bitkom

Zukunft der Polizei gestalten

Projektgruppe Zukunft der Polizei

Aktuelle Herausforderung der Polizeibehörden und deren Implikationen

Auf einen Blick

Aktuelle Herausforderungen der Polizeibehörden und deren Implikationen

Ausgangslage

Ca. 99 Prozent der digitalen Straftaten liegen im Dunkelfeld. Von den bekannten digitalen Straftaten werden weniger als 30 Prozent aufgeklärt. Dabei agieren die Täterinnen und Täter immer strukturierter und smart. Dies beeinflusst immer stärker die operative und strategische Arbeit der Polizei.

Es gilt sich diesen Gegebenheiten flexibel anzupassen, um Schritt halten zu können. Dies erfordert strukturelle Reformen und ein Umdenken bei jahrzehntelang bewährten Prozessen, die durch die digitale Transformation zunehmend nicht mehr greifen.

Die Projektgruppe (PG)»Zukunft der Polizeiarbeit des Bitkom agiert interdisziplinär mit Vertreterinnen und Vertretern aus Wirtschaft, Polizei, Wissenschaft und Gesellschaft. Die Projektgruppe widmet sich in einem ersten Ideenpapier, den, durch die Digitale Transformation aktuell drängendsten, Herausforderungen für die Polizeibehörden.

Wer nicht digitalisiert, verliert!

Das Wichtigste

- Um die stetig steigenden Datenmengen, mit denen die Polizeibehörden umgehen müssen, zu bewältigen, bedarf es infrastruktureller, fiskalischer und personeller Anpassungen.
- Das Thema Datenschutz muss konstruktiver umgesetzt werden.
- Eine verstärkte Kooperation zwischen den Behörden und mit der Wirtschaft, ist essentiell, um den neuen Herausforderungen zu begegnen.

Inhalt

Gesamtüberblick 4

1 Herausforderung Verarbeiten großer Datenmengen 6

1.1 Notwendige Ertüchtigung der Infrastruktur von Sicherheitsbehörden 7

1.2 Lösungsansätze bei großen Datenmengen 8

2 Herausforderung Datenschutz und Informationssicherheit 10

2.1 Hemmende Faktoren beim Datenschutz und der Informationssicherheit 11

2.2 Lösungsansätze Faktoren beim Datenschutz und der Informationssicherheit in den Sicherheitsbehörden 13

3 Herausforderungen von Verbund- oder Einzellösungen bei den Sicherheitsbehörden 15

3.1 Verbund- oder Einzellösungen: Anforderungscluster 16

Budget 16

Politik 17

Rechtliche Aspekte 17

3.2 Lösungsansätze bei der Entscheidung Verbund- oder Einzellösungen 17

4 Herausforderungen New Work und Arbeitswelt 4.0 18

4.1 Was spricht für New Work in Sicherheitsbehörden? 21

4.2 Lösungsansätze für New Work in Sicherheitsbehörden 22

Gesamtüberblick

Im Jahr 2021 wurden über 5 047 860 Straftaten in Deutschland festgestellt – das entspricht 4,9 Prozent weniger Taten als im Vorjahr. Über 58,7 Prozent dieser Taten konnten aufgeklärt werden.[1] Gleichzeitig steigt der Anteil digitaler Delikte auf über 124 137 Straftaten im Cyberbereich. Ein Zuwachs von über 12 Prozent. Weniger als 30 Prozent dieser Taten wurden bislang aufgeklärt.[2] Zusätzlich besteht eine hohe Dunkelziffer. Die Dunkelziffer umfasst alle Delikte, die zwar begangen, den Strafverfolgungsbehörden aber nicht bekannt geworden sind. Die Zahlen dazu erscheinen nicht in der offiziellen Kriminalstatistik.[3] Eine Studie aus Mecklenburg-Vorpommern geht insbesondere im digitalen Raum von einer Dunkelziffer von über 99 Prozent aus.[4]

99%

der digitalen Straftaten sind nicht bekannt.

In der analogen Welt erprobte Prozesse und Strukturen kommen immer stärker an ihre Grenzen.

Die digitale Transformation bietet Chancen, stellt jedoch die Gesellschaft und die Sicherheitsbehörden gleichzeitig vor enorme Herausforderungen. Sie verändert die Kriminalitätsformen der analogen Welt und beeinflusst immer stärker die operative und strategische Arbeit der Polizei. Über Jahrzehnte in der analogen Welt erprobte Prozesse und Strukturen, kommen immer stärker an ihre Grenzen oder erreichen ihre Obsoleszenz. Der technologische Wandel vollzieht sich zudem in immer schnelleren Zyklen und erfordert oft neue Ansätze, Plattformen und Lösungen. Das polizeiliche Gegenüber agiert zunehmend technologisch versierter, agiler, arbeitsteiliger und internationaler.

Zentrale Herausforderungen der Polizei und Megatrends in den kommenden Jahren

Sicherheitsbehörden müssen sich diesen Gegebenheiten flexibel anpassen, um Schritt zu halten zu können. Dies benötigt eine strukturierte Vorausschau gegenüber neuen Trends und Technologien sowie aktive Hinterfragung aktueller Strukturen und die Fähigkeit, Erkenntnisse schnell und flexibel umzusetzen. Das gelingt nur im gemeinsamen Schulterschluss zwischen Behörden, Wirtschaft und Wissenschaft und der Etablierung eines digitalen Mindsets. Die Projektgruppe »Zukunft der Polizeiarbeit« des Bitkom, welche aus dem Arbeitskreis »Öffentliche Sicherheit« entstanden ist,

1 Polizeiliche Kriminalitätsstatistik 2021 | Bundesregierung

2 cybercrimeBundeslagebild2021.pdf

3 Endbericht_DuFeStuI_MV.pdf, S. 15.

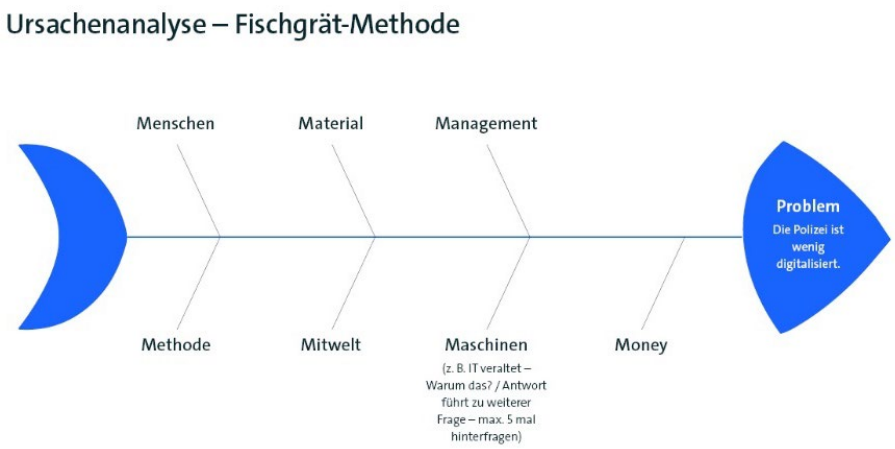
4 Endbericht_DuFeStuI_MV.pdf, S. 67.

adressiert diese aktive Zusammenarbeit. Die PG informierte sich zunächst mit Unterstützung von Zukunftsforscherinnen und -forschern über zukünftige Megatrends, die auf die Gesellschaft einwirken. Anschließend verständigten sich die Beteiligten auf die, für die Polizei relevanten, Megatrends Globalisierung | Mobilität | New Work | Konnektivität und Human Capital, die die Entwicklung der Wissensgesellschaft prägen.

