VITAKO

Kommunale IT gemeinsam schützen – Resilienz und Cybersicherheit im Fokus

VITAKO – Perspektive und Position zur kommunalen IT-Sicherheit

Stand: 12. Juni 2024

CYBERSICHERHEIT GEMEINSAM UMSETZEN

Kommunen sind als wesentlicher Bestandteil der staatlichen Daseinsvorsorge systemrelevant. Cyberattacken legen zunehmen kommunale Verwaltungs-IT lahm. Es entstehen eklatante Schäden für Verwaltung, Bevölkerung und Wirtschaft mit teilweise existenzbedrohenden Ausmaßen. Die Gewährleistung der kommunalen Cybersicherheit ist eine gesamtstaatliche Aufgabe und muss über die föderalen Ebenen hinweg miteinander verzahnt werden.

GOVERNANCE:

1. Das BSI zur Zentralstelle im Bund-Länder-Verhältnis ausbauen. Die Kommunen und ihre IT-Dienstleister erhalten vollumfänglichen Zugriff auf die Lageinformationen des BSI und werden sowohl präventiv als auch bei einem IT-Sicherheitsvorfall umfassend durch das BSI bei Analyse und Wiederanlauf unterstützt.
2. Kommunen und ihre IT-Dienstleister müssen verbindlich und flächendeckend in einheitliche interföderale Vernetzungs- und Unterstützungsstrukturen eingebunden werden. Bund und Länder ermöglichen dabei den vollumfänglichen Zugang der Kommunen zu Informationen und Unterstützung durch die Landes-CERTs.

REGULATORISCHER RAHMEN:

3. Die kommunale IT muss KRITIS werden, damit die Sicherheit der kommunalen Verwaltungs-IT verbindlich und einheitlich festgelegt ist. Gleichzeitig stellen Bund und Länder sicher, dass die Kommunen ausreichend finanzielle Mittel erhalten, um die nötigen Schutzmaßnahmen umzusetzen.

VITAKO'S MISSION:

4. Kommunale IT-Dienstleister bündeln Ressourcen und Knowhow in ihren Rechenzentren, bieten darüber hinaus umfassende Angebote an IT-Services und Dienstleistungen und erhöhen so die Cybersicherheit der kommunalen IT. Der komplexe und vielschichtige Betrieb und vor allem die auf vielen unterschiedlichen Plattformen eingesetzte (Fach-) Software sowie deren Basiskomponenten müssen jedoch noch sicherer werden. Hierbei stehen die Modernisierung und Standardisierung von Infrastrukturen und digitalen Anwendungen nach dem Prinzip Security-by-Design im Fokus. VITAKO wirkt bei der interföderalen Standardisierung mit und entwickelt partnerschaftlich Maßnahmen und Architekturen zur Erhöhung der Resilienz in den kommunalen Systemlandschaften.

BEDROHUNGSLAGE UND SCHADENSAUSMAß

Kommunen sind als wesentlicher **Bestandteil der staatlichen Daseinsvorsorge systemrelevant** für die Bereitstellung von notwendigen Gütern und Dienstleistungen. Sie erbringen über 80 Prozent der staatlichen Verwaltungsleistungen und verarbeiten dabei zahlreiche personenbezogene Daten der Bürgerinnen und Bürger. Besonders kritisch ist hierbei: Kommunen sichern die Existenz zahlreicher Bürgerinnen und Bürger bspw. über die Auszahlung von Bürgergeld und anderen Sozialleistungen.

Die ständig fortschreitende Vernetzung unserer digitalen Welt ermöglicht es Kriminellen, Einfallstore in öffentliche Infrastrukturen zu nutzen, weshalb auch Kommunen im Hinblick auf ihre hohe Relevanz im Staat regelmäßig von Cyberkriminellen angegriffen werden. Sind Kommunen nicht mehr handlungsfähig, führt das zu eklatanten Einschränkungen für Bürgerinnen und Bürgern weshalb das **Vertrauen in den Staat als verlässlicher Souverän massiv bedroht** ist.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) nennt **Ransomware-Angriffe** neben gelenkten Cyberangriffen durch andere Staaten als größte Bedrohung. Durchschnittlich werden zwei Angriffe dieser Art pro Monat auf Kommunalverwaltungen oder kommunale Betriebe bekannt[1].

