Arbeitsgemeinschaft der kommunalen Spitzenverbände Nordrhein-Westfalen

Landtag NRW
Herrn Landtagspräsidenten André Kuper MdL
Platz des Landtags 1
40221 Düsseldorf

Ausschließlich per E-Mail:

LANDTAG
NORDRHEIN-WESTFALEN
17. WAHLPERIODE

STELLUNGNAHME
17/4074

Alle Abg

Anhörung im Ausschuss für Digitalisierung und Innovation des Landtags Nordrhein-Westfalen - LT-Drucksache 17/13081
Ihr Schreiben vom 10.05.2021 GZ.: I.A.1/A20)

Datum

Städtetag NRW
Dr. Hanna Sommer
Referentin
Telefon 030 37711-770
hanna.sommer@staedtetag.de
Hausvogteiplatz 1
10117 Berlin
www.staedtetag-nrw.de
Aktenzeichen: 10.55.00

Landkreistag NRW
Karim Ahaljiu
Referent
Telefon 0211 300491-340
k.ahaljiu@lkt-nrw.de
Kavalleriestraße 8
40213 Düsseldorf
www.lkt-nrw.de
Aktenzeichen: 10.51.05

Städte- und Gemeindebund NRW
Christiane Bongartz
Referentin
Telefon 0211 4587-226
christiane.bongartz@kommunen.nrw
Kaiserwerther Straße 199 - 201
40474 Düsseldorf
www.kommunen.nrw
Aktenzeichen: 17.0.6.4.1-004/001

Sehr geehrter Herr Landtagspräsident Kuper,

vielen Dank für die Möglichkeit, zu dem o.g. Antrag der Fraktion der CDU und der Fraktion der FDP Stellung nehmen zu können. Wir begrüßen ausdrücklich die Behandlung dieser wichtigen Thematik im Ausschuss für Digitalisierung und Innovation des Landtags NRW. Zu dem Antrag ist aus unserer Sicht Folgendes anzumerken:

Die Kommunen sind im IT-Bereich organisatorisch wie technisch unterschiedlich aufgestellt (kommunale Organisationshoheit). Für den Betrieb eines CERTs sind detaillierte Kenntnisse und Erfahrungen im direkten Umgang mit Behördenleitungen, technischen Ansprechpartnern und kommunalen IT-Dienstleistern eine zwingende Voraussetzung. Dabei hilft es, weitest möglich auf Wissen und Erfahrungen aus einem etablierten CERT-Betrieb und bestehende Netzwerke zu setzen. Diese Netzwerke gilt es zu nutzen, um die kommunale IT-Sicherheit zu stärken.

1. Verwaltungsdigitalisierung: Onlinezugangsgesetz (OZG), E-Government-Gesetz (E-GovG)

Die Verwaltungsdigitalisierung ist in vielerlei Hinsicht der Schlüssel für die Sicherstellung einer zukünftigen handlungsfähigen Verwaltung. Dabei sind alle Lebensbereiche betroffen. Zuletzt ist beispielsweise in der Corona-Pandemie deutlich geworden, dass mit digitalen Anwendungen und einer aktiven verwaltungsübergreifenden Vernetzung der Gesundheitsschutz verbessert werden kann. Home-Office, digitale Mobilitätskonzepte und der Einsatz von Sensorik leisten einen nachhaltigen Beitrag zum Umweltschutz. Unternehmen werden –

um ein weiteres Beispiel zu geben – durch sicheren Datenaustausch von analogem bürokratischen Aufwand entlastet. Das stärkt einerseits die Wettbewerbsfähigkeit, sichert andererseits Arbeitsplätze und Steuereinnahmen zur Finanzierung des Gemeinwohls und trägt letztlich im Sinne der Bürgerinnen und Bürger zu einem lebenswerten und sicheren Umfeld bei. Das mit dem OZG verfolgte Ziel eines zeitpunkt- und ortsunabhängigen Zugangs zu allen digitalen Verwaltungsleistungen kann nur erreicht werden, wenn eine durchgehende Vernetzung zwischen Bund, Ländern, Kommunen, Unternehmen, Bürgerinnen und Bürgern etabliert wird. Die so verstandene, durchgehende Vernetzung bedingt eine persistente IT-Sicherheit. Die Installierung von CERTs ist hierbei ein wesentliches Standbein.

