, und dies bedingt, dass wir uns dieser Aufgabe mit einer realistischen Aufwands- und Kostenbetrachtung annehmen.

Thorsten Bullerdiek: Ich möchte noch ein paar Punkte ergänzen, die die Samtgemeinden betreffen.

Die Mitgliedsgemeinden von Samtgemeinden werden beispielsweise dazu verpflichtet, eine eigene Homepage zu erstellen, diese zu pflegen, ihre Dienstleistungen dort vorzuhalten und künftig E-Rechnungen zu stellen. Wir haben angemerkt, dass man dafür ja auch in irgendeiner Form eine Kostenerstattung erwarten kann, und wurden darauf hingewiesen, dass dieses eine Aufgabe ist, die die Samtgemeinden für ihre Mitgliedsgemeinden übernehmen können.

Das können wir natürlich machen, aber dann geben wir ein Stück weit Identität vor Ort auf. Das ist eigentlich eine versteckte Gebietsreform, wenn die kleinen Kommunen letztlich dahin gedrängt werden, dass sie Dienstleister in Anspruch nehmen - entweder privater Natur oder in Form der Samtgemeinde. Wir sind der Auffassung, dass wir die Digitalisierung eher dazu nutzen müssen, die Dezentralität zu stärken. Das gilt beispielsweise auch für Sicherheitsfragen. Wenn wir ganz zentral agieren, erleiden wir eher Schiffbruch als mit einer kontrollierten Dezentralität.

Wir haben eine einmalige Chance. Wir haben richtig viel Geld im System. In dieser Legislaturperiode kann viel entstehen. Sie haben sich ehrgeizige Ziele bis 2022 gesetzt. Aber schauen Sie einmal auf Ihr Smartphone! Wie viele Verwaltungsanwendungen nutzen Sie tatsächlich? Und Sie sind ein qualifizierter Bürger. Ich glaube, ein durchschnittlicher Bürger hat noch viel weniger Verwaltungsanwendungen auf dem Smartphone als Sie. Das Ziel muss sein, bis 2022 die Bürger zu erreichen. Das tun Sie nur, wenn Sie die Kommunen jetzt aktiv einbinden.

Wir erwarten, dass wir dieses Projekt zusammen umsetzen. Wie das geht, zeigt uns Baden-Württemberg. Ich habe die Kollegin dort heute angerufen. Im aktuellen Haushalt sind dort allein für Dinge wie die Qualifikation von Digitallotsen und die Schaffung eines kommunalen Kompetenzzentrums 20 Millionen Euro für Transferleistungen an die Kommunen eingestellt. Die arbeiten schon seit Jahren sehr gut zusammen und machen Bestandsaufnahmen vor Ort. Wir hoffen, dass wir da auch in Niedersachsen aktiver werden.

Und wir müssen natürlich auch das Thema Breitband im Blick behalten, auch wenn es nicht Gegenstand dieses Gesetzentwurfes ist. Denn was nützen die schönsten Anwendungen, wenn man sie nachher im ländlichen Raum nicht nutzen kann?

Abg. **Belit Onay** (GRÜNE): Sie hatten eingangs gesagt, dass es eine entsprechende finanzielle Ausstattung der Kommunen geben müsse. Herr Bullerdiek hatte in einem Interview von 180 Millionen Euro gesprochen. Ist das die Summe, die Ihnen vorschwebt?

Prof. **Dr. Hubert Meyer**: Ich möchte hier heute ungern eine konkrete Zahl nennen, weil sie nicht seriös belegt werden kann. Ganz sicher bin ich mir, dass es um deutlich mehr als 2 Millionen Euro geht. Das ist die Summe, über die wir bisher als Erheblichkeitsschwelle im Lande diskutiert haben. Die Zahl, die Herr Bullerdiek genannt hat, entspricht ungefähr 1 % davon. Wir liegen bei der Einschätzung der Kosten um Welten auseinander.

Aber uns geht es heute nicht darum, für eine bestimmte Zahl zu streiten, sondern wir streiten dafür, dass anerkannt wird, dass die Umsetzung im kommunalen Bereich mit Kosten verbunden sein wird.

Abg. **Belit Onay** (GRÜNE): Sie haben eine stärkere Einbindung der kommunalen Ebene gefordert. Wie ist bisher die Kooperation mit der Landesregierung verlaufen, und wo wünschen Sie sich Verbesserungen? Sie haben Baden-Württemberg genannt. Aus Baden-Württemberg ist leider kein Anzuhörender anwesend - heute sind die bayerischen Kolleginnen und Kollegen hier -, aber in Baden-Württemberg gibt es das System des Kompetenzzentrums und der Digitallotsen mit relativ vielen, ich glaube, mit 1 600 bis 1 700 Personen. Erwarten Sie Ähnliches für Niedersachsen? Wie verlaufen die Gespräche mit der Landesregierung? Gibt es eine Rückmeldung zu der Finanzsumme seitens der Landesregierung?

Prof. **Dr. Hubert Meyer**: Ich glaube, wir sind jetzt an einer Stelle, an der sich im praktischen Ablauf etwas ändert. Wir waren bisher gut eingebunden hinsichtlich der strategischen Ausrichtung der verschiedenen Gremien im Innenministerium und verschiedener anderer Dinge. Der Kollege Malzahn hat in den vergangenen Jahren viele Stunden in entsprechenden Gremien verbracht. Wir sind jetzt aber in einer Phase, in der es nicht mehr nur darum geht, strategische Entscheidungen zu treffen, sondern wir gelangen in eine konkrete Umsetzungsphase.

Beim Innenministerium sind 16 Projekte aufgesetzt. Diese Projekte müssen auch von der kommunalen Ebene komplett begleitet werden. Das sind Dinge, die wir mit den Kapazitäten unserer Geschäftsstellen - da darf ich für alle drei Verbände sprechen - alleine nicht mehr begleiten können. Und das können wir auch nicht nur dadurch begleiten, indem wir jeweils Fachleute, die wissen, wie das konkrete Verfahren läuft, aus den Verwaltungen dazuholen. Die Fachleute brauchen wir auch, wir brauchen sie zusätzlich. Wir brauchen zudem Kapazitäten, die sozusagen die Verkoppelung zwischen dem, was in der Praxis passiert, und dem, was auf Landesebene dazu konzeptionell aufgesetzt werden muss, sicherstellen. Das ist der Bereich, den der Kollege Bullerdiek angesprochen hat. Ich glaube, Baden-Württemberg ist uns da voraus und weiß, wie man diese Projekte konkret mit Personal und Geldmitteln unterlegt. Wir sollten uns auf den Weg machen, damit wir - zumindest in Ansätzen - eine solche Konstellation auch in Niedersachsen schaffen.

Thorsten Bullerdiek: Ich möchte kurz ergänzen. Die Summe von 180 Millionen Euro stammt aus

der Ursprungsrechnung zum OZG-Handlungsplan. Das Land hat gesagt, dass es mit ungefähr 180 Millionen Euro rechne. Zum Vergleich: Baden-Württemberg setzt im aktuellen Haushalt 1 Milliarde Euro an. Diese 180 Millionen Euro haben wir grob gerechnet. 575 Verwaltungsdienstleistungen werden ja derzeit schon von den Kommunen direkt zum Bürger gebracht, da gibt es also laufende Prozesse, in die man eingreift. Wenn wir nun alles das, was jetzt im Moment in Rede steht, umsetzen wollen, dann werden die 2 Millionen Euro vielleicht schon in einer Stadt oder in zwei Städten ganz schnell ausgegeben sein, um diese Prozesse entsprechend anzupassen.

Abg. **Belit Onay** (GRÜNE): Sie haben in Ihrer schriftlichen Stellungnahme auf Seite 10 richtigerweise darauf hingewiesen, dass es Unterschiede zwischen dem Landesnetz und den kommunalen Netzen gibt, aber dennoch eine Verflechtung besteht. Sie sagten, dass das Thema Sicherheit auch in der Fläche verankert sein müsse und nicht nur zentral beispielsweise in Hannover. Wie müsste aus Ihrer Sicht das Sicherheitskonzept aussehen? Welche Aspekte müssten zusätzlich beachtet werden?

Thorsten Bullerdiek: Wir können Ihnen noch keine abschließende Lösung vorschlagen. Wir stehen am Anfang dieses Projekts, wobei wir natürlich darauf hinweisen, dass es mit Blick darauf, wie diese Angriffe bzw. diese Cyberattacken letztlich ablaufen, aus unserer Sicht sehr viel Sinn macht, dass Zentralität und Dezentralität sehr gut zusammenarbeiten. Ich glaube, mit Blick auf die Verwundbarkeit des Systems kann uns Dezentralität auch helfen. Deswegen ist unser Appell, die kleineren Einheiten zu stärken und denen ein Rückgrat zu geben.

Abg. **Sebastian Lechner** (CDU): Da möchte ich einmal einhaken. Gibt es schon Vorstellungen der Kommunen darüber, wie man den Verpflichtungen, die die IT-Sicherheit betreffen und die im neuen NDIG festgeschrieben werden sollen, in einem Sicherheitsverbund nachkommen will?

Herr Meyer sprach davon, dass das Sicherheitsniveau „mit einem vertretbaren Aufwand erreichbar“ sein solle. Wir müssen aber eigentlich mit einem anderen Anspruch an die Sache herangehen, nämlich mit dem, dass wir die Sicherheit, die wir brauchen, gewährleisten müssen. Wir können bei der Sicherheit keine Abstriche in Kauf nehmen, weil das sonst „vom Aufwand her nicht vertretbar“ wäre. Solch ein Sicherheitsverbund - das ist meine Information - kann schnell in Problemlagen geraten, wenn die schwächsten Glieder in der Kette nicht ausreichend Sicherheit gewährleisten, sodass darüber auch auf andere Systeme zugegriffen werden kann. Das ist die Problematik dabei.

Insofern muss sichergestellt werden, dass wir mit den Kommunen zusammen ein Konzept entwickeln können, das die jeweiligen Kommunen, Städte und Gemeinden in die Lage versetzt, diesen Anforderungen gerecht zu werden.

Ich habe in der Stellungnahme gelesen, dass man verstärkt über kommunale Dienstleister arbeiten möchte. Wie ist denn derzeit die Struktur in den Kommunen? Ich habe den Eindruck, dass es viele Kommunen gibt, die noch ihre eigenen Server im Keller stehen haben und einen eigenen Systemadministrator für die Pflege beschäftigen. Wie häufig wird schon mit zentralen Dienstleistern zusammengearbeitet? Wie ist das Konzept der Kommunen, und wo will man hin?

Im Grunde gibt es zwei Möglichkeiten. Wir könnten jetzt entweder alle gemeinsam an größeren Strukturen mit kommunalen IT-Dienstleistern in Anbindung an eine sogenannte Niedersachsen-Cloud - worüber wir auch diskutieren - arbeiten, weil man das einfach besser schützen und zentral koordinieren kann.

Oder aber man überlegt sich - das ist das, was Sie eben gesagt haben - ein dezentrales Konzept. Dazu ist es aber - bei aller Liebe zur Dezentralität - notwendig, dass man Mechanismen schafft, die dafür Sorge tragen, dass die dezentralen Einheiten mit allen anderen im Orchester laufen. Das heißt ganz klar, dass die Zentralstelle der Informationssicherheit die Möglichkeit haben müsste, kommunale Verwaltungen anzuweisen bzw. darauf hinzuweisen, dass ein gewisser Patch aufgespielt oder ein gewisses Update gemacht werden muss und man andernfalls Gefahr liefe, eine gewisse Zeit vom Landesnetz ausgeschlossen zu werden, um die IT-Sicherheitslücke zu schließen.

Diese beiden Extreme sind möglich. Ich möchte gern wissen, welche Vorstellungen die Kommunen haben, in welche Richtung es gehen soll und welche konzeptionellen Ideen es für die IT-Sicherheit gibt.

Manfred Malzahn: Wir reden hier im Grundsatz über die gemeinsame Nutzung des Landesnetzes. Wenn wir als Kommunen auf das Landesnetz zurückgreifen - das können inzwischen alle Kommunen -, schaltet IT.N zurzeit eine Firewall zwischen, um jeglichen Verkehr zu überprüfen. Im kommunalen Bereich machen wir das genauso. Unsere Landkreise bzw. unsere kommunalen Datenzentralen haben auch eine Firewall, um alles vom Land Kommende zu überprüfen. Jetzt kann man sich die Frage stellen: Wenn wir in einem Landesnetz arbeiten, sollten wir dann nicht sinnvollerweise mit Regeln arbeiten, die zu einem gegenseitigen Vertrauen führen? Diese Regeln müssen natürlich erarbeitet werden. Dafür stehen wir auch gerne zur Verfügung. Das Problem ist nur: Wenn wir solche Lösungen schaffen, dann müssen wir auch ganz klar sagen, was wir damit sicherstellen wollen.

