accenture

POLIZEIARBEIT

KOMPLEXER KRIMINALITÄT DIGITAL AUF DIE SCHLICHE KOMMEN

POLIZEIARBEIT

KOMPLEXER KRIMINALITÄT DIGITAL AUF DIE SCHLICHE KOMMEN

Polizeiarbeit bleibt auch in digitalisierten und global vernetzten Zeiten im Kern gleich, muss sich aber auf ein dramatisch erhöhtes Tempo und neuartige Anforderungen einstellen. Dafür sorgen globale Trends wie hohe Erwartungen der Bürger trotz limitierter Ressourcen sowie zunehmend mehr und vielfältige Daten. Ebenso wichtig ist aber, dass eine ganz neue Kriminalität entsteht, die sich häufig über Grenzen hinweg organisiert –und außerordentlich schwer zu identifizieren und beobachten ist.

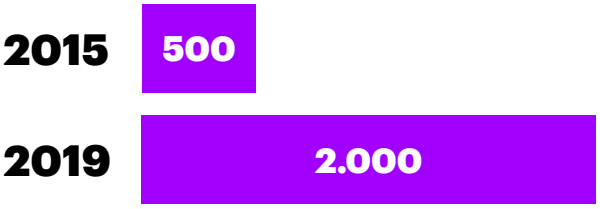
Wer an Verbrechen denkt, hat vermutlich einen Einbruch oder Raubüberfall vor Augen. Tatsächlich sind die Zahlen für diese traditionellen Arten von Kriminalität mit meist überschaubarem Schaden für das Opfer in vielen entwickelten Ländern aber eher rückläufig. Die Polizeiarbeit wird dadurch dennoch kaum entlastet. Denn Kriminalität wird immer komplexer und bislang unbekannte Straftaten entwickeln sich.

Der Zugriff auf digitale Technologien macht es möglich: Hier öffnen sich ganz neue Kanäle für Straftäter. Grenzen zwischen Staaten und Bundesländern spielen dann häufig keine Rolle mehr. Die historische Trennung der zuständigen Sicherheitsbehörden erschweren in diesen Fällen aber die Ermittlung: Ungehinderte Kommunikation und Kooperation sollen hier nun Abhilfe schaffen – und zwar dringend.

Das lässt sich illustrieren: Im Jahr 2015 beliefen sich die globalen Kosten in Zusammenhang mit Cyberkriminalität noch auf vergleichsweise geringe 500 Millionen Dollar. Nach Schätzungen könnten sie im Jahr 2019 bereits mehr als zwei Billionen Dollar betragen[1]. In anderen Worten: Die globalisierte Welt schafft globalisierte Kriminalität, die organisiert vorgeht und auf regionaler und internationaler Ebene grenzüberschreitend agiert.

Schon jetzt lässt sich hier ein massiver Anstieg verzeichnen: Alleine in den OECD-Ländern ist die organisierte Kriminalität in den letzten zehn Jahren um 127 Prozent gestiegen[2]. Dieser Besorgnis erregende Trend hat sich im öffentlichen Bewusstsein bislang aber noch nicht recht etabliert, wohl weil neue Bedrohungslagen wie Terrorismus entsprechende Diskussionen dominieren.

Globale Kosten Cyberkriminalität
(in Mio. US$)



Organisierte Kriminalität
(OECD Länder)

+127 %
in 10 Jahren

Dabei sind diese Trends eine kriminelle Bedrohung, die einer sehr viel größeren Zahl von Opfern insgesamt höheren Schaden zufügt. Und sie stellt die Sicherheitsbehörden vor gewaltige Herausforderungen, weil sie so außerordentlich schwer zu antizipieren und nur unter erheblichen Kosten zu analysieren ist. Lokale und nationale Maßnahmen sowie individuelle Ansätze stoßen hier schnell an ihr Limit. Wo Straftäter organisiert und über Grenzen aller Art hinweg operieren, müssen die Sicherheitsbehörden folgen.

Gesucht sind weltweit also neue Modelle der Zusammenarbeit, die zielgerichtet effektive und gemeinschaftliche Lösungen liefern. Die „Saarbrücker Agenda“ für eine moderne und einheitliche Informationsarchitektur der Polizei in Bund und Ländern weist hier in Deutschland den Weg. Sicherheitsbehörden, die diese Transformation nicht aktiv gestalten wollen, riskieren dagegen, die Erwartungen und Ansprüche der Öffentlichkeit nicht mehr erfüllen und damit ihr Serviceniveau nicht erhalten zu können.

[1] Juniper Research, Cybercrime will cost business over $2 trillion by 2019, 2015.

[2] United Nations Office on Drugs and Crime, Globalisation of Crime, 2010.

> Mit zunehmender Komplexität der Kriminalität und steigenden Kosten ihrer Bekämpfung führen Einzellösungen nicht mehr ans Ziel, auch wenn es natürlich weiterhin Leuchtturmprojekte einzelner Polizeiorganisationen geben soll und muss. Essentiell für eine erfolgreiche Polizeiarbeit in diesem dramatisch veränderten und sich immer weiter wandelnden Umfeld ist aber die partnerschaftliche Zusammenarbeit aller Sicherheitsbehörden für nationale Lösungen.