Gemeinsam wurden, durch Vertreterinnen und Vertreter der Polizei und von Unternehmen, aus diesen Megatrends vier zentrale Herausforderungen für die aktuelle Arbeit der Polizei identifiziert: Der Umgang mit immer größeren Datenmengen | Datenschutz | die Abwägung von Einzel- vs. Verbundlösungen | New Work im Rahmen der Polizeiarbeit.

Im Anschluss analysierte die PG diese Herausforderungen in Arbeitsgruppen mit Hilfe der Fischgrät-Methode (Abb.2). Diese ermöglicht es, mittels der sieben »M« (Money Management | Material | Maschinen | Mitwelt | Menschen und Methode), Ursachen von Herausforderungen zu analysieren. Dazu werden vertiefende Fragen angewendet. So kann z. B. unter dem Aspekt »Menschen« gefragt werden: “Wer interessiert sich für das Berufsbild und steht dazu zur Verfügung?”, “Warum finden wir bestimmtes Personal mit relevantem Wissen und Fähigkeiten nicht?”, usw. Diese Ebenen wurden mit bis zu fünf Folgefragen vertieft.

Danach erarbeiteten die Arbeitsgruppen Lösungsansätze mit Hilfe der »Kraftfeldmethode« (Abb.3).



Diese fokussiert sich auf die zentralen hemmenden und förderlichen Faktoren einer Herausforderung und dient der Erarbeitung eines Lösungsansatzes. Die PG agierte dazu iterativ in einem offenen Austausch zwischen Vertreterinnen und Vertretern aus Polizei, Digitalwirtschaft, Wissenschaft und Gesellschaft. Ihnen gilt unser Dank.

1 Herausforderung Verarbeiten großer Datenmengen

Weltweit beträgt das Datenvolumen etwa 64,2 Zetabyte.[5] 2025 werden es laut Europäischer Kommission bereits 175 Zettabyte sein. Das Verarbeiten großer Datenmengen ist bereits heute eine große Herausforderung für die Sicherheitsbehörden, da der Großteil davon unstrukturierte Daten sind. Allein in der Polizei Niedersachsen sind etwa 7,5 Petabyte Daten gespeichert. Diese Menge an Daten würde etwa 150 Millionen Aktenschränke füllen. [6] Durch den weiteren Anstieg an Sensoren, mobilen Endgeräten (Smartphones, Tablets, etc.) sowie den Kapazitäten auf Speichermedien, wird diese Herausforderung weiter steigen. Hinzu kommt, dass sich Kriminalitätsphänomene immer weiter in den digitalen Raum verlagern und Sicherheitsbehörden stärker mit Daten in digitaler Form konfrontiert sind. Dies erfordert den Aufbau von weiteren Behördenkompetenzen, u. a. in der digitalen Forensik und Open Source Intelligence (OSINT). Es stellen sich technische Fragen nach Speicherkapazitäten, Rechenkapazitäten sowie geeigneter Software zur Auswertung dieser Daten. Diese Herausforderungen können nur im Dreiklang aus Politik (Rahmensetzung), Behörden (Durchführung) und Wirtschaft (Digitale Kompetenzen und Ressourcen) konstruktiv und kooperativ gelöst werden. Die Herausforderungen in Bezug auf die Verarbeitung großer Datenmengen werden innerhalb von vier Dimensionen betrachtet.

150 Mio.
Aktenschränke

Würden allein gespeicherte Daten der Polizei in Niedersachsen füllen.

Der Großteil dieser Daten, ist zudem unstrukturiert.

5 Datenmenge explodiert - iwd.de

6 Niedersachsens Polizei kämpft gegen Datenmengen: Hilft KI? | NDR.de - Nachrichten - Niedersachsen

Lösungen durch die Kraftfeldanalyse

1.1 Notwendige Ertüchtigung der Infrastruktur von Sicherheitsbehörden

Cloudmodelle stellen zunehmend den Standard bei der Datenspeicherung, weg von ortsgebundenen Rechenzentren

Die schiere Menge an Daten bringt infrastrukturelle Herausforderungen mit sich, welche nicht mit herkömmlichen Datenträgern abgefangen werden können. Zusätzliche Kapazitäten schaffen Rechenzentren (RZ). Dabei verlieren ortsgebundene RZ, so genannte »On Premise« Rechenzentren, gegenüber Cloudbereitstellungs-modellen zunehmend an Bedeutung. Bis 2025 wird der Colocation-Anteil (d. h. [7] Dies ist für die Behörden, u. a. aus Kosten- und Umsetzungsgründen, ein ernstzunehmender Trend. Bisherige Strukturen fokussieren oft die lokale Nutzung von Daten. Gegebenen-falls besteht die Vorstellung, eigene RZ zu errichten Der Bedarf besteht jedoch darin, vor dem Hintergrund einer länderübergreifenden digitalen Kriminalität und einer immer höheren Datenmenge, ortsungebundene, offene und VS-gebundene Daten ab-rufen zu können. Ein wesentlicher Lösungsansatz sind Cloudlösungen. Als logischen Schritt können die Sicherheitsbehörden erwägen, eigene oder hybride Cloudlösungen anzustreben. Dazu benötigen sie mehrere RZ, um Ausfallsicherheit und Lastverteilung zu gewährleisten. Das bringt erhöhte Kosten mit sich. Auch ist ein hoher Personal-ansatz nötig, um diese RZ zu betreiben. Sicherheitsbehörden müssten sich auf sig-nifikante Investitionen für Sonderlösungen einstellen, wenn sie auf handelsübliche

7 Rechenzentren in Deutschland 2021 (bitkom.org), S.18-19.

kommerziell verfügbare Lösungen, verzichten wollen. Lösungsansätze im Bereich von Cloudinfrastrukturen können insgesamt eine sichere, digitale Souveränität bieten.

Das in Belgien umgesetzte »I-Police-Programm« ist ein Beispiel, wie Behörden neue Strukturen etablieren[8]. Zentralistisch organisierte Data Lakes sind die Voraussetzung, um komplexe Analysen mit verschiedenen Blickweisen auf einen Sachverhalt, zu realisieren.

Eine Vernetzung soll Schnelligkeit schaffen und Redundanzen verhindern. Die Infrastruktur muss gleichzeitig mit einem aktiven Wissensmanagementsystem ausgestattet sein. Die eingesetzte Software muss daher große Datensätze strukturiert und nutzerfreundlich bearbeiten können. Dort entstehende Datenräume sollten auf gemeinsamen Standards (oder Werten, Technologien, Schnittstellen) basieren und die Transaktion von Daten erlauben und befördern.[9]

Die Software stellt somit nicht nur ein Datenhaus zur Verfügung, sondern auch die Voraussetzung, für die sinnvolle Nutzung von mobilen Kommunikationstechnologien (z. B. Edge-Computing). Solche komplexen Systeme lassen sich kaum in Eigenentwicklungen lösen oder gar betreiben. Gerade hinsichtlich geeigneter Software sollte, neben der Digitalwirtschaft, auch eine Einbeziehung innovativer Forschungsinstitutionen stattfinden, um Zugang zu zukunftsfähigen Lösungen zu erhalten.

Dabei ist das Thema der digitalen Souveränität ein wesentlicher Faktor. Sie bedeutet nicht Autarkie, sondern vielmehr die Wahl zu haben, zwischen eigenen Optionen und denen von vertrauensvollen (auch internationalen) Partnerinnen und Partnern.

