Positionspapier

Digitalisierung für die Öffentliche Sicherheit - Beschaffung, Innovation, Funktionalität und Sicherheit ins Gleichgewicht bringen

08.07.2020

Zusammenfassung

In diesem Papier sind die zentralen Forderungen des Bitkom für die Digitalisierung der Öffentlichen Sicherheit und die Erwartungen an eine zeitgemäße und auftragsunterstützende IT-Infrastruktur für die Behörden und Organisationen mit Sicherheitsaufgaben (BOS) zusammengefasst. Der Leitgedanke ist hierbei, dass die Dimensionen Beschaffung, Innovation, Funktionalität und Sicherheit in ein Gleichgewicht gebracht werden müssen. Die Potenziale und Risiken von neuen Technologien für die Öffentliche Sicherheit müssen evaluiert und in einem ganzheitlichen Ansatz konzeptioniert werden, auch mit dem Ziel, Innovationen schnell und effizient für die BOS nutzbar zu machen.

Bitkom
Bundesverband
Informationswirtschaft,
Telekommunikation
und Neue Medien e.V.

Dr. Christian Weber
Bereichsleiter Öffentliche Sicherheit & Verteidigung
T +49 30 27576-136
c.weber@bitkom.org

Albrechtstraße 10
10117 Berlin

Präsident
Achim Berg

Hauptgeschäftsführer
Dr. Bernhard Rohleder

Inhalt

Seite

Inhalt 2
1 Einleitung 3
2 Handlungsfelder 3
2.1 Innovationskultur fördern 3
2.2 Ganzheitliche Beschaffungsorganisation 4
2.3 Zur Digitalen Souveränität befähigen 5
2.4 Zusammenarbeit ermöglichen und Informationsaustausch fördern 6
2.5 Krisenmanagement 7
2.6 Personal qualifizieren/ Kompetenzen ausbauen 7

1 Einleitung

Öffentliche Sicherheit ist ein hoch brisantes Thema – in der analogen, wie in der digitalen Welt. Die föderale Organisation der Öffentlichen Sicherheit impliziert eine Vielzahl an unterschiedlichen Anforderungen in Bezug auf rechtliche, fachliche, technische und organisatorische Rahmenbedingungen. Die Optimierung dieser Handlungsdimensionen trägt dazu bei, dass der Staat die Sicherheit seiner Bürgerinnen und Bürger schützt. Eine isolierte Betrachtung einzelner Dimensionen ist wenig erfolgversprechend. Vielmehr bedarf es aufgrund komplexer Wechselwirkungen und vielfältiger Interdependenzen einer ganzheitlichen Betrachtung.
Dieses Phänomen spiegelt sich in der IT-Landschaft unserer Sicherheitsbehörden wider. Gekennzeichnet durch eine Vielzahl an eigenen Entwicklungen, spezifischen Lösungen, fehlenden Schnittstellen und unterschiedlicher Dateiformate, vermag die IT-Ausstattung im Umfeld der Behörden und Organisationen mit Sicherheitsaufgaben (BOS) nicht in allen Bereichen die Chancen der Digitalisierung auf dem heutigen Stand der Technik zu nutzen, was die Auftragserfüllung durch die BOS zunehmend erschwert. Nicht adäquate Beschaffungsorganisationen und Prozesse bremsen Innovationen und gefährden die Handlungsfähigkeit der Sicherheitsbehörden. Der Grundgedanke der folgenden Überlegungen lautet, dass die Dimensionen Beschaffung, Innovation, Funktionalität und Sicherheit für eine erfolgreiche digitale Transformation der Sicherheitsbehörden ins Gleichgewicht gebracht werden müssen. Dieser Gedanke wird im Folgenden auf einzelne Handlungsfelder übertragen, die in diesem Papier näher betrachtet werden. Der Fokus wird auf Anwendungsfälle und Prozesse gelegt, die mit einem möglichst standardisierten Baukasten/Standard-Sortiment erreicht werden müssen

2 Handlungsfelder

2.1 Innovationskultur fördern

Wir setzen uns für eine Innovationskultur ein, die dazu führt, dass Organisationen der Öffentlichen Sicherheit von neuen Technologien profitieren können. Einen etablierten Rahmen bildet hierfür bereits die Sicherheitskooperation Cybercrime zwischen dem Bitkom und mittlerweile sechs Landekriminalämtern, deren Ziel auch im Kompetenzerwerb- und dem Austausch zwischen Industrie und den BOS besteht.

