Im Einsatz – im Thema.
POLIZEI PRAXIS

3 TRENDS, DIE IM JAHR 2021 DIE DIGITALE POLIZEIARBEIT MASSGEBLICH VERÄNDERTEN

Solide Kompetenzen im Bereich der digitalen Beweismittelerfassung sind heute unverzichtbar. Nur durch Gewinnung aussagekräftiger Informationen können Fälle schnell aufgeklärt werden.

Polizeibehörden gehen davon aus, dass künftig bei nahezu allen Ermittlungen Beweismittel aus digitalen Geräten im Spiel sein werden. Ein Beispiel hierfür ist die Fülle digitaler Beweismittel, die zur Identifikation und Anklage der Teilnehmer des Sturms auf das US-amerikanische Kapitol am 6. Januar 2021 führte. Medienberichten zufolge trug eine Vielzahl von Daten – von GPS-Daten über Textnachrichten und Videos bis hin zu Social-Media-Posts – zur Verhaftung der Tatverdächtigen.

Digital „unterstützte“ Verbrechen sind ein äußerst vielschichtiges Thema. Damit Polizeibedienstete hier mit den ständigen Neuerungen Schritt halten können, braucht es fortlaufende Schulungen und fortschrittliche Digital-Intelligence-Technologie. (Digital Intelligence bezeichnet zum einen die aus digitalen Quellen wie Smartphones, Computer, Cloud usw. erfassten Daten – und zum anderen den Prozess, mit dem Behörden diese Informationen sammeln, überprüfen, analysieren, verwalten und für effizientere Ermittlungen nutzbar machen.)

Nicht nur die Anzahl der Geräte ist größer, sondern auch die Komplexität der Technologien, beispielsweise Verschlüsselung. Dadurch sind ein höherer Zeitaufwand und Personalbedarf unvermeidlich.

Hinzu kommt, dass die Sorge seitens der Bürger und Regierungsbediensteten über den Zugriff der Exekutive auf personenbezogene Daten zu strengen Bedingungen für die Erfassung von Gerätedaten geführt hat. Zudem müssen die genutzten Tools eine Reihe von Funktionen umfassen, die einen angemessenen Schutz der Privatsphäre gewährleisten. Es ist daher wesentlich, die aktuellen Trends im Bereich der digitalen Polizeiarbeit zu verstehen.

TREND 1: DIE DATENFLUT

Viele dieser digitalen Ressourcen und die zu ihrer sinnvollen Nutzung erforderlichen Technologien gab es vor fünf Jahren noch nicht. Ermittler berichten regelmäßig, dass angesichts der Fülle digitaler Geräte eine Überlastung ihrer Labore droht.

Erschwerend hinzu kommt, dass die Technologie selbst Kriminalität ermöglicht und die Aufklärung deutlich verkompliziert, aber auch, dass Kriminelle ihre Taten weltweit verüben können. Mobile Technologie und Transaktionen mit Kryptowährungen beispielsweise kommen sowohl bei Straftaten selbst als auch in der Ermittlung zum Einsatz. Sowohl INTERPOL als auch die Vereinten Nationen melden in puncto Cyberkriminalität einen Zuwachs um 30 % bis 600 % während der Corona-Pandemie, je nach Art der Verbrechen.

Wie wirkt sich diese Datenfülle aus? Ohne die Schulungs- und Technologie-Tools für den Zugriff, die Überprüfung, die Analyse und die Weitergabe von Daten in einem prüffähigen Format und auf automatisierte Weise wird der analysierte Datenbestand unzureichend ausgeschöpft. Das wiederum führt dazu, dass Zusammenhänge und Muster, die für die Aufklärung unverzichtbar sind, übersehen werden. Exekutivbedienstete werden bei der Erfassung und Interpretation digitaler Beweismittel effizienter arbeiten müssen, um genau die Details zutage zu fördern, die letztlich zur Aufklärung des Falles führen.

Im Zuge einer Digital-Intelligence-Analyse können die Ermittler „Wegweiser“ ausmachen, die zur Aufklärung von Straftaten, Lokalisierung von Opfern und Verhaftung von Tatverdächtigen führen. Im englischen Leicestershire werteten Polizeiteams bei Ermittlungen zum Verschwinden eines jungen Mädchens GPS- und Anrufdaten aus den Telefonen der Tatverdächtigen aus. Damit konnten sie die Begegnung zwischen diesen nachvollziehen und ermitteln, wo sich Kleidung und Telefon des Mädchens befanden. Darüber hinaus wurden noch weitere Nachrichten- und Standortdaten genutzt, um einen Tatverdächtigen zu einem Geständnis zu bewegen, der die Polizei daraufhin zur Leiche des Mädchens führte.

Im texanischen Brazoria wiederum nutzten Ermittler die Standort- und Internetsuche, um einem Tatverdächtigen eine Reihe von Apotheken-Raubüberfällen zuordnen zu können. Das Team ordnete Standorte, die es anhand der Daten seines Telefons ermittelt hatte, den Zeitpunkten und Orten der Raubüberfälle zu. Ergänzend extrahiert das Team Daten zur Internetsuche. Dabei zeigte sich, dass der Mann unmittelbar vor dem Zeitpunkt der Raubüberfälle nach Informationen über die lokalen Dienstschichten der Polizeibehörde gesucht hatte, in der Hoffnung, dass diese während des Überfalls spärlich besetzt sein würde. Mit diesem umfangreichen Datenbestand konfrontiert, gestand der Täter die Raubüberfälle.