1.2 Lösungsansätze bei großen Datenmengen

- **Monetäre Herausforderungen meistern**
  Der stets angespannte öffentliche Haushalt staatlicher Stellen verringert sich durch die Corona-Pandemie und internationaler Konflikte nicht nur, er wird auch anders eingesetzt. Notwendige Investitionen sind dadurch schwieriger durchzuführen. Gleichwohl steht der Haushalt gestiegenen Anforderungen gegenüber, u. a. an die Öffentliche Sicherheit und an den Schutz kritischer Infrastrukturen. Digitale Lösungen müssen daher verstärkt Interoperabilität, auf Basis offener Standards, gewährleisten.

- **Personelle Voraussetzungen und Qualifikationen von Behördenpersonal**
  Gleichzeitig ändert sich das Aufgabenprofil der Beschäftigten der Sicherheitsbehörden. Sie werden zusätzlich zu ihren Tätigkeiten, zukünftig u. a. stärker mit dem Auswerten großer Datenmengen konfrontiert sein. Die Ausbildung muss daher in diesem Bereich angepasst werden. Es sollten auch andere Möglichkeiten in Betracht gezogen werden: Der Quereinstieg (entsprechend ausgebildeter Personen) oder

8 »i-Police«, die »digitale Revolution« der belgischen Polizei, wird 300 Mio. € kosten | VRT NWS: nachrichten

9 220531_LF_Data_Mesh.pdf (bitkom.org)

das Einkaufen von externer Fachexpertise sind Möglichkeiten, diesen Herausforderungen zu begegnen.

- **Management der Sicherheitsbehörden-Landschaft**

  Die föderale Struktur in der Bundesrepublik macht die Koordinierung von Aktivitäten der Sicherheitsbehörden nicht einfach. Gerade, weil insbesondere die Polizeiarbeit in die Zuständigkeit der Länder fällt. Nicht alle Daten stehen allen Beteiligten in Bund und Ländern immer zur Verfügung, sodass bei übergreifenden Kriminalitätsphänomenen zum Teil nicht die richtigen Analysen durchgeführt- und Schlussfolgerungen in Ermittlungsprozessen gezogen werden können. Das gilt sowohl im nationalen Raum (über Grenzen der Bundesländer), als auch im inter-nationalen Raum (über Ländergrenzen). Eine zentrale Analyse unter den gegebenen Sicherheitsaspekten, könnte einen großen Mehrwert für die Sicherheitsbehörden enthalten. Gleichzeitig könnten Infrastrukturen dadurch effizienter genutzt werden. Bislang ist eine zentrale, länderübergreifende Datenverarbeitung nur eingeschränkt möglich.

- Digitale Transformation als Querschnittsthema muss ganzheitlich gedacht werden. Datensilos, die früher zu einer effizienten Bearbeitung von Sachverhalten gewählt wurden, müssen aufgebrochen werden. Außerdem müssen Prozesse digital, über den gesamten Wertschöpfungsprozess der Organisation, betrachtet werden. Hier ist das Programm P20 und das geplante zentrale Datenhaus ein erster Ansatz. Zudem gilt es sicherzustellen, dass die Daten im täglichen operativen Einsatz verfügbar sind.

> Datensilos sind zu vermeiden. Ein zentrales Datenhaus wäre ein erster Ansatz

2 Herausforderung Datenschutz und Informationssicherheit

Seitdem das Bundesverfassungsgericht (BVerfG) 1983 in seinem Volkszählungsurteil das Recht auf informationelle Selbstbestimmung als Grundrecht anerkannte, hat der Datenschutz in Deutschland und in Europa erheblich an Bedeutung gewonnen. Die europäische Datenschutzgrundverordnung (DS-GVO) hat das Ziel, einheitliche Datenschutzregeln und somit einheitliche Wettbewerbsbedingungen in Europa zu schaffen. Jedoch sehen 70 Prozent der Unternehmen aufgrund der unterschiedlichen Auslegung der DS-GVO in den Mitgliedsstaaten, noch keinen EU-weiten, einheitlichen Datenschutz. So wird z. B. die Richtlinie zum Datenschutz 2016/680 nicht einheitlich umgesetzt. Die DS-GVO ist kein Punkteplan, den man sich vornimmt und dann einmalig umsetzt. Sie erfordert dauerhafte Anstrengungen, insbesondere bei der Einführung neuer Prozesse und digitaler Technologien. Datenschutzaspekte sollten nicht gelockert werden. Es gilt, Lösungen innerhalb einer Organisation zu finden, die das Potenzial der verfügbaren Daten nutzen und gleichzeitig angemessen auf den Datenschutz eingehen. Der verantwortungsvolle, sichere und rechtmäßige Umgang mit Daten durch Sicherheitsbehörden und eine zeitgemäße gesetzliche Regelung sind die Schlüssel für Innovationen und Vertrauen in eine moderne Polizeiarbeit. Nationale Gesetze wie die Landes- und Bundesdatenschutzgesetze oder europarechtliche Vorschriften, wie die Datenschutzgrundverordnung oder der aktuelle Entwurf der KI-Verordnung, sind hinzugekommen. Diese rechtlichen Vorgaben haben die Anforderungen an die Sicherheitsbehörden im Umgang mit Daten erheblich angehoben. Dies stützt auch die aktuelle Rechtsprechung des BVerfG, bspw. zum Bundeskriminalamtsgesetz (BKAG) 2016, wonach eine Weiterverarbeitung von personenbezogenen Daten nur nach Prüfung der Zulässigkeit einer hypothetischen Datenneuerhebung (HyDaNe) zulässig ist. Die evolutionäre Entwicklung der Kriminalität durch die Megatrends Digitalisierung und Internationalisierung, führt bei Sicherheitsbehörden zu einem Anfall von Massendaten. Dies steigert den Bedarf, diese Daten über die föderalen und nationalen Grenzen hinweg auszutauschen und zu analysieren. Insbesondere aufgrund der zunehmenden Dislozierung von Tatorten, Täterinnen und Tätern und sachbearbeitender Dienststellen, ist eine Erkennung von Redundanzen dringend erforderlich, um Mehraufwand bei Arbeiten zu vermeiden.

> Datenschutzaspekte sollten nicht gelockert werden. Jedoch sollten verfügbare Daten auch angemessen nutzbar sein.
>
> Dazu zählt auch der Austausch von Daten zwischen Behörden, da Tatbestände länderübergreifend

2.1 Hemmende Faktoren beim Datenschutz und der Informationssicherheit

Datenschutz und die Anforderungen an die Informationssicherheit stellen oft einen wichtigen und gleichfalls hemmenden Einflussfaktor für die Zukunft der Polizeiarbeit dar. Dabei stehen die rechtlichen Anforderungen und deren Umsetzung immer wieder den notwendigen Anforderungen an eine sichere und effektive Polizeiarbeit gegenüber und benötigen eine entsprechende Abwägung.