Wir haben z. B. den Fall des Veterinärwesens. Wir haben ein einheitliches Veterinärprogramm, in dem alle Landkreise, alle kreisfreien Städte mit verschiedenen Ministerien zusammenarbeiten. Und dieses Programm brauchen wir in jedem Krisenfall ganz, ganz dringend. Das muss dann zur Verfügung stehen. Das hat oberste Priorität. Denn wir haben es immer wieder erlebt, dass diese Krisenfälle leider zu Zeiten auftreten, z. B. an Wochenenden, wenn nicht jeder an seinem Arbeitsplatz ist.

Das wird zurzeit sowohl auf der Kreisebene als auch bei den kreisfreien Städten und genauso beim Land ohne Probleme gewährleistet. Wir haben dazu Vereinbarungen getroffen und mit IT.N ergänzende Vereinbarungen abgeschlossen, um den Servicelevel zu erhöhen. Darum muss es jetzt bei allen anderen Verfahren auch gehen.

Denn mit Blick auf die Umsetzung des OZG geht es ja um wesentlich mehr Verfahren, die in Zukunft über das Landesnetz laufen sollen. Das ist aus unserer Sicht auch unstrittig. Sie müssen über das Landesnetz laufen, damit wir sicher sein können, dass nicht irgendjemand mithört. Insofern sind wir im Konsens.

Aber wir brauchen gemeinsame Regelungen, und dazu brauchen wir einen gemeinsamen Aufschlag und müssen sehen, was wir jeweils machen können. Die Technik ist bei den großen Anwendern im kommunalen Bereich genauso vorhanden. Sie haben recht, dass das bei den kleinen Anwendern nicht immer so sein wird. Wir haben auch ganz unterschiedliche Lösungen. Es gibt durchaus kleine Gemeinden, die mit eigenen Infrastrukturen arbeiten. Aber man muss auch feststellen, dass es dort Verbesserungen gibt. In unseren Kreisverwaltungen haben wir in jüngster Zeit Vorfälle gehabt - die durchaus presserelevant waren -, bei denen E-Mails Systeme verseucht haben und z. B. die Kfz-Zulassung nicht mehr zur Verfügung stand. Dort wurde inzwischen nachgerüstet. Im Grundsatz haben wir inzwischen auch im kommunalen Bereich ein durchaus messbares Sicherheitsniveau.

Jetzt müssen wir es hinbekommen, eindeutig zu beantworten, wie die Struktur, die auf der Landeseite vorhanden ist, mit der der Kommunen in Einklang zu bringen ist und wie man sich auf ein gemeinsames Sicherheitsniveau einigen kann.

Abg. **Sebastian Lechner** (CDU): Sie sagten eben, die Technik sei bei den kommunalen Dienstleistern genauso vorhanden. Das will ich erst einmal glauben. Auf dem Niveau von IT.N sind sie sicherlich. Nur wollen wir mit diesem Gesetzentwurf mit den sogenannten Intrusion Detection Systems (IDS) ein ganz anderes technisches Niveau einführen. Da gibt es ja durchaus technische Varianten, die äußerst anspruchsvoll sind und laufend gepflegt werden sollten.

Das BSI - deren Vertreter tragen später noch vor - ist dort schon sehr weit vorn, weil es sehr viel in die Forschung investiert. Insofern frage ich, ob man nicht überlegen sollte, das zu nutzen und miteinander gleichzuschalten. Denn ich habe schon den Eindruck, dass es, sobald wir mit solchen neuen Systemen arbeiten, durchaus den Bedarf geben wird, dass die Kommunen gut auf den Stand der Forschung zugreifen können, ohne alles selbst neu erfinden und am Laufen halten zu müssen. Das ist der Hintergrund dessen, warum ich nach der Cloud-Lösung gefragt habe.

Man muss schon überlegen, wie man es hinbekommt, den Datenverkehr, der in den Kommunen läuft, durch solche Systeme zu schützen. Dafür müssten die Daten durch Server geleitet werden, auf denen diese Systeme laufen und die zentral verwaltet und gemanagt werden und womit der Datenaustausch zwischen den Kommunen, dem Land und am besten sogar mit dem Bund organisiert wird.

Das habe ich dabei im Hinterkopf. Und das wird natürlich schwierig, wenn es nicht wenigstens eine gewisse zentrale Orchestrierung gibt.

Manfred Malzahn: Vergleichbares ist in einigen Verfahren schon passiert. Bestes Beispiel ist das sogenannte nationale Waffenregister. Dort gibt es eindeutige Vorgaben des BSI, die für alle Landkreise und alle kreisfreien Städte gelten und inzwischen auch erfüllt worden sind. Dort wird das Landesnetz quasi nur als Transportnetz zum Bundesnetz genutzt, um auf die Waffendatenbank des Bundesinnenministeriums zu kommen. Wir haben solche Fälle also durchaus.

Das zweite Beispiel ist das Verfahren i-Kfz-Zulassung. Der Bundesrat hat gerade eine Verordnung der Bundesregierung gebilligt, sodass wir jetzt die dritte Stufe von i-Kfz einführen werden. Auch dort gibt es Vorgaben vom BSI, die nun umgesetzt werden. Damit haben wir überhaupt kein Problem. Das Problem hier ist: Wir müssen zunächst gemeinsam definieren, welches Sicherheitsniveau wir in Niedersachsen für sinnvoll halten, damit dies dann auch überall organisiert werden kann.

Zu den Servern: Nach meinem Kenntnisstand ist die KDO Oldenburg sogar BSI-zertifiziert.

Die Landesbeauftragte für den Datenschutz Niedersachsen

Anwesend:

*- **Dr. Christoph Lahmann**, Stellvertreter der LfD*

Dr. Christoph Lahmann: Grundsätzlich begrüßt die LfD das Gesetzgebungsvorhaben ausdrücklich. In den ersten beiden Teilen, bei denen es um Regelungen zu Einführung, Ausbau oder Standardisierung des eGovernment geht, ist es ein besonderes Anliegen der LfD, dass diese Regelungen möglichst datenschutzfreundlich ausgestaltet sind. Im dritten Teil geht es um die Schaffung einer Rechtsgrundlage für deutlich erweiterte Maßnahmen zur Wahrung der IT-Sicherheit im Landesdatennetz.

IT-Sicherheit in ein grundlegendes Anliegen im Datenschutz. Die Wahrung des Datenschutzes kann im Grunde nur auf der Basis einer stabilen, angemessenen und wirksamen IT-Sicherheit gewährleistet werden. Folgerichtig beschreibt die DS-GVO im Artikel 32 „Sicherheit der Verarbeitung“ Maßnahmen und insbesondere Ziele zur Aufrechterhaltung der Sicherheit als Auftrag an die verantwortliche Stelle. Ausdrücklich ist hier der Rede vom Stand der Technik, der durchgängig zu berücksichtigen ist. Nichts anderes, als dorthin aufzuschließen, soll dieser Gesetzentwurf bewirken. Aber dabei müssen die getroffenen Maßnahmen verhältnismäßig sein, also geeignet, erforderlich und angemessen. Es gilt also auch hier wiederum, einen möglichst grundrechtsschonenden Ansatz durch eine ausgewogene Relation zwischen Zwecken und Mitteln zu realisieren.

Wir haben im Rahmen der Verbandsbeteiligung eine ausführliche Stellungnahme zum Entwurf abgegeben. Ich werde mich im mündlichen Vortrag auf drei Punkte beschränken. Erstens wäre bei der Begriffsbestimmung mehr Klarheit wünschenswert, zweitens ist aus unserer Sicht eine ergänzende Regelung zur Protokollierung der elektronischen Aktenführung erforderlich, und drittens und schließlich geht es um die Ausgestaltung der Eingriffsbefugnisse zur umfangreichen Auswertung von personenbezogenen Daten und sogar von Kommunikationsinhalten im Landesdatennetz und den IT-Systemen der Landesverwaltung.

Zum ersten Teil, den Begriffsbestimmungen. Es wäre zweckmäßig, wenn diese nicht zu einer Begriffsverwirrung im Datenschutzrecht führen würden. In dem vorliegenden Entwurf sind Inhaltsdaten als Informationen definiert, die bei einem Kommunikationsvorgang übertragen werden und um derentwillen die Telekommunikation stattfindet und die keine Verkehrsdaten sind. Auf europäischer Ebene, insbesondere im Rahmen der E-Privacy-Verordnung, wird der Begriff der elektronischen Kommunikationsmetadaten, also der Verkehrsdaten, verwendet und abgegrenzt gegen den der Kommunikationsinhaltsdaten. Das sind solche Inhalte, die mittels elektronischer Kommunikationsdienste übermittelt werden, z. B. Textnachrichten, Sprache, Videos, Bilder und Ton. Solche Begriffsverwirrungen führen nicht dazu, dass das ohnehin als kompliziert geltende Datenschutzrecht leichter zugänglich wird, und sollten deshalb vermieden werden.

Zweitens, E-Akte. Mit § 10 des Entwurfs wird die Einführung der elektronischen Aktenführung in der Landesverwaltung geregelt. Von datenschutzrechtlicher Relevanz ist insbesondere der Absatz 3, der u. a. die Sicherstellung der Verfügbarkeit und Vertraulichkeit

der Akte vorschreibt. Auf Grundlage dieser Vorschrift werden die Behörden Systeme zur Protokollierung des Zugriffs auf die elektronische Akte implementieren. So können z. B. Änderungen an der Akte oder auch nur der einfache Aufruf protokolliert werden. Damit wird die Arbeit der Beschäftigten mit den elektronischen Akten umfassend erfasst. Diese Erfassung des Verhaltens der Beschäftigten zur Sicherung der elektronischen Akten darf aber den erforderlichen Umfang nicht überschreiten. Um diesen Konflikt zu lösen, bzw. gar nicht erst aufkommen zu lassen, sollten Speicherfristen für die Protokolldaten geregelt und in den Gesetzentwurf aufgenommen werden. So kann ein „Wildwuchs“ in der Landesverwaltung bei der Protokollierung verhindert und sowohl für die Behörden als auch die Beschäftigten mehr Rechtssicherheit geschaffen werden.

Zum dritten Teil, Informationssicherheit. Der vorliegende Entwurf enthält in den §§ 17 ff. Eingriffsbefugnisse von außerordentlichem Gewicht, die sowohl die Beschäftigten in den Behörden als auch deren Kommunikationspartner betreffen. Zur Gewährleistung der Informationssicherheit ist es vorgesehen, dass umfangreiche Auswertungen auch von personenbezogenen Daten und sogar von Kommunikationsinhalten vorgenommen werden. Das betrifft beispielsweise Telefonate. Dabei ist ein Eskalationsmodell vorgesehen, bei dem es im ersten Schritt um die automatisierte Auswertung von Protokoll- und Verkehrsdaten und im zweiten auch um Inhaltsdaten geht. Im vierten und schwerwiegendsten Schritt ist sogar die nichtautomatisierte Auswertung von Inhaltsdaten vorgesehen. Die besondere Schwere dieses Eingriffs in das Fernmeldegeheimnis und das Grundrecht auf informationelle Selbstbestimmung ergibt sich aus mehreren Gesichtspunkten:

Es geht zunächst um die Art der Daten, die ausgewertet werden können. In dem Entwurf geht es, wie schon erwähnt, nicht nur um die automatisierte Analyse von Verkehrsdaten, also wer wann mit wem kommuniziert hat, sondern auch darum, dass nichtautomatisiert Einblick in die Inhalte der Kommunikation genommen werden kann. Dabei ist insbesondere zu erwähnen, dass in vielen Behörden in Niedersachsen die private Nutzung der IT-Systeme durch die Beschäftigten inzwischen erlaubt worden ist. Es geht also nicht nur, wie man zunächst meinen könnte, um rein dienstliche Kommunikation, sondern auch private Kommunikation kann Gegenstand der Eingriffsbefugnisse sein.

Zudem gehen die im Gesetzentwurf geregelten Befugnisse über das hinaus, was nach der Gesetzesbegründung beabsichtigt ist. Obwohl ausweislich der Gesetzesbegründung vom Einsatz bestimmter Security-Anwendungen ausgegangen wird, nämlich von sogenannten Intrusion Detection Systems und Security Information Event Management Systems, das sind quasi Sammel- und Auswertezentralen, wurden der Gesetzentwurf selbst technikneutral formuliert und schafft technikneutral Befugnisse für alle mit dem Landesdatennetz verbundenen Behörden.