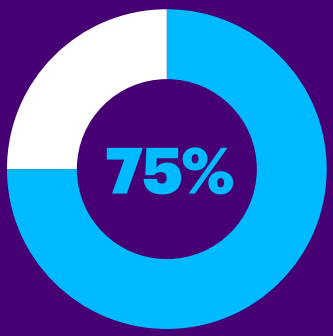
Was bedeutet das konkret? Von entscheidender Bedeutung ist, dass Daten und Informationen sowie deren Auswertung allen beteiligten Sicherheitsbehörden jederzeit bei Bedarf zur Verfügung stehen. Das kann nur eine nationale Plattform leisten, auf der Daten gesammelt, getauscht und analysiert werden. So wird verhindert,dass Informationen verlorengehen, Datenberge undurchdringlich werden oder deren Analyse zu komplex wird.

Noch ist diese Art der Kooperation nur in begrenztem Umfang möglich. Alternde IT-Landschaften, Unterschiede im Datenmanagement, nicht kompatible Systeme oder manuelle Methoden der Analyse verhindern den ungehinderten Austausch und die Auswertung von Daten, vor allem wenn sie von verschiedenen Sicherheitsbehörden eingeholt wurden. Anders gesagt: Der Prozess ist wenig effizient, weil aus den verfügbaren Daten nicht das Maximum an Erkenntnissen geholt werden kann.

Gerade in der Polizeiarbeit basieren effektive Entscheidungen auf Erkenntnissen, die aus ermittelten Rohdaten mit möglichst geringem Zeitverlust gewonnen werden. Fortschrittliche Analytik ist also essentiell für erkenntnisgestützte Polizeiarbeit. Und es gibt bereits viele erprobte Techniken und Ansätze zur Verwertung von Daten, etwa Cloud Computing, maschinelles Lernen und rechnergestützte Visualisierung. In ihrem Output gehen sie weit über das hinaus, was herkömmliche Methoden leisten können.

> Eine fortschrittliche Analytik ist aber auch gerade bei komplexer werdender Kriminalität und neuartigen Straftaten unverzichtbar. Dann geht es darum, sich entwickelnde Arten von Kriminalität zu verstehen, um gezielt und frühzeitig intervenieren zu können. Wenn sich neuartige, aber auch altbekannte Straftaten vorhersagen lassen, können sie in gewissem Umfang auch ohne zusätzliches Personal und Ressourcen verhindert werden.

Dann könnte Polizeiarbeit von ihrem eigenen Erfolg überholt werden: Antizipierte und entsprechend verhinderte Straftaten tauchen nicht unbedingt in Statistiken auf. Hier müssten möglicherweise neue Maßstäbe etabliert werden. Ebenso wichtig ist maximale Transparenz gegenüber der Öffentlichkeit, vor allem wenn es um die privaten Daten einzelner Bürger geht. Es geht um Teamarbeit, wie eine Accenture-Studie ergab, bei der mehrere Tausend Personen in acht Ländern befragt wurden.



Rund drei Viertel der Teilnehmer wollten eine aktive Rolle bei der Berichterstattung von Kriminalität spielen und auch zeitnahe Informationen von den Sicherheitsbehörden erhalten, etwa über digitale Medien[3].

Bei allem Bedarf an Informationen darf also nicht das Vertrauen der Öffentlichkeit in die Sicherheitsbehörden enttäuscht werden.

Dieser Anspruch gehört ebenso zum unantastbaren Kern von Polizeiarbeit wie die Wahrung der öffentlichen Sicherheit sowie die Bekämpfung und Vermeidung von Kriminalität – ob lokal oder grenzüberschreitend, ob einfach oder komplex.

[3] Accenture, Accenture Citizen Pulse Survey, 2014.

AUTOREN

BERND KARL

Managing Director
Öffentlicher Sektor, Post und Gesundheitswesen
bernd.karl@accenture.com
https://www.linkedin.com/in/berndkarl/
@BKarlAccenture

UWE LANGER

Leiter Öffentliche Sicherheit für Deutschland, Accenture
uwe.langer@accenture.com
https://www.linkedin.com/in/uwe-langer-5b109870/

ÜBER ACCENTURE

Accenture ist ein weltweit führendes Dienstleistungsunternehmen, das ein breites Portfolio von Services und Lösungen in den Bereichen Strategie, Consulting, Digital, Technologie und Operations anbietet. Mit umfassender Erfahrung und spezialisierten Fähigkeiten über mehr als 40 Branchen und alle Unternehmensfunktionen hinweg – gestützt auf das weltweit größte Delivery-Netzwerk – arbeitet Accenture an der Schnittstelle von Business und Technologie, um Kunden dabei zu unterstützen, ihre Leistungsfähigkeit zu verbessern und nachhaltigen Wert für ihre Stakeholder zu schaffen. Mit rund 459.000 Mitarbeitern, die für Kunden in über 120 Ländern tätig sind, treibt Accenture Innovationen voran, um die Art und Weise, wie die Welt lebt und arbeitet, zu verbessern. Besuchen Sie uns unter www.accenture.de.