2. Kommunale IT-Sicherheit sicherstellen - Aufbau eines zentralen Kommunal-CERT

In den Kommunalverwaltungen werden sensible und hochgradig kritische Informationen aus allen Lebensbereichen verarbeitet. Die Datenlage lässt sich mit dem virtuellen Abbild der Bürgerinnen und Bürger beschreiben. In Teilen gehören Aufgaben der Kommunalverwaltungen zur kritischen Infrastruktur (KRITIS).

In Zeiten fortschreitender Digitalisierung und Vernetzung sowie sich verschärfender Bedrohungslagen mit einer zunehmenden Zahl von Cyberangriffen ist die Informationssicherheit der Schlüssel für ein verlässliches und nachvollziehbares Verwaltungshandeln. Im öffentlichen Sektor betreiben daher neben dem Bund alle Bundesländer eigene CERTs. Auch in größeren privatwirtschaftlichen Organisationen gehören CERTs zur grundlegenden Ausstattung. Das Ziel ist die Bündelung von Expertenwissen in einem Team, um Angriffe im Vorfeld zu reduzieren, zu detektieren und im Falle eines Vorfalls angemessen zu reagieren sowie im Nachgang die Rückkehr zum Regelbetrieb professionell und sicher zu managen.

Wir sehen im CERT der civitec ein positives Beispiel für eine eigenständige und regional-kommunale CERT-Infrastruktur. Allerdings ist für die Einbettung aller Kommunen in die öffentliche Cybersicherheitsarchitektur ein umfassendes CERT-Konzept erforderlich. Auf der kommunalen Ebene besteht noch kein eigenes, übergreifendes Lagezentrum, welches sich als unabhängige und unparteiische Instanz präventiv, reaktiv und nachhaltig um die Sicherheitsbelange der kommunalen IT-Infrastruktur kümmern würde. Grundsätzlich sehen wir daher den Bedarf für ein gemeinsames Kommunal-CERT in NRW.

Die kommunalen Spitzenverbände haben bereits im Jahre 2017 in Zusammenarbeit mit dem Dachverband der kommunalen IT-Dienstleister (KDN) ein erstes Grobkonzept für ein solches Kommunal-CERT erstellt. Auf der Grundlage anschließender Beratungen zwischen dem CIO der Landesregierung und den kommunalen Spitzenverbänden wurde im Rahmen der Sitzung des IT-Kooperationsrats am 12.03.2021 in einem ersten Schritt die Öffnung ausgewählter CERT-Leistungen des Landes für die kommunale Ebene beschlossen. Dazu zählen der Zugang zum Warn- und Informationsdienst, die Etablierung des CERT NRW als Meldekopf und die Bereitstellung eines Mobile Incident Response Teams (MIRT) zur Beratung bei möglichen Sicherheitsvorfällen.

3. Antrag der Fraktion der CDU und der Fraktion der FDP

Wir begrüßen vor diesem Hintergrund die mit dem vorliegenden Antrag verfolgte Zielsetzung. Von einer entsprechenden Beschlussfassung erwarten wir eine weitere Erhöhung der IT-Sicherheit. Wir teilen die Auffassung, dass lokale Cyberangriffe infolge eines „Dominoeffektes“ zur landesweiten Gefährdung anwachsen können. Somit ist die Sicherung der schwächsten Glieder einer IT-Sicherheitsarchitektur der Garant für Resilienz des Gesamtsystems.