Dies hat **eklatante Schäden für Kommunen und Bürgerinnen, Bürger sowie Unternehmen** zur Folge. Häufig werden infolge eines Cyberangriffs die IT-Systeme und Fachverfahren der Kommunen zunächst abgeschaltet. Dadurch sind beispielsweise monatliche Auszahlungen im Sozial- und Unternehmensbereich schlagartig ausgesetzt. Wer kein Bürgergeld oder andere Sozialleistungen mehr erhält, ist in höchstem Maße existenzgefährdet. Besonderes Krisenpotential besitzen darüber hinaus Einschränkungen im Pass- und Ausweiswesen sowie stark frequentierte Verwaltungsleistungen wie das Melde- und Kfz-Zulassungswesen. Hinzu kommen sehr hohe finanzielle und personelle Aufwände, um die IT der Verwaltung neu aufzubauen und alle Fachverfahren wieder in Betrieb zu nehmen. So dauerte der Wiederaufbau der Systeme in Anhalt-Bitterfeld rund ein Jahr und verursachte Kosten in Höhe von rund zwei Millionen Euro.

Ein Ausfall der kommunalen IT in den relevanten Kernanwendungen führt kurzfristig gerade bei Multi-Krisenszenarien und Großschadensereignissen wie zum Beispiel Naturkatastrophen, Terroranschlägen und Bedrohung der nationalen Sicherheit zu stark erschwerten Bedingungen für die unmittelbare Unterstützung der Beteiligten. Mittel- bis langfristig gefährdet dies auch den Zusammenhalt und das Wirken aller Teile der Gesellschaft.

BSI ALS INTERFÖDERALE ZENTRALSTELLE

Öffentliche Verwaltungen vor Cyberangriffen zu schützen und resilient gegen den Ausfall der IT-Systeme aufzustellen, ist eine **Gemeinschaftsaufgabe über alle föderalen Ebenen** hinweg. So wie die Digitalisierung Bund, Länder und Kommunen zunehmend stärker vernetzt, muss auch die Zusammenarbeit bei der Gewährleistung von Cybersicherheit verstärkt werden.

Als Bundesbehörde kann das BSI den Kommunen **bisher nur sehr eingeschränkt direkte Unterstützung** zukommen lassen. Die Cyber-Sicherheitswarnungen werden vom BSI zwar täglich auf seiner Homepage veröffentlicht, ohne jedoch über differenzierte Informationen zu

[1]https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2023.pdf?__blob=publicationFile&v=8

angegriffenen oder gefährdeten Kommunen zu verfügen. Zudem ist eine zielgerichtete Meldestruktur in der Praxis aufgrund von Informationsflut schwer zu realisieren bzw. durch die Mitarbeitenden in den Kommunen zu bewältigen. Auch kann das BSI bei IT-Sicherheitsvorfällen auf der kommunalen Ebene nur kurzzeitig mit Fachexpertinnen und -experten vor Ort unterstützen. Allein die Analyse eines Angriffs kann mehrere Wochen in Anspruch nehmen und erfordert meist die Beauftragung von Fachfirmen, was zu den Schadenskosten weitere hohe Kosten verursacht.