Organisatorisch ergibt sich, durch die föderale Sicherheitsarchitektur im Bereich des Datenschutzes, ein Geflecht zwischen 16 Länderpolizeien, dem Bundeskriminalamt, der Bundespolizei und der Polizei des Deutschen Bundestags sowie den 17 Landesdatenschutzbehörden, der Behörde des Bundesbeauftragten für den Datenschutz und die Informationssicherheit (BfDI) und dem Bundesamt für Sicherheit in der Informationstechnik (BSI). Dies führt mitunter dazu, dass datenschutzrechtliche Fragestellungen unterschiedlich beurteilt werden, was sich insbesondere bei bundesweiten technischen Lösungen als problematisch erweist. Im Bereich der IT-Sicherheit kann grundsätzlich auf einheitliche Regelwerke, wie bspw. den IT-Grund-schutz des BSI oder die IuK-Standards der Polizei, zurückgegriffen werden. Allerdings unterscheiden sich die sogenannten »Allgemeinen Verwaltungsvorschriften zum Geheimschutz« (Verschlusssachenanweisung (VSA) es Bundes und der Länder. Dies führt, insbesondere im Bereich der VS-IT, zu unterschiedlichen Auslegungen der erforderlichen IT-Sicherheitsmaßnahmen. Insbesondere der aktuelle Wandel der Arbeitswelt, zu flexiblen, mobilen und ortsunabhängigen Arbeitsmodellen, führt zu neuen Anforderungen an die Informationssicherheit. Des Weiteren ist vorrangig bei den Themenfeldern Datenschutz, IT-Sicherheit und IT-Technologie festzustellen, dass einer Vielzahl von Bedarfsträgern, einem Mangel an Fachkräften gegenübersteht. Dadurch wird eine interdisziplinäre Bearbeitung der oben genannten Problemstellungen nicht nur deutlich erschwert; sie wird zum Teil, aufgrund von fehlendem Fachwissen, fast unmöglich.

Es gilt daher folgende Hemmnisse anzugehen:

- **Datenschutz und IT-Sicherheit sind oftmals negativ belegt**

  Die partiell zu hörende Meinung lautet: »Datenschutz ist Täterschutz«. Dies legt nahe, dass Anforderungen des Datenschutzes und der IT-Sicherheit in Sicherheitsbehörden oftmals als Hemmnis für die Wahrnehmung der eigenen

Aufgaben gesehen werden. Dies ist nicht der Fall. Der Datenschutz ist ein wichtiger Bestandteil der polizeilichen Arbeit und ist ein Grundprinzip nach dem gehandelt werden muss. Jedoch ist hier immer eine Abwägung zwischen Schutz der Personen und ihren Persönlichkeitsrechten und dem allgemeinen Schutz der Bevölkerung nötig. Diese darf nicht zu Lasten von Einsatzkräften geschehen. Der Datenschutz soll die Arbeit der Sicherheitskräfte erhöhen und Rechtssicherheit schaffen.

- **Intransparenz/ mangelndes Vertrauen**

  Es erfolgt innerhalb der Behörden/ Organisationen wenig offene Kommunikation zur Herstellung von Transparenz, über den Sinn und Zweck von Datenschutz und IT-Sicherheit. Oftmals fehlt es an einem direkten und vertrauensvollen innerbehördlichen Austausch sowie dem Austausch zwischen Behörden und den Datenschutzaufsichtsbehörden.

> Zu einer Vielzahl von Fragestellungen im Datenschutz existieren noch keine rechtlichen Positionen

- **Fachkräftemangel – Stellenmangel**

  Die behördlichen Datenschutzbeauftragten sowie die IT-Sicherheitsbeauftragten sind personell oft zu schlecht aufgestellt, um ihrer Beratungsleistung adäquat gerecht zu werden. Des Weiteren sind auch Fachkräfte mit dem polizeispezifischen Fachwissen in den Themenfeldern Datenschutz und IT-Sicherheit kaum vorhanden, bzw. können beiden Anforderungen im gleichen Maße nicht gerecht werden.
  In der digitalen Welt wandeln sich die Muster des Wissenserwerbs hin zu Kompetenzorientierung und lebenslangem Lernen. Auch für die Mitarbeitenden der Polizeibehörden wird die Digitalkompetenz zu einer Kernaufgabe und damit ähnlich bedeutsam wie fachliche und soziale Kompetenzen. Entsprechend muss in die Weiterbildung und die Qualifikation der Mitarbeitenden der Sicherheitsbehörden investiert- und die Voraussetzung für lebenslanges und informelles Lernen geschaffen werden.

> Digitalkompetenz wird zunehmend zur Kernkompetenz im Dienstalltag

- **Steigende rechtliche Anforderungen**

  Im Bereich des Datenschutzes sind zunehmend föderale, nationale und supranationale Regelwerke zu beachten (u. a. die Europäische Datenschutzgrundverordnung (DSGVO), das Bundesdatenschutzgesetz (BDSG) sowie Verfahrensgesetze und die Landesdatenschutzgesetze, bzw. die Polizeigesetze). Diese enthalten zahlreiche Regelungen, welche Anforderungen bei der Verarbeitung personenbezogener Daten zu beachten sind, um diese Daten angemessen und wirksam zu schützen.
  Des Weiteren führen eine Vielzahl von Rechtsauslegungen zum Datenschutz, durch gerichtliche Urteile sowie verfassungsrechtliche Entscheidungen, zu einer zunehmenden Rechtsunsicherheit bei den Beteiligten. Zu einer Vielzahl der neuen datenschutzrechtlichen Fragestellungen existieren überhaupt noch keine rechtlichen Positionen, da diese erst entwickelt werden müssen.

- **Föderale Gesetzlagen**

  In bundeslandübergreifenden Projekten kommt es zu unterschiedlichen Interpretationen und Auslegungen der jeweiligen Rechtslage. Dies führt dazu, dass zeitintensive Einigungen und Abstimmungen mit einer Vielzahl von Akteuren herbeigeführt werden müssen.

2.2 Lösungsansätze Faktoren beim Datenschutz und der Informationssicherheit in den Sicherheitsbehörden

- **Die Kultur muss sich ändern**

  Der Datenschutz ist ein Enabler und kein Disabler. Die mit dem Datenschutz beauftragten Behörden, müssen sich auch als entwickelnde und beratende Instanzen sehen und nicht nur als Aufsichtsbehörden oder Regulatoren. Im Gegenzug müssen die anderweitig beteiligten Behörden, auf diesem gemeinsamen Weg, den Datenschutz als Partner kennenlernen, der die Möglichkeit bietet, gemeinschaftlich rechtskonforme Lösungen zu entwickeln. Durch die Schaffung eines gemeinsamen Verständnisses und die frühzeitige Einbindung und Berücksichtigung der beiden Perspektiven, kann ein gemeinsames Verständnis und mehr Transparenz geschaffen werden. Für die Industrie, Kleine und Mittelständische Unternehmen (KMU) und Startups bestehen hier – neben der Umsetzung adäquater Lösungen – auch neue Potentiale, u. a. durch den Einsatz von künstlicher Intelligenz.

- **Stringente Beachtung des Grundsatzes von »Design«**

  Behördliche Datenschutzbeauftragte und IT-Sicherheitsbeauftragte müssen bereits in der Planung in die IT-Projekte eingebunden werden. Eine proaktive Begleitung der Vorhaben ist zu gewährleisten. Dadurch wird »Privacy und Security by Design« umgesetzt. Dies kann im Schulterschluss zwischen Wirtschaft und der Behördenlandschaft, z. B. über Wirtschaftsverbände, als neutrale Dialogplattform im vorwettbewerblichen Raum unterstützt werden.

- **Technische Unterstützung der behördlichen Datenschutzbeauftragen**

  Behördliche Datenschutzbeauftragte haben gemäß Art. 39 DSGVO, die Aufgabe der Unterstützung, Beratung und Kontrolle aller Behördenbediensteten. Es stellt sich die Frage, inwieweit die behördlichen Datenschutzbeauftragten durch Technik, bei der Wahrnehmung ihrer Kontrollaufgabe, unterstützt werden können. Beispielsweise sind Systeme denkbar, die automatisiert Anomalien bei der Datenverarbeitung detektieren und entsprechende Reports erstellen (analog eines Security Information and Event-Management (SIEM)). Hier könnten, in gemeinsamen Workshopformaten mit der Wirtschaft, adäquate Lösungen erarbeitet werden.