Dies ist aus mehreren Gründen problematisch. Zunächst liegt es in der Natur der Sache, dass technikoffene Regelungen weniger bestimmt sind. Durch technische Entwicklungen könnten die Normen, die jetzt erlassen werden sollen, in Zukunft die Basis für den Einsatz noch wesentlich mächtigerer Analysesysteme sein. Ein Risiko, das vor dem Hintergrund der Gesetzesbegründung nicht notwendig ist. Aber auch die Streubreite der Befugnisse ist nicht notwendig. Es ist nicht ersichtlich, dass die notwendige Fachkunde zum ordnungsgemäßen Betrieb von Überwachungssystemen flächendeckend bei den Behörden verfügbar ist oder mit vertretbarem Aufwand verfügbar gemacht werden kann. Die im Entwurf enthaltenen Befugnisse bergen damit durch ihre Technikneutralität und Streubreite die Gefahr, dass unabhängig von dem eigentlich vorgesehenen Einsatzszenario nicht absehbar ist, in welcher Art und Weise die Behördenleitungen von den neuen Befugnissen Gebrauch machen werden.

Wie ich eingangs schon sagte, ein hohes Niveau beim Schutz der Vertraulichkeit, Integrität und Verfügbarkeit von personenbezogenen Daten ist ein Kernanliegen des Datenschutzes. Uns ist deshalb bewusst, dass die beabsichtigten Eingriffe zur Wahrung der Informationssicherheit erforderlich sind. Moderne Bedrohungen und zunehmend professionelle Angreifer dürfen die Informationssicherheit in der Landesverwaltung nicht gefährden. Die Kritik richtet sich folglich auch nicht gegen die Schaffung von Rechtsgrundlagen für den Einsatz dieser Systeme, sondern gegen die Verhältnismäßigkeit der konkreten Regelungen im Entwurf. Vor dem Hintergrund der eben erläuterten Ein-

griffsintensität müssen höchste Anforderungen im Hinblick auf den Schutz der betroffenen Personen erfüllt werden. Ein fahrlässiger oder vorsätzlicher Missbrauch der Eingriffsbefugnisse muss praktisch ausgeschlossen sein.

Um dieses Ziel zu erreichen, muss insbesondere die Befugnis zur Anordnung einer nichtautomatisierten Auswertung von Inhaltsdaten in § 22 Abs. 3 überarbeitet werden. Im vorliegenden Entwurf ist vorgesehen, dass die entsprechende Anordnung durch „eine Behördenleitung gemeinsam mit einem oder einer Beschäftigten der Behörde mit der Befähigung zum Richteramt“ erfolgt. Diese Regelung kann den hohen Anforderungen nicht genügen. Erforderlich ist vielmehr, dass der tiefgreifende Grundrechtseingriff einer unabhängigen vorbeugenden Kontrolle unterzogen wird. Da den betroffenen Personen aufgrund der Heimlichkeit der Maßnahme eine Überprüfung vor Durchführung verwehrt ist, muss durch eine unabhängige Kontrolle sichergestellt werden, dass die Interessen der betroffenen Personen angemessen geschützt werden.

Ich erinnere daran, dass eine ähnliche Problematik bei der Telekommunikationsüberwachung nach § 100 a StPO besteht. Die Norm sieht für die Strafverfolgungsbehörden die Befugnis vor, bei dem Verdacht auf eine schwere Straftat die Telekommunikation einer betroffenen Person ohne deren Wissen zu überwachen und aufzuzeichnen. Eine solche Telekommunikationsüberwachung kann gemäß § 100 e StPO grundsätzlich nur durch das Gericht auf Antrag der Staatsanwaltschaft angeordnet werden.

Mit der aktuellen Gesetzesvorlage wird eine vergleichbare Lage geschaffen. Die betroffenen Personen können nicht wissen, aufgrund welcher Tatsachen und wann eine nichtautomatisierte Auswertung von Inhaltsdaten vorgenommen wird. Dementsprechend können sie selbst auch keine vorbeugende Überprüfung des Grundrechtseingriffs bewirken und ihre eigenen Interessen vertreten. Deshalb ist es erforderlich, dass die Anordnung einem Richtervorbehalt unterliegt. Richter können, ich zitiere das Bundesverfassungsgericht, „aufgrund ihrer persönlichen und sachlichen Unabhängigkeit und ihrer ausschließlichen Bindung an das Gesetz die Rechte des Betroffenen im Einzelfall am besten und sichersten wahren“. Der Richtervorbehalt hätte zudem den positiven Effekt, dass die Behördenleitungen das Vorliegen der Tatbestandsvoraussetzungen so plausibel und klar darlegen müssten, dass dies für den entscheidenden Richter oder die Richterin auch in kurzer Zeit gut nachvollziehbar wäre.

Die im Entwurf vorgesehene Anordnung durch die Behördenleitung und eine Beschäftigte oder einen Beschäftigten mit der Befähigung zum Richteramt kann keine persönliche und sachliche Unabhängigkeit und noch nicht einmal eine persönliche oder sachliche Distanz gewährleisten. Ein vergleichbarer Schutz kann so nicht gewährleistet werden.

Kurioserweise kommt noch hinzu, dass wenn in der anordnenden Behörde keine Person mit der Befähigung zum Richteramt beschäftigt ist, die Anordnung durch einen entsprechenden Mitarbeiter der Aufsichtsbehörde getroffen werden muss. Dies wäre der Ausnahmefall. Durch die damit verbundene organisatorische Distanz werden die betroffenen Personen damit im Ausnahmefall sogar besser geschützt als im Regelfall.

Ich hoffe, ich konnte Ihnen zeigen, dass die Landesregierung mit diesen Regelungen eine Rechtsgrundlage für ein massives Überwachungsinstrumentarium schafft, das zu Einschränkungen des Fernmeldegeheimnisses nach Artikel 10 GG und zur Einschränkung des Grundrechts auf informationelle Selbstbestimmung führt. Daher müssen die Maßstäbe an die Verhältnismäßigkeit der Maßnahmen besonders hoch angelegt werden.

Abg. **Sebastian Lechner** (CDU): Sie haben darauf hingewiesen, dass es manche Behörden gibt, in denen privater Datenverkehr nach außen erlaubt ist. Allerdings muss man bezüglich einer Einschätzung Ihrer juristischen Ausführungen fairerweise sagen: Wenn klar ist, dass im Landesdatennetz in Niedersachsen IDS ermächtigt sind, den Datenverkehr nach außen und nach innen mitzulesen, dann habe ich als Mitarbeiter die Wahl, meine Kommunikation über dieses Netz zu führen oder nicht. Wenn ich mich entscheide, dass ich über das Landesdatennetz private Kommunikation führe, dann tue ich das wohl in dem Wissen, dass diese protokolliert oder mitgeschnitten wird. Das ist ein qualitativer Unterschied: Niemand ist gezwungen, privaten Datenverkehr über das Landesnetz zu führen.

Ich teile durchaus Ihre Kritik, was die Anordnung durch die Behördenleitung angeht. So, wie ich den Gesetzentwurf verstehe, gibt es zwar eine zentrale Behörde, die für das Netz verantwortlich ist, die Systeme pflegt und darauf schaut, dass die automatisierte Auswertung funktioniert, aber jede einzelne Behörde, die an das Netz angeschlossen ist, darf dann auf Warnung des jeweiligen IDS selbst durch die Behördenleitung und einen entsprechend befähigten Beschäftigen bzw. eine solche Beschäftigte entscheiden, ob sie weitere Inhaltsdatenauswertungen vornimmt. Dies erfolgt also eben nicht durch eine zentrale Anordnung.

So verstehe ich das im Moment, und damit habe ich zwei praktische Probleme. Erstens muss man die Wahnhinweise, die das IDS gibt, verstehen, und zweitens bedarf es, glaube ich, schon einer gewissen technischen Befähigung, dann zu entscheiden, dass man, um den Sicherheitsvorfall aufzuklären, in die nichtautomatisierte Auswertung von Inhaltsdaten übergeht.

Das müsste man wohl stärker zentralisieren. Man könnte ja - nur so als Idee - die sogenannte Zentralstelle für Informationssicherheit, die hier im Gesetzentwurf auch verankert wird, dazu befähigen, diese Anordnung in einem ersten Schritt zu erteilen.

Es ist ja ein gestuftes Verfahren: Es gibt eine Auswertung ohne Inhaltsdaten, und dann gibt es eine Auswertung mit Inhaltsdaten. Insofern kann man ein mehrstufiges Verfahren vorsehen, d. h. die Zentralstelle wird ermächtigt, die Anordnung auszuführen für Auswertungen ohne Inhaltsdaten, und um wirklich in den Kernbereich zu gehen, also um tatsächlich Inhalte von E-Mails zu prüfen, muss man vielleicht einen Mechanismus mit einer - wie Sie schon anmerkten - Überprüfung durch einen Richtervorbehalt einführen.

Allerdings will ich darauf hinweisen, dass das nicht ohne eine Eilfallmöglichkeit gehen kann. Meine Wahrnehmung ist, dass es relativ viele Angriffe, auch in einer hohen Frequenz, geben kann, die man sich angucken muss. Das BSI wird dazu gleich sicherlich noch etwas sagen. Und wenn man dann immer einen Antrag bei Gericht stellen muss, kann das am Ende ein größeres Sicherheitsrisiko hervorrufen. Deswegen denke ich, es müsste eine Eilfallregelung geben, die es erlaubt, im Nachhinein zu prüfen.

Wie würden Sie zu so einer Eilfallregelung stehen, und wie würden Sie zu einer zentralisierten Kompetenz der Zentralstelle für Informationssicherheit, was die Anordnung angeht, stehen?**Dr. Christoph Lahmann**: Diese Streubreite der Anordnungsbefugnisse macht uns große Kopfschmerzen. Das liegt daran, dass der Gesetzentwurf so formuliert ist, dass die Verdachtsmomente nicht notwendigerweise aus einem bestimmten System kommen müssen. Der Gesetzentwurf sieht vor, dass der zentrale Dienstleister ein solches System, eine Information System Security, aufbauen muss. Die anderen können dies. Und da wird auch nicht spezifiziert, welcher Art dieses System sein muss. Es wird nur gesagt, dass dazu ein Sicherheitskonzept vorliegen muss. Das heißt, jeder Behördenleiter, der von seiner Administration einen schlüssig begründeten Verdachtsmoment vorgelegt bekommt, kann im Prinzip unter Zuhilfenahme bzw. Mitzeichnung seines Justiziars eine solche Anordnung verfügen. Das kann meiner Ansicht nach nicht die Intention des Gesetzes sein. So kann man es aber momentan zur Anwendung bringen.

Insofern wäre uns die Zentralisierung dieser Befugnisse ein großes Anliegen. Dafür gibt es ja auch gute Beispiele. Das BSI arbeitet nach diesem Schema. Es ist selbst nicht Betreiber des Bundesnetzes, aber sehr wohl mit den Security-Aufgaben betraut.

Im BSIG ist die Anordnungsbefugnis auch anders geregelt. Ein ähnliches Beispiel gibt es in Bayern. Dort gibt es ebenfalls eine Anordnungsbefugnis für die Leitung dieses Landesamtes. Insofern kann man sich sicherlich an anderen Gesetzen orientieren. Das wäre das Mindeste, wobei wir aufgrund der Eingriffsintensität natürlich nach wie vor den Richtervorbehalt als maximale Sicherheit zur Wahrung des Grundrechtsschutzes im Bereich der Inhaltsdatenanalyse an die erste Stelle stellen würden.

Bezüglich einer Eilfallregelung: Das ist ja eine gängige Praxis und sicherlich etwas, dem man sich anschließen könnte.

Abg. **Jan-Christoph Oetjen** (FDP): Meine Frage bezieht sich auf die Verarbeitung von personenbezogenen Daten, die nicht im Landesnetz stattfindet, sondern durch vom Land beauftragte Dritte erfolgt. Ich habe vor einiger Zeit eine Anfrage bezüglich des Niedersächsischen Hunderegisters gestellt, dort ist ein externer Dritter mit der Verarbeitung von personenbezogenen Daten beauf-

tragt. Bei der Anfrage ist beispielsweise herausgekommen, dass es nur alle vier Jahre ein Audit gibt und dass die Seite mit Blick auf deren Struktur und den Sicherheitsvorkehrungen offenbar relativ anfällig ist. Halten Sie es für notwendig, dass wir im Hinblick auf die Datenverarbeitung durch Dritte im NDIG noch Regeln ergänzen?