TREND 2: TECHNOLOGIEFEINDLICHKEIT AUS ANGST VOR ÜBERWACHUNG

Nutzer von Mobilgeräten lieben Tools wie Messaging und die Turn-by-Turn-Navigation. Viele unserer täglichen Tätigkeiten sind nur dank Smartphones möglich. Viele Menschen aber möchten nicht, dass die von ihnen erzeugten Daten zur durchgehenden strafrechtlichen Überwachung genutzt werden, insbesondere, wenn Behörden mit künstlicher Intelligenz und Lösungen für maschinelles Lernen experimentieren, etwa Gesichtserkennung. Strafverfolgungsbehörden werden von Datenschutz- und Bürgerrechtsanwälten dazu

gedrängt, bei der Nutzung KI-fähiger Tools ethische Vorgehensweisen einzuhalten und bei der Nutzung von Gesichtserkennungssoftware algorithmische Voreingenommenheit („Bias“) zu vermeiden.

Daher ist es wichtig, dass Strafverfolgungsbehörden entsprechende interne Richtlinien für den Umgang mit Geräten und Daten schaffen, um die Privatsphäre der Bürger zu schützen. Zudem müssen sie jeden Mitarbeiter, der mit der Bevölkerung interagiert, in die Nutzung und Umsetzung der Richtlinien im Arbeitsalltag einweisen. Die Arbeitsabläufe zur Einführung von Technologie und Nutzung von Daten sollten nach folgenden Kriterien erfolgen:

Fair: Algorithmisch fair, basierend auf unvoreingenommenen Daten

Erklärbar: Vielen Beteiligten gegenüber

Robust: Sicher und vertraulich, mit einem Menschen am Steuer

Nachverfolgbar: Klare Herkunft der Trainingsdatensätze und Metadaten

Transparent: Berichte im Prozess, Kommunikation der Ergebnisse, prüffähig

TREND 3: PLATTFORMEN DER NÄCHSTEN GENERATION FÜR DIE WICHTIGSTEN VORGÄNGE

Der digitale Wandel vollzieht sich nicht nur in der Welt der Verbrauchergeräte. Strafverfolgungsbehörden ist auch bewusst, dass sie zur zeitgerechten Erfassung, Analyse und Weitergabe von Daten fortschrittliche digitale Plattformen benötigen, um die Ermittlungsabläufe zu vereinfachen. Solche Plattformen sind mittlerweile unverzichtbar, um die Fülle an digitalen Datenträgern im Rahmen eines Falles effizient zu analysieren.

Um jedoch neue Technologien nutzen zu können, sind Schulungen und der Ausbau der Qualifikationen der aktuell und neu eingestellten Polizeibediensteten erforderlich. Hierzu zählen alle Mitarbeiter, nicht nur die Bediensteten digitaler Labore.

EIN IDEALER KRÄFTEMULTIPLIKATOR IM BEREICH DER POLIZEIARBEIT DIGITAL INTELLIGENCE

Moderne Strafverfolgungsbehörden müssen schnelle Arbeit leisten. Wie aber lässt sich dies erreichen? Durch die gekonnte Kombination von polizeilichem Know-how mit automatisierten, intelligenten Tools, die im Handumdrehen Zusammenhänge und Muster zutage fördern und so zur Aufklärung von Fällen beitragen. Diese Fähigkeit beinhaltet mehr als nur das Herunterladen von Textnachrichten aus Mobiltelefonen. Vielmehr gilt es, integrierte, skalierbare und durchsuchbare Lösungen als digitale Partner geschulter Polizeibeamter zu nutzen, um bessere Ergebnisse zu erzielen.

Die rasante Zunahme digitaler Daten führt zwangsläufig zu einem Chaos. Um Ordnung in dieses Chaos zu bringen, auf die oben genannten Trends zu reagieren und das Vertrauen der Gesellschaft in Polizeiarbeit zu stärken, benötigen Strafverfolgungsbehörden Unterstützung durch Lösungen, die eine sichere Verwaltung der Ermittlungsdaten und die Umwandlung dieser in aussagekräftige Informationen ermöglichen.

Text: Leeor Ben-Peretz

Über den Autor:

Leeor Ben-Peretz leitet die Strategie, das Business Development, die Advanced Services sowie die Trainingsfunktionen von Cellebrite. Er bringt über 20 Jahre berufliche Erfahrung in den Bereichen Forensik, Telekommunikation und Softwaresicherheit mit sich. Leeor hatte bedeutende strategische Geschäftsentwicklungs- und produktbezogene Positionen bei branchenführenden Unternehmen inne wie Aladdin Knowledge Systems (NASDAQ: ALDN), Pelephone Communications, Comverse (NASDAQ: CMVT) und InfoGin. Während seiner neunjährigen Tätigkeit bei Cellebrite hat Ben-Peretz wesentlich zur Entwicklung des Angebots des Unternehmens von einem einzigen hardwarebasierten Produkt bis zu einem reichhaltigen Portfolio innovativer Produkte, Lösungen und Services beigetragen. Herr Ben-Peretz besitzt einen Executive MBA von der Hebräischen Universität Jerusalem sowie einen BA in Wirtschaftswissenschaften vom Academic College in Tel-Aviv.

Weitere Informationen:

Cellebrite

Herr Peter Zontek

Mail: peter.zontek(at)cellebrite.com

Web: www.cellebrite.com

Alle Artikel dieser Kategorie