- **Förderale Regulatorik durch nationale Regelungen harmonisieren**

  Die entsprechenden Normen für die Datenverarbeitung sind fortzuentwickeln und rechtlich zu harmonisieren, um die Ziele der Saarbrücker Agenda zu erreichen. Für den Einsatz von neuen Technologien bedarf es modernen, bereichsspezifischen und hinreichend bestimmten Befugnisnormen, um Innovationen nicht zu gefährden.

- **Kommunikation zwischen den Sicherheitsbehörden und den Datenschutzbehörden muss verbessert werden**

  Ein regelmäßiges, nationales Austauschformat zwischen Sicherheitsbehörden und Datenschutzaufsichtsbehörden dürfte geeignet sein, um das Vertrauen zwischen

den beteiligten Organisationen zu stärken und insgesamt die Transparenz zu erhöhen.

- **Fachkräftemangel begegnen – Stellenpläne anpassen**

  Auf Leitungsebene muss der erhöhte Bedarf an Fachkräften im Datenschutz- und IT-Sicherheitsbereich erkannt- und im Stellenplan abgebildet werden. Gleichzeitig bleibt eine attraktive Vergütungs- und Besoldungsstruktur im Öffentlichen Dienst die wesentliche Voraussetzung, um Fachpersonal zu werben und zu halten. Auch Fortbildungen könnten, gemeinsam mit der Wirtschaft, erfolgen. Deren Produkte müssen letztendlich auf die behördlichen Anforderungen abgestimmt sein. Digitalisierung ist auf allen Hierarchieebenen als Führungsaufgabe anzusehen. Der öffentliche Dienst bietet seinen Mitarbeitenden eine ganze Reihe von Vorteilen. Diese müssen, zusammen mit den zahlreichen Weiterbildungs- und auch Weiterentwicklungsmöglichkeiten, ganzheitlich bei der Betrachtung eines Berufslebens berücksichtigt werden. Gegenseitige Hospitationen zwischen Sicherheitsbehörden und ziviler Wirtschaft, wie sie auch die Sicherheitskooperation Cybercrime vorsieht, fördern das gegenseitige Verständnis und die Kompetenzen der jeweiligen Mitarbeitenden. Auch könnte die Nutzung neuer Technologien (z. B. KI) unterstützend eingesetzt werden, um Personalressourcen zu entlasten. Auch sollte ein kollaborativer und länderübergreifender Einsatz von Fachpersonal im Bereich Datenschutz- und Informationssicherheit, nach dem »Once-Only-Prinzip«, forciert und gefördert werden.

> Fehlende Fachkräfte im Datenschutz- und IT-Sicherheitsbereich müssen zunächst im Stellenplan abgebildet werden.

3 Herausforderungen von Verbund- oder Einzellösungen bei den Sicherheitsbehörden

Die Organisation der Polizei ist, gemäß der föderalen Strukturen, Ländersache. Daher stellt sich im Bereich der Polizeien immer wieder die Frage nach Einzel- oder Verbundlösungen. Die Polizei steht vor den größten Veränderungen der letzten Jahrzehnte. Mit dem Programm »P20« sollen Prozesse vereinheitlicht werden. Mit der Modernisierung und Konsolidierung der IT-Landschaft der Sicherheitsbehörden von Bund und Ländern, soll ein gemeinsames »Datenhaus« entstehen. Damit verbunden sind weitere neue Systeme und Neuvergaben, z. B. bei »Inpol-neu« (ein vom BKA betriebenes, bundesländerübergreifendes, personengebundenes Informationssystem). Dabei kommt es immer wieder zu gravierenden Herausforderungen, wie beim Polizeilichen Informations- und Analyseverbund (*PIAV*). Bei diesem kommt es zu erheblichen Mehraufwänden und unbrauchbaren Analysedaten. Die Erfahrungen der Länder zeigen, dass ein einheitliches Vorgehen herausfordernd ist. Dabei spielen Souveränitätsvorbehalte sowie wirtschaftspolitische Überlegungen eine Rolle.

Bei landesspezifischen Programmen besteht die Möglichkeit, lokale Wirtschaftsakteure zu fördern.Programme auf Bundesebene tun dies nicht immer. Außerdem agieren die Sicherheitsbehörden in einer heterogenen Prozesslandschaft, was eine einheitliche Gestaltung von IT-Lösungen verzögert, statt Schnittstellen zu schaffen, um einmal entwickelte Lösungen in der Fläche auszurollen. Dennoch erfordern Ressourcenknappheiten bei Personal und Haushaltsmitteln bessere Lösungen und Methodiken. Dafür müssen Ressourcen gebündelt werden. Somit startet »P20« als Verbundprojekt bereits mit Vergabeverfahren und wird zukünftig auch praktisch angegangen. Dies geschieht mit unzähligen Anlagen und Auflagen, welche auch viele heimische Unternehmen, darunter vor allem KMU, ausschließen.

Auch in verwaltungsübergreifenden Bereichen, wie dem Online-Zugangs-Gesetz (OZG) und dem geforderten Portalverbund von Bund, Ländern und Kommunen sowie einheitlichen IT-Sicherheitsstandards, wird aktuell viel getan. Aber einzelne finanzstarke Länder wählen immer wieder den Weg der Einzellösung: z. B. Hybride integrative Plattform Polizeilicher Sondernetze (HiPos).[10]

10 NRW Police Cloud: The quantum leap for cybercrime forensics (t-systems.com)

3.1 Verbund- oder Einzellösungen: Anforderungscluster

Die Abwägung von Verbund- vs. Einzellösungen ist nicht einfach. Während der Überlegungen der PG »Zukunft der Polizeiarbeit« des Bitkom, haben sich vier Themenfelder herauskristallisiert, welche die Entscheidung maßgeblich beeinflussen: Innovationsfähigkeit | Budget | Politik | Rechtliche Aspekte.

Es gilt zu klären, welche Fähigkeiten die Sicherheitsbehörden haben, um allein Innovationen zu entwickeln- bzw. diese umzusetzen. Im Gegenzug ist die Frage zu klären, wie agil ein gemeinsamer Verbund Innovationen managen kann. Dabei ist zu beachten, dass Sicherheitsbehörden mit einem geringen Personalkörper, bzw. mangelnden fachlichen Kompetenzen, sich scheuen auf Verbundlösungen zurückzugreifen, da sie eine Überforderung befürchten. Auch spielt die Frage nach der Umsetzungsgeschwindigkeit eine Rolle. Agiert hier der Verbund mit seinen diversen Abstimmungsschleifen schneller als die Einzellösung, gerade bei zeitkritischen Umsetzungsbedarfen?