Dr. Christoph Lahmann: Prinzipiell muss man, wann immer man aus dem Landesnetz heraustritt und Dienstleister von außen nutzt, sicherstellen, dass das Sicherheitsniveau in der Verarbeitung aufseiten des Dienstleisters dem entspricht, was man durch Leitlinien, Richtlinien usw. vorgesehen hat. Anders kann es nicht gehen. Wir hatten vorhin schon einmal das Beispiel von der Kette und deren schwächstem Glied.

Wir haben im Datenschutzrecht zudem die Notwendigkeit, einen Auftragsverarbeitungsvertrag schließen zu müssen, in dem genau diese Dinge geregelt werden - einschließlich der Kontrollbefugnis und der Verpflichtung der verantwortlichen Stelle im Hinblick auf die Bedingungen, unter denen beim Drittanbieter gearbeitet wird. Ich denke, das ist ein ganz zentraler Punkt, und da kann es auch keine zwei Meinungen geben. Wir können natürlich nur bei Dienstleistern arbeiten lassen, die unser Sicherheitsniveau mittragen können. Das gilt für jedes System, das über unser Landesdatennetz erreichbar wird.

Bundesamt für Sicherheit in der Informationstechnik

Schriftliche Stellungnahme: Vorlage 5

***Anwesend**:*

- ***Ariane Müller-Hoepken** (Verbindungsbeamtin Norddeutschland)*
- ***Steve Ritter** (Referatsleiter IT-Sicherheit und Recht)*

Steve Ritter: Das BSIG enthält - wie gerade schon erwähnt wurde - ganz ähnliche Regelungen zur Angriffserkennung wie die, die Sie jetzt mit dem NDIG einführen möchten. Wir haben damit also einige Erfahrungen - auch wenn die Norm etwas anders strukturiert ist -, und dazu möchte ich im Folgenden berichten.

Bei praktisch jedem Netzwerkverkehr - das betrifft nicht nur Telefonate, sondern auch jede E-Mail und jeden Aufruf einer Website - gibt es Fernmeldebeziehungen, und sobald Sie Schutzmaßnahmen vornehmen - selbst mit einem Virenscanner -, greifen Sie in das Fernmeldegeheimnis ein. Herr Lahmann hatte in diesem Zusammenhang gesagt, dass die Regelung zur Anordnungsbefugnis aus Sicht der LfD nicht ausreichend sei. Aber stellen Sie sich einmal vor, dass ein Mitarbeiter einer Behörde immer erst zur Behördenleitung gehen muss bzw. eine Anordnung der Behördenleitung und eines Juristen aus dem Amt benötigt, wenn er einen Vorfall bemerkt - z. B. wenn der Virenscanner anschlägt -, bevor er sich das näher anschauen darf. Sie werden sehr schnell feststellen: Das ist ein Problem. - Darauf komme ich gleich noch einmal zu sprechen.

Im Wesentlichen hat mich gewundert, dass die Länder erst so spät damit angefangen haben, in diesem Bereich Gesetze auf den Weg zu bringen. Ich bin mir relativ sicher, dass auch Sie bereits Virenscanner und Firewall-Systeme betrieben haben. Das hoffe ich jedenfalls. Dann stellt sich natürlich die Frage, wie Sie die Eingriffe in das Fernmeldegeheimnis bisher gerechtfertigt haben. - Ich will darauf keine Antwort. Verstehen Sie die Frage eher als Denkanstoß.

Insofern begrüße ich, dass das Land Niedersachsen jetzt einen entsprechenden Gesetzentwurf vorgelegt hat. Ich finde ihn grundsätzlich auch sehr gut, weil er tatsächlich eine gesetzliche Grundlage für entsprechende Sicherheitsmaßnahmen bietet.

Ich möchte im Folgenden kurz auf einige Punkte eingehen. Im Zusammenhang mit Online-Portalen steht in § 4 des Gesetzentwurfs, dass „Maßnahmen“ zur Absicherung getroffen werden sollen. In Artikel 32 der DS-GVO ist das Niveau, das solche Sicherheitsmaßnahmen erfüllen müssen, noch ein bisschen besser beschrieben. Dort werden die Angemessenheit und der Stand der Technik als Maßstab verwendet. Ich würde empfehlen, die Regelung an dieser Stelle anzugleichen.

Die Bereiche „Technikoffenheit“, „Schutzregelungen“ und „Zusammenarbeit mit anderen Ländern oder dem Bund“ würde ich als Problempunkte bezeichnen.

- Technikoffenheit -

Herr Lahmann hatte die Regelungen als sehr technikoffen bezeichnet. Ich würde ihm an dieser Stelle widersprechen wollen: Ich finde den Gesetzentwurf an einigen Stellen sogar ausgesprochen wenig technikoffen. Wenn es z. B. in § 19 - Auswertung gespeicherter Daten - um die Frage geht, aus welchen Systemen Ereignisprotokolle ausgewertet werden dürfen, ist von Anwendungsservern, E-Mail-Servern und Netzwerksystemen die Rede. Aber was ist denn z. B. mit Ereignisprotokollen von lokalen Anwendungen auf einem System? Wenn ein Angreifer sich durch ein Netzwerk arbeitet, arbeitet er eben auch auf lokalen Systemen, und da nützt Ihnen dann das Mitprotokollieren auf einem Server erst einmal gar nichts. Sie müssen auch Logdaten von lokal installierter Anwendersoftware auswerten können, um diesen Angriff aufzuklären, um herauszufinden, wie der Angreifer vorgegangen ist, welche Lücken er genutzt hat und an welcher Stelle bereinigt werden muss bzw. wo künftig Lücken geschlossen werden müssen.

In § 18 taucht der Begriff der „digitalen Daten“ auf. Ich habe mich gefragt, was damit gemeint ist. Wenn dies eine Festlegung auf die digitale Datenverarbeitung bedeutet, ist die Regelung nicht sehr entwicklungsoffen. JAVIS zeigt ganz gut, wie wir heute Datenverarbeitungssysteme machen, nämlich sehr binär. Bei Quantencomputern und Chips mit Memristoren handelt es sich schon nicht mehr um digitale Datenverarbeitungen. Solche Systeme würden Sie mit der Regelung in der jetzigen Form ausschließen. Meine Empfehlung wäre, die Regelung an dieser Stelle möglichst technikneutral zu belassen.

Herr Lahmann hat zu Recht den Einwand gebracht, dass das alles irgendwo eingegrenzt werden muss; denn - darüber müssen wir uns keine Illusionen machen - hier wird ein tiefgreifender Eingriff vorgenommen. Ich glaube, dass dieser Eingriff notwendig ist und dass man ihn über das Merkmal der „Erforderlichkeit“ einfangen kann: Ist diese Datenverarbeitung, dieser konkrete Verarbeitungsschritt notwendig, um weiter analysieren zu können, ob ein Angriff vorliegt oder ob es notwendig ist, um einen Angriff, der läuft, abzuwenden?

Das Merkmal der Erforderlichkeit ist ein sehr starkes Instrument, und im BSIG wird ebenso vorgegangen. Das BSIG - auch die entsprechende Regelung in § 5 - war übrigens bereits Gegenstand einer Verfassungsbeschwerde, und § 5 ist unverändert geblieben. Insofern ist das aus meiner Sicht ein Weg, den man gehen kann.

- Schutzregelungen -

Ich hatte bereits am Beispiel des Virenscanners dargestellt, dass es nicht immer praktikabel sein wird, wenn Maßnahmen grundsätzlich der Anordnung durch eine Behördenleitung und durch einen Juristen bedürfen. Wir stellen fest, dass die klassischen kommerziellen Schutzsysteme, hinter denen unser Schadsoftware-Erkennungssystem hängt, immer noch sehr viele Sachen durchlassen, die wir erst später detektieren. Das bedeutet, wir reden da schon über hohe Angriffszahlen. Gehen Sie also davon aus, dass solche Anordnungen durchaus häufiger vorkommen. Müsste jede einzelne Verarbeitung durch die Behördenleitung gemacht werden, dann hoffe ich, dass jede Behördenleitung einen Stellvertreter hat, der nichts anderes macht.

Wir haben im BSIG die Anordnung der Behördenleitung an einer Stelle vorgesehen, und zwar in § 5, wenn es darum geht, Protokolldaten, die - sofern sie auf Vorrat gehalten werden - zu pseudonymisieren sind und nicht im Klartext verarbeitet werden dürfen, zu depseudonymisieren. Möchte man das Ganze technisch absichern, sodass tatsächlich kein Zugriff möglich ist, ohne dass die Behördenleitung das angeordnet hat, muss man an dieser Stelle mit kryptografischen Verfahren arbeiten, sodass tatsächlich nur die Behördenleitung den kryptografischen Schlüssel hat, und der Mitarbeiter im BSI diese Daten nicht einmal depseudonymisieren könnte, wenn man ihm eine Pistole vorhalten würde.

Stellt man sich das Ganze einmal in der Praxis vor, wird klar, dass die Behördenleitung ihren Depseudonymisierungsschlüssel im Prinzip immer bei sich haben und auf Anforderung den Zugang zu den Daten ermöglichen müsste. Das wird schwierig. Wir überlegen tatsächlich, ob wir da nicht über eine Gesetzesänderung neue Wege suchen müssen, um das Ganze praktikabler zu machen.

Bei Ihnen wäre das Problem sogar noch etwas verschärft, denn Sie haben vorgesehen, dass die Daten nur für sieben Tage gespeichert werden dürfen. Jetzt stellen Sie sich einmal vor, dass das nicht sofort bearbeitet wird. Im Zweifelsfall kommt die Anordnung, nachdem die Daten schon längst gelöscht sind. Insofern halte ich das für schwierig zu realisieren.

Umgekehrt habe ich andere Schutzregelungen, die wir z. B. im BSIG haben, im NDIG-Entwurf nicht gefunden, beispielsweise die Möglichkeit oder die Pflicht der jeweiligen Behörde, den Innenausschuss jährlich darüber zu unterrichten, wie sie diese Befugnis genutzt hat. Das finde ich durchaus wichtig angesichts des Eingriffsgewichts. Denn - da hat Herr Lahmann absolut recht - der Eingriff ist schwerwiegend, und wir müssen Schutzvorkehrungen treffen. Ich halte eine Kontrolle sowohl durch die entsprechende Landesdatenschutzbehörde als auch durch das Parlament angesichts der Schwere des Eingriffs tatsächlich für geboten. Ich empfehle, das aufzunehmen. Die Änderung wäre relativ leicht vorzunehmen.

Was auch - vor allem im Vergleich zum BSIG - aufgefallen ist: Sie haben auf der einen Seite eine sehr strenge Zweckbindung mit Blick auf die IT-Sicherheit, die aber am Ende zu einem gewissen Grad wieder aufgelöst wird, indem die Übermittlung der Daten z. B. an den Verfassungsschutz und die Polizeibehörden auch zu anderen Zwecken erlaubt werden soll.

Zudem ist mir aufgefallen, dass die Betroffenen nicht benachrichtigt werden sollen, wenn ihre Daten im Zusammenhang mit einem Disziplinarverfahren verarbeitet wurden. Ich habe im Gesetz überhaupt nicht die Möglichkeit gefunden, dass die Daten dafür verwendet werden dürfen. Darauf sollte man einmal den Blick werfen.

- Zusammenarbeit mit anderen Ländern oder dem Bund -

Es wird immer wieder überlegt, wie man die Ressourcen, die es in diesem Bereich gibt, sinnvoll bündeln kann. Es gab auch die Überlegungen, ob es nicht sinnvoll ist, dass die Länder sich an Schutzsysteme des Bundes anschließen. Das wäre mit der Norm, wie sie bisher ist, meines Erachtens nicht möglich, da die Struktur fundamental anders ist als die z. B. im BSIG und bisher auch keine Öffnungsklausel irgendeiner Art vorgesehen ist. Beispielsweise unterscheiden Sie sehr stark nach Inhaltsdaten, Nicht-Inhaltsdaten und Logdaten aus Ereignisprotokollen. Das haben wir im BSIG so nicht. Wir unterscheiden hauptsächlich danach, wo Informationen angefallen sind, nämlich an den Schnittstellen der Kommunikationstechnik des Bundes. Sie können sich das wie eine Art Stadtmauer vorstellen, und die Schnittstellen sind die Stadttore, und an denen schauen wir uns den Datenverkehr an. Das hat den Vorteil, dass - um im Bild zu bleiben - selbst wenn sich dahinter kleinere Kastelle innerhalb der Stadt befinden, doch alle an diesem zentralen Tor vorbei müssen. Wenn es dahinter schwächere Maßnahmen gibt, ist das erst einmal egal, weil es vorn am Tor schon einmal einen starken Filter gibt. Das könnte an der Stelle vielleicht der Bund darstellen.

