KDN Dachverband kommunaler IT-Dienstleister

Mühlenstr. 51
53721 Siegburg

Ihr Ansprechpartner:
Prof. Dr. Andreas Engel

Tel. +49 151 46198983
Andreas.Engel@kdn.de
www.kdn.de

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

per E-Mail

18.06.2021

Anhörung im Ausschuss für Digitalisierung und Innovation des Landtags Nordrhein-Westfalen - LT-Drucksache 17/13081

Ihr Schreiben vom 11.05.2021 GZ.: I.A.1/A20)

Sehr geehrter Herr Landtagspräsident Kuper,

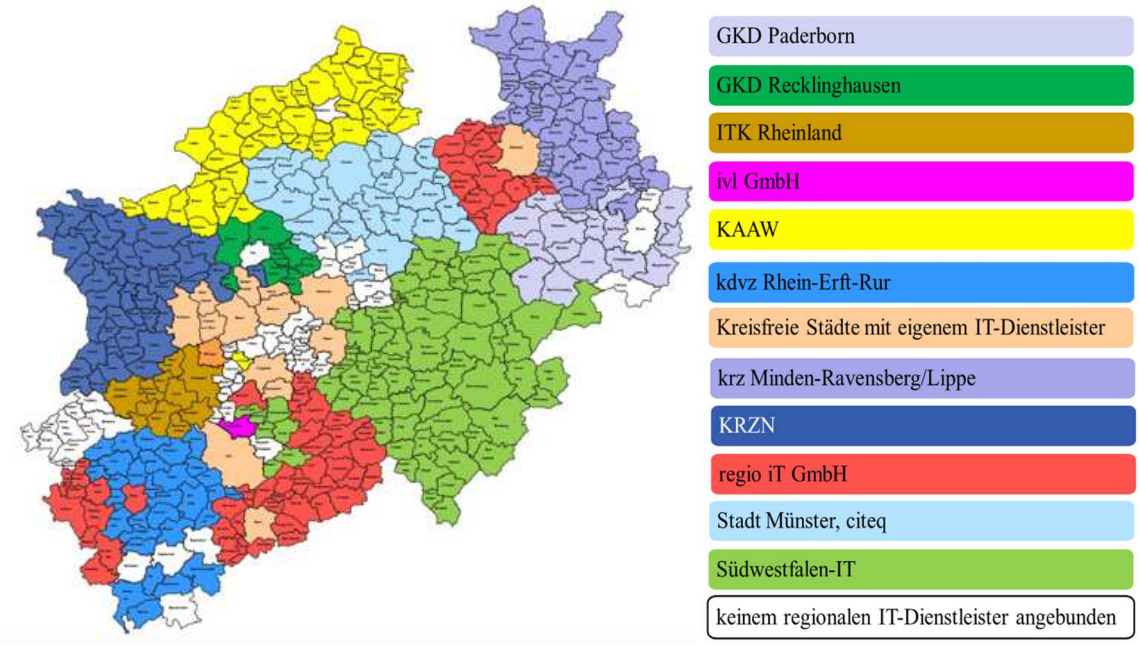
vielen Dank für die Gelegenheit zur Stellungnahme zum o.g. Antrag der Fraktionen von CDU und FDP zum Aufbau eines Kommunal-CERT NRW. Erste Schritte auf dem Weg dahin sind bereits von der Landesregierung unternommen worden. So ist der Chief Information Security Officer (CISO) auf die Kommunen und kommunale IT-Dienstleister zugegangen,

- um die dem CERT-NRW vorliegenden Warn- und Informationsmeldungen an kommunale Stellen weiterzuleiten;
- um das CERT NRW als Meldekopf auch für die Kommunen zu den angeschlossenen CERT-Verbünden zu nutzen und
- perspektivisch auch ein Mobile Incident Response Teams (MIRT) zur lokalen Unterstützung im Falle von Sicherheitsvorfällen den Kommunen beiseite zu stellen.

Die folgenden Überlegungen dienen dazu, die im Antrag vorgeschlagenen Maßnahmen in Bezug auf die jeweils spezifische Ausgangslage und Bedarfssituation in den Kommunen zu konkretisieren. Sie bauen auf Empfehlungen auf, die der Facharbeitskreis IT-Sicherheit des KDN Dachverband kommunaler IT-Dienstleister im Auftrag des Gemeinsamen IT-Lenkungsausschusses der Arbeitsgemeinschaft der kommunalen Spitzenverbände entwickelt hat.

1. Ausgangslage: die Kommunale IT-Landschaft in NRW

Die IT-Infrastruktur und IT-Anwendungen der kommunalen Gebietskörperschaften im Land werden zum weitaus größten Teil von 27 kommunalen IT-Dienstleistern betrieben (vgl. die Karte der kommunalen IT-Landschaft in NRW).