Darüber hinaus regen wir an, dass die Koordinierungsstelle für Cybersicherheit noch klarer den Leistungsschnitt zwischen dem CERT-NRW, kommunalen IT-Dienstleistern sowie kommunaler IT-Verantwortlichen darstellen bzw. vereinbaren sollte. Die Schaffung von Meldewegen, die Leistungsabgrenzung sowie eine

tragfähige Organisations- und Finanzierungsvereinbarung mit den Kommunen könnten für die nötige Transparenz sorgen. Die Schaffung von kontinuierlichen Formaten zum Erfahrungsaustausch, zur IT-Sicherheitsberatung und -schulung sehen wir als weitere Elemente zur Stärkung der kommunalen IT-Sicherheit. Zur perspektivischen Erweiterung des IT-Sicherheitsgesetz 2.0 gehört neben der Ergänzung, dass Kommunalverwaltungen als besonders schützenswert anzusehen sind, auch eine Regelung zur Bereitstellung von Ressourcen und Mitteln zur Bewältigung dieser Aufgabe. Unter diesem Gesichtspunkt sehen wir auch das Land in der Pflicht, zumal ohne eine grundlegende Absicherung der Kommunen ein landes- bzw. bundesweites Cybersicherheits-Lagebild nicht vollständig wäre.

a) Anforderungen an ein Kommunal-CERT

Ein künftiges Kommunal-CERT sollte eine unparteiische und unbeeinflussbare Einrichtung sein, die eine hohe Reputation erfährt. Dazu bedarf es eines verlässlichen Kernteams, das keine unmittelbaren operativen Aufgaben im IT-Betrieb innehat, sondern zentral in einem eigenständigen Netzwerk aktuelle systemrelevanten Meldungen empfängt sowie verarbeitet und den fachlichen Austausch mit den Verantwortlichen im IT-Betrieb proaktiv fördert. Diese zentrale Bündelung von Expertenwissen hilft, eventuelle Risiken zu detektieren, aktuelle Sicherheitsmeldung einzuordnen und zielgerichtet auszuschalten.

Dabei birgt die grundsätzlich wünschenswerte Vernetzung zwischen Land und Kommunalbehörden auch Risiken, die eine nähere Betrachtung erfordern. Das hat die Landesregierung erkannt und erste CERT-Services in Aussicht gestellt. Jetzt müssen zeitnah weitere Schritte erfolgen, insbesondere die Erarbeitung und Umsetzung eines gemeinsamen Konzepts für ein Kommunal-CERT. Dabei könnten die mögliche Eintrittswahrscheinlichkeit und Schadenshöhe elaboriert, geeignete präventive und reaktive Gegenmaßnahmen sowie deren Umsetzung vereinbart werden. Diese eruierten Risiken sollten, um einen Überblick über die kommunal eingesetzte IT-Ausstattung zu erhalten, inventarisiert werden.

Neben dem Aufbau eines generischen interkommunalen Angebotes von Präventivmaßnahmen/-arbeit sowie regelmäßiger Sensibilisierungskampagnen in den Kommunalverwaltungen wäre die Entwicklung eines entsprechenden Fortbildungskonzepts wünschenswert. Insoweit wäre ein gleichrangiger Zugang zum speziellen Fortbildungsprogramm des Landes hilfreich. Dieses kann durch die Stärkung des IT-Fortbildungsprogramms des MWIDE, ausgedehnt auf kommunale Mitarbeiter mit einem gleichrangigen Zugang zu den IT-Sicherheitsschulungen, unterstützt werden.

Mittelfristig sind neben der Nutzung der Expertise aus den kommunalen IT-Dienstleistern auch lokale Fachexperten gefordert (flächendeckende Einführung eines Informationssicherheitsmanagementsystems – ISMS – mit Befähigung bzw. Fortbildung des Fachpersonals hin zur Informationssicherheitsbeauftragten). Insbesondere für kleinere Kommunen bedarf es niederschwelliger Zugänge zu entsprechende Schulungs- und Beratungsleistung. Hierbei könnten die weiterentwickelten Institutionen des BSI einen Beitrag leisten.