Die zweite Möglichkeit, die wir kennen, sind Protokolldaten, und auch an der Stelle ist es im BSIG sehr viel technikoffener formuliert. Anders als im NDIG-E sind keine einzelnen Protokolle wie http genannt.

Man muss dazu sagen: Die Technik entwickelt sich weiter. Es gibt neben http weitere Protokolle. Es gibt welche zur Dateiübertragung wie FTP, es gibt Systeme für Netzwerkspeicher und SMB-Protokolle, sie alle sind nicht genannt. Das Mail-Protokoll fehlt auch. Ich habe Zweifel, ob Sie tatsächlich alles erschlagen, und wenn etwas Neues dazu kommt, dann wären Sie wohl sehr schnell raus.

Ich betreue unser SES seit ungefähr 2011 durchgehend juristisch. Tatsächlich hat es sich insbesondere mit Blick auf die Entwicklung bei den Angriffsformen und die Notwendigkeit, die Detektion immer wieder an neue Angriffswege anzupassen, als sehr hilfreich erwiesen, dass das Gesetz dort technikneutral aufgebaut ist und man lieber versucht, über eine sehr enge Erforderlichkeitsabstufung zu arbeiten.

Gesetzgebung ist ein wenig so, als wenn man mit einem Auto nach vorn fährt, während man die ganze Zeit in den Rückspiegel schaut. Was die Benennung einzelner Techniken angeht, sind Sie bei diesem Gesetzentwurf sehr oft so verfahren. Das würde ich vielleicht anders machen und dort offener gestalten.

Im BSIG haben wir es anders gemacht, und unser System ist technisch sehr eng am juristischen Aufbau des BSIG orientiert. Das ist eine Grundsatzentscheidung, die man irgendwann treffen muss. Insofern glaube ich, dass, wenn der Entwurf so bliebe, man an dieser Stelle - sofern Sie und auch der Bund es wollten - nicht schnell aneinander anschließen könnte.

Ich fände das schade, weil ich glaube, dass wir auch im Vergleich mit kommerziellen Anbietern, die darauf verweisen, dass sie mit KI usw. Angriffe sehr gut erkennen können, relativ gut sind. Das

hängt aber auch damit zusammen, dass das nicht nur Technik ist, sondern auch sehr viel menschliche Analysten-Power dahinter steckt. Die Technik prüft eben nur, ob das ein Fingerabdruck einer bestimmten Schadsoftware ist, und sobald auch nur eine Linie verändert wird - bei einer Schadsoftware ist das über eine leichte Anpassung des Codes möglich -, detektiert sie ihn nicht mehr. Wenn man Analysten hat, die ordentliche Signaturen bauen, geht das gut, es ist aber sehr aufwendig. Ich weiß nicht, ob Sie das als Land so machen wollen. Das ist eine große Aufgabe.

Abg. **Sebastian Lechner** (CDU): Sie haben als Letztes einen der auch aus meiner Sicht schwierigsten Punkte angesprochen. Ich würde die Grundsatzentscheidung gern so treffen, dass die Zusammenarbeit mit Ihnen möglich ist. Denn ich habe die Befürchtung, dass es nur in Zusammenarbeit und gemeinsam gelingt, die IT-Sicherheit auch bei den Kommunen ordentlich und sicher aufzustellen. Sie haben eben über signaturgetriebene Systeme gesprochen. Es gibt aber auch Systeme, die durch KI betrieben werden. Mit Blick darauf habe ich noch mehr Schwierigkeiten mit der Frage, wie jedes einzelne Land IT-Sicherheit gewährleisten soll. Insofern wäre ich Ihnen verbunden, wenn Sie uns eine Idee geben könnten, vielleicht schriftlich, wie eine mögliche Öffnungsklausel zu diesem Paragrafen aussehen könnte oder wie man eine Erforderlichkeitsabstufung vornehmen könnte, um das NDIG etwas mehr mit dem BSIG zu synchronisieren.

Steve Ritter: Was die Öffnungsklausel betrifft: Das wird nicht trivial, das muss man ganz klar sagen. Wir müssen uns bewusst machen, dass es sich um einen Eingriff in das Fernmeldegeheimnis handelt, um eine Einschränkung von Artikel 10 GG. Wenn hier Landesbehörden und Bundesbehörden entsprechende Befugnisse haben möchten, wird man sowohl eine entsprechende Regelung auf Bundesebene brauchen als auch gleichzeitig bei allen Ländern, die sich daran beteiligen möchten. Der Bund hat nicht die Gesetzgebungskompetenz für die Gefahrenabwehr auf Länderebene. Das liegt völlig zu Recht bei den Ländern, und dementsprechend muss es auf jeden Fall einen Anker bei Ihnen im Landesgesetz geben. Gleichzeitig können Sie natürlich nicht in einem Landesgesetz eine Bundesbehörde unmittelbar beauftragen. Das heißt, auch der Bund muss für sich selbst eine entsprechend konkrete Befugnis für das BSI treffen, die aber gleichzeitig irgendeine Einbindung des Landes zulässt. Wir bewegen uns hier rechtlich ein Stück weit auf Neuland.

Wenn ich spontan etwas sagen müsste: Vielleicht eine dynamische Verweisung im Landesgesetz auf eine Regelung in einem Bundesgesetz und im Bundesgesetz eine Öffnung. Und wenn ein Land darum ersucht oder Land und Bund sich einigen, dann darf das entsprechend dieser landesgesetzlichen und bundesgesetzlichen Regelung erfolgen. Aber, wie gesagt, das ist sehr ins Unreine gesprochen. Man müsste noch einmal viel Hirnschmalz investieren in die Frage, wie man das sauber abbilden kann.

Abg. **Sebastian Lechner** (CDU): Sie haben die Speicherfrist von sieben Tagen angesprochen. Ich würde gern wissen, wie das bei Ihnen geregelt ist. Wie lange dürfen Sie speichern? Ich habe auch schon oft gehört, dass diese sieben Tage kaum ausreichen werden, um Sicherheitsvorfälle im Nachhinein analysieren zu können. Jeden Tag werden Datenbestände gelöscht, weil die Sieben-Tages-Frist eingehalten werden muss, und man muss dagegen anarbeiten. Das ist wohl kaum praktikabel.

Steve Ritter: Wir haben das im BSIG unterschiedlich geregelt. Bei den Schnittstellendaten haben wir tatsächlich nur das Merkmal der Erforderlichkeit, d. h. die Daten dürfen solange verwendet werden, wie es erforderlich ist, um erst einmal den Verdacht zu bestätigen, später den Angriff zu verhindern oder auch die Angriffserkennung zu verbessern. Denn oftmals, wenn Sie z. B. schadhafte Dokumente wie ein Bild oder eine PDF-Datei haben, in denen Schadgut versteckt ist, wird es nicht damit erledigt sein, sie einmal auszuwerten und eine Signatur zu basteln. Sie müssen immer wieder an diesen Systemen arbeiten, um die Erkennung zu schärfen. Das heißt, Sie müssen Dokumente im Zweifelsfall auch mal behalten, um immer wieder zu schärfen, was das gemeinsame Merkmal und der genaue Angriffsvektor ist. Da macht eine feststehende Frist also wenig Sinn.

Bei Protokolldaten, wo es ja tatsächlich sehr konkret um den einzelnen Kommunikationsvorgang geht, haben wir eine Frist von drei Monaten, die ganz klar auch ein Kompromiss ist. Man liest verschiedenste Zahlen, wann APTs, also zielgerichtete z. B. nachrichtendienstliche Angriffe, entdeckt werden. Je nach Quelle findet man irgendwas um 200 bis 280 Tage. Das wird dann schon schwierig.

Die Spanne ist aber notwendig, weil Angriffe sehr spät entdeckt werden, und wenn man sich dann

daranmacht, sie aufgrund von Protokolldaten, Logdaten zu analysieren, ist es natürlich wichtig, möglichst weit zurückgehen zu können, in der Hoffnung, den initialen Angriff noch zu sehen und dann weiter verfolgen zu können. Je kürzer die Frist ist, desto schwieriger wird das. Klar ist: Irgendwo muss man eine Frist setzen, um den Datenschutzbedenken und auch den Grundrechten gerecht zu werden. Aber: Je länger, desto besser. Das muss man so sagen.

Abg. **Sebastian Lechner** (CDU): Soweit ich es verstanden habe, hat das BSI weitreichende zentrale Anordnungsbefugnisse auch gegenüber anderen Behörden. Ist das richtig? Sind Sie auch bevollmächtigt, anordnen zu dürfen, Inhaltsdaten manuell auszulesen? Dürfen Sie sich diese angucken? Oder ist das auf Bundesebene so geregelt, dass das nur jede Behörde selbst darf? Wenn Letzteres der Fall ist: Wie stellt das BSI sicher, dass in den entscheidenden Fällen auch wirklich dort hineingeguckt wird und alles den Ansprüchen entsprechend vollzogen wird?

Steve Ritter: Das System ist so gestaltet, dass die Sensoren sozusagen an den Stadtgrenzen stehen. Sie müssen sich vorstellen: Der Bund hat ein gemeinsames Netz, den IVBB, in dem befinden sich sozusagen die einzelnen Behördennetze. Man hat zentrale Übergänge ins Internet, und an diesen zentralen Übergängen sind die Sensoren des BSI. Das heißt, wir müssen an der Stelle erst einmal noch gar nicht auf eine Behörde zugehen und sagen, dass da etwas durchgelaufen ist und um Inhaltsdaten bitten etc. Das sind unsere Sensoren. Der Datenverkehr wird dann quasi zum BSI ausgeleitet, und in unseren Analysesystemen wird durchleuchtet, ob ein Angriff vorliegt. Wenn es dafür Anhaltspunkte gibt, schaut sich das ein Analyst an. Wenn das manuell erfolgt, muss das dann ein Bediensteter mit der Befähigung zum Richteramt anordnen. Das wäre wieder die Hürde.

Abg. **Sebastian Lechner** (CDU): Sitzt der Analyst bei Ihnen oder in der Behörde?

Steve Ritter: Der sitzt tatsächlich bei uns. Die Angriffserkennungsmechanismen sind zentral im BSI. Wir haben das zentralisiert.

Abg. **Sebastian Lechner** (CDU): Und wenn dann in die Inhaltsdaten geschaut werden muss, wer entscheidet dann über eine solche Erlaubnis? Auch Sie?

Steve Ritter: Genau. Das passiert bei uns, noch nicht einmal gemeinsam mit der Behördenleitung. Es gibt aber regelmäßige Kontrollbesuche des BFDI, der sich die Anordnungen anschaut. Ich würde auch dringend empfehlen, dass sich die Landesdatenschutzbeauftragte die Anordnungen anschauen kann.

Wir müssen zudem - ähnlich wie das hier vorgesehen ist - ein Datenerhebungs- und -verwendungskonzept vorhalten, d. h. was machen wir mit den Daten, und unter welchen Voraussetzungen machen wir das. Auch das stimmen wir mit dem BFDI ab, genauso wie jede Form der Grundsatzentscheidung zum Umgang mit Daten. Wir pflegen ein sehr enges Verhältnis, um den Grundrechtsinteressen gerecht zu werden.

Bayerisches Staatsministerium der Finanzen und für Heimat

***Anwesend**:*

*- **Dr. Jan Remy** (Referatsleiter)*

Dr. Jan Remy: Ich werde mich nicht zu dem Gesetzentwurf selbst äußern, sondern Ihnen stattdessen berichten, wie unsere Erfahrungen bei dem Thema sind. Ich leite im Finanzministerium das Referat, das die IT-Sicherheit und die IT-Infrastruktur, sprich unsere Netze und die IT-Strategie, abdeckt. Wir haben vor gut einem Jahr ein E-Government-Gesetz auf den Weg gebracht.

- Handlungsfeld -

Wir haben erstens ein Behördennetz mit 2 000 Standorten. Das geht von kleinen Forsthütten bis hin zu großen Behörden und schließt auch die Landratsämter mit ein, und an diesen Landratsämtern wiederum sind kommunale Netze angebunden, über die sich dann Gemeinden mit dem Behördennetz verbinden. 60 % unserer rund 2 000 Kommunen sind so angebunden.