Von der Nutzung neuer Technologien profitieren die BOS auf verschiedenen Ebenen.
So steigern moderne Arbeitsmittel, wie z.B. Telearbeitslösungen, auch die Attraktivität als Arbeitgeber. Technologien wie z.B. Smart-Devices ermöglichen ein ortsunabhängiges

Zusammenarbeiten in unterschiedlichen Arbeitsstrukturen. Dies erhöht die Flexibilität bei der Arbeit, z.B. durch Kollaboration bei einsatzangepassten Organisationsstrukturen. Cloud Infrastrukturen fokussieren das IT-Fachpersonal auf Kernaufgaben (Service Bereitstellung), indem Kapazitäten beim Infrastrukturbetrieb eingespart werden.
Die Potenziale dieser Technologien sollten durch die BOS sowie für die Weiterentwicklung des Katastrophen- und Bevölkerungsschutzes konsequent genutzt werden. Die notwendigen Rahmenbedingungen sind hierfür zu schaffen. Eine Möglichkeit wäre es zum Beispiel, unter dem Dach der ZITiS ein Innovationslabor zu schaffen, in dem BOS und Wirtschaft konkrete Innovationen gemeinsam verproben und die Ergebnisse präsentieren können.

2.2 Ganzheitliche Beschaffungsorganisation

Beschaffungsorganisation und -verhalten darf nicht auf einen kurzfristigen Bedarf oder auf eine Teillösung reduziert sein, sondern sollte ganzheitlich auch im Sinne der Innovationsförderung, Nachhaltigkeit und unter dem Gesichtspunkt der Digitalen Souveränität erfolgen.

Der Bereich der Öffentlichen Sicherheit sollte als Nachfragende aktiv in der Beschaffungs- und Innovationspolitik daran mitarbeiten, dass von der Bundesregierung benannte Schlüsseltechnologien weiterhin national bzw. europäisch vorgehalten werden.
Im Einzelnen gilt dies gemäß der Strategie der Bundesregierung zur Stärkung der Sicherheits- und Verteidigungsindustrie insbesondere für folgende Technologiebereiche:[1]

- Sicherheitsrelevante IT- und Kommunikationstechnologien (insb. Chip-, Netzwerk- und Verschlüsselungstechnologien)
- Vernetzte Operationsführung/ Krypto
- Künstliche Intelligenz
- Sensorik

Als Beitrag der Nachfragenden zu einer neuen Beschaffungs- und Innovationspolitik schlagen wir vor, dass die folgenden Spielräume des Vergaberechts im Sicherheitsbereich (VSVgV) angewendet werden:

- Einsatz aller Vergabemöglichkeiten (beschränkte Verfahren, ohne TNA, ...) und dadurch Beschleunigung von Vergabeverfahren im Bereich Verteidigung und Sicherheit

[1] https://www.bmwi.de/Redaktion/DE/Downloads/S-T/strategiepapier-staerkung-sicherits-und-verteidigungsindustrie.pdf?__blob=publicationFile&v=4

- frühzeitige Einbindung der Industrie in den Beschaffungsprozess, um deren fachliche und technische Expertise stärker zu nutzen

- Fragen der IT-Sicherheit und der Vertrauenswürdigkeit der verschiedenen Hersteller sollen auch in Vergabeverfahren verstärkt berücksichtigt werden

- Beteiligung innovativer Start-ups sowie kleiner und mittelständischer Unternehmen durch entsprechende vergaberechtliche Instrumente ermöglichen (z. B. vorab veröffentlichte Rahmenvertrags-Roadmaps, konkrete Abrufzahlen bei Rahmenvereinbarungen und Losaufteilung)

- Digitalisierung des Beschaffungsprozesses auch im Vorfeld und im Nachgang eines Vergabeverfahrens unter Einbeziehung der Geschäftsprozesse beim Auftragnehmer

- Heterogene Rechtslage zu beschäftigungspolitischen Zielen, Nachhaltigkeitskriterien und Umweltaspekten im Vergabeverfahren überwinden