Der Einsatz von sogenannten Penetrationstests (PEN-Test) zur Aufdeckung von Sicherheitslücken, bspw. durch Social-Engineering sollten vornehmlich als „White-Box-Tests“, d.h. mit vollem Zugang zum System und Zugriff auf den Quellcode, erfolgen. Damit können mehr Schwächen aufgedeckt und geschlossen werden als bei reinen „Black-Box-Tests“, die der Annahme nachgehen, dass potenzielle Hacker keine Kenntnis(e) der internen Systemprozesse haben.

Für die präventive und reaktive Arbeit wäre der Aufbau eines ständigen und standardisierten Informationskanals zum NRW-CERT, zur Zentral- und Ansprechstelle Cybercrime (ZAC) NRW und der Koordinierungsstelle Cybersicherheit zu empfehlen. Im konkreten Schadensfall könnten auf einer hohen Vertrauensbasis sofortige reaktive Unterstützungsmaßnahmen eingeleitet werden. Zugang zu Experten in der IT-Forensik auf Landes- und Bundesebene helfen außerdem in der Nachschau bei der Aufklärung von tatsächlichen oder vermuteten IT-Sicherheitsvorfällen.

Im Bereich der IT-Sicherheit herrschen Anbieter- und Ressourcenknappheit. Die Anwerbung von geeignetem Fachpersonal für den CERT-Betrieb sowie die qualitäts- und zeitgerechte Bereitstellung technischer Ausstattung für den Betrieb einer Hochsicherheits-Infrastruktur ist eine große Herausforderung. Kommunalverwaltungen verarbeiten häufig schützenswerte Daten mit hohem IT-Sicherheitsbedarf. So ist bei der Personalgewinnung im Besonderen auf die Attraktivität des Arbeitsplatzes und der Fortbildung zu achten. Weiterhin können über gemeinsame Rahmenverträge und einem schmalen Vergabemanagement die Verhandlungsposition der Kommunen gegenüber mächtigen Lieferanten von gefragter technischer Ausstattung eine Augenhöhe erreicht werden, die eine kontinuierliche Versorgung zu akzeptablem Kosten sicherstellt.

Zusammenfassend ist festzustellen, dass die Herausforderungen an das Land und die Kommunen ähnlich gelagert sind. Die fortschreitende Vernetzung der Behördenlandschaft bedingt in der IT-Sicherheit einen engen Austausch und enge Zusammenarbeit. Insofern besteht eine gegenseitige Abhängigkeit – Investition der Kommunen in die IT-Sicherheit bedeutet ein Mehr an Sicherheit auch bei den Landesbehörden.

b) Finanzierung eines Kommunal-CERT

Mit dem Aufbau eines Kommunal-CERT NRW wäre ein erster Schritt zu einheitlichen Strukturen auf kommunaler Ebene im Bereich der IT-Sicherheit getan. Damit wäre zugleich die Grundlage für eine weitere intensive ebenenübergreifende Zusammenarbeit zwischen Kommunen und Land gelegt. Den auf kommunaler Ebene bereits eingeleiteten Prozess sollte das Land durch geeignete Maßnahmen unterstützen. Dazu gehört die Zusage des NRW-CERT zu einer engen Zusammenarbeit sowie zur Weitergabe von Meldungen über Sicherheitsvorfälle an einem Kommunal-CERT NRW und ebenso gehört dazu die Bereitschaft zu einem vertieften Austausch über erkannte Sicherheitsrisiken und zur gegenseitigen Informationsbereitstellung dazu.

Die vorstehend skizzierten Maßnahmen beschreiben ein Bündel von Aufgaben, die nicht nur hohe Erstinvestitionen, sondern auch kontinuierlich weitere Ausgaben erfordern, welche von den Kommunen nicht allein geschultert werden können. Daher sollte sich das Land zu einer dauerhaften Mitfinanzierung des Kommunal-CERT NRW bereiterklären.

Mit freundlichen Grüßen
In Vertretung

Dr. Uda Bastians
Beigeordnete
Städtetag Nordrhein-Westfalen

Dr. Marco Kuhn
Erster Beigeordneter
Landkreistag Nordrhein-Westfalen

Andreas Wohland
Beigeordneter
Städte- und Gemeindesbund
Nordrhein-Westfalen