Zweitens gibt es unsere Rechenzentren, insbesondere das staatliche Rechenzentrum für die Verwaltung und die Gerichte und das Steuerrechenzentrum, das einen sehr sensiblen Datenbestand hat.

Das sind die beiden Schutzziele. Hinzu kommt noch ein drittes: Wir haben in unserem E-Government-Gesetz schon länger die Kommu-

nen verpflichtet, IT-Sicherheit umzusetzen und auch Konzepte, sprich Informationssicherheitsmanagementsysteme, aufzustellen. Sie haben eine Frist bis Anfang nächsten Jahres.

- IT-Sicherheit -

Wie ist IT-Sicherheit bei uns organisiert? - Erst einmal ist das Landesamt für Sicherheit in der Informationstechnik (LSI) beim Finanzministerium angesiedelt, dort werden die Rechenzentren und das Behördennetz verantwortet. Bei uns ist IT-Sicherheit ein Thema, dessen sich die Beamten an der Spitze des Hauses sehr eng annehmen. Unser Amtschef sieht sich als Spitze der Organisation. Wir selbst führen die Fachaufsicht über das LSI und sind auch dafür verantwortlich, dass in der ganzen Verwaltung ein Informationsmanagementsystem eingeführt wird.

Das LSI ist am 1. Dezember 2017 gegründet worden. Das Errichtungsgesetz ist damals einstimmig durch den Landtag gegangen. Dass wir dabei die Unterstützung aller Fraktionen hatten, hat uns sehr gefreut. Das Gesetz schafft neben der Errichtung des LSI auch die notwendigen gesetzlichen Grundlagen für weitergehende Sensorik im Netz. Ähnlich wie in Niedersachsen gibt es im Grundsatz die automatische Verarbeitung. Die manuelle Durchsicht von Daten, Inhaltsdaten und Protokolldaten ist die Ausnahme.

Wir haben einen sehr guten Arbeitskontakt auf ministerieller und natürlich auch auf operativer Ebene mit Verfassungsschutz und Landeskriminalamt. Das ist, denke ich, ein wichtiger Erfolgsfaktor, den wir in den nächsten Jahren auch noch verstärken wollen.

Die Ressorts und die Behörden müssen bei uns eigene IT-Sicherheitsstrukturen aufbauen. Das Behördennetz ist sehr zentralisiert und wird zentral vom LSI behandelt, aber wir sind der Meinung - das war auch eine Motivation für das LSI -: Um die IT-Sicherheit muss sich jeder selbst kümmern. Das kann man nicht delegieren, sondern dort, wo die Herausforderungen und die Probleme sind, müssen sie auch gelöst werden. Deshalb haben wir auch einen dezentralen Ansatz, der einen guten Teil der Verantwortung denen zuschiebt, die auch die Systeme betreiben.

Trotzdem ist das LSI als Behörde, die alle berät, Kopf dieser Struktur. Sie macht zentrale Vorgaben, erstellt Sicherheitsrichtlinien usw.

Die zweite Aufgabe des LSI betrifft den kommunalen Bereich. Wir haben, wie gesagt, rund 2 000 Gemeinden. Viele sind kleine Landgemeinden. Das LSI hat einen Beratungsauftrag, nur hilft es natürlich niemandem, wenn es nur irgendeine Beratung gibt. Unsere Zielsetzung ist es, in den nächsten Jahren eine sehr enge Vernetzung aufzubauen und die Kommunen sehr individuell beraten zu können.

Was wir im Moment z. B. konkret über das LSI machen, ist das Veranstalten von regionalen Sicherheitskonferenzen, bei denen wir Kommunalvertreter versammeln. Sie sind in der Regel sehr gut besucht. Ich würde sogar sagen, es sind fast alle Kommunen da, und das zeigt auch, dass das Thema dort Interesse findet und angekommen ist.

Ein weiteres Handlungsfeld betrifft die KRITIS-Betreiber. Das ist ein Bereich, den man sich erst über die Jahre hin aufbauen muss. Konkret befassen wir uns gerade mit kommunalen Wasserwerken.

- Praxiserfahrungen -

Was ist unsere Praxiserfahrung nach einem Jahr? Unabhängig von der Gesetzgebung war der Landtag sehr großzügig zu uns, was Stellen betrifft. Zielsetzung ist, 200 Stellen aufzubauen. Im Moment haben wir 60 Kolleginnen und Kollegen plus zehn Anwärter. Wir setzen im Moment eher darauf, wirkliche Fachkräfte zu gewinnen als möglichst schnell 200 Mitarbeiter zu haben. Ich glaube, damit fährt man auf Dauer besser.

Wir denken, ein Gewinn durch das LSI ist auch, dass die IT-Sicherheit einen ganz anderen Stand bekommen hat. Das liegt nicht nur am Landesamt sondern auch daran, dass das Thema mit dem E-Government-Gesetz damals eine eigene gesetzliche Grundlage bekommen hat, die Befugnisse begründet, die uns mit Blick auf die Analysemöglichkeiten, die wir brauchen, den Rücken freihalten.

In dieser kommunalen Struktur, die wir haben, ist eine wirksame Beratung und Unterstützung eigentlich überhaupt nur in der Struktur eines Landesamts möglich. Ich denke, dass man bei diesem Thema sehr in die Fläche gehen muss, dass man auch vor Ort sein und die kommunale Ebene gut kennen muss. Ich denke, das kann keine Behörde einfach nebenbei leisten.

Umgekehrt hilft die Struktur eines LSI natürlich auch, dass die kommunale Seite uns sieht und wir als Ansprechpartner wahrgenommen werden.

Wie gesagt, das Thema ist erst in der Aufbauphase, aber einiger Mehrwert bietet sich jetzt schon.

Abg. **Sebastian Lechner** (CDU): Sie haben gesagt, Sie haben einen dezentralen Ansatz. Aber irgendwie haben Sie auch einen zentralen Ansatz, weil das LSI der Kopf dieser dezentralen Struktur ist. Dann hatten Sie geschildert, dass das LSI Beratungsleistungen erbringt, aber Sie haben auch gesagt, dass es trotzdem zentrale Vorgaben gibt. Können Sie ausführen, was das genau bedeutet? Beraten Sie die Kommunen nur, oder gibt es die konkrete Vereinbarung zwischen der kommunalen Ebene und dem LSI, dass die zentralen Vorgaben auch umzusetzen sind? Gibt es vielleicht sogar gesetzliche Grundlagen, sodass man dann auch diesen dezentralen Verbund ein wenig orchestrieren kann?

Dr. Jan Remy: Es ist gut, dass Sie nachhaken. Es gibt zunächst die Struktur auf staatlicher Seite, die hierarchisch von oben nach unten geht, von einem Landessicherheitsbeauftragten zu den Ressortssicherheitsbeaufragten, zu solchen, die dann für die Behörden zuständig sind. Uns ist wichtig, dass es diese Struktur bei den Behörden in der Fläche gibt.

Bei den Kommunen ist es ein bisschen anders. Sie leben erst einmal ihr Eigenleben. Natürlich gibt es durch den Anschluss an das Behördennetz Bedingungen, die einzuhalten sind - das ist klar - und es gibt gesetzliche Vorgabe aus dem E-Government-Gesetz. Das enthält, um es vor dem Hintergrund der Konnexität umsetzen zu können, natürlich keine konkreten Vorgaben, sondern dort wird eher der Ansatz verfolgt, dass man sich eben um IT-Sicherheit kümmern muss. Das kann heute keiner mehr ernsthaft anders sehen. Deshalb ist der Ansatz eher, die Kommunen zu beraten. Wir wollen auf Dauer eher zu einem Dialog kommen, uns nicht in Form eines Audits aufdrängen, sondern eher das Gespräch suchen.

Abg. **Sebastian Lechner** (CDU): Und wenn die Anschlussbedingungen nicht eingehalten werden, kann man sich nicht an Ihr Netz anschließen?

Dr. Jan Remy: So ist es.

Abg. **Sebastian Lechner** (CDU): Und sollten Sie feststellen - das kann man ja von außen tun -, dass es Verstöße gibt, schalten Sie dann ab, oder geben Sie einen Hinweis, dass Sie die Verbindung kappen, wenn ein Verstoß nicht behoben wird?

Dr. Jan Remy: Letzteres ist der Fall. Da gab es bisher aber nie ein Problem.

Abg. **Sebastian Lechner** (CDU): Sie haben gesagt, der große Vorteil des LSI sei vor allem die Mannstärke und die Beratungskapazität. Ist der Leiter des LSI ein Abteilungsleiter oder der Bevollmächtigte, der für Informationssicherheit des ganzen Landes zuständig ist? Wie ist das mit Blick auf die Verantwortlichkeiten strukturiert?

Dr. Jan Remy: Das Landesamt ist eine eigenständige Behörde mit einem Präsidenten. Es ist eine nachgeordnete Behörde in unserem Geschäftsbereich. Der Präsident leitet seine Behörde wie beispielsweise der Präsident eines Landesamts für Steuern. Das LSI ist keine Abteilung oder sonst irgendwo angegliedert, sondern eine eigenständige Behörde mit Sitz in Nürnberg.

IT.Niedersachsen

Schriftliche Stellungnahme: Vorlage 3 neu

***Anwesend**:*

*- **Axel Beims** (Geschäftsführer)*

Axel Beims: Wie Sie sicherlich wissen, ist IT.Niedersachsen (IT.N) ein nachgeordneter Bereich bzw. ein Landesbetrieb des Innenministeriums. Insofern hatten wir bei der Erarbeitung des Gesetzentwurfs zum NDIG umfassend und hinreichend die Möglichkeit und Chance, uns miteinzubringen.

IT.N begrüßt und unterstützt das NDIG vollumfänglich. Es bietet für uns die erforderliche Grundlage, erstens der operativen Verantwortung für die Digitalisierung der Landesverwaltung gerecht zu werden, und zweitens eben diese stärker und effektiver abzusichern, von außen wie von innen. Insbesondere der dritte Teil des NDIG schafft das erforderliche Fundament, den Schutz des Landesnetzes auf eine neue, herausragende Qualitätsstufe anzuheben. Es ermöglicht, die Sicherungsmaßnahmen von einem reinen Perimeterschutz hin zu einem Inhaltsschutz zu verbessern, wodurch eine erheblich frühere und zielführende-

re Erkennung etwaiger Bedrohungen ermöglicht wird.

Der zweite Teil des NDIG stellt die Grundlage zur Umsetzung des OZG dar. IT.N verantwortet die operative Umsetzung in Bezug auf die öffentlich-rechtliche Verwaltungstätigkeit des Landes. Insofern entfaltet das NDIG hier unmittelbare Wirkung und stellt die nötigen Leitplanken für die konkrete Ausgestaltung in den kommenden Jahren zur Verfügung.

Die Umsetzung des OZG bzw. des Handlungsplans ist eines der Kernelemente der Strategie Niedersachsens zur digitalen Transformation, die im Masterplan Digitalisierung des Niedersächsischen Ministeriums für Wirtschaft, Arbeit, Verkehr und Digitalisierung erhalten ist.

IT.N erhält durch das Gesetz einen guten mittelbaren Rahmen für seine Aufgaben als IT-Dienstleister des Landes. Die fachliche Ausgestaltung der Umsetzung erfolgt aktuell in enger Abstimmung mit der Gesamtprogrammleitung im Innenministerium.

Wie bereits einleitend hervorgehoben, schafft der dritte Teil des NDIG den nötigen Rahmen zum Einsatz von Technologien, die den Grad der Informationssicherheit substanziell erhöhen. Im Rahmen der Genese dieses Gesetzesteils wurde IT.N - wie bereits gesagt - umfassend beteiligt. Wir empfinden den Gesetzentwurf als sehr guten Rahmen und halten ihn auch für umsetzbar.

Die Daten des Landes sind ein hohes Gut. Sie dauerhaft allumfassend gegen immer filigranere Angriffslogiken zu schützen, ist eine ganz wesentliche Aufgabe. Das NDIG gibt die Gewähr, dem Thema die vollumfängliche Aufmerksamkeit zuteilwerden zu lassen, die es verdient.

Abg. **Sebastian Lechner** (CDU): Herr Beims, im Gesetzentwurf ist die Rede von der „das Landesdatennetz betreibende[n] Behörde“. Ich habe mich gefragt, wer das eigentlich ist. Wer betreibt das Landesnetz? IT.N ist ein Landesbetrieb, aber sind Sie auch eine Behörde? Oder ist es das MI, das über IT.N das Landesnetz betreibt? Wer ist nach der fachlichen Logik des Gesetzentwurfs zuständig?