- Rechtsvereinfachung durch Beseitigung des Flickenteppichs unterschiedlicher Landesvergabegesetze

2.3 Zur Digitalen Souveränität befähigen

Nicht nur Entscheider, sondern alle handelnden Personen in einer Organisation müssen befähigt werden „digitale Themen“ zu verstehen und „digitale Potenziale/Risiken“ auch zu erkennen. Dies gilt in besonderem Maße für die Sicherheitsbehörden. Digitalkompetenz ist eine notwendige Basiskompetenz. Ohne diese Grundvoraussetzung kann es keine sinnvollen, gesamtheitlichen Entscheidungen geben. Damit ein staatliches Handeln auch in Krisensituationen jederzeit gewährleistet ist, müssen Schlüsseltechnologien, wie z.B. Kommunikations- und Sicherheitstechnik, aus vertrauenswürdigen Quellen bezogen werden. Neben wirtschaftspolitischen Erwägungen, wie der Förderung von europäischen oder nationalen Anbietern, ermöglichen europäische oder nationale Lieferanten eine unabhängige Zertifizierung von Qualitäts- oder Sicherheitseigenschaften, z.B. durch das BSI. Weiterhin kann so die Blockade von Technologie- und Kooperationsoptionen durch kurzfristige politische Interessenlagen von Drittstaaten abgefangen werden.
Es muss daher mit Schlüsseltechnologien und Schlüsselfähigkeiten als bewusst avisierte und geplante Optionen im größeren volkswirtschaftlichen Zusammenhang gearbeitet werden. Dort wo Schlüsseltechnologien nicht mehr souverän vorhanden sind, bleiben Schlüsselfähigkeiten (bspw. Schaffung sicherer Gesamtarchitekturen trotz potenziell unsicherer Teilkomponenten) relevant. Dies bedingt ein solides Verständnis der

Nutzerorganisationen von Technologieabhängigkeiten und die Bewertungsfähigkeit von Technologieansätzen und Architekturen.
Interoperabilität und Austauschbarkeit sowie die Fähigkeiten Daten über offene Schnittstellen kontrolliert fließen zu lassen, sind essentielle Eckpfeiler der Datensouveränität im Datenhaus der deutschen Polizei. Es ist wichtig, solche Anforderungen stärker im Auswahl- und Beschaffungsprozess von Produkten und Basistechnologien zu berücksichtigen.

2.4 Zusammenarbeit ermöglichen und Informationsaustausch fördern

Aufgrund des deutschen föderalen Systems existiert in der Öffentlichen Sicherheit eine große Bandbreite an Organisationen, eingesetzten IT Verfahren und letztendlich eine Vielzahl an verteilten und getrennten Anwendungslandschaften und Daten. In weiten Teilen dominieren weiterhin Standard-Büroarbeitsplätze sowie Kommunikationsinfrastrukturen auf Basis von Telefon und Fax. Aktuelle Herausforderungen der öffentlichen Sicherheit, wie z.B. die Sars-Cov-2 Pandemie oder immer wieder auftretende Umweltereignisse (Sturm-, Hochwassersituationen, Waldbrände, ...) zeigen, dass ein aktuelles, einheitliches, konsistentes Lagebild über alle beteiligten Instanzen, einschließlich aller Zwischenebenen (Kommune, Bezirk, Land, Bund) für eine erfolgreiche Zusammenarbeit unerlässlich ist. Die große Aufgabe besteht darin, effektive, digitale und sichere Kommunikationskanäle über alle Ebenen hinweg zu schaffen sowie Anwendungen und Daten einsatz- und benutzergerecht so zu kombinieren, dass entsprechende Lagebilder in Lagezentren auf allen Ebenen entstehen und vorhandene (IT)-Ressourcen effektiv von allen Beteiligten genutzt werden können. Mit der weitgehend automatisierten Erstellung von aktuellen Lagebildern in den einzelnen Lagezentren werden ein ganzheitliches Krisenmanagement und eine bedarfsgerechte schnelle und effektive Reaktion erst ermöglicht. Aus Perspektive der Digitalwirtschaft besteht hier weiterhin großer Handlungsbedarf.