Damit auch Kommunen und ihre IT-Dienstleister direkt von der umfassenden und dauerhaften Unterstützung des BSI bei Prävention und Schadensbeseitigung profitieren können, soll das **BSI unter Anpassung der rechtlichen Grundlagen** zur **Zentralstelle von Bund, Ländern und Kommunen** mit folgenden Kernaufgaben ausgebaut werden:

- ➔ **Effektive Informationsflüsse** zu aktuellen Bedrohungen sind ein wesentlicher Baustein für eine gute Absicherung aller kommunalen IT-Systeme. Als Zentralstelle sammelt das BSI Informationen von allen föderalen Ebenen. Es muss sichergestellt werden, dass die kommunale Ebene an den **nationalen Lagebildern**, die in den Cybersicherheitsstrukturen des Bundes und der Länder entwickelt werden, partizipieren kann.
- ➔ Von Cyberangriffen betroffene Kommunalverwaltungen benötigen die **professionelle Hilfe des BSI** bei **Analyse und Wiederanlauf**, um ihre Dienste für die Bürgerinnen, Bürger und Unternehmen schnellstmöglich wieder zu aktivieren, vor allem dann, wenn sie keine Dienste eines kommunalen IT-Dienstleisters nutzen.

Das BSI wird zur Zentralstelle im Bund-Länder-Verhältnis ausgebaut. Die Kommunen und ihre IT-Dienstleister erhalten vollumfänglichen Zugriff auf die Lageinformationen des BSI. Das BSI unterstützt gemeinsam mit den Ländern und mit den kommunalen IT-Dienstleistern den Wiederanlauf der kommunalen IT.

LANDES-CERTS ALS INTERFÖDERALE KOOPERATIONEN

Mit steigender Bedrohungslage und vor dem Hintergrund der Bedeutung von kommunalen Verwaltungsleistungen, muss der Schutz von Verwaltungs-IT als **gesamtstaatliche Aufgabe** angesehen werden. Die Kommunen und ihre IT-Dienstleister müssen auch **im Katastrophenfall handlungsfähig sein und Verwaltungsleistungen** erbringen. Darüber hinaus müssen in Notlagen zusätzliche verteilte **Rechenzentrumskapazitäten für die Gefahrenabwehr bereitgestellt** werden können. Durch eine stärkere interföderale Vernetzung werden auch **Bundes- und Landesbehörden für Katastrophenschutz sowie** die Teilstreitkraft **Cyber- und Informationsraum der Bundeswehr** (CIR) eingebunden.

Mithilfe einer derartigen Vernetzung versorgen sich die Kommunen besser mit Informationen über mögliche Bedrohungen und erhalten im Notfall Unterstützung von Landes- und Bundesebene.

- ➔ Diese Kooperations- und Vernetzungsaktivitäten finden vielerorts bereits statt, benötigen jedoch **geregelte Informationsstrukturen** und müssen **einheitlich und flächendeckend** gestaltet werden.
- ➔ Beratungsangebote durch die **Computer Emergency Response Teams (CERTs)** der Länder müssen ausgebaut und ebenfalls vereinheitlichet werden, um IT-Sicherheit und Resilienz der kommunalen Verwaltung in ganz Deutschland auf ein besseres Niveau zu heben.
- ➔ Informationsaustausch erfordert ein hohes Maß an Vertrauen zwischen unterschiedlichen Akteuren im Bereich Cybersicherheit auf allen föderalen Ebenen. Teil dieses Netzwerkes zu

sein, bietet den Kommunen und ihren IT-Dienstleistern die Möglichkeit, entsprechendes **Vertrauen aufzubauen** und von den **Informationen der Landes-CERTs** zu profitieren.

➔ Kommunen erhalten vollumfänglichen **Zugang zu den Lageinformationen** von Bund und Ländern und greifen bei einem Sicherheitsvorfall auf **Unterstützung** durch die Expertinnen und Experten der **Landes-CERTs** zurück.

Kommunen und ihre IT-Dienstleister werden verbindlich und flächendeckend in einheitliche interföderale Vernetzungs- und Unterstützungsstrukturen eingebunden. Bund und Länder ermöglichen dabei den vollumfänglichen Zugang der Kommunen zu Informationen und Unterstützung durch die Landes-CERTs.