Axel Beims: Wir sind Auftragnehmer und technischer Betreiber des Landesnetzes. Je nach Begriffsdefinition, ob es ein technischer Betreiber oder ein verantwortlicher Betreiber ist, da mag es verschiedene Interpretationen geben. Wir sind der technische Betreiber des Landesdatennetzes.

Abg. **Sebastian Lechner** (CDU): Dann ist das MI die das Landesdatennetz betreibende Behörde?

Axel Beims: Es ist unser Auftraggeber.

Abg. **Sebastian Lechner** (CDU): Oder soll es die neue Zentralstelle für Informationssicherheit sein?

(Zuruf)

- Also das Innenministerium?

Vors. Abg. **Thomas Adasch** (CDU): Wir befinden uns mitten in einer Anhörung. Das müssten wir im Anschluss klären.

Abg. **Sebastian Lechner** (CDU): Das wäre gut. Es sind ja Vertreter des MI anwesend, die könnten das im Anschluss vielleicht einmal aufklären; denn das würde mich sehr interessieren.

Herr Beims, IT.N ist also der technische Betreiber. Bei Ihnen werden in Zukunft die IDS laufen?

Axel Beims: Genau.

Abg. **Sebastian Lechner** (CDU): Das heißt, Sie betreiben sie, Sie pflegen sie, und Sie machen die Signaturarbeit, die vom BSI geschildert wurde? Sie bauen also auch die menschlichen Analysekapazitäten auf, die benötigt werden, um das zu tun? Oder sollen die dann in den jeweiligen Behörden aufgebaut werden?

Axel Beims: Nach den bisherigen Ansätzen und Logiken machen wir die technischen Analysen und führen dann Erkenntnisse herbei, wo irgendwelche Störungen, Irritationen, Bedrohungen oder Angriffe aufgetreten sind. Wir stellen diese Anomalien fest, und je nach weiteren Erforderlichkeiten bzw. je nach festgestelltem Inhalt hört unsere Arbeit irgendwann auf. Dann geht es z. B. an eine Behörde, bei der sich irgendein Sachverhalt bemerkbar gemacht hat. Wir werden die ersten Analysen durchführen, das N-CERT und dann auch die entsprechenden, zuständigen Sicherheitsdomänen der Behörden bzw. der Ressorts informieren, um dort weitere Analysen durchführen und Maßnahmen ergreifen zu können.

Abg. **Sebastian Lechner** (CDU): Sie machen also, wenn ich das richtig verstehe, die technische Erstanalyse, vor allen Dingen die automatisierte Analyse, und wenn es dort Hinweise gibt, gehen

die Daten zur weiteren Analyse zum N-CERT oder zu einer Behörde?

Axel Beims: Wir werden weitestgehend analysieren. Wo genau die Grenze zu ziehen ist, wird am Ende auch vom Einzelfall abhängen. Aber die Erstanalyse machen wir, und ich verstehe es momentan nicht so, dass wir händische Inhaltsanalysen durchführen sollen.

Abg. **Sebastian Lechner** (CDU): Das heißt, es gibt eine geteilte Analyse?

Axel Beims: Möglicherweise.

Kommunale Datenverarbeitung Oldenburg (KDO) – IT für Kommunen

Schriftliche Stellungnahme: Vorlage 10

***Anwesend**:*

*- **Dr. Rolf Beyer** (Verbandsgeschäftsführer)*

Dr. Rolf Beyer: Als kommunaler Zweckverband sind wir sehr kommunal verortet. Insofern wird es Sie nicht wundern, dass ich mich den Ausführungen der kommunalen Spitzenverbände anschließe. Ich möchte aber auch noch ein paar zusätzliche Kommentierungen vortragen, die aus unserer Betroffenheit herrühren.

Wir sind einerseits indirekt betroffen, weil wir das, was das OZG und jetzt auch dieses Gesetz vorschreiben, von den Kommunen in der Umsetzung beauftragt bekommen. Wir machen das für viele Kommunen in Niedersachsen, zum Teil auch kooperativ mit anderen Datenzentralen. Wir betreiben aber auch ein Rechenzentrum und kommunale Netzwerke, sodass wir vom IT-Sicherheits-Teil des Gesetzentwurfs auch direkt betroffen sind.

Zum ersten Teil, dem E-Government-Teil des Gesetzentwurfs: Es ist höchste Zeit und insofern ausdrücklich zu begrüßen, dass ein Rechtsrahmen geschaffen wird. Denn viele Kommunen begeben sich nicht nur gezwungenermaßen auf den Weg ins E-Government, sondern sie wollen das auch und benötigen dafür einen entsprechenden Rechtsrahmen.

§ 4 - Elektronischer Zugang zur Verwaltung

Die elektronischen Zugänge zur Verwaltung werden üblicherweise über Nutzerkonten angelegt. So ist es auch im Gesetzentwurf vorgesehen. Bundesweit spricht man im Allgemeinen von Servicekonten für Bürger und Unternehmen. Sie wollen aber gleichzeitig einen weiteren Zugang über eine De-Mail-Adresse schaffen. Das halten wir schlichtweg für überflüssig - erstens, weil die Zugangseröffnung schon in § 4 Abs. 1 gegeben ist, und zweitens, weil das zu einer Unsicherheit führen könnte und insbesondere der Zielführung, die Nutzerkonten flächendeckend zu nutzen und in die Prozesse einzubinden, nicht zuträglich erscheint.

Ich würde darauf verzichten, an dieser Stelle ein konkretes Produkt vorzuschreiben, auch im Sinne der Technikneutralität. Ich schließe mich da im Übrigen den Ausführungen des Vertreters des BSI an: Je technikneutraler ein Gesetz gehalten ist, desto sinnvoller und langfristiger kann es wirken. Unsere Branche ist sehr stark von Technikveränderungen geprägt, und Sie müssten sehr schnell und häufig Novellen erlassen, um mit dieser Geschwindigkeit mitzuhalten.

§ 7 - Nachweise

Ich komme zu unserem Hauptpunkt: Wir begrüßen sehr, dass elektronische Nachweise direkt von einer Behörde zur anderen geschickt werden können, wenn der Betroffene damit einverstanden ist. Dieses Einverständnis muss natürlich protokolliert und registriert werden. Dazu sind die Nutzerkonten ideal geeignet. In einer früheren Version des Gesetzentwurfs war das schon einmal konkreter geregelt. Ich denke, es sollte an dieser Stelle vielleicht auch klargestellt werden, dass dafür das Nutzerkonto ideal genutzt werden kann und sollte.

Ich würde sogar noch einen Schritt weiter gehen wollen: Man sollte an dieser Stelle eine generelle Experimentierklausel einfügen. Denn durch die Elektronifizierung vieler Prozesse ergeben sich ganz neue Möglichkeiten. Diese werden durch die derzeit geltenden Fachgesetze allerdings häufig eingeschränkt, was im Zweifel zulasten der Kreativität geht und Effizienzsteigerungen - sowohl für Bürger als auch für die Verwaltung - im Wege steht. Das Problem ist nicht die technologische Umsetzung, sondern häufig ist einfach der rechtliche Rahmen nicht gegeben. Insofern wäre eine Experimentierklausel, wie sie auch in den E-Government-Gesetzen anderer Bundesländer vorgesehen ist, durchaus hilfreich.

Begründung - Gesamtauflistung der erforderlichen Haushaltsmittel

Auch mir ist aufgefallen, dass laut Gesetzentwurf bei den Kommunen keine Kosten entstehen sollen. In der Begründung wird auch darauf hingewiesen, dass der Basisdienst für die Assistenzsysteme kostenlos zur Verfügung gestellt werde.

Der Aussage, dass den Kommunen keine Kosten entstehen, würde ich allerdings strikt widersprechen wollen. Die Kosten werden immens sein. Die Informationen aus den Online-Formularen bzw. aus den Assistenzsystemen kommen in der Verwaltung üblicherweise bei den diversen Fachverfahren an und müssen dorthin elektronisch überführt werden. Eine durchschnittliche Kommune hat auf ihren Rechnern zwischen 50 und - bei Kreisverwaltungen - bis zu 250 elektronische Fachverfahren am Laufen. Wenn die Daten automatisiert übertragen werden sollen - alles andere macht keinen Sinn -, muss das entsprechend angepasst werden. Insofern kommen auf jede Kommune Anpassungskosten zu. Diese werden mindestens in gleicher Größenordnung entstehen, wie für die Landesbehörden veranschlagt. Das werden natürlich auch wir als Datenverarbeiter zu spüren bekommen. Sie müssen auch sehen, dass es eine Vielzahl von Fachanwendungen für ein und dieselbe kommunale Aufgabe gibt. Der Aufwand ist also enorm, und Sie bekommen nicht beides - d. h. die Umsetzung und die Standardisierung - gleichzeitig in der vorgegebenen Frist hin.

Sonst - das will ich ausdrücklich sagen - ist der Gesetzentwurf sinnvoll und zielführend, weil das OZG damit konsequent umgesetzt wird. Ob die Zeitskala realistisch ist, wird sich zeigen. Das kann man schwer vorhersagen.

§ 24 - Sicherheitskonzept

Ich habe bereits gesagt, dass ich Technikneutralität sehr wichtig finde. In früheren Entwürfen war viel mehr Technikorientierung enthalten. Ich finde gut, dass dies weniger geworden ist. Es kann meines Erachtens aber gern noch weniger werden. Sonst läuft man, wie gesagt, in die Situation, dass das Gesetz gegenüber dem, was tatsächlich stattfindet, veraltet ist.

In § 24 wird von den Behörden ein Sicherheitskonzept gefordert, um von den Ermächtigungen der §§ 19 bis 22 Gebrauch machen zu können. „Sicherheitskonzept“ ist ein sehr weicher Begriff. Wir haben das bei der Umsetzung des Waffengesetzes erlebt. Da wurden auch Sicherheitskonzepte verlangt. Schlussendlich ist das ein formaler Akt. Ein Sicherheitskonzept kann zwei Seiten lang sein - Hauptsache, die Unterschrift ist drunter, um es salopp zu formulieren -, oder es kann mehrere Hundert Seiten lang sein, wie es in unserem Haus der Fall ist. Im Übrigen ist so ein Sicherheitskonzept quasi am Tag der Verabschiedung veraltet, weil sich die Technologie ständig ändert.

Ich plädiere grundsätzlich dafür, Informationssicherheitsmanagementsysteme einzuführen, weil diese sich auf die Prozesse in einer Behörde beziehen. In Konzepten für die IT-Sicherheit lässt sich das schlecht darlegen. Diese Managementsysteme müssen funktionieren, und sie sind auch zertifizierbar und auditierbar. Wir selbst sind ISO 27001-zertifiziert, d. h. der TÜV kommt jedes Jahr und überprüft unser Haus. Damit ist sichergestellt, dass wir bestimmte Grundprinzipien einhalten, und ich denke, das sollte eine Voraussetzung sein, wenn man Maßnahmen, wie sie im Gesetzentwurf genannt sind, ausführt. Meine Empfehlung wäre also, statt eines Sicherheitskonzeptes eine Zertifizierung einzuführen.

Abg. **Sebastian Lechner** (CDU): Laufen in Ihrem Betrieb IDS und ähnliche Dinge?

Dr. Rolf Beyer: Ja, solche Systeme laufen bei uns. IDS sind im Aufbau. Sie sind sehr aufwendig und teuer. Unsere kommunalen Auftraggeber beauftragen uns üblicherweise nicht damit, aber sie erwarten, dass wir das tun, und insofern müssen wir das auch leisten können. In einem so großen Rechenzentrum, wie wir es betreiben, werden natürlich alle Sicherheitstechnologien eingesetzt, wenn auch vielleicht nicht immer in vollster Ausbaustufe. Wir betreiben z. B. auch ein Security Information and Event Management (SIEM), d. h. ein System, um technische Daten zu analysieren und um Hinweise zu bekommen, dass wir angegriffen werden.

CIPHRON GmbH

Schriftliche Stellungnahme: Vorlage 11

***Anwesend**:*

- ***Sebastian Horzela** (Geschäftsführer)*
- ***Frithjof Schulze***

Sebastian Horzela: Wir sind ein Dienstleister im Bereich Offensive Cyber Security. Sie haben bisher sehr viel über die Verteidigerseite gehört. Wir vertreten eher die Angreiferseite, d. h wir sind diejenigen, die Systeme hacken, die diese ganzen Sachen, die in den Medien als Cyberwaffen bezeichnet werden - wir nennen sie lieber Exploits -, entwickeln und die daran sehen, welche Sicherheitsmaßnahmen funktionieren und welche nicht.