Erste Projekte auf Bundesebene verfolgen den Ansatz vorhandene Verfahren zu konsolidieren, z.B. über die IT-Konsolidierung Bund und Anwendungen, Daten und Ressourcen besser miteinander zu vernetzen. Mit dem Leuchtturmprojekt Polizei2020 zur Konsolidierung der kriminalpolizeilichen Fachanwendungen in Richtung gemeinsamer Entwicklung und Nutzung wird zudem aktuell versucht, die Zusammenarbeit durch Digitalisierung zwischen den Polizeien zu ermöglichen. Diese Projekte berücksichtigen jedoch nicht die vielfältigen Organisationen und Beteiligten im Bevölkerungsschutz.

Damit die Chancen einer vernetzen digitalen Gesellschaft durch die Öffentliche Sicherheit genutzt werden, braucht es einen ganzheitlichen Ansatz, der Digitalisierung und sicheren

Vernetzung föderal organisierter BOS sowie deren Verfahren. Dazu sollte neben der reinen technischen Konsolidierung ein gemeinsames Prozess- und Zusammenarbeitsmodell entlang der Herausforderungen der Öffentlichen Sicherheit entwickelt werden.

Um dieses zu ermöglichen, müssen gemeinsam nutzbare Infrastrukturen wie Netzwerke, Leitstellen und Lagezentren, Rechenzentren sowie interoperable Anwendungen und Datenstrukturen geschaffen werden. Ohne übergreifende Rollen- und Berechtigungsmodelle, eingebettet in einer verlässlichen Cyber-Sicherheitsarchitektur, kann dieser Prozess nicht sicher und Datenschutzkonform etabliert werden.

2.5 Krisenmanagement

Die Corona-Pandemie hat den Bedarf für ein optimiertes internes (Digitalisierungs-) Krisenmanagement aufgezeigt. Neue Systemarchitekturen und dezentrale Arbeits- und Geschäftsprozesse erfordern ein vorbereitetes und robustes internes Krisenmanagement, welches neue Risiken wie Pandemien, Cyberrisiken aber auch Störungen der IT durch Strom- oder Telekommunikationsausfälle berücksichtigt. Die Erreichbarkeit von dezentral angebundenen Mitarbeitern stellt eine wesentliche Voraussetzung für ein effizientes Krisenmanagement dar und muss entsprechend geplant werden.

Dies betrifft besonders die Bereiche:

- Führungsfähigkeit
- Lagemanagement
- Einsatzfähigkeit
- Logistik

Dies erfordert ein Umdenken in Sicherheit und Vertrauen, welches nur durch moderne Technologien unterstützt werden kann. Insbesondere länger andauernde Krisen sollten technisch und organisatorisch vorgeplant werden, damit der Krisenmodus im Home Office weitestgehend dem Arbeitsmodus im Tagesgeschäft entspricht.

2.6 Personal qualifizieren/ Kompetenzen ausbauen

In der Digitalen Welt wandeln sich die Muster des Wissenserwerbs hin zu Kompetenzorientierung und lebenslangem Lernen. Auch für die Mitarbeiter der BOS wird die Digitalkompetenz zu einer Kernkompetenz und damit ähnlich bedeutsam wie fachliche und soziale Kompetenzen. Entsprechend muss in die Weiterbildung und die Qualifikation der Mitarbeiter der Sicherheitsbehörden investiert und die Voraussetzung für lebenslanges und informelles Lernen geschaffen werden. Digitalisierung ist auf allen

Hierarchieebenen als Führungsaufgabe anzusehen. Der öffentliche Dienst bietet seinen Mitarbeitern eine ganze Reihe von Vorteilen, die einschließlich der zahlreichen Weiterbildungs- und auch Weiterentwicklungsmöglichkeiten ganzheitlich bei der Betrachtung eines Berufslebens berücksichtigt werden müssen. Gleichzeitig bleibt eine angemessene Vergütungs- und Besoldungsstruktur im Öffentlichen Dienst, die wesentliche Voraussetzung um IT-Fachpersonal zu werben und zu halten. Gegenseitige Hospitationen zwischen Sicherheitsbehörden und ziviler Wirtschaft, wie sie auch die Sicherheitskooperation Cybercrime vorsieht, fördern das gegenseitige Verständnis und die Kompetenzen der jeweiligen Mitarbeiter.