10 regionale IT-Dienstleister betreiben die IT-Infrastruktur und Anwendungssysteme von insgesamt 323 Städten und Gemeinden sowie der 31 Kreise, einschließlich der Städteregion Aachen. Dies entspricht 81 % der Kommunen und 100 % der Kreise. Zwei regionale IT-Dienstleister nutzen ein gemeinsames Rechenzentrum. Sieben regionale IT-Dienstleister sind sicherheitszertifiziert (nach BSI-Grundschutz und/oder ISO 27.001) und zwei beabsichtigen eine Zertifizierung in den kommenden drei Jahren.

15 Kreisfreie Städte betreiben ihre IT-Infrastruktur selbst. Drei städtische IT-Dienstleister sind sicherheitszertifiziert nach BSI-Grundschutz und/oder ISO 27.001, drei beabsichtigen es innerhalb der kommenden drei Jahre.

Auch die beiden **Landschaftsverbände** unterhalten eigene IT-Betriebe. Sie haben oder planen jeweils ein gemeinsames Rechenzentrum mit einem städtischen IT-Dienstleister. Ein IT-Betrieb ist zertifiziert, der andere plant es innerhalb der nächsten drei Jahre.

Die 27 im KDN zusammen geschlossenen kommunalen IT-Dienstleister aus NRW sind verantwortlich für den Betrieb von ca. 365.000 Endgeräten (stationäre und mobile), davon ca. 300.000 im Vollservice. Nimmt man die Zahl der stationären Endgeräte als Indikator, werden von diesen IT-Dienstleistern insgesamt ca. 245.000 IT-Arbeitsplätze in den Kommunen des Landes gemanagt und betreut.

Alle 27 KDN-Mitglieder haben einen IT-Sicherheitsverantwortlichen und ein Informationssicherheitsmanagement-System (ISMS) etabliert. Die IT-Sicherheitsverantwortlichen treffen sich regelmäßig im Facharbeitskreis IT-Sicherheit zum Erfahrungsaustausch. Dass es auf der Ebene der IT-Dienstleister bisher weitgehend bei erfolglosen Angriffen geblieben ist, liegt zu einem guten Teil daran, dass die Sicherheitsmaßnahmen in den letzten Jahren kontinuierlich ausgebaut wurden.

58 meist kleinere, kreisangehörige Städte und Gemeinden mit Einwohnerzahlen zwischen 8.000 und 111.000 sind keinem regionalen IT-Dienstleister angeschlossen (15 % der Kommunen in NRW mit etwa 11 % der Einwohner), nehmen aber gelegentlich Leistungen von diesen entgegen. Über die Betriebsformen und den Sicherheitsstatus der IT-Infrastruktur in diesen Kommunen liegen keine verlässlichen Informationen vor.

2. Unterschiedliche Bedarfslagen

Der zielorientierte Aufbau eines Kommunal-CERT in NRW muss von den beschriebenen IT-Betriebsstrukturen auf der kommunalen Ebene und den damit verbundenen unterschiedlichen Ausgangslagen zur Gewährleistung der Sicherheitsanforderungen ausgehen. Dabei können drei grundlegende Bedarfslagen unterschieden werden:

1. Die Sicherheitssituation in den **58 kreisangehörigen Städten und Gemeinden**, die keinem regionalen IT-Dienstleister angeschlossen sind, sollte genauer untersucht werden. Es ist jedoch davon auszugehen, dass der IT-Betrieb in diesen Kommunen unter einem vergleichsweise **hohen Sicherheitsrisiko** stattfindet. Bewertungen und Reaktionen auf Informationen und Warnungen aus dem Landes-CERT finden dort in der täglichen Arbeit eher nicht statt. Von den Verwaltungsleitungen wird zuweilen auch die Sinnhaftigkeit im Verhältnis zum Aufwand angezweifelt. Hier bedarf es insbesondere der Aufklärung und Beratung, der (erstmaligen) Implementierung eines Informationssicherheitsmanagement-Systems (ISMS), der Bestellung von Informationssicherheitsbeauftragten und des Audits der Sicherheitsarchitektur. Mittelfristig ist eine Überführung der lokalen Betriebsstrukturen in zertifizierte IT-Betriebe notwendig, um dauerhaft und nachhaltig ein hohes Grundschutzniveau zu erreichen und zu bewahren.
2. Bei den kreisfreien Städten und den Städten und Gemeinden im kreisangehörigen Raum, die **keine zertifizierten IT-Betriebe** haben, besteht ein **mittleres Sicherheitsrisiko**, weil in der Regel ein ISMS aufgebaut wurde, aber nicht auf einem Niveau, dass schon zertifizierungsfähig ist. In diesen Kommunen steht die Entscheidung an, entweder das ISMS auszubauen, damit eine Sicherheitszertifizierung durchgeführt werden kann, oder auch hier den Betrieb der IT-Infrastruktur auf einen zertifizierten IT-Dienstleister zu übertragen.
3. Bei Kommunen, die entweder einen eigenen **zertifizierten IT-Betrieb** haben oder von einem zertifizierten IT-Dienstleister versorgt werden, kann von einer **ausreichenden technischen und organisatorischen IT-Sicherheitsarchitektur** ausgegangen werden, die einer lokalen bzw. regionalen CERT-Struktur entspricht. Sie sind grundsätzlich so aufgestellt, dass sie sich einer landesweiten kommunalen CERT-Organisation anschließen und kompetent mitarbeiten können.