Budget

Das Agieren im Verbund offeriert meist für die Sicherheitsbehörden unterschiedliche Budgets, u. a. auf Bundes- oder EU-Ebene. Diese sind auch an Umsetzungskriterien gekoppelt. Dies kann die Handlungsfreiheit einschränken. Die Suche nach diversen Fördertöpfen und deren rechtssicherer Handhabung kann dabei viele personelle Ressourcen binden. Allerdings steht die Frage im Raum: “Ist es sinnvoll, pro Bundesland, Polizei, etc. unzählige lokale Lösungen und »Daten-Töpfe« mit diversen Einzelforderungen zu etablieren, die wiederum die Digitalwirtschaft und deren Personalressourcen überfordern?” Insbesondere innovative Lösungen von KMU, darunter auch Startups, würden ausgeschlossen, da sie nicht über die personellen Ressourcen zur Bearbeitung der individuellen Anforderungen verfügen. Durch Einmalentwicklung und eine geregelte, lizenzierte Nachnutzung durch mehrere Partner, könnten hier fiskalische Vorteile geschaffen werden. Auch könnten bundesländerübergreifende Rahmenverträge Kosten einsparen, möglichst viele Unternehmen einbinden und den Sicherheitsbehörden Flexibilität verschaffen.

Politik

Poltische Prozesse sind geprägt von den Prinzipien »Teilhabe« und »Kompromiss«. Somit ist die Einbeziehung relevanter Bedarfsträger und Dienstleister und damit verbundene Abstimmungen und Abwägungen von Einzelinteressen, Bestandteil des Prozesses. Je mehr Akteure einbezogen werden, umso komplexer werden Vorgänge. Auch besteht die Gefahr der Verwässerung von Forderungen, um einen möglichst breiten Konsens zu erwirken. Vor dem Hintergrund der Digitalen Transformation, mit den damit verbundenen schnelllebigen Innovationszyklen, ist fraglich, ob herkömmliche, politisch-bürokratische Abstimmungen geeignet sind, um über digitale Fachthemen zu entscheiden. Zu empfehlen ist eine allgemeine politische Festlegung auf Ziele, die mit IT-Lösungen erreicht werden sollen und eine anschließende Umsetzung- und Übertragung der Entscheidungsgewalt auf fachlicher Ebene. Dies impliziert auch die Etablierung bestimmter Standards und Datenformate. Hierbei sollten gemeinsame Ziele und innovative Lösungsansätze, als landes- oder behördenspezifische Anforderungen, im Vordergrund stehen.

> Es ist fraglich, ob die Digitale Transformation durch herkömmliche politisch/ bürokratische Prozesse bewältigt werden kann.

Rechtliche Aspekte

Die Erhebung, Nutzung, Speicherung und Verteilung von Daten sind an hohe rechtliche Standards gebunden, u. a. an den Datenschutz und die IT-Sicherheit. Gemeinsame Lösungen stellen dabei oft neue Ansätze dar, die auch weiteren rechtlichen Anforderungen, wie zum Beispiel Einsatz künstlicher Intelligenz nach deutscher und europäischer Rechtsprechung, gerecht werden müssen. Dabei muss geklärt werden wie, ob und welche Daten und Prozesse ausgetauscht werden, bzw. wer darauf zugreifen kann. Gleichzeitig ist Transparenz erforderlich (siehe Abschnitt Datenschutz und Informationssicherheit).

3.2 Lösungsansätze bei der Entscheidung Verbund- oder Einzellösungen

Für eine Verbundlösung von Systemen sprechen viele Faktoren: So könnten Budget- und Personalressourcen effizienter eingesetzt werden und durch Kollaborationen können gemeinsame Standards beim Datenschutz, Datenformaten oder Zertifizierungen erreicht werden. Jedoch bedarf dies einer ausgeprägten Teamkultur und der Bereitschaft, eigene Prozesse und Strukturen anzupassen. Gerade ein einheitliches Ökosystem, Schnittstellen und gemeinsame Vertragsstandards bedeuten schnellere Produkt- und Vertragslösungen. Dadurch werden auch interoperable, lokale Einzellösungen, ermöglicht.

Standardisierung führt zu einheitlicher Information. Dabei können auch verstärkt innovative Lösungen von KMU genutzt werden. Allerdings besteht die Gefahr, ineffektive Strukturen, durch mangelnde Mittel, zu zementieren. Dies kann die nötige Handlungsfähigkeit, vor dem Hintergrund einer digitalen, internationalen Kriminalität, einschränken.

Einzellösungen können es auch der Digitalwirtschaft erschweren, innovative Lösungen anzubieten, da diverse Landesgesetze für sie überfordernd wirken oder sie explizit

andere Technologien ausschließen. Hierbei gilt es sogenannte »Lock-In« Effekte zu vermeiden. Lösungen müssen stets nutzerzentriert gestaltet werden. Nutzerinnen und Nutzer verfahren meist nach dem Grundprinzip der Datenverarbeitung: EVA (Eingabe – Verarbeitung – Ausgabe). Das bedeutet, dass Nutzerinnen und Nutzern, die Hintergründe von Lösungen egal sind. Sie benötigen ein verständliches, einfach zu bedienendes System, was ihren Arbeits- und Dienstalltag erleichtert. Hierfür müssen einige Voraussetzungen geschaffen werden – seitens des Bundes oder der Länder. Dazu zählen u. a. klar definierte Datenstandards, einheitliche Register/Datenbanken und das Bereitstellen von interoperablen Services. Dann könnte »Einer für Alle« funktionieren und die Vorteile aus beiden Welten (Verbund- & Einzellösungen) kombiniert werden schnell einzeln, mit hoher Innovationskraft entwickeln, anschließend auf alle Mitglieder ausrollen, um Effizienz und Synergien zu heben.

Einheitliche Richtlinien könnten erarbeitet werden. Diese sollten klären: Wann Einzel- oder Verbundlösungen ratsam sind. Dabei stehen die Fragen im Raum, wie schnell die Zielerreichung gewünscht ist, wie viele Kompetenzen oder Budget verfügbar sind und ob es sinnvoll ist, bestehende Prozesse und Systeme anzupassen. Es müssen zudem finanzielle und politische Anreize für die Teilnahme an Verbundlösungen geschaffen werden. Zusammen mit der Bündelung von Kompetenzen bieten sich Vorteile für alle Seiten. Dies sollte gemeinsam in einer Projektgruppe, bestehend aus Vertreterinnen und Vertretern der Verwaltung, Politik und Wirtschaft, angegangen werden.

> Ein einheitliches Ökosystem/Schnittstellen und gemeinsame Vertragsstandards bedeuten schnellere Produkt- und Vertragslösungen

4 Herausforderungen New Work und Arbeitswelt 4.0

Neue Prozesse und Technologien verändern nicht nur unsere Wirtschaft, sondern auch die Art und Weise, wie wir heute und in Zukunft arbeiten werden. Sie führen zu einem stärkeren Produktivitätswachstum, besseren Dienstleistungen und können den Arbeitsalltag erleichtern. Sie ermöglichen neue Geschäftsmodelle und innovative Arbeitsweisen, die, sowohl Arbeitgebern als auch Arbeitnehmerinnen und Arbeitnehmern, mehr Flexibilität bieten. Die digitale Transformation der Arbeitswelt ist eine gesamtgesellschaftliche Aufgabe. Dabei verändern sich auch Arbeitsformen, Arbeitsinhalte und Berufsbilder. Die digitalisierte Arbeitswelt ist gekennzeichnet von einem großen Bedürfnis nach Souveränität und Flexibilität, weniger Hierarchie und Bürokratie sowie ständiger Veränderung. Mit den Arbeitsinhalten verändern sich auch die Anforderungen an Arbeitnehmerinnen und Arbeitnehmern. Deshalb sind Maßnahmen zu ergreifen, die den vielfältigen Herausforderungen, bedingt durch den digitalen, kulturellen oder demografischen Wandel, Rechnung tragen. Relevante Handlungsfelder liegen vor allem in folgenden Bereichen: allgemeine Bildung und Weiterbildung, Fachkräftesicherung und Arbeitsrecht, einschließlich Regelungen zur Vereinbarkeit von Privatleben und Beruf.