Im Allgemeinen möchte ich mich Herrn Ritter vom BSI anschließen. Er hat sehr viele Dinge genannt, die wir auch adressieren würden. Auf diese Punkte werde ich jetzt nicht mehr im Einzelnen eingehen.

Ich möchte vielmehr über den Bereich Security Incident Management sprechen - darunter fallen die IDS - und im Anschluss noch zwei Themen ansprechen, die bisher ein bisschen untergegangen sind, nämlich das Schwachstellenmanagement und die Verschlüsselung. Diese drei Paradigmen sind aus Angreiferperspektive wesentlich daran beteiligt, Security Incidents zu verhindern. Das sind Technologien, die am Markt sind und die funktionieren.

Zum Thema Security Incident Management: Das ist ein Verfahren, das wirklich gut funktioniert. Das Detektieren von Sicherheitslücken und der Umgang mit Vorfällen führen in der Organisation unglaublich schnell dazu, dass man Sicherheitslücken identifizieren und Angriffe erkennen kann. Zunächst einmal muss man natürlich mitbekommen, dass ein Incident stattfindet. Dafür brauchen wir diese IDS. In der Vorfallsbearbeitung müssen wir dann so viele Protokolldaten haben wie irgend möglich. Jedes Bit, das Sie erheben bzw. protokollieren können, hilft Ihnen im Falle eines Falles dabei, den Vorfall zu analysieren und zu verstehen, was passiert ist. Wenn ein Angreifer bei Ihnen im Netz ist, nimmt er sich erst einmal ein System vor, und dann bewegt er sich lateral durch die ganze Organisation, im Zweifelsfall durch mehrere Organisationen. Deshalb brauchen Sie so viele Logs wie möglich über einen möglichst langen Zeitraum. Ich würde sagen, dass Sie in den hier angedachten sieben Tagen nicht die Menge an Ressourcen zusammenbekommen werden, um einen ernsthaften Incident zu analysieren.

Was ebenfalls unglaublich wichtig ist, ist das Thema Zusammenarbeit. Organisationen gleicher Art werden häufig gleichzeitig angegriffen, und sie müssen in der Lage sein, im Falle eines Security Incidents zusammenzuarbeiten. Man übt diese Security Incidents regelmäßig in Notfallübungen, und man macht das Ganze klassischerweise auch über Organisationsstrukturen hinweg. Ein Angreifer sucht sich nämlich immer genau diese Verantwortungsübergänge, d. h. eine Stelle, an der die technische Verantwortung nicht ganz klar ist. Dort hat er nämlich mehr Zeit, er kann sich länger festsetzen, und bis das Ganze geklärt ist, ist er über alle Berge.

Das Nächste ist der Austausch von Informationen: Wenn Sie einen Security-Vorfall hatten, teilen Sie die Ergebnisse! Teilen Sie die Ergebnisse in der Community, teilen Sie das Ganze mit anderen Ländern, teilen Sie das Ganze mit dem BSI, tauschen Sie die Informationen aus! Das ist eine der wesentlichen Sachen, die im Bereich Security Incident Management wirklich gut funktionieren: Erkenntnisse haben und Erkenntnisse teilen, sodass andere diese sogenannten Indicators of Compromise - also die Verdachtsmomente, dass man gehackt wurde - auf sich selbst anwenden und sehen können, ob etwas passiert ist.

Sehr gut funktioniert auch das Schwachstellen- oder Sicherheitslückenmanagement. Wir haben heutzutage relativ gute Systeme, um bekannte Sicherheitslücken automatisiert messbar bzw. erkennbar zu machen. Wenn Sie jetzt eine Zentralstelle für Informationssicherheit einrichten wollen, wäre es eine gute Chance, dieser Zentralstelle das Mandat zu geben, jeden Partizipant im Landesnetz auf diese bekannten Sicherheitslücken zu prüfen. Denn ein Angreifer hat Zeit. Er sucht nach einer geeigneten Sicherheitslücke oder einem ahnungslosen Anwender, der seine Angriffe ausführt. Wenn er dann erst mal im Netz ist und auf die nächste Sicherheitslücke wartet, erkennt ihn kein Intrusion Detection System der Welt, solange er sich nicht rührt.

Es gibt ja ein gewisses Zeitfenster im sogenannten Patch Management. Richtig gut ist man, wenn man eine Sicherheitslücke noch am selben Tag schließt. So, wie ich es bisher mitbekommen habe, klopft man sich in der öffentlichen Verwaltung

schon auf die Schulter, wenn man das in 7 bis 30 Tagen schafft. Das ist ein bisschen lange. Ein Angreifer hat dann die Möglichkeit, das nächste System zu übernehmen und kann sich so peu à peu durch die ganze Organisation arbeiten.

Bekannte Sicherheitslücken können Sie messen und auswerten. Das sollte in meinen Augen durch eine neutrale Stelle erfolgen, die sagt: Halt, stopp! Da gibt es Schwachstellen, die müssen behoben werden, sonst kapseln wir dich vom Landesnetz ab; denn das ist eine Bedrohung für den Rest der Akteure. - Das ist bei der Zentralstelle inhaltlich ein bisschen angerissen, aber es fehlt die Ausgestaltung des Mandats. Ich würde empfehlen: Versuchen Sie, das mitaufzunehmen.

Eine dritte Sache, die mir am Herzen liegt, ist das Thema Man-in-the-Middle-Angriffe. Sie wollen im Prinzip das HTTPS-Protokoll öffnen, also knacken und analysieren. Das kann man machen, um Sicherheitslücken oder Angriffe zu finden. Es handelt sich dabei allerdings um ein zweischneidiges Schwert. Das HTTPS-Protokoll funktioniert sehr gut, d. h. es handelt sich um eine sehr gute Schutzmaßnahme. Wenn Sie diesen Schutz zurücknehmen wollen, um darin Angriffe festzustellen, müssen Sie zwangsläufig technologisch eine Umgebung schaffen, in der Sie diese Vertrauensstrukturen zerstören. Sie würden also eine Zertifizierungsautorität einrichten, und die ist per se für alle Nutzer, die über diese Geräte eine Internetverbindung aufbauen, 100 % vertrauenswürdig. Als Angreifer würde ich sofort versuchen, irgendwie an dieses Stammzertifikat, an diese Root-CA heranzukommen, und ich hätte damit die Möglichkeit, mich überall in der Landesumgebung als absolut vertrauenswürdig zu bezeugen. - Das heißt: Wenn Sie das machen wollen, sollten Sie wirklich sehr genau wissen, was Sie tun.

Abg. **Sebastian Lechner** (CDU): Wir haben von Herrn Ritter und Herrn Beyer geschildert bekommen, dass IDS sehr teuer und aufwendig zu pflegen sind. Können Sie sagen, wie da heute der Industriestandard ist und ob es wirklich wahrscheinlich ist, dass man diese Systeme an vielen Einzelstandorten einrichtet, oder ob es nicht eher zentrale Dienstleister geben sollte?

Sebastian Horzela: Die IDS-Analyse sollte möglichst zentral erfolgen. Das Erheben der Daten kann man dezentral machen, wenn man die Ergebnisse dann irgendwo zusammenführt.

Abg. **Sebastian Lechner** (CDU): Vorhin wurde angemerkt, dass man, wenn man IT-Sicherheit komplett organisieren will, im Grunde genommen auch Logdaten von lokal installierter Anwendersoftware auswerten muss. Würde ein solches Logdaten-Management die Messung bei den jeweiligen Teilnehmern auf Sicherheitslücken ersetzen, oder ist das eine Ergänzung? Das heißt, muss ich das Mandat auch dann erweitern, wenn ich an jeder Anwendung Logdaten erhebe, oder ist das dann überflüssig?

Sebastian Horzela: Es gibt sozusagen mehrere Sicherheitsebenen. Sie reden im Moment über „infrastrukturelle Sicherheit“. Dabei handelt es sich um einen relativ einfachen Teil im Bereich der Cyber-Sicherheit. Darüber steht der ganze Themenkomplex Anwendungssicherheit oder Application Security. Application Security ist um Längen schwieriger umzusetzen, weil jede Anwendung einzeln dasteht. Es gibt dort keine Standards. Wenn Sie es richtig machen wollen, binden Sie alle Anwendungsdaten in solche Strukturen ein, und zwar sowohl die Authentifikationsdaten als auch die Fehlerdaten.

Zum Thema Dezentralität beim Sicherheitslückenmanagement: Es handelt sich um relativ große Datenmengen, und es ist schwierig, das Ganze auszuwerten bzw. zu implementieren. Deswegen sind eigentlich alle größeren Organisationen inzwischen dazu übergegangen, die Informationen dezentral einzusammeln, die Analyse aber stets zentral vorzunehmen, weil es dort Spezialisten gibt, die die Sicherheitsvorfälle erkennen können. Ein normaler Administrator in einer Kommune wird im Zweifelsfall die Angriffsmuster gar nicht erkennen.

Das heißt: Ja, Anwendungsdaten gehören dort mithinein. Idealerweise sollten zunächst aber erst einmal die Infrastrukturdaten mit aufgenommen werden.

Abg. **Sebastian Lechner** (CDU): Die Messsysteme, d. h. dass ich jeden Teilnehmer auf Sicherheitslücken überprüfe, brauche ich also trotz Anwendungsprotokollierung?

Sebastian Horzela: Ja, natürlich. Sie brauchen beides.

*

Nachdem sich keine weiteren Wortmeldungen ergeben hatten und die Anhörung abgeschlossen war, kam der **Ausschuss** auf die Frage des Abg.

Sebastian Lechner (CDU) zurück, wer genau mit „die das Landesdatennetz betreibende Behörde“ gemeint sei, die in § 27 NDIG-E genannt wird.

MR **Dr. Zimmer** (MI) erläuterte, IT.N sei Bestandteil der unmittelbaren Landesverwaltung. Er sei als Landesbetrieb organisiert, und er sei nach dem Verständnis des MI eine Behörde der unmittelbaren Landesverwaltung. IT.N betreibe das Landesdatennetz, und nach Interpretation des MI sei im Gesetzentwurf mit „die das Landesdatennetz betreibende Behörde“ im Klartext IT.N gemeint.

Abg. **Sebastian Lechner** (CDU) wollte daraufhin wissen, in welchem Zusammenhang nach dem vorliegenden Gesetzentwurf das N-CERT zum IT.N stehe.

MR **Dr. Zimmer** (MI) antwortete, im IT.N werde ein Kompetenzteam aufgebaut, das sogenannte Security Operations Center bzw. Cyber Defense Operational Center. Die Mitarbeiterinnen und Mitarbeiter dort würden die in Rede stehenden Systeme betreiben, die maschinellen Analysen fahren und dann auf Signal aktiv werden.

Das N-CERT habe eher die Rolle eines koordinierenden CERTs. In anderen Ländern und Organisationen führten CERTs auch operative Maßnahmen durch. Das sei in Niedersachsen nicht der Fall. Das N-CERT sei ressortübergreifend aktiv, mit allen IT-betreibenden Stellen in der Landesverwaltung vernetzt, und es stehe bereits mit vielen Kommunen in Verbindung, um die Themen der Informationssicherheit in den kommunalen Bereich zu bringen.

Abg. **Sebastian Lechner** (CDU) fragte ferner, auf welche Stelle man die Befugnis zur Anordnung einer nichtautomatisierten Auswertung von Inhaltsdaten nach Meinung des MI übertragen könnte, um hier eine Zentralisierung zu erreichen.

MR **Dr. Zimmer** (MI) sagte, seitens der Landesregierung sei vorgeschlagen worden, die Anordnungsbefugnis auf die zuständigen Behördenleitungen zu übertragen, und dies sei in dem Gesetzentwurf auch so umgesetzt worden.

***

Tagesordnungspunkt 3:

Bleiberechtsregelung verbessern - echte Perspektiven für integrierte junge Menschen schaffen

Antrag der Fraktion Bündnis 90/Die Grünen - Drs. 18/1528

erste Beratung: 26. Plenarsitzung am 14.09.2018 AfluS

zuletzt beraten: 37. Sitzung am 29.11.2018

Einem Vorschlag des Abg. **Belit Onay** (GRÜNE) folgend, bat der **Ausschuss** die Kommission zu Fragen der Migration und Teilhabe gemäß § 18 b Abs. 4 Satz 4 GO LT um eine Stellungnahme.

***