Daten-Management

Auch bei der Polizei wichtig

[29.09.2020] Überwachungskameras, Bodycams, automatische Nummernschilderkennung: Bei der Polizei werden massenweise Daten erfasst. Um diese Daten optimal nutzen zu können, ist ein effektives Management gefragt. Dazu zählt die intelligente Klassifizierung, die Informationen schnell auffindbar macht.

Bilder von Überwachungskameras und Bodycams, Ergebnisse der automatischen Nummernschilderkennung (ANPR), Telefonaufzeichnungen oder Informationen von Regierungsbehörden: Die Polizei muss sich mit immer größeren Datenmengen aus vielen unterschiedlichen Quellen beschäftigen. Nicht selten werden für einen einzigen Fall bis zu 20 verschiedene Geräte analysiert – etwa Smartphones, Tablets, Smart TVs, Desktop-PCs, Laptops und Server, aber auch sprachgesteuerte Anwendungen. Die digitale Forensik, mit deren Hilfe sich Muster von Straftaten und Tätern aufzeigen lassen, ist mittlerweile ein integraler Bestandteil fast jeder Untersuchung. Nicht zu unterschätzen sind zudem die Daten aus den sozialen Medien und Online-Foren. Vor allem bei der Verfolgung von Terrordrohungen und kriminellen Aktivitäten können die hier geposteten Beiträge wertvolle Informationen liefern.

Endstation Datensilo

Durch die Unterstützung digitaler Endgeräte und die gezielte Datenauswertung ist die Polizeiarbeit zwar wesentlich effektiver geworden. Die Verwaltung wird jedoch immer aufwendiger. Viele Informationen sind an verschiedenen Orten gespeichert – oft mehrfach in den Server-Räumen und Rechenzentren der Polizeidienststellen, auf den Laptops, Tablets und Kameras der Beamten sowie in Aktenordnern. Das macht es schwer, bei Bedarf schnell darauf zuzugreifen und sie zu visualisieren. Das wiederum hat zur Folge, dass die Polizeibeamten ihr Potenzial nicht voll ausschöpfen können. Auch die Einhaltung gesetzlicher Bestimmungen wird durch die Aufbewahrung in Datensilos erschwert. Um agiler zu werden, ihre IT-Infrastruktur skalieren zu können und hohe IT-Investitionen zu vermeiden, setzt laut Untersuchungen des Unternehmens Veritas die Hälfte der Unternehmen auf Cloud Computing. Für die Polizei sind das ebenfalls überzeugende Argumente, nicht nur wegen der knappen Budgets. Sie muss auch rund um die Uhr einsatzbereit sein. Daher benötigen die Dienststellen eine permanent verfügbare IT-Infrastruktur, die plötzliche Daten-Peaks bewältigen kann.

Hybride und Multi-Cloud-Umgebungen

Die Cloud bietet dafür die idealen Voraussetzungen. Aus Datenschutzgründen haben die Polizeibehörden bislang jedoch davon abgesehen, Dienste ausschließlich in der Cloud aufzusetzen. Weil sie mit sensiblen Informationen hantieren, werden Applikationen auf lokalen Systemen oder in einer hybriden Infrastruktur betrieben. Der hybride Cloud- oder Multi-Cloud-Ansatz eignet sich für Polizeidienststellen besonders gut, da er typische Cloud-Eigenschaften wie Flexibilität, Skalierbarkeit und Agilität mit der Möglichkeit kombiniert, ausgewählte Daten lokal zu speichern. Allerdings wächst damit wieder die Gefahr, dass Datensilos entstehen und Informationen redundant in separaten Infrastrukturen gesichert werden. Abhilfe schafft eine Daten-Management-Strategie, die das Aufbewahren und Löschen von Informationen genau definiert und dedizierte Tools für ihre Verwaltung vorsieht. Dadurch erhält man den Überblick, welche

Daten wo gespeichert sind, wie sie verwendet werden, wem sie gehören, wer auf sie zugreift und wann sie gelöscht werden können. Zudem lassen sich Informationen damit automatisch klassifizieren – etwa beim Hochladen – und Fristen festsetzen, nach deren Ablauf sie verfallen.

Compliance als Gebot der Stunde

Tools für die Datenverwaltung erhöhen die Produktivität und entlasten die Polizeibeamten, vor allem weil sie die Suche nach Informationen, die etwa für eine strafrechtliche Ermittlung benötigt werden, erleichtern und ihre Analyse beschleunigen. Voraussetzung ist aber, dass die Mitarbeiter den Umgang damit in Schulungen lernen – etwa Dateien richtig zu benennen, Metadaten korrekt zu verwenden und die Zahl unnötiger Kopien zu reduzieren. Denn sowohl beim Speichern vor Ort als auch in der Cloud liegt die Verantwortung für den Schutz der Daten weitgehend aufseiten des Anwenders. Zudem sind die regulatorischen Anforderungen in den letzten Jahren stark gestiegen. Vor allem seit Einführung der DSGVO haben Unternehmen begonnen, ihre Mitarbeiter für das Thema Datenschutz zu sensibilisieren und entsprechende Prozesse und Richtlinien einzuführen. Schulungen, Incentives sowie aktualisierte Verträge sollen dazu beitragen, dass den Mitarbeitern ihre persönliche Verantwortung für die Datensicherheit im Unternehmen stärker bewusst wird.

Vertrauen nicht verspielen

Auch bei der Polizei spricht alles für eine Compliance-Kultur: Seit Anfang 2018 wurde in mindestens 158 Verfahren gegen Beamte ermittelt, die rechtswidrig über Dienstