Landtag
Nordrhein-Westfalen
17. Wahlperiode

Ausschussprotokoll
APr 17/1483
24.06.2021

Ausschuss für Digitalisierung und Innovation

55. Sitzung (öffentlich)

24. Juni 2021

Düsseldorf – Haus des Landtags

16:34 Uhr bis 17:47 Uhr

Vorsitz: Thorsten Schick

Protokoll: Sitzungsdokumentarischer Dienst

Verhandlungspunkt:

Antrag
der Fraktion der CDU und
der Fraktion der FDP
Drucksache 17/13081

– Anhörung von Sachverständigen *(s. Anlage)*

* * *

Kommunale IT-Sicherheit sicherstellen – Aufbau eines zentralen Kommunal-CERT

Antrag
der Fraktion der CDU und
der Fraktion der FDP
Drucksache 17/13081

– Anhörung von Sachverständigen *(s. Anlage)*

Vorsitzender Thorsten Schick: Meine sehr geehrten Damen und Herren! Ich darf Sie sehr herzlich zur 55. Sitzung des Ausschusses für Digitalisierung und Innovation begrüßen. Ich darf mich sehr herzlich beim Sitzungsdokumentarischen Dienst bedanken, der uns heute unterstützen wird, aber auch sehr herzlich bei den Sachverständigen, die uns ihre Expertise schon in schriftlicher Form haben zukommen lassen.

Der Antrag wurde uns durch das Plenum am 24. März zur Federführung zugewiesen.

Mitberatend sind der Ausschuss für Heimat, Kommunales, Bauen und Wohnen und der Innenausschuss.

Die Anhörung wird live gestreamt.

Die Tagesordnung ist Ihnen mit der Nummer E 17/1870 zugegangen.

Gibt es Ihrerseits Einwände gegen die Tagesordnung? – Das ist nicht der Fall.

Damit eröffne ich die Anhörung zum Antrag der Fraktion der CDU und der Fraktion der FDP und erteile als Erstem für die antragstellende Fraktion der CDU Herrn Dr. Untrieser das Wort.

Dr. Christian Untrieser (CDU): Herr Vorsitzender! Meine sehr verehrten Herren Sachverständige, herzlichen Dank, dass Sie uns heute mit Ihrem Sachverstand zur Verfügung stehen, ebenso herzlichen Dank für Ihre schriftlichen Stellungnahmen.

Meine erste Frage richtet sich an die kommunalen Spitzenverbände. Sie schreiben:

> Die Schaffung von kontinuierlichen Formaten zum Erfahrungsaustausch, zur IT-Sicherheitsberatung und -schulung sehen wir als weitere Elemente zur Stärkung der kommunalen IT-Sicherheit.

Wer soll diese Schulungen anbieten? Ist das die Bundesebene? Sind das Externe? Zwischen wem genau soll der Erfahrungsaustausch stattfinden, und wie sollen sich die Kommunen daran beteiligen?

Meine zweite Frage richtet sich an Herrn Atug. Sie schreiben:

> Insgesamt zeigt sich, dass viele einzelne Kommunalverwaltungen nicht in der Lage sein werden, das nötige Fachpersonal zu finden oder einzustellen. Daher sollten die Kommunalverwaltungen lieber ein Pooling betreiben, um die Kosten aufzuteilen und dem Mangel entgegenzuwirken.

Können Sie bitte beschreiben, wie dieses Pooling aussehen kann und wie es dann den Bedarf aller Kommunen decken könnte? – Herzlichen Dank.

Rainer Matheisen (FDP): Herr Vorsitzender! Liebe Kolleginnen und Kollegen! Liebe Sachverständige, herzlichen Dank für Ihre Stellungnahmen und dafür, dass Sie sich heute die Zeit nehmen, um unsere Fragen zu beantworten.

Herr Professor Engel, in Ihrer Stellungnahme beschreiben Sie die heterogene Struktur der kommunalen IT-Landschaft. Teilen Sie die Auffassung, dass mehr und verbesserte interkommunale Zusammenarbeit geeignet ist, auch die kommunale IT-Sicherheit zu verbessern?

Herr Atug, sollten alle Kommunen verpflichtet werden, sich an einem Kommunal-CERT zu beteiligen? – Herzlichen Dank.

Christina Kampmann (SPD): Unsere erste Frage richtet sich an Herrn Ahajliu. Sie haben sich in Ihrer Stellungnahme dazu geäußert, wie hoch Sie den Finanzierungsbedarf des Landes für das CERT einschätzen. Sie haben sich auch zu den weiteren Maßnahmen geäußert, die es für eine umfassende IT-Sicherheit im kommunalen Bereich bedürfte. Welche Maßnahmen sehen Sie als notwendig an?

Herr Untrieser hat es schon ein wenig angesprochen. Der Faktor „Mensch“ wird bei diesem Thema oft als die größte Schwachstelle angesehen. Sie haben sich für Weiterbildung ausgesprochen. Was könnte man darüber hinaus noch tun, um das Personal in diesem Bereich zu sensibilisieren?

Herr Professor Engel, wie bewerten Sie im Moment die Lage zum Thema „IT-Sicherheit der Kommunen“ insgesamt? Das ist ein Thema, mit dem wir uns hier im Ausschuss noch nicht so häufig beschäftigt haben, das aber im Rahmen der Umsetzung des OZG immer mehr an Bedeutung gewinnt. – Vielen Dank.

Sven Werner Tritschler (AfD): Herr Vorsitzender! Meine Damen und Herren! Vielen Dank auch von unserer Seite für die Stellungnahmen.

Unsere ersten Fragen richten sich an Herrn Rehfeld und Herrn Professor Engel. Im März dieses Jahres kam es zu einem größeren IT-Sicherheitsvorfall. Es gab Sicherheitslücken bei Microsoft Exchange Servern, die deutlich weiter verbreitet sind als Citrix-Netzwerkkomponenten. Welche Erfahrungen haben Sie damit bei kommunalen Verwaltungen gemacht?

Zweitens. Inwieweit spielen denn nach Ihrer Erfahrung unterschiedliche Ausstattungen, also sowohl in personeller als auch in finanzieller bzw. materieller Sicht, eine Rolle bei den Kommunen?

Die dritte Frage richtet sich an die Vertreter der kommunalen Spitzenverbände und an Herrn Rehfeld. 2017, als der Artikel 91c Grundgesetz in einer Anhörung im Bundestag vorlag, gab es eine Reihe von Sachverständigen, die sich für mehr Harmonisierung ausgesprochen haben, unter anderem Herr Professor Siegel von der FU Berlin. Wie

bewerten Sie das? Wo hören die Vorteile einer kommunalen Selbstorganisation in Fragen der IT auf, und wo fangen die Nachteile an? – Vielen Dank

Matthi Bolte-Richter (GRÜNE): Herr Vorsitzender! Meine Damen und Herren! Auch seitens der Grünenfraktion ganz herzlichen Dank für Ihre Stellungnahmen.

Ich habe zunächst eine Frage an die kommunalen Spitzenverbände. In Ihrer Stellungnahme heißt es, dass bestehende Strukturen gestärkt und bestehendes Wissen und Erfahrungen für den Betrieb eines Kommunal-CERT genutzt werden sollten. Welche Strukturen sehen Sie, die in diesem geplanten Kommunal-CERT aufgehen sollen? Oder sollte es zu einem zentralen Kommunal-CERT ausgebaut werden?

Herr Fischer, Sie schreiben, dass das CERT NRW gewisse Leistungen für die Kommunen durchführen könne, was deren Planungen und Dienste ersetzen könne. Der Ausschuss ist auch schon darüber unterrichtet worden, dass Sie auch für die Kommunen bestimmte Leistungen anbieten. Vor dem Hintergrund der aktuellen Planungen möchte ich wissen, ob es bei Ihnen nur um weitere Leistungen geht, oder was bräuchte es, damit diese Leistungen Kommunen auch angeboten werden könnten?

Herr Atug, an welchen Stellen muss das Land neue rechtliche Regelungen treffen, damit ein Kommunal-CERT nicht nur etabliert, sondern auch erfolgreich arbeiten kann?

Was muss das Land konkret tun, damit in Zukunft – das war auch Thema in Ihrer Stellungnahme – ausreichend IT-Fachkräfte vorhanden sind? Brauchen wir nur mehr Informatikunterricht und mehr Studienplätze, oder welche Handlungsoptionen gibt es darüber hinaus?

Sie haben in Ihrer Stellungnahme die Situation der kommunalen IT-Sicherheit als kritisch bezeichnet. Wo sehen Sie die größten Schwachstellen, den größten Handlungsbedarf, und wo passiert Ihrer Meinung nach zu wenig? Was sollten wir aus Ihrer Sicht konkret tun?

Vorsitzender Thorsten Schick: Vielen Dank. – Damit kommen wir zur ersten Antwortrunde, und Herr Karim Ahajliu von den kommunalen Spitzenverbänden beginnt. Bitte schön.

Karim Ahajliu (Arbeitsgemeinschaft der kommunalen Spitzenverbände Nordrhein-Westfalen *[per Video zugeschaltet]***):** Sehr geehrter Herr Vorsitzender! Liebe Kolleginnen und Kollegen! Vielen Dank für die Einladung und dafür, dass wir heute zu diesem wichtigen Thema Stellung nehmen dürfen.

Herr Dr. Untrieser, Sie haben gefragt, wie ein Austausch erfolgen kann und wer sich daran beteiligen darf. Der Austausch ist ein wichtiger Punkt in der IT-Sicherheitsszene; denn viele Fälle und Problemstellungen sind in der aktuellen Literatur nicht zu finden. Es gibt Handbücher usw., aber letztendlich ist der wichtigste Punkt in Sachen IT-Sicherheit und CERT-Betrieb und CERT-Nutzung der Austausch diesbezüglich.

Wer sollte sich daran beteiligen? Natürlich denken wir an das CERT NRW, zu dem mittlerweile gute Kontakte bestehen und mit dessen Vertretern wir uns kontinuierlich treffen. Das ist der Startpunkt, um diesen Austausch entsprechend auszubauen. Es gibt noch weitere Institutionen, beispielsweise das BSI und verschiedene Cybersicherheitsgremien, die man mit einbeziehen könnte. So könnte man einen Kreis bilden, und in diesem Kreis könnte ein vertrauensvoller Erfahrungsaustausch stattfinden. Das wäre für alle Seiten eine hilfreiche Möglichkeit, um ihre Erfahrungen auszutauschen und von den Erfahrungen der anderen zu profitieren. Denn nur so können wir Vertrauen schaffen und uns über Maßnahmen und Möglichkeiten austauschen, mit welcher Aufgabenstellung zu reagieren ist. Das gehört zur präventiven und reaktiven Möglichkeit, um IT-Sicherheitsvorfälle zu bearbeiten.

Frau Kampmann, Sie fragten, welche Maßnahmen man ergreifen sollte. Wichtig ist, dass wir, was die flächendeckende Abdeckung eines Kommunal-CERTs angeht, noch ganz am Anfang stehen. Der Aufbau eines solchen CERTs benötigt viel Fachwissen, viel Erfahrungsaustausch, und hierbei werden auch Institutionen wie das Landes-CERT gefordert sein, um diesen Austausch sicherstellen zu können, von den positiven Erfahrungen zu lernen und beim Aufbau erfolgreich zu sein.

Dazu gehören – das ist ein Knackpunkt – einerseits die finanzielle Ausstattung, andererseits – denn Geld alleine macht nicht glücklich – Fachkräfte. Das heißt, wir müssen Fachkräfte anwerben, die ein solches CERT mit aufbauen. Das Landes-CERT hat schon die Erfahrung machen müssen, dass es Schwierigkeiten gibt, Fachkräfte dafür zu finden. Insofern ist es wichtig, dass wir auf diesem Gebiet Unterstützung bekommen, um qualitativ hochwertiges Fachpersonal zu gewinnen. Darüber hinaus ist die zeitnahe Bereitstellung der technischen Ausrüstung von großer Bedeutung.

Das sind große Herausforderungen für kleine Kommunen, wenn sie unterwegs sind. Wenn wir allerdings gemeinsam in einem Kommunal-CERT mit Unterstützung des Landes und in Zusammenarbeit mit anderen Institutionen unterwegs sind, haben wir gute Möglichkeiten, den Aufbau mittelfristig hinzubekommen.

Herr Tritschler, Sie sprachen die Harmonisierung der IT-Landschaft gerade im kommunalen Bereich an. Zutreffend ist, auf kommunaler Ebene findet man eine sehr heterogene IT-Landschaft vor. Das hat natürlich auch etwas mit der kommunalen Selbstverwaltung zu tun. Es gibt allerdings auch lokale Gegebenheiten, die diese Unterschiede begründen.

In diesem Prozess ist zu überlegen, wie ein Austausch mit den anderen Institutionen und eine Standardisierung eine Stärkung der IT-Sicherheit für alle mit sich bringen. Das würden wir unterstützen. Denn letztendlich ist das gemeinsame Ziel, die Systeme der Kommunen zu stärken und damit auch die Systeme der Landesbehörden und anderer angeschlossenen Behörden sicher und resilient darzustellen.

Wo die Vorteile der kommunalen Selbstverwaltung anfangen und die Nachteile beginnen, darüber könnte man jetzt lange Listen führen. Letztendlich bedarf es einer gesunden Abwägung zwischen IT-Sicherheit, Kosten und lokalen Gegebenheiten. Grundsätzlich ist es in der IT-Sicherheit allerdings von Vorteil, dass man standardisierte Prozesse oder standardisierte Systeme einsetzt.

Herr Bolte-Richter, was es bedeutet, die bestehenden Strukturen zu stärken, ist gemünzt auf das CERT NRW. Da gibt es schon Strukturen, die gestärkt werden können, indem die kommunale Ebene auch abgedeckt wird. Denn ein IT-Sicherheitslagebild oder IT-Cybersicherheitslagebild kann nur mit den Kommunen entstehen. Ansonsten wäre ein Großteil der Bevölkerung, ein Großteil der Systeme der Verwaltung nicht wirklich abgedeckt. Deswegen ist das größtenteils auf das Landes-CERT bezogen. – Vielen Dank.

Vorsitzender Thorsten Schick: Vielen Dank für Ihre Ausführungen. Wir konnten bei der Gelegenheit auch feststellen, dass der Landkreistag Nordrhein-Westfalen nicht in ländlicher Idylle, sondern an einer stark befahrenen Straße beheimatet ist. Auch diesen Einblick mit all den Störgeräuschen kann man in Videokonferenzen gewinnen. – Jetzt spricht Herr Professor Engel.

Prof. Dr. Andreas Engel (KDN Dachverband kommunaler IT-Dienstleister *[per Video zugeschaltet]***):** Herr Vorsitzender! Meine sehr verehrten Damen und Herren! Vielen Dank für die Gelegenheit und die Fragen, die Sie an mich gerichtet haben.

Herr Matheisen, Sie haben gefragt, wie ich die Ausgangslage einschätze und ob man durch mehr und verbesserte interkommunale Zusammenarbeit auch die Sicherheitslage verbessern kann. Ja, das meine ich. Die Ausgangslage habe ich in meiner Stellungnahme beschrieben, wobei diese Anhörung für mich auch Anlass war, einmal genauer hinzuschauen. Ich habe drei Kategorien von Kommunen unterschieden, und die Spannbreite ist sehr groß. Auf der einen Seite sind es 58 kreisangehörige Städte und Gemeinden, die nicht von einem professionellen, zertifizierten kommunalen IT-Dienstleister betreut werden. Auf der anderen Seite gibt es die nach BSI oder ISO zertifizierten kommunalen IT-Dienstleister, die nach dem Stand der Technik die organisatorischen und auch technischen Voraussetzungen für den sicheren Betrieb von kommunalen Verwaltungssystemen erfüllen. Wir haben es also mit einer großen Bandbreite zu tun.

Der Vorschlag des KDN, des Dachverbands der kommunalen IT-Dienstleister, geht genau in die Richtung, dass die gut aufgestellten kommunalen IT-Dienstleister eine CERT-Funktion in der Region für Kommunen übernehmen, so wie es das KomCERT der regio iT für 40 Kommunen in ihrem Einzugsbereich auch macht. Denn die Sicherheitslage in den Kommunen kann zum einen dadurch verbessert werden, dass man vor Ort in den Kommunen organisatorische Strukturen schafft, also ein Informationssicherheitsmanagementsystem mit der Etablierung von Prozessen bei der Inbetriebnahme von Software und dergleichen, die Sicherheitsstandards erfüllen. Zum anderen kann man sie durch den sicheren Betrieb der IT-Systeme erreichen.

Eine CERT-Funktion kann nur von einem entsprechend professionell aufgestellten IT-Dienstleister wahrgenommen werden. CERT-Funktion bedeutet ja beispielsweise, dass pro Tag 20, 40, 60 Warnhinweise oder Meldungen zu Sicherheitslücken ankommen, die bewertet werden müssen und auf die man mit entsprechenden Maßnahmen reagieren muss. Das können die so zertifizierten und aufgestellten IT-Dienstleister auch für angeschlossene Kommunen machen. Wenn dann die regionalen CERTs zu

einem landesweiten CERT zusammengefasst werden, ist das eine weitere Verbesserung, weil dann die Koordination untereinander und die Orientierung an gleichen Sicherheitsstrategien und Leitlinien verbessert werden können.

Frau Kampmann, Sie haben gefragt, wie man die Sicherheitslage mit Blick auf die Umsetzung des Onlinezugangsgesetzes im Land bewerten muss. Da bin ich optimistischer. Denn die Umsetzung des Onlinezugangsgesetzes im Land wird getragen von den IT-Dienstleistern, die auch sicherheitsmäßig gut aufgestellt sind. An dieser Anhörung nimmt auch der Kollege Rehfeld teil, der mit der regio iT das Kommunalportal betreibt. Hier haben wir die Sicherheitsanforderungen erfüllt. Hier haben wir schon eine Situation, in der wir durch die Zentralisierung von Diensteangeboten in einem professionellen Betrieb die Sicherheitslage verbessern. Das ist eine Entwicklung, die in dem Sinne positiv ist.

Sie, Herr Tritschler, haben das Problem mit den Microsoft Exchange Servern angesprochen, das im Frühjahr bestand. Das war ein Problem, das anders geartet war als die Ransomware-Angriffe, die teilweise auch erfolgreich waren. Bei dem Problem mit den Microsoft Exchange Servern war es ja so, dass Sicherheitslücken bekannt geworden sind, und dann kam es darauf an, die Systeme möglichst schnell zu patchen, damit diese Sicherheitslücken geschlossen werden konnten. Das ist ein gutes Beispiel dafür, dass CERT-Strukturen – hier war vor allem das BSI der Treiber für die entsprechenden Warnmeldungen – erfolgreich waren. Denn im kommunalen Bereich konnten wir keine Vorfälle feststellen, die darauf beruhten, dass diese Sicherheitslücke ausgenutzt werden konnte.

Insofern stärkt mich das in meiner Forderung, dass wir ein landesweites CERT aufbauen sollten, das auch operativ durch regionale IT-Dienstleister umgesetzt wird, die die CERT-Funktion für einen größeren Kreis von Kommunen übernehmen; wir haben im Land fast 400 Kommunen. Perspektivisch kann ich mir eine Entwicklung hin zu einem professionellen CERT vorstellen, das als eigene Institution im Land aufgebaut wird. Die Zusammenarbeit mit dem Landes-CERT ist essenziell, und zwar nicht nur jetzt in der Nutzung und im Austausch über die Warnhinweise und die Sicherheitsmeldungen, sondern auch mit Blick auf den Austausch darüber, was geeignete Maßnahmen sind, um den erkannten Sicherheitslücken zu begegnen. – Vielen Dank.

Manuel Atug (AG KRITIS): Die erste Frage bezog sich darauf, wie das Personal-Pooling genau aussehen soll und wie es den Bedarf der Kommunen decken kann. Wenn jede einzelne Kommune in NRW das gesamte Know-how eigenständig und vollständig vorhalten soll, dann ist das ein Kostenfaktor, der nicht repräsentierbar ist. Darüber hinaus stellt das fehlende Fachpersonal einen großen Mangel dar. Die Kommunen stehen schließlich auch im Wettbewerb mit der Wirtschaft, und dabei ziehen sie oft den Kürzeren, bedenkt man, dass das durchschnittliche Jahresbruttogehalt bereits in 2016 bei einer leitenden IT-Position bei ca. 110.000 € lag. Außerdem reicht nicht nur ein Leiter, sondern man braucht auch noch ein paar fleißige Bienchen, die Fachexpertise haben. Diese Fachexpertise baut sich durch entsprechende Ausbildungen, durch entsprechende Schulungen auf. Die können durchaus 10.000 € in den ersten Jahren kosten und sind notwendig, um Präventions-, Incident-Response- und

Forensikkenntnisse aufzubauen. Das ist nichts, was man einfach so auf dem Markt abgreifen kann, und das kann man auch nicht bei jeder einzelnen Kommune sinnvoll skalieren. Diese Experten würden dann auch gefühlt die meiste Zeit Däumchen drehen und ein bisschen Awareness-Maßnahmen machen, aber für ihre Fachexpertise nicht abgerufen werden.

Wenn man das Ganze in einem Kommunal-CERT poolt, dann kann man gezielt versuchen, diese – keine Ahnung – 15 bis 20 Personen zu finden und zu motivieren, und diese Personen würden dann in den umliegenden Kommunen ihre Dienstleistungen erbringen, sodass sie dann auch weiterhin motiviert blieben, etwas zu tun. Viele Menschen machen diesen Job nicht nur wegen des Geldes, sondern weil sie tatsächlich helfen wollen, eine sichere Cyberwelt zu gestalten, in der sie großgeworden sind und in der sie sicher leben wollen.

Insofern hätten wir in einem Kommunal-CERT die Möglichkeit, den Kleinsten in der Kette – Bund, Länder, Kommunen – diese Hilfestellung zu geben, und sie würden wiederum dankbare Bürger als Antwort erhalten.

Dieses Pooling sähe also so aus, dass man wenige Leute für 10.000 € pro Jahr ausbilden würde, und dann müsste nicht jede Kommune dieses Investment machen. Dann hätte mein ein Dutzend Experten, die das gezielt für alle Kommunen darstellen und abbilden könnten, und dann müsste das nicht jede Kommune für sich selbst aufbauen.

Zur Frage, ob alle Kommunen verpflichtet werden sollten, sich an einem Kommunal-CERT zu beteiligen. Eine gesetzliche Vorschrift zur verpflichtenden Teilnahme sollte es aus diesem einzigen Grund geben: Wenn die Kommunen das entscheiden dürfen, werden einige sagen: Selbst die 10.000 € im Jahr habe ich nicht im Stadtsäckel übrig. Das Geld spare ich mir lieber. Ich habe sowieso kaum Know-how im Haus. – Wenn das eine kleine Kommune mit nur 22 Angestellten ist, hat sie keinen Fachexperten. Dann stellt sich die Frage, was der dann mit einem Kommunal-CERT groß abstimmen soll. Wenn eine Kommune allerdings verpflichtet wird, sich daran zu beteiligen, und auch Informationen bekommt, dann wird sie diese auch auswerten wollen. Dann wird sich die Kommune auch darum kümmern, das entsprechende Know-how aufzubauen. Daher bin ich für eine Verpflichtung; denn sonst skaliert das Ganze nicht. Zum einen verursacht jeder, der nicht mitmacht, das Risiko für einen Angriff durch Ransomware, mit dem die Kommune um Millionen erpresst werden könnte. Zum anderen würde es für die anderen Kommunen, die teilnehmen möchten, immer teurer und damit uninteressanter, daran teilzunehmen.

Dann kam eine Frage zu den Regelungen und Gefahren. Welche neuen rechtlichen Regelungen müsste es geben? Die Verpflichtung habe ich gerade dargestellt.

Darüber hinaus sollte dieses Kommunal-CERT in den Infrastrukturen eines IT-Dienstleisters aktiv werden dürfen. Das ist eine Befugnis oder Berechtigung, in fremden Systemen oder Rechenzentren Hilfestellung leisten zu dürfen, zu können und zu müssen. Denn sonst sagen die Dienstleister vielleicht: Mit denen habe ich keinen Vertrag, und daher will ich die auch nicht in mein System reinlassen. – Dann hätten wir auch nichts davon, dass die Hilfe da wäre. Dann würden wir mit den Forensikeinsatzkoffern vor der Tür scharren, aber keinen Einlass bekommen. Das passiert übrigens regelmäßig

in der Privatwirtschaft, weil viele Unternehmen Angst haben, dass ihre Fehlprozesse bekannt und sie daraufhin Regressansprüchen ausgesetzt würden. Dann kommen lieber die Anwälte und sagen: Sie dürfen hier nicht rein. Auf Basis welcher Befugnis wollen Sie denn rein? – Das hilft niemandem, aber man versucht erst mal, alles von sich zu halten. Insoweit wäre das eine wichtige Regelung, die man adressieren sollte.

Was muss Nordrhein-Westfalen konkret tun? Brauchen wir mehr Informatikunterricht, oder was fehlt, um auf mehr Know-how und mehr Fachkräfte zurückgreifen zu können? Man muss eine Ausbildung für die Massen schaffen. Die Bildungspolitik muss adressieren, dass wir den Wandel von einer Industriegesellschaft zu einer Informations- und Wissenschaftsgesellschaft schon längst vollzogen haben. Wenn ich mir die Bildungspolitik anschaue, kann ich nur sagen: In den Grundschulen gibt es keine Medienkompetenz, keine IT-Kompetenz, keine Ethik und Verantwortung. Schaue ich in die weiterführenden Schulen, sehe ich vielleicht noch eine AG Informatik, die freiwillig von einem Mathematik- oder Informatiklehrer angeboten wird. An den Universitäten gibt es Exzellenzcluster, die wenige Dutzend Menschen pro Jahr ausbilden. Aber selbst dann kann ich immer noch Software entwickeln, indem ich ein paar Frameworks zusammenklicke. Ich kann das in kritischen Infrastrukturen wie Staat und Verwaltung laufen lassen und keiner fragt, ob und wie das sicher programmiert wurde, weil es schlichtweg keine Abnahmeprozesse gibt, die man lebt. Das heißt, es wäre wesentlich, dass man in der Bildungspolitik den Schritt geht, diese Informationsgesellschaft entsprechend auszustatten, um dieses Wissen tatsächlich in der Masse zu haben. Dann wird auch die Wahrscheinlichkeit größer, dass sich Menschen für Dinge im Zusammenhang mit Cybercrime und Computer und damit für Forensik, Incident Response, Security Awareness, Penetrationstests und all diese Dienstleistungen interessieren, die ein Kommunal-CERT bereitstellen kann.

Darüber hinaus kann man Unternehmen und Privatleute dazu motivieren, Schulungen zu besuchen, genauso wie man Kommunen und die Mitarbeiter von CERTs dazu motivieren sollte, diese Schulungen zu besuchen und diese Ausbildungen wahrzunehmen. Das kann das Know-how nur fördern und damit insgesamt die Sicherheit erhöhen.

Zu den größten Schwachstellen in den Kommunen. Das ist in vielen verschiedenen Schichten zu betrachten. Der erste Punkt ist, dass man empfiehlt, so etwas wie den BSI-IT-Grundschutz zu empfehlen und umzusetzen. Ich kann aus unserer Erfahrung sagen, dass jemand, der ein Informationssicherheitsmanagementsystem mit Business Continuity Management so lebt und mit Maßnahmen versieht, wie es beispielsweise das BSI-IT-Grundschutzkonzept erklärt, eher weniger der Kandidat ist, der mit einer Ransomware beglückt und anschließend kompromittiert wird. Denn er hat laufende Prozesse und lebt kontinuierliche Sicherheit. Das heißt, eine der größten Schwachstellen in Kommunen ist, dass diese nicht ein ISMS mit BCM leben, sondern aus der Not heraus irgendwie ihre Systeme betreiben, teilweise Fachverfahren noch auf Windows-98-System laufen lassen. Dabei wurden weder diese Fachverfahren noch das System geupdatet, weil Windows 98 seit vielen Monden keine Updates mehr bekommt. Das ist fast grob fahrlässig, aber wenn man keine Ressourcen und auch kein Know-how hat, dann ergibt sich so etwas regelmäßig von selbst in den Kommunen.

Es gäbe die Möglichkeit einer Verpflichtung, so etwas wie den BSI-IT-Grundschutz umzusetzen und auch zu beaufsichtigen, ob es umgesetzt wurde. Es hilft nämlich nichts, so etwas nur zu empfehlen; dann machen es viele nicht. Und schlecht ist es auch, wenn es verpflichtend ist, aber es niemanden interessiert, ob es umgesetzt wurde. Das sollte also entsprechend nachgehalten werden.

Transparenz macht viel aus. Wenn man transparent macht, wie der Sicherheitszustand einer Kommune ist, dann fühlt sie sich auch eher dazu genötigt, mehr Sorgfaltspflicht an den Tag zu legen, weil öffentlich wird, wie der Sicherheitszustand ist. Und wenn dieser desolat ist, werden die BürgerInnen auch sagen: So geht es nicht. Ich lebe hier, und das ist ein Risiko. – Kommunen betreiben oft nicht nur sich selbst, sondern Transport und Verkehr, Wasserwerke, Energie- oder Telekommunikationsunternehmen, also Netzwerkanbindungen als Subdienstleister oder als Betreiber.

„Fehlerkultur statt Fingerpointing“ ist ein Punkt. Es ist wichtig, dass wir in einer Fehlerkultur leben, in der man offen mit den Fehlern umgeht und nach der Ursache der Auswirkungen forscht, um sie zu beheben, statt Fingerpointing zu betreiben und zu fragen: Wer hat das eigentlich entschieden? Wer ist daran eigentlich schuld? – Die Schuldfrage interessiert in der IT-Sicherheitswelt eigentlich niemanden. Interesse besteht immer nur an der Ursache. Und wie können wir die Ursache durch eine Prozessveränderung nachhaltig eliminieren? – Das würde auch viel bringen.

Letzter Punkt: fehlende Standardisierung und Open-Source-Nutzung. Man sollte deutlich mehr Standards nutzen. Dann wäre es auch einfacher, ein Upgrade oder eine Anpassung eines Fachverfahrens vorzunehmen. Das Ganze endet nicht bei „Wir haben jetzt Open Source eingesetzt“, sondern es muss auch ein angeschlossenes Open Development geben. Das heißt, es geht darum, mit der Community gemeinsam diese Standards und Software zu entwickeln, zu nutzen, sich als Kommunen vielleicht sogar zusammenzuschließen, um das zu machen, und vielleicht sogar – das wäre bahnbrechend – in Ausschreibungen reinzuschreiben, dass ein Kickback an die Community fließt. Schließlich nutzt man diese Software der Community, man nutzt das Know-how der Community. Man gibt ihr einen erzwungenen Kickback zurück. Der Betreiber, der das sozusagen für die Kommunen macht, muss dann einen Teil an die Community zurückgeben, und diese kann das nutzen, um die Software weiterzuentwickeln und sicherer zu machen, wovon dann wieder alle Kommunen profitieren. – Danke.

Hans Josef Fischer (IT.NRW): Herr Vorsitzender! Meine Damen und Herren Abgeordnete! Vielen Dank, dass Sie mich und Herrn Vieweg, den Leiter des CERT NRW bei IT.NRW, zu dieser Anhörung eingeladen haben.

Sie befassen sich heute mit einem sehr wichtigen Thema. Denn die Informationssicherheit ist die Grundlage für ein sicheres digitales Arbeiten in der öffentlichen Verwaltung in Nordrhein-Westfalen, und das gilt für die Landesverwaltung genauso wie für die kommunale Verwaltung. Bei der Informationssicherheit kann man nicht zu viel tun. Informationssicherheit ist sicherlich ein Ressourcenkiller, und das, was Herr Atug ausgeführt hat, dass es schwer ist, auf dem Arbeitsmarkt dieses Fachpersonal zu finden, führt eben dazu, dass man darüber nachdenken muss, wie man dieser wichtigen

Aufgabe bei begrenzten Finanzmitteln, aber vor allem auch bei begrenzten Fachkräfteressourcen gerecht werden kann.

Die Informationssicherheit antwortet auf diese Herausforderung mit einem Netzwerkgedanken. Es kann nicht jeder alles machen. Der deutsche CERT-Verbund ist ein bestehendes Netzwerk, und diesen Gedanken sollte man bei der Überlegung, wie die kommunale Familie in dieses Netzwerk eingebunden werden kann, zugrunde legen.

Sie, Herr Bolte-Richter, haben gefragt, was es dazu bedarf, um dieses Angebot jetzt zu machen. Wir müssen die kommunale Familie und das CERT NRW in einem Netzwerk verbinden. Die kommunale Familie besteht ja nicht nur aus dem Kollegen Rehfeld und den anderen Kollegen, die sich im KDN oder auch außerhalb des KDN als IT-Dienstleister für die Kommunen verdient machen, sondern es ist jede der 396 nordrhein-westfälischen Kommunen gefragt. Denn überall sind die Arbeitsplätze mit PCs ausgestattet, und diese PCs sind das Einfallstor in die Informationssicherheit. Deswegen müssen wir das Netzwerk nicht nur im Bereich der Dienstleister sehen, sondern auch im Bereich der Behörden, also aller 396 Kommunen und der Kreise.

Das, was wir als IT.NRW kurzfristig anbieten können – das ist in dem dafür zuständigen Gremium nach dem E-Government-Gesetz, dem IT-Kooperationsrat NRW, auch schon vorgestellt worden –, ist die Teilnahme oder die Integration der kommunalen Familie in den Warn- und Informationsdienst von Nordrhein-Westfalen, den IT.NRW für die nordrhein-westfälischen Landesbehörden bereitstellt und der eben Ausfluss dieses Netzwerkgedankens ist. Wir sammeln alle Warninformationen, Sicherheitshinweise für die Landesverwaltung, die sich aus dem CERT-NRW-Verbund ergeben, und stellen sie den nordrhein-westfälischen Behörden zur Verfügung. Es ist technisch, faktisch einfach, das natürlich auch der kommunalen Familie zur Verfügung zu stellen. Wenn Sie jetzt fragen, was es dazu bedarf: Es bedarf der Zustimmung des Finanzministers. Er muss sagen, dass es okay ist, dass NRW-Steuermittel dafür auch in den kommunalen Bereich gegeben werden. – Das ist jetzt vereinfacht gesagt. Wir erproben das bereits mit den Kommunen, und wenn das technisch gut klappt, dann können wir es kurzfristig realisieren.

Der zweite Punkt ist, sich ein umfassendes Lagebild über die Situation der Informationssicherheit in Nordrhein-Westfalen zu machen. Das kann erreicht werden, indem alle Sicherheitsvorfälle, also nicht nur in den Landesbehörden, sondern auch im kommunalen Bereich, in einer zentralen Stelle zusammenlaufen. Das kann auch eine virtuelle Zentrale sein. IT.NRW hat viele Aufgaben zu erledigen. Ich werbe jetzt also nicht Aufgaben ein, aber wir bieten an, als eine solche Stelle zu fungieren, bei der alle Sicherheitsvorfälle gemeldet werden, zusammenlaufen, damit eine Grundlage geschaffen wird, um schnell reagieren zu können.

Das dritte Angebot ist ein Angebot, das sich nicht kurzfristig realisieren lässt, nämlich das MIRT, das Mobile Incident Response Team. Das ist so etwas wie eine schnelle Eingriffstruppe. Wir bei IT.NRW können in unseren zentralen Strukturen sehr schnell helfen, aber für eine forensische Untersuchung in einer Behörde brauche ich Leute, die in die Behörde fahren. Wir unterstützen Behörden landesweit. Das ist also ein landesweiter Einsatz. Das macht man nicht so neben bei. Das muss vergütet werden. Dafür bedarf es einer entsprechenden Dienstleistungsvereinbarung mit IT.NRW, auf

deren Grundlage wir dieses MIRT aufbauen können. Das ist für die Landesverwaltung in Planung. Ich sage es mal so: Wenn wir zur Bezirksregierung Detmold fahren, könnten wir auf dem Weg auch zur Stadt Paderborn fahren, wenn die gerade ein Problem hätte. Das wäre der Ansatz, eine solche Infrastruktur, ein solches MIRT-Team entweder durch eine Ausweitung des Service bei IT.NRW auch für den kommunalen Bereich zu öffnen oder entsprechende Kapazitäten auch bei den kommunalen Dienstleistern – Stichwort: Netzwerk – aufzubauen und über einen Verbundcharakter dem Land und den Kommunen nutzbar zu machen. Da wir hier auch nicht über eine ebenenübergreifende Zusammenarbeit zwischen dem Bund und dem Land sprechen, haben wir auch kein Mischverwaltungsproblem, sondern das könnte bei einem entsprechenden politischen Willen auch so umgesetzt werden.

Für die Landesverwaltung machen wir es schon, und es ist ein Angebot, dieses, wenn es aufgebaut ist, auch für den kommunalen Bereich zur Verfügung zu stellen.

Dieter Rehfeld (regio iT *[per Video zugeschaltet]***):** Herr Vorsitzender! Meine Damen und Herren! Es ist schon viel gesagt worden, und auch wegen der schlechten Verbindung möchte ich mich kurzfassen. Lassen Sie mich auf zwei, drei wichtige Punkte aus meiner Sicht eingehen.

Erstens. Ich begrüße die Initiative des Landes in Richtung eines Kommunal-CERTs außerordentlich. Das halte ich für den richtigen Weg. Wir haben das auch schon mal im KDN – Andreas Engel hat es gesagt – diskutiert, aber bisher sind wir nicht zu durchgängigen Strukturen gekommen, die aus meiner Sicht notwendig sind. Ich möchte aufgreifen, was Andreas Engel gesagt hat. Meiner Meinung nach ist es notwendig, dass die leistungsfähigen und vielleicht größeren kommunalen IT-Dienstleister zusammenarbeiten, aber nicht nur aus guter Absicht, sondern weil man eine Organisation dafür schafft. Das ist die Erfahrung, die meine Kollegen – früher civitec, heute regio iT – machen, dass wir eine klare Organisation brauchen. Insofern würde ich es sehr begrüßen, wenn diese Organisation so gestaltet wird, dass das Land mitwirkt. Das kann in einer aktiven Unterstützung erfolgen, wie sie gerade auch von IT.NRW aufgebaut wird. Auch das finde ich außerordentlich gut. Wir haben …

(Aussetzer im Livestream)

Vorsitzender Thorsten Schick: Jetzt hängt die Leitung. Vielleicht reicht die Bandbreite, wenn Sie die Bildübertragung ausschalten.

Dieter Rehfeld (regio iT *[per Video zugeschaltet]***):** Funktioniert es wieder?

Vorsitzender Thorsten Schick: Ja.

Dieter Rehfeld (regio iT *[per Video zugeschaltet]***):** Wie gesagt, ich finde es gut, dass das Land Nordrhein-Westfalen und das …

(Aussetzer im Livestream)

Vorsitzender Thorsten Schick: Ich bekomme gerade von der Ausschussassistenz den Hinweis, dass wir Sie auch als „Telefonjoker“ dazuschalten können. Ansonsten wird es schwierig, Ihrem zerstückelten Wortbeitrag folgen zu können. Dann warten wir erst einmal ab.

Wenn ich es mir richtig notiert habe, hat es keine Fragen an Herrn Professor Schwenk gegeben. Das kann schon mal vorkommen, wenn man sehr pointiert formuliert hat. Das war zumindest mein Eindruck, als ich Ihre Stellungnahme gelesen haben. Sie haben darin sehr stark zwischen Datenschutz und Datensicherheit unterschieden. Diese Themen hängen natürlich zusammen. Können Sie vielleicht deutlich machen, warum Sie sagen, es sei so wichtig, sich beim Kommunal-CERT nur auf Datensicherheit zu fokussieren? Ich nehme mir jetzt einfach mal die Freiheit, diese Frage zu stellen, bis Herr Rehfeld wieder dabei ist.

Prof. Dr. Jörg Schwenk (Ruhr-Universität Bochum *[per Video zugeschaltet]***):** Herr Vorsitzender! Meine Damen und Herren! Ich denke, dass der Datenschutz auf allen Ebenen schon sehr gut aufgestellt ist. Ich versuche auch immer, diese Themen strikt voneinander zu trennen. Wenn ich zum Datenschutz befragt werden, sage ich immer, dass ich davon überhaupt nichts verstehe. Ich bin schließlich kein Jurist, sondern Techniker. Die Begriffe werden oft ähnlich verwandt, und natürlich ist die Datensicherheit wichtig für den Datenschutz. Aber ein CERT hat nun einmal die Aufgabe, die Datensicherheit zu gewährleisten.

Vorsitzender Thorsten Schick: Vielen Dank für diese Darstellung. – Wir fragen noch mal ins Off, ob Herr Rehfeld da ist. – Das ist nicht der Fall.

Damit steigen wir in die zweite Runde ein, und ich erteile Frau Kampmann das Wort. Bitte.

Christina Kampmann (SPD): Vielen Dank, Herr Vorsitzender. – Meine Frage an Herrn Rehfeld stelle ich erst einmal nicht; es sei denn, er taucht wieder auf.

Herr Professor Schwenk, Sie schreiben in Ihrer Stellungnahme, dass die Bedrohungslage für die Kommunen eigentlich noch unklar ist. Können Sie erläutern, was schon gesichert ist? Wer sind die Angreifer? Auf welche Daten fokussieren sich die Angreifer? Welche Erkenntnisse haben Sie darüber? Welche Erkenntnisse fehlen Ihnen?

Ich habe noch eine Frage zu den Ausführungen von Herrn Fischer. Wie schätzen Sie die Akzeptanz bei den Kommunen ein, Sicherheitsvorfälle auch tatsächlich zu melden? Mir hat das BSI einmal gesagt, dass Unternehmen solche sehr oft nicht melden, weil sie um ihre Reputation fürchten. Ich denke, kurz vor der Wahl wird der Oberbürgermeister sicherlich nicht gerne öffentlich machen, dass Daten beispielsweise aus dem Steueramt in größerem Stil abhandengekommen sind. Dazu interessiert mich Ihre Einschätzung. – Vielen Dank.

Vorsitzender Thorsten Schick: Sie können Ihre Frage an Herrn Rehfeld direkt daran anschließen. Er ist wieder zu uns gestoßen.