> New Work ist mehr als nur mobiles Arbeiten.
>
> Es entstehen neue Anforderungen an Führung, Handeln und das Wissen über neue Technologien.

Es sind aber nicht nur die politischen Rahmenbedingungen, die den Wandel beeinflussen. Für einen erfolgreichen Transformationsprozess ist auch Offenheit für eine veränderte Kultur, bei Unternehmen, Behörden und Beschäftigten gefragt.[11]
Um das Thema in Bezug auf die Sicherheitsbehörden zu betrachten, sollte zunächst klar sein, dass vermutlich jeder etwas anderes unter »New Work« versteht. Bekannte Stichworte sind: mobiles Arbeiten | flexiblere Arbeitszeiten | steigende Digitalisierung | Work-Life-Balance, usw.

Wissenschaftlich betrachtet ist »New Work« aber kein Synonym für die oben genannten Punkte. Stattdessen ist es ein Mindset zum Paradigmenwechsel. Ausgehend vom Konzept des österreichisch-US-amerikanischen Philosophen Frithjof Bergmann, sollten Menschen das tun, was sie wirklich wollen. Dem würden Sinn und Effizienz praktisch folgen. »New Work« oder die »Arbeit der Zukunft« sind eben nicht nur geprägt durch mobiles Arbeiten. Sie umfasst vielmehr die Fähigkeit, neue Organisationsstrukturen umzusetzen, in denen Mitarbeitende sich, gemäß ihrer Fähigkeiten, entfalten und einer sinnstiftenden Tätigkeit nachgehen können. »New Work« ist demnach zunächst »New Leadership«. Führungskräfte entwickeln bestmögliche Rahmenbedingungen und motivieren Mitarbeitende, damit diese ihr volles Potenzial entfalten können.

Dazu benötigen Führungskräfte auch Wissen um neue Technologien.

Sie brauchen Antworten auf die Frage, welche Technologien in ihrem Bereich eigentlich eingesetzt werden sollen: KI-Lösungen? Big Data-Analysen? Was ist das eigentlich genau und was heißt das für den jeweiligen Bereich? Sie müssen Mitarbeitenden erklären können, wie sich die eingesetzten neuen Technologien auf Arbeitsplatz und Berufsprofil auswirken und welche Weiterbildungen nötig werden. Auch Mitarbeitende müssen die Bereitschaft entwickeln, Dinge auszuprobieren und miteinander zu lernen. Daher sollten Führungskräfte und Mitarbeitende den Prozess der digitalen Transformation gemeinsam gestalten.

> Weiterbildungen sollten sich auch nach Interessenlagen der Beschäftigten richten. Ein breites Spektrum an Bildung erhöht die Beschäftigungsfähigkeit insgesamt.

Darüber hinaus werden ethische Fragestellungen für Führungskräfte eine immer größere Rolle spielen: Vieles, was wir uns heute vorstellen können, wird technologisch irgendwann machbar sein. Daher ist es eine Komponente von Digitalleadership, zu reflektieren, welche Technologien in den Sicherheitsbehörden eingesetzt und welche nicht eingesetzt werden sollen.[12]

Gerade in den Sicherheitsbehörden ist die Frage nach dem Sinn ihrer Arbeit vergleichsweise leicht zu beantworten, da dies schon im Vorfeld entscheidend bei der Berufswahl ist. In Bezug auf Entwicklungsmaßnahmen gilt es jedoch, tiefgreifendere Maßnahmen umzusetzen. Sicherheitsbehörden agieren in Hierarchien. Entwicklungsangebote orientieren sich meist nach Laufbahnen, anstatt nach individuellen Fähigkeiten. Weiterbildungen richten sich daher oft nicht nach den Interessenlagen der Beschäftigten, sondern dienen Personalentwicklungszwecken. Weiterbildungen im breiten Spektrum der Belegschaft sind jedoch der Schlüssel zur

11 Bitkom Positionspapier_Future of Work (bitkom.org)

12 Bitkom Positionspapier_Future of Work (bitkom.org), S.4

Stärkung der Beschäftigungsfähigkeit und auch ein Weg, um dem Mangel an Fachkräften zu begegnen. Hier muss eine gewisse Durchlässigkeit bzgl. der persönlichen Weiterentwicklungsmöglichkeiten bestehen Dadurch werden zu starre Grenzen zwischen den verschiedenen Laufbahnmöglichkeiten aufgehoben und persönliche und fachliche Weiterentwicklungsmöglichkeiten realisierbar.

Im Punkt soziale Verantwortung gilt es, Standards hervorzuheben und diese zu leben. Bei den Punkten »Freiheit« und »Selbstverantwortung« sollte auch bei Sicherheitsbehörden Raum geschaffen werden, um neue Wege zu gehen. So agiert z. B. das Innenministerium Nordrhein-Westfalen bei Innovationsthemen nach diesem Prinzip. Das in Duisburg geschaffene »Innovation Lab« der Polizei kann hier u. a. auch neue Technologien erproben, zu denen es noch keinen konkreten Bedarfsfall in der Polizei gibt. Auch Hessen und Niedersachsen haben solche Innovationshubs für die Polizei geschaffen. Andere Sicherheitsbehörden, wie die Bundeswehr, verfügen ebenfalls über solche Einrichtungen. Zwischen diesen Innovationslaboren sollten Synergien geschaffen werden. Dies ist nötig, denn oftmals können so erst Bedarfe entdeckt werden. Frei nach dem, angeblich von Henry Ford stammenden, Motto: »Wenn ich die Leute gefragt hätte, was sie wollen, hätten sie geantwortet: schnellere Pferde.« Dies verdeutlicht nur, dass Menschen an Bewährtem festhalten und sich schwer zukünftige Alternativen vorstellen können.

Dazu benötigen die Sicherheitsbehörden auch agile Arbeitsmethoden und ein digitales Mindset, verbunden mit einer toleranten Fehlerkultur. Agilität bezeichnet die Fähigkeit, schnell, effektiv und gewinnbringend auf sich ändernde Gegebenheiten reagieren zu können. Dies benötigt verschiedene Rahmenbedingungen bezüglich der Führungsebene, der Mitarbeitenden und der Behördenkultur. Wenn diese »Future of Work-Empfehlungen« für den Arbeitsmarkt von morgen gelingen, können Bürgerbezug sowie Produktivitätssteigerungen realisiert werden. Agile Teams erarbeiten sich in einem kreativen und innovativen Prozess, ihre Aufgabenstellung selbst – und parallel sofort die Lösung. Durch die Vernetzung im agilen Team können die kollektiven Erfahrungen bei der Entscheidungsfindung und Problemlösung genutzt werden. Zudem zählt die Förderung durchlässiger Hierarchien zu den agilen Kriterien und Verfahren, die schnell und flexibel Veränderungen im Markt aufnehmen und darauf adäquat reagieren können. Agile Prinzipien wie »Transparenz« und »Selbstorganisation« reduzieren also die Notwendigkeit von Weisungen traditioneller, strenger hierarchisch organisierter Formen der Zusammenarbeit. Aufgaben werden also »vom Team selbst« entwickelt und nicht angewiesen. Die Umstellung auf agile Methoden betrifft auch die Zusammenarbeit von Sicherheitsbehörden mit externen Expertinnen und Experten, die sie z. B. bei IT-Projekten unterstützen. Um agile Methoden optimal umsetzen zu können, müssten Externe jedoch partiell Teil des Teams sein. Dabei kreiertes Wissen sollte in der Behörde verbleiben und nutzbar gemacht werden. Ein Weg, dies praktisch umzusetzen, bieten aktiv gestaltete Hospitationsprogramme zwischen Behörden oder auch Behörden und Industrie. Einen bestehenden Rahmen dazu böte z. B. die Sicherheitskooperation »Cybercrime« zwischen dem Bitkom und den Landeskriminalämtern Nordrhein-Westfalen, Hessen, Rheinland-Pfalz, Niedersachen, Baden-Württemberg und Sachsen. Dabei ginge jedoch der Austauschbedarf über das Thema Cybercrime hinaus. Innerhalb der Polizei treffen eine Vielzahl verschiedenster Tätigkeitsbereiche aufeinander, die in einem New Work-

Ansatz einzeln betrachtet werden müssen: Verwaltung/IT | Labor/Forensik/KTU | Einsatz | unterstützende Tätigkeiten.

