LANDTAG
NORDRHEIN-WESTFALEN
17. WAHLPERIODE

STELLUNGNAHME
17/4028

Alle Abg

regio iT

regio iT • Lombardenstraße 24 • 52070 Aachen

Herrn
Andrè Kuper
Präsident des Landtags Nordrhein-Westfalen
Postfach 10 11 43
40002 Düsseldorf

regio iT gesellschaft für
informationstechnologie mbh

Lombardenstraße 24
52070 Aachen

Ihr/e Ansprechpartner/in
Dieter Rehfeld

Tel.: +49 241 413 59 - 1602
Fax: +49 241 413 540 - 1602

Dieter.Rehfeld@regioit.de
www.regioit.de

Datum: 08.06.2021

Stellungnahme MMD17-13081 - Aufbau eines kommunalen CERT in NRW

Sehr geehrter Herr Präsident,

vielen Dank für die Gelegenheit zur Stellungnahme bezüglich des Aufbaus eines kommunalen CERTs in NRW, welcher ich gerne nachkomme.

Die Digitalisierung der Kommunen in Deutschland schreitet mit großen Schritten voran. Eine stärkere Vernetzung der Behörden untereinander und der Wunsch nach digitaler Souveränität der Bürgerinnen und Bürger verstärkt sich. Gleichzeitig kann man beobachten, dass die Bedrohungen aus dem Cyberraum deutlich zunehmen. Die Verwaltung der Daten unserer Bürgerinnen und Bürger in den Kommunalverwaltungen wird somit immer mehr in den Fokus gezielter Angriffe rücken. Mithin ist es notwendig, den kommunalen Sektor bezogen auf die IT–Sicherheit weiter zu ertüchtigen und die Verantwortlichen auf dieser Ebene zu unterstützen.

Ein kommunales CERT in NRW zu errichten, ist deshalb ein probates Mittel, um sowohl präventiv wie auch reaktiv die Kommunen zu unterstützen. Der kommunale Sektor unterscheidet sich durch die kommunale Selbstverwaltung deutlich von der Landes- und Bundesebene, so dass hier eine entsprechend spezielle Ausrichtung und das Fachwissen aus diesem Bereich gefragt sind. Die Initiative der Landesregierung zur Stärkung der Sicherheit im kommunalen Umfeld befürworte ich daher sehr.

Zum einen ist eine stärkere Verpflichtung der Kommunen zur Etablierung von Sicherheitsstandards (z.B. ISO 27001, BSI Grundschutz) zwingend erforderlich, da vielfach die Kritikalität der verarbeiteten Daten seitens der Behördenleitungen unterschätzt wird und Investitionen in Informationssicherheit als „freiwillige Leistungen" eingeschätzt werden. Dies äußert sich beispielsweise darin, dass viele – gerade kleine Kommunen – nicht einmal die Rolle eines Informationssicherheitsbeauftragten besetzen und sich entsprechend nicht mit der Einrichtung und dem Betrieb eines Informationssicherheitsmanagement-Systems befasst haben.

Gerade im Hinblick auf die Vielzahl kommunaler Fachanwendungen (von Friedhofswesen über Daten mit psychischen Erkrankten bis hin zum Einwohnermeldewesen mit biometrischen und Ausweisdaten) ist ein stärkerer Fokus auf die untere staatliche Ebene notwendig. Der Großteil der staatlichen Verwaltungsdaten ist sicherlich auf dieser Ebene angesiedelt und bislang durch die Gesetzgebung des Bundes und der Länder nicht berücksichtigt.

Nordrhein-Westfalen als das Land mit den meisten Bürgerinnen und Bürgern bedarf aus meiner Sicht einer Stärkung der Sicherheitsinfrastruktur im Kommunalumfeld. Die Einrichtung einer zentralen Anlaufstelle für Cyberbedrohungen für Kommunen, Kreise und kommunale Einrichtungen ist daher aus meiner Sicht überfällig und wird daher befürwortet.

Ziel sollte es sein, die bereits bestehenden Strukturen zu stärken und eine fokussierte Ausrichtung auf die Spezialbelange der Städte und Gemeinden sicher zu stellen. Die gezielte Ausrichtung und die Erfahrungen aus der kommunalen Wirklichkeit stellen aus meiner Sicht einen wichtigen Erfolgsfaktor für die Akzeptanz eines kommunalen CERTs seitens der Verwaltungen dar. Dabei ist aus meiner Sicht ein wesentlicher Erfolgsfaktor das Angebot einer umfassenden Beratung.

Aus diesem Grunde wäre meine Empfehlung ein Fach-CERT für Kommunen im Rahmen einer Kooperation zwischen Land und Kommunen und zwischen den kommunalen IT-Dienstleistern in NRW und dem Land, beispielsweise als Public-Public Partnership, also einer gemeinsamen Organisationseinheit. Die Träger einer solchen gemeinsamen Organisationseinheit zur Stärkung der kommunalen IT–Sicherheit könnte das Land und die Kommune sein. Eine enge Zusammenarbeit mit den CERT–Einrichtungen des Landes und Bundes ist dabei ein wichtiger Erfolgsfaktor. Der andere Erfolgsfaktor ist die Akzeptanz bei den Kommunen und den kommunalen IT–Dienstleistern. IT–Sicherheit kann nicht delegiert werden.