KOMMUNALE IT ALS KRITISCHE INFRASTRUKTUR

Bis zum 17.10.2024 müssen alle EU-Mitgliedsstaaten die NIS-2-Richtlinie[2] der EU in nationales Recht umsetzen. Ein entsprechendes Bundesgesetz (**NIS2UmsuCG**) sowie jeweils Gesetze der Länder werden derzeit erarbeitet. Mit dieser gesetzlichen Vorgabe werden zahlreiche Unternehmen und Einrichtungen **als kritische Infrastrukturen klassifiziert**. Diese müssen, entsprechend dem Risiko für ihre IT, technische und organisatorische Maßnahmen auf dem Stand der Technik umsetzen. Außerdem wird die Leitungsebene der betroffenen Einrichtungen gesetzlich und direkt in die Verantwortung genommen. Auch Einrichtungen der öffentlichen Verwaltungen sind davon erfasst.

Es steht den Mitgliedsstaaten frei, ob sie die **kommunale Verwaltung** in die Regelungen mit einbeziehen. Genau dies ist nach aktuellem Stand in Deutschland **nicht vorgesehen**. Der IT-Planungsrat bittet Bund und Länder in einem Beschluss „von der Option, den Anwendungsbereich der NIS-2-Richtlinie auf Einrichtungen der öffentlichen Verwaltung auf lokaler Ebene und Bildungseinrichtungen zu erstrecken, keinen Gebrauch zu machen“[3].

➔ Aus Sicht von VITAKO ist es notwendig, **einheitliche Regelungen für die kommunale Ebene verbindlich** festzulegen. Die **kommunale IT muss KRITIS** werden.

➔ Alle **Einrichtungen werden verpflichtet**, Konzepte für die Sicherheit ihrer Informationssysteme, für die Bewältigung von Sicherheitsvorfällen und für die Aufrechterhaltung des Betriebs umzusetzen sowie ein Risikomanagement mit Blick auf den verstärkten Einsatz von Cloud-Strukturen.

➔ **Technische Mindeststandards** wie Multi-Faktor-Authentifizierung und Verschlüsselung sind **zwingend** umzusetzen.

➔ Kommunen und ihre IT-Dienstleister benötigen von Bund und Ländern ausreichend **finanzielle Mittel für Personal, Qualifizierung und Investitionen in die Modernisierung von Hard- und Softwaresysteme**.

Für ein verbindliches und einheitliches Sicherheitsniveau der kommunalen Verwaltungs-IT muss diese KRITIS werden. Gleichzeitig stellen Bund und Länder sicher, dass die Kommunen ausreichend finanzielle Mittel erhalten, um die nötigen Schutzmaßnahmen umzusetzen.

[2] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32022L2555#d1e4531-80-1

[3] https://www.it-planungsrat.de/beschluss/beschluss-2023-39

UNSERE MISSION: VITAKO ALS TREIBERIN FÜR KOMMUNALE CYBERSICHERHEIT

Cybersicherheit benötigt eine **Priorisierung** des Themas bei der Verwaltungsleitung. Generell ist es schwer auf der kommunalen Ebene in Konkurrenz mit der freien Wirtschaft qualifiziertes Personal zu finden und zu halten. Eine Rolle spielt auch, welche Priorität die Verwaltungsspitze dem Thema einräumt, oftmals wird IT-Sicherheit an die Fachabteilungen delegiert. Den nunmehr zuständigen Verwaltungsmitarbeitenden fehlt es häufig an der notwendigen **Digitalisierungs- und IT-Kompetenz** sowie Zeit und Budget, um das Thema adäquat zu bearbeiten. Die Verantwortlichen können teilweise gar nicht beurteilen wo Einfallstore für Angriffe existieren, welche Auswirkungen diese haben und welche Maßnahmen hilfreich wären, die IT-Sicherheit zu steigern. Zudem spielt auch Resignation gegenüber der Komplexität eine Rolle.

- ➔ **Kommunale IT-Dienstleister** stellen das erforderliche Personal und Knowhow für die Bereitstellung von IT-Systemlandschaften, Fachverfahren und digitalen Anwendungen bereit. Sie agieren im Auftrag kommunaler Zusammenschlüsse und entlasten die Verwaltungen, indem sie die **Verwaltungs-IT in ihren Rechenzentren bündeln**.