Christina Kampmann (SPD): Herr Rehfeld hat wieder Kontakt zu uns aufgenommen. Das ist schön. – Herr Rehfeld, Sie schreiben in Ihrer Stellungnahme auch etwas zum Thema „Akzeptanz bei den Kommunen“. Diese ist Grundlage dafür, dass so ein CERT letztendlich funktioniert. Was braucht es denn aus Ihrer Sicht, um diese Akzeptanz bei den Kommunen herzustellen, damit möglichst alle dabei sind, wenn es denn eingerichtet wird?

Florian Braun (CDU): Herr Professor Schwenk, wir haben in unserem Antrag formuliert, dass wir das Ziel verfolgen, das IT-Grundschutzkompendium des BSI als Grundlage für die Datenverarbeitung zu nutzen und digitale Infrastrukturen der Kommunalverwaltung perspektivisch auch vom IT-Sicherheitsgesetz zu erfassen. Ich möchte jetzt nicht in das Fettnäpfchen „Datenschutz und Datensicherheit“ treten. Trotzdem interessiert es mich, ob Sie auch dazu eine Einschätzung abgeben können.

Meine zweite Frage richtet sich an die kommunalen Spitzenverbänden. Mit unserem Antrag verfolgen wir das Ziel, den Kommunen einen Anschub zu geben, um ein zentrales kommunales Lagezentrum aufzubauen. Herr Fischer hat gerade beschrieben, was mit den ersten ausgewählten CERT-Leistungen seit März dieses Jahres bereits gemeinsam angestoßen worden ist. Herr Engel und Herr Atug haben in ihren Stellungnahmen beschrieben, wie sich diese Aufbauphasen aufteilen könnten. Herr Atug hat sogar Finanzierungshinweise gegeben. Vor diesem Hintergrund interessiert mich die Einschätzung der kommunalen Spitzenverbänden, was aus ihrer Sicht die nächsten sinnvollen notwendigen Schritte wären und ob sie sich auch eine Einschätzung der Finanzierungsideen von Herrn Atug zutrauen. – Vielen Dank.

Vorsitzender Thorsten Schick: Ich schaue in die Runde, ob es seitens der Abgeordneten weitere Fragen gibt. – Das ist nicht der Fall.

Dann steigen wir in die nächste Antwortrunde ein, und wir beginnen mit Herrn Rehfeld. Bitte schön.

Dieter Rehfeld (regio iT *[per Video zugeschaltet]***):** Danke schön. – Noch mal zu dem, was ich vorhin ausführte. Aus meiner Sicht ist es sinnvoll, eine gemeinsame Einrichtung zu schaffen, die in der Tat in einem Netzwerk arbeiten muss. Das heißt, dass die Kommunen Zugriff auf und Zugang zu Informationen bekommen. Mir scheint es sehr wichtig zu sein, dass es dann auch diese Beratung gibt. Denn das Verteilen von CERT-Meldungen alleine ist nicht hilfreich. Das ist jedenfalls unsere Erfahrung. Vielmehr müssen diese aufbereitet und dann gegebenenfalls, wenn es darauf ankommt, auch mit Beratung versehen werden.

Ich möchte die Frage aufgreifen, die ich gerade noch am Rande gehört habe. Da ging es um Vertrauen. Ich bin überzeugt davon, dass es eine wichtige Voraussetzung ist, dass eine Sicherheitsinfrastruktur für den kommunalen Bereich von den Kommunen und kommunalen Einrichtungen mit getragen wird und dass sie sich daran beteiligen können. Das ist eine wesentliche Voraussetzung, um Vertrauen zu haben. Denn – das hat Herr Atug vorhin auch gesagt – man hat Probleme damit, wenn externe Sicherheitsexperten in die eigene Verwaltung schauen, in den eigenen IT-Dienstleister

schauen. Das ist letztendlich eine Frage des Vertrauens. Wir brauchen eine Vertrauensstruktur zwischen den kommunalen IT-Dienstleistern, dem Land Nordrhein-Westfalen und den Kommunen, um ein realistisches Lagebild zu bekommen. Denn das Vertrauen untereinander ist aus meiner Sicht einer der wichtigen Erfolgsfaktoren für eine langfristige, gut funktionierende Sicherheitsstruktur. Deswegen plädiere ich dafür, bei der Umsetzung dieses guten Gedankens, der im Antrag von CDU und FDP beschrieben ist, sehr sorgfältig darüber nachzudenken, wie wir eine Organisationstruktur schaffen, die meiner Meinung nach mehr sein sollte als nur eine Netzwerk- oder freiwillige Zusammenarbeit von regionalen IT-Dienstleistern.

Die Fragen zu Microsoft Exchange sind schon beantwortet worden.

Die kommunale Selbstverwaltung sollte gerade dadurch realisiert und gesichert werden, dass wir solche Strukturen schaffen, in denen Kommunen, kommunale Spitzenverbände, kommunale IT-Dienstleister auch Einfluss ausüben können. – Danke schön.

Prof. Dr. Jörg Schwenk (Ruhr-Universität Bochum *[per Video zugeschaltet]***):** Zur Bedrohungslage. Ich hatte versucht, zu recherchieren, was Daten wert sind, die irgendwo gestohlen werden. Dazu gibt es leider nicht viel Literatur. Es gibt ein paar Schätzungen, was Daten wert sind, aber darunter sind wenige Daten, die von Kommunen gepflegt werden. Das ist der Teil der Bedrohungslage, der zumindest für mich unklar ist. Ich weiß nicht, was mit Daten passiert, die gestohlen werden und was diese auf dem Markt wert sind.

Sehr viel klarer ist die Lage bei Massenphänomenen wie Ransomware-Angriffen. Hier ist das Geschäftsmodell klar. Hier werden Gelder erpresst, und die Höhe der erpressten Gelder ist sehr viel geringer als der Schaden, der entstehen würde, wenn man das Lösegeld nicht zahlen würde.

Hier fehlt es also an Transparenz. Wir verstehen die Massenphänomene Ransomware-Angriffe, aber was Angreifer dazu treibt, gezielt Daten von Kommunen zu stehlen, wissen wir nicht. Ich habe im Detail auch dafür plädiert, dass man bei diesen Betrachtungen den Profit der Angreifer in den Vordergrund stellt und nicht so sehr den Schaden bei den Betroffenen. Bei Ransomware klaffen diese Summen sehr stark auseinander. Ich glaube, es ist der Profit, der diese Angriffe treibt.

Vielleicht ist das eine gute Überleitung zum IT-Sicherheitsgesetz. Eine Meldepflicht, eine Sammlung von Daten, die nicht völlig offen diskutiert werden müssen, würde sicherlich Transparenz schaffen. Man könnte sich besser vorbereiten. Man wüste besser, welche Daten stark geschützt werden müssen und welche vielleicht nicht so sehr im Visier der Angreifer sind.

Zum IT-Grundschutz. Mein Punkt war, die 810 Seiten, die der Standard mittlerweile stark ist, nicht einfach so einer Kommune vorzulegen, sondern sie durch diesen IT-Grundschutz zu leiten und Hilfestellung zu leisten, wie man dieses Handbuch umsetzen kann. Ich denke, wenn man dieses Kompendium einfach nur so sieht und vorgelegt bekommt, dann ist es ein schwer verdaubarer Brocken. Da braucht man Experten, die das kennen und Handreichungen bieten.