Sicherheit basiert sehr stark auf einer vertrauensvollen Zusammenarbeit – ohne Vertrauen wird keine Akzeptanz und somit kein so wichtiger, wirkungsvoller Einsatz eines kommunalen CERTs möglich sein. Gerade die Vernetzung der IT-Dienstleister untereinander ermöglicht, neben einer zentralen Ansprechstelle für Sicherheitsvorfälle und den allgemeinen CERT-Leistungen auch die Chance, lokale Krisenreaktionsteams (Mobile Incident Response Teams – MIRT) über die regional verteilten IT-Dienstleister zur Verfügung zu stellen und damit schnellere vor-Ort-Einsätze zu ermöglichen.

Zusätzlich zum Vertrauen ist ein weiterer kritischer Erfolgsfaktor die Fachkenntnis der Applikationslandschaft und der IT-Bedarfe der Kommunen vor Ort, welche sich sehr heterogen darstellt. Hier gilt es das Verständnis für die unterschiedlichen Belange (vom Schulsekretariat über das Ordnungsamt bis hinauf zu Rat und Fraktionen) im Blick zu haben und adressatengerecht mit Vorfällen und Bedrohungslagen zu interagieren.

Erst wenn diese Voraussetzungen gegeben sind, werden Kommunen bereit sein, mit einem CERT aktiv zu interagieren und somit auch dann erst die Erstellung eines Lagebildes für Sicherheitsereignisse auf der kommunalen Ebene zu ermöglichen, welches über Landes-CERT an das BSI zur Integration in ein bundesweites Lagebild ermöglicht wird.

Es liegen praktische Erfahrungen vor, wie ein kommunales CERT arbeiten könnte. Ähnlich wie das CERT-NRW ist das KomCERT der regio iT (früher civitec Zweckverband mit Sitz in Siegburg) seit 2018 Mitglied im Deutschen CERT-Verbund und unterstützt bereits seit 2014 mit seinem Warn- und Informationsdienst über 40 Kommunen und kommunale Einrichtungen in NRW. Die Dienstleistungen reichen hierbei von Awareness-Maßnahmen im Umfeld der Kommunalpolitik über vor Ort Einsätze bei Ransomware-Angriffen, ausgenutzten Software-Schwachstellen (z.B. Citrix-Lücke) bis zu gezielten Drohungen gegen kommunale Einrichtungen. Darüber hinaus wird das KomCERT regelmäßig im Umfeld von Responsible Vulnerability Disclosure als Ansprechpartner für betroffene Software im kommunalen Sektor genutzt und steht im regelmäßigen Austausch mit dem Bundesamt für Sicherheit in der Informationstechnik (CERT-Bund), dem CERT-NRW, der zentralen Ansprechstelle für Cybercrime der Staatsanwaltschaft Köln (ZAC), dem LKA, dem Verfassungsschutz und vielen anderen Organisationen.

Zur Verdeutlichung der Notwendigkeit eines landesweiten Kommunal-CERT möchte ich hier kurz ein paar Kennzahlen aus dem KomCERT im Jahr 2020 darstellen:

Angeschlossene Kunden (Kommunal):	41
Versandte Meldungen im Warn- und Informationsdienst:	1.583
Geleistet Beratungsstunden in Kommunen	1.319
Beantwortung von Fragen zu potentiell gefährlichen E-Mails:	ca. 200
Behandlung von Coordinated Vulnerability Disclosers:	3
Behandlung von Abuse-Meldungen:	143

Gravierende Sicherheitsvorkommnisse mit aktiver Begleitung in 2020:

- Ausgenutzte Citrix Lücke (#shitrix) – Komplette Kompromittierung
- Untersuchung einer Solar Winds Infrastruktur
- DDoS-Angriffswelle
- Komplettverschlüsselung eines Kundenstandortes mit Lösegeldforderung
- Verdachtsfall auf APT bei einer Kommune
- Dreimal Einsatz des Mobile Incident Response Teams (MIRT)

Das KomCERT bezieht unter anderem Meldungen internationaler CERTs aus den USA, Japan, Frankreich, Italien, Australien mit in die Meldungen ein.

Im Sinne der proaktiven Sicherheit werden Schwachstellenscans, Sensibilisierungen von Verwaltungsleitungen und Mitarbeitenden in den Kommunen angeboten sowie die Einführung des kommunalen Grundschutzprofils begleitet.

Mit freundlichen Grüßen

regio iT
gesellschaft für informationstechnologie mbh

Dieter Rehfeld
Vorsitzender der Geschäftsführung