3. Strukturvorschlag für eine kommunale CERT-Organisation in NRW

Ziel eines kommunalen CERT sollte es sein, die Kommunen bei der Wahrnehmung ihrer Sicherheitsaufgaben zu unterstützen, das Sicherheitsniveau in allen Kommunen auf ein angemessen hohes Niveau anzuheben und durch die enge und vertrauensvolle Zusammenarbeit mit zertifizierten kommunalen IT-Dienstleistern zu stärken. Es sollte durch eine effektive Koordination der landesweiten Aktivitäten den ressourcensparenden Mitteleinsatz fördern.

Das vorgeschlagene und auch von der Arbeitsgemeinschaft der Kommunalen Spitzenverbände befürwortete Kommunal-CERT NRW sollte als eine eigenständige Organisation mit Kommunen und kommunalen IT-Dienstleistern als Trägern aufgebaut und perspektivisch auch in den Landes-CERT-Verbund aufgenommen werden. Hier wird aber nur ein Kommunal-CERT betrachtet. Den beschriebenen, lokalen Bedarfslagen entsprechend wäre ein dreistufiger Aufbau zu empfehlen mit:

1. **Kommunen**, die organisatorisch ein ISMS aufgebaut haben und technisch mit eigenen IT-Betrieben oder als Kunden eines kommunalen IT-Dienstleisters dem kommunalen CERT-Verbund angeschlossen sind.
2. qualifizierte und zertifizierte **kommunale IT-Dienstleister als lokale CERT-Organisationen**, die für Kommunen und kommunale IT-Dienstleister CERT-Aufgaben wahrnehmen und beratend tätig werden können.
3. Ein **zentrales CERT-Lagezentrum** als Koordinationsstelle für die lokalen CERT-Organisationen und Ansprechpartner für das Landes-CERT sowie andere CERT-Verbünde und Sicherheitsbehörden

Das Kommunal-CERT NRW sollte Mitglied im Deutschen CERT-Verbund, mit Unterstützung des Landes auch im Verwaltungs-CERT-Verbund (VCV) sowie der Allianz für Cybersicherheit werden.

4. Schwerpunktaufgaben der kommunalen CERT-Organisation

Aufgaben des zentralen CERT-Lagezentrums

Die Hauptaufgabe eines CERT ist der Betrieb eines Warn- und Informationsdienstes. Darüber werden Informationen zu neuen Schwachstellen und Sicherheitslücken in Soft- und Hardware publiziert, die in der Regel auf der ursprünglichen Sicherheitsempfehlung /-information des Herstellers beruhen. Darüber hinaus bieten die meisten CERT auch eine Unterstützung (z.B. forensische Untersuchungen) bei der Bearbeitung von kritischen Sicherheitsvorfällen an.

Das zentrale CERT-Lagezentrum als Teil des Kommunal-CERT NRW sollte als zentrale Koordinierungsstelle und interne wie externe Kontaktstelle eingerichtet werden. Es ist (wie die lokalen CERT-Organisationen) an das Meldesystem des Landes-CERT angeschlossen und tauscht sich kontinuierlich mit den lokalen CERT-Organisationen und dem Landes-CERT über aktuelle und potentielle Bedrohungslagen sowie geeignete Maßnahmen zur Prävention und Reaktion aus. Es ist der Adressat für die Meldung von Sicherheitsvorfällen aus den Kommunen und analysiert und dokumentiert kontinuierlich die Sicherheitslage. Berichte über Sicherheitsvorfälle sind in einem kommunalen Lagebild zur IT-Sicherheit darzustellen. Die gewonnenen Informationen werden sowohl den lokalen CERT, dem Landes-CERT wie auch anderen berechtigten Behörden und Organisationen regelmäßig zur Verfügung gestellt.