Den aktuell dringend benötigten, intensiven Investitionen in qualifiziertes Personal, in die Modernisierung von Hard- und Software sowie in die Betriebsinfrastrukturen steht die seit Jahren angespannte Haushaltslage in den Kommunen gegenüber. Die geringe Priorisierung von IT und Digitalisierung hat zu einem **Investitionsstau** bei den IT-Infrastrukturen geführt. Es werden aktuell mitunter Jahrzehnte alte Systeme betrieben, die vom Hersteller nicht mehr mit Sicherheitsupdates unterstützt werden und ein sicherer Betrieb damit so gut wie ausgeschlossen ist. In diesem Zusammenhang müssen insbesondere die **wachsenden Anforderungen an die Softwarebetreiber** betrachtet werden. Sie müssen Sicherheitslücken identifizieren und schließen, Sicherheitspatches einspielen oder andere Behelfslösungen finden. Dies bindet ein hohes Maß an personellen Ressourcen.

- ➔ **Software muss moderner und sicherer werden**, um den zeitgenössischen Herausforderungen der Cybersicherheit und anderer Digitalisierungsanforderungen der Cloudifizierung, der Registermodernisierung und der BundID-/EUDI-Wallet-Anbindung gerecht zu werden.
- ➔ Öffentlich-rechtliche und private Softwarehersteller wenden bei der Entwicklung von Anwendungen zwingend das Prinzip **Security-by-Design** an, damit möglichst wenig Sicherheitslücken in der Software entstehen. Entsprechend muss die öffentliche Verwaltung bei **Beschaffungen diese Anforderung konsequent durchsetzen**.

Die Zunahme der erfolgreichen Cyberangriffe auf Kommunen und ihre IT-Dienstleister ist auch darauf zurückzuführen, dass das IT-Sicherheitsniveau aufgrund fehlender verbindlicher IT-**Sicherheitsstandards** in den Kommunen stark schwankt und so einem Flickenteppich in den Kommunen und in den Ländern gleicht.

- ➔ Kommunen und ihre IT-Dienstleister benötigen ein **interföderales, einheitliches und verbindliches Sicherheitsniveau**.
- ➔ **VITAKO** treibt in interföderalen Gremien (Standardisierungsboard und RegMo-Beirat des IT-Planungsrates) Prozesse, wie die **Standardisierung** von Basisinfrastrukturen voran und entwickelt für eine effektive Zusammenarbeit auf der kommunalen Ebene technische Lösungen für mehr Cybersicherheit.

- ➔ **VITAKO** entwickelt auf Basis des IT-Grundschutzprofils „Basis Absicherung Kommunalverwaltung“ des BSI sowie bestehender Zertifizierungen ein **eigenes Rahmenwerk.**
- ➔ **VITAKO** entwickelt sein Netzwerk weiter zu **Partnerschaften für gemeinsame Sicherheitsvorfallübungen** und für die Bündelung von Knowhow und Ressourcen. Gemeinsam mit der govdigital und der ProVitako stellt VITAKO ein effektives **Leistungspaket zur kommunalen Cybersicherheit** für die Kommunen zur Verfügung.

Kommunale IT-Dienstleister bündeln Ressourcen und Knowhow in ihren Rechenzentren, bieten darüber hinaus umfassende Angebote an IT-Services und Dienstleistungen und erhöhen so die Cybersicherheit der kommunalen IT. Der komplexe und vielschichtige Betrieb und vor allem die auf vielen unterschiedlichen Plattformen eingesetzte (Fach-) Software sowie deren Basiskomponenten müssen jedoch noch sicherer werden. Hierbei stehen die Modernisierung und Standardisierung von Infrastrukturen und digitalen Anwendungen nach dem Prinzip Security-by-Design im Fokus. VITAKO wirkt bei der interföderalen Standardisierung mit und entwickelt partnerschaftlich Maßnahmen und Architekturen zur Erhöhung der Resilienz in den kommunalen Systemlandschaften.