Diese Aspekte treffen auf heterogene Arbeiten, Altersstrukturen und bestimmte Erwartungen bei Mitarbeitenden. Auch erlauben es bestimmte Bereiche aus Sicherheitsgründen nicht, dass Arbeit aus dem Homeoffice verrichtet werden darf.

Anwendungsgebiete von New Work bei der Polizei ist mehr als nur flexibles Arbeiten

-7%

potentiell weniger Berufstätige bis 2040. New Work ist daher essentiell, um die Attraktivität der Sicherheitsbehörden zu steigern.

Dabei böte zumindest der Stand der Technologie durchaus Möglichkeiten. So existieren bereits VS-kompatible Hardware und VS-sichere Cloudlösungen, auch unter Beachtung datenschutzrechtlicher Aspekte. Dazu bedarf es jedoch gesetzlicher Anpassungen, sowie Vertrauen, dass unbefugte Dritte keine Daten einsehen können. Manche Bereiche, wie komplexe Ermittlungen im Bereich der organisierten Kriminalität oder Kinderpornographie, sind hier besonders sensibel.

4.1 Was spricht für New Work in Sicherheitsbehörden?

Für die Wirtschaft ist New Work mittlerweile Standard. Damit steht die Wirtschaft in Konkurrenz mit den Sicherheitsbehörden. Die Notwendigkeit für New Work in den Sicherheitsbehörden ergibt sich damit nicht nur vor den Hintergründen der Corona-Pandemie, die ein dezentrales Arbeiten erforderlich machte. Der demographische Wandel und der damit verbundene Fachkräftemangel sowie der »War for Talents« betrifft alle. Dabei geht es vor allem um Effektivität und Effizienz von Prozessen und die Nutzung von Ressourcen. New Work kann der Effizienzsteigerung der Behörden dienen. Derzeit sind die Bewerberzahlen der Polizei, z. B. in Nordrhein-Westfalen, noch gut. Jedoch werden sich sinkende Geburtenjahrgänge und die Rekrutierung anderer Sicherheitsbehörden, wie der Bundeswehr, ggf. negativ auswirken.[13] So werden allein bis 2040 die Zahl der 20 – 67-Jährigen um sieben Prozent sinken, bis 2060 sogar um über elf Prozent.[14]

13 Ausbildung bei der Polizei jetzt auch ohne Abitur - Landespolitik - Nachrichten - WDR

14 Ergebnisse der 14. koordinierten Bevölkerungsvorausberechnung - Statistisches Bundesamt (destatis.de)

Die Generation Z ist zudem geprägt durch die Neugierde und das Hinterfragen von Normen und eine hohe Technikaffinität. Hinzu kommt, dass, generationsunabhängig, der Wunsch nach Work-Life-Balance immer stärker wird.

Auch der Druck durch höhere Ansprüche an die Digitalisierung (zur Bekämpfung von Cybercrime und durch die allgemeine Erwartung der Bevölkerung) sowie durch soziale und umweltpolitische Standards zu punkten, wird für die Polizeien größer.

4.2 Lösungsansätze für New Work in Sicherheitsbehörden

Im Bereich New Work müssen gesetzliche Reglungen angepasst werden. Dabei gilt es, polizeiliche Belange zu berücksichtigen. Dies ist eine klare Führungsaufgabe.
Diese Aufgabe impliziert die Einbeziehung aller Hierarchieebenen sowie Pro- und Contra-Argumentationen. Das Thema New Work ist auch ein Beispiel für länderübergreifende Zusammenarbeit, um Redundanzen bei negativen Erfahrungen zu vermeiden und iterativ dazu zu lernen. Best-Practice-Beispiele aus dem In- und Ausland dienen der Offenlegung von Möglichkeiten. Es bedarf dazu einer gelebten Fehlerkultur, bei der nicht alles auf Anhieb funktioniert, doch die Option für Versuche besteht. Dies impliziert Prozesse und Strukturen im Gesamtüberblick zu hinterfragen.
Die Ernennung eines Chief-Digital-Officers (CDO), welcher Initiativen wie Innovations- oder Datenlabore initialisiert, Strukturveränderungen entwirft und mit fundiertem politischem Mandat umsetzen kann, ist dazu Grundvoraussetzung für den Erfolg. Der CDO bedarf auch eines entsprechenden Teams, um Projekte unterstützend umzusetzen. Dies impliziert ausreichende Budget-Mittel. Ausschreibungen sollten nur mit Bedarfen und nicht mit dezidierten Produktanforderungen umgesetzt werden.
Zudem muss in dem Bereich der technischen Lösungen und Endgeräte, neuen Anforderungen an das New Work im Fokus stehen. So müssen beispielsweise, unter Berücksichtigung der IT-Sicherheitsanforderungen, auch flexiblere Arbeitsmodelle und -formen möglich sein. Dies geht nur mit einer geeigneten Kommunikationsinfrastruktur und entsprechenden Endgeräten. Arbeitsstrukturen- und Prozesse müssen dafür angepasst werden. Dies erfordert die angesprochene Flexibilisierung.

Bitkom vertritt mehr als 2.000 Mitgliedsunternehmen aus der digitalen Wirtschaft. Sie erzielen allein mit IT- und Telekommunikationsleistungen jährlich Umsätze von 190 Milliarden Euro, darunter Exporte in Höhe von 50 Milliarden Euro. Die Bitkom-Mitglieder beschäftigen in Deutschland mehr als 2 Millionen Mitarbeiterinnen und Mitarbeiter. Zu den Mitgliedern zählen mehr als 1.000 Mittelständler, über 500 Startups und nahezu alle Global Player. Sie bieten Software, IT-Services, Telekommunikations- oder Internetdienste an, stellen Geräte und Bauteile her, sind im Bereich der digitalen Medien tätig oder in anderer Weise Teil der digitalen Wirtschaft. 80 Prozent der Unternehmen haben ihren Hauptsitz in Deutschland, jeweils 8 Prozent kommen aus Europa und den USA, 4 Prozent aus anderen Regionen. Bitkom fördert und treibt die digitale Transformation der deutschen Wirtschaft und setzt sich für eine breite gesellschaftliche Teilhabe an den digitalen Entwicklungen ein. Ziel ist es, Deutschland zu einem weltweit führenden Digitalstandort zu machen.

Herausgeber
Bitkom e.V.
Albrechtstr. 10 | 10117 Berlin

Ansprechpartner
Stephan Ursuleac | Referent Verteidigung & Öffentliche Sicherheit
M +49 151 148 24 836 | Email: s.ursuleac@bitkom.org

Verantwortliches Bitkom-Gremium
AK Verteidigung