Das zentrale Lagezentrum sollte die lokalen CERT-Organisationen in organisatorischen und technischen Maßnahmen zum CERT-Betrieb entsprechend der Definitionen des RfC2350 (Expectations for Computer Security Incident Response) beraten. Mit den lokalen CERT und anderen CERT-Organisationen entwickelt es Strategien zur Verbesserung der IT-Sicherheitsmaßnahmen. Eine wichtige Aufgabe besteht auch in der Konzeption und Umsetzung von Fortbildungs- und Sensibilisierungsmaßnahmen für Mitarbeitende und Führungskräfte. Es ist der zentrale Ansprech- und Kooperationspartner für das CERT NRW, andere CERT-Verbünde und die Sicherheitsbehörden.

Aufgaben der lokalen CERT-Organisationen (CERT vor Ort):

Die lokalen, bei zertifizierten IT-Dienstleistern angesiedelten CERT-Organisationen, übernehmen überwiegend die Aufgabe der operativen **Umsetzung in organisatorischer und technischer Hinsicht,** soweit sie nicht von den Kommunen selbst wahrgenommen werden. Sie handeln im Auftrag der Kommunen und sollten die Verhältnisse vor Ort kennen.

Organisatorisch beraten und unterstützen sie die Kommunen beim Aufbau bzw. Ausbau eines professionellen Risiko- und Informationssicherheitsmanagements (ISMS), einschließlich der Entwicklung einer, an den Leitlinien des Kommunal-CERT orientierten IT-Sicherheitsstrategie, eines IT-Sicherheitskonzepts und eines IT-Notfallhandbuchs, soweit dies nicht im Rahmen der Übernahme des IT-Betriebs für die Kommunen von ihnen selbst wahrgenommen wird.

Technisch beraten sie die Kommunen und ggf. andere kommunale IT-Dienstleister spezifisch auf die eigene Systemlandschaft zugeschnitten und fokussiert in Fragen der IT-Sicherheitsarchitektur, Technikausstattung, zum Rechenzentrumsbetrieb, Netzwerkverkabelung etc., soweit Kommunen noch (in Teilen) eigene IT-Betriebe unterhalten. Sie führen ggf. Sicherheitsaudits durch und beraten und unterstützen die kommunalen IT-Verantwortlichen bei der Behebung von Sicherheitslücken, auch in akuten Bedrohungslagen. Sie sind erste Anlaufstellen bei Sicherheitsvorfällen, ggf. in enger Zusammenarbeit mit dem geplanten Mobile Incident Response Teams (MIRT) des Landes.

Für die Mitarbeitenden und Führungskräfte in den Verwaltungen vor Ort bieten die lokalen CERT-Organisationen Sensibilisierungs- und Schulungsmaßnahmen an.

Sollte das Sicherheitsgesetzes 2.0 zukünftig auch für Kommunalverwaltungen gelten, wären die meisten kleineren und mittleren Kommunen personell und finanziell überfordert. In Abstimmung mit dem BSI sollte daher das Kompendium Kommunal-Verwaltung als Branchenstandard erklärt werden. Die dann alle 2 Jahre erforderliche Auditierung könnte von den lokalen CERT-Organisationen als Dienstleistung übernommen werden.

Aufgaben der Kommunen

Kommunen sind für den Aufbau und die kontinuierliche Weiterentwicklung eines ISMS verantwortlich, einschließlich der Qualifizierung und Sensibilisierung der Mitarbeitenden und Führungskräfte in Sicherheitsfragen. Die Verwaltungsleitungen sollten vor allem über Complianceanforderungen, Haftungsfragen und Aufwände in den Gemeinden und Gemeindeverbände unterrichtet werden.

Je nach ihrer Rolle als Auftraggeber, als Träger eines kommunalen IT-Dienstleisters oder als Betreiber eigener IT-Systeme tragen sie die Verantwortung für die Umsetzung von IT-Sicherheitsmaßnahmen. Dabei sollten sie sich an den Empfehlungen des Kommunal-CERT NRW orientieren.

Der Aufbau eines Kommunal-CERT NRW muss die unterschiedlichen Ausgangslagen der Kommunen im Land berücksichtigen und schrittweise auf ein gemeinsames, hohes Sicherheitsniveau anheben. Dies ist auch angesichts der immer engeren Vernetzung der IT-Systeme zwischen Land und Kommunen notwendig. Dabei sind die Kommunen auf die Unterstützung des Landes bzw. des Landes-CERT NRW angewiesen – auch finanziell.

Mit freundlichen Grüßen
im Auftrag

Andreas Engel
(Geschäftsführer)