Hans Josef Fischer (IT.NRW): Frau Abgeordnete Kampmann, ja, wie schätze ich die Akzeptanz im kommunalen Bereich ein, Sicherheitsvorfälle tatsächlich zu melden? Das ist eine schwierige Frage. Ich denke, das hängt immer sehr von den Personen ab. Wir haben in der Diskussion heute schon einige Aspekte angesprochen, die bei der Beantwortung dieser Frage prägend oder zielführend sein dürften.

Das eine ist, ein CERT-Verbund ist ein Unterstützungs- und Hilfsnetzwerk. Wenn ich Hilfe und Unterstützung annehmen will, dann muss ich auch sagen, dass ich Hilfe und Unterstützung brauche. Es geht nicht um Schuldzuweisung. Daher brauchen wir auch so etwas wie eine Vertrauenskultur. Das ist sehr wichtig. Die Kommunen müssen sagen: Wir arbeiten zusammen, um uns gegenseitig zu unterstützen, damit wir gemeinsam Informationssicherheit managen.

In so einem Verbund muss die Erkenntnis sein, dass es kein persönliches Versagen ist, wenn es zu einem Informationssicherheitsvorfall kommt. Ich kann Ihnen als Betriebsleiter von IT.NRW nicht garantieren, dass ich morgen keinen Informationssicherheitsvorfall habe. Das Einzige, was ich tun kann, ist, dass ich mich aufstelle, um das zu verhindern. Das nennt man dann Informationssicherheitsmanagement, und wir bei IT.NRW machen das so, dass wir nicht nur ein Informationssicherheitsmanagement auf Grundlage von DIN ISO 27001 BSI-Grundschutz haben, sondern uns auch zertifizieren lassen. Das heißt, wir lassen andere gucken, ob wir das richtig machen. Die gucken gründlich, und dann sagen die uns auch: Nein, da müsst ihr besser werden, und das müsst ihr anders machen.

Das ist das, was meiner Meinung nach jeder Bürgermeister und jeder Landrat im Kopf haben müsste: Sie tragen Verantwortung für ihre Gemeinde, für ihren Landkreis, und sie müssen im Falle eines Informationssicherheitsvorfalls ihren Bürgerinnen und Bürgern Rede und Antwort stehen, wenn sie gefragt werden: Hast du wirklich alles Mögliche getan, um das zu verhindern?

Man kann es nicht zu 100 % ausschalten, aber ein gutes Informationssicherheitsmanagement hilft dabei. Das ist dieses Mindset, das unbedingt erforderlich ist, um Sicherheitsvorfälle zu melden, damit Unterstützung geleistet werden kann. Meiner Meinung nach ist es sehr wichtig, dass die Politik genau diese Botschaft aussendet.

Karim Ahajliu (Arbeitsgemeinschaft der kommunalen Spitzenverbände Nordrhein-Westfalen *[per Video zugeschaltet]***):** Herr Braun, Sie fragten nach den nächsten Schritten. Selbstverständlich ist der Kontakt zu den anderen IT-Sicherheitsinstitutionen wichtig. Wir müssen dafür die vorhandene IT-Infrastruktur auf der kommunalen Ebene inventarisieren. Wir müssen wissen, was es vor Ort gibt. Schließlich ist eine heterogene IT-Landschaft vorhanden.

Es geht darüber hinaus um die Erstellung eines Risikoprofils. Das heißt, welcher Einsatz bringt welches Risiko bzw. welchen Nutzen mit sich? Hier ist vor allem die Stärkung der … (akustisch unverständlich) interessant. Das heißt, nicht jede Kommune hat einen Informationssicherheitsbeauftragten. Gerade die kleineren Kommunen habe nicht die Ressourcen dafür. Daher ist es wichtig, bei dem Aufbau dieses Know-hows darauf zu schauen, dass in jeder Kommune oder in einem Verbund ein Informations-

sicherheitsbeauftragter vor Ort existiert. Denn nur so können auch vor Ort gewisse Risiken eingeschätzt und Maßnahmen ergriffen werden.

Auch die Einführung eines Informationssicherheitsmanagementsystems ist in diesem Zusammenhang zu empfehlen. Dabei ist das ein Punkt, der eine gewisse finanzielle Unterstützung des Landes notwendig macht.

Kostenbeispiele und Bewertungen, wie teuer das Ganze werden kann, können wir nicht geben, da diese Frage mit einer gewissen Dynamik verbunden ist. Wichtig ist, dass dieser Herausforderung auch mit anderen Institutionen begegnet wird. Ich nenne hier IT.NRW, die ein CERT betreiben. Das kann als Blaupause, gerade was die Kosten und Aufwände angeht, dienen.

Wichtig ist dabei auch, dass nicht nur hohe Erstinvestitionen zu tätigen sind, sondern es eine kontinuierliche Aufgabe ist, die mit laufenden Kosten verbunden ist, die in den kommunalen Haushalten berücksichtigt werden müssen. Das kann in der Regel nicht alleine geschultert werden. Insofern fänden wir es vorteilhaft, wenn das Land den Anschub mitfinanzieren und sich auch anschließend kontinuierlich an den Kosten beteiligen würde. Denn jede Finanzierung, die kommunal stattfindet, bedeutet mehr IT-Sicherheit für das gesamte System, und gerade im Hinblick auf das OZG und die Verknüpfung aller Systeme ist das für alle von Vorteil. – Vielen Dank.

Vorsitzender Thorsten Schick: Ich schaue noch mal in die Runde. Gibt es weiteren Fragebedarf? – Nein.

Dann darf ich mich sehr herzlich bei unseren Sachverständigen bedanken.

Das Protokoll ist nach Fertigstellung auf der Seite des Ausschusses einsehbar.

Ich wünsche Ihnen noch einen schönen Resttag.

Die Sitzung ist geschlossen.

gez. Thorsten Schick
Vorsitzender

Anlage
19.07.2021/11.08.2021
10

Stand: 19.07.2021

Anhörung von Sachverständigen
Sitzung des Ausschusses für Digitalisierung und Innovation

Kommunale IT-Sicherheit sicherstellen – Aufbau eines zentralen Kommunal-CERT
Antrag der Fraktion der CDU und der Fraktion der FDP, Drucksache 17/13081
am 24. Juni 2021
16.30 Uhr, Plenarsaal

Tableau

eingeladen	Teilnehmer/innen	Stellungnahme
Städtetag Nordrhein-Westfalen Köln	**Karim Ahajliu** *per Video zugeschaltet*	17/4074
Städte- und Gemeindebund Nordrhein-Westfalen e.V. Düsseldorf		
Landkreistag Nordrhein-Westfalen Düsseldorf		
KDN – Dachverband kommunaler IT-Dienstleister Siegburg	**Professor Dr. Engel** *per Video zugeschaltet*	17/4088
AG KRITIS Bonn	**Manuel Atug**	17/4072
Information und Technik Nordrhein-Westfalen (IT.NRW) Düsseldorf	**Hans Josef Fischer** Jens Vieweg	17/4063
regio iT gesellschaft für informationstechnologie mbh Aachen	**Dieter Rehfeld** *per Video zugeschaltet*	17/4028
Exzellenzcluster CASA / Horst-Görtz-Institut für IT-Sicherheit Ruhr-Universität Bochum Bochum	**Professor Dr. Schwenk** *per Video zugeschaltet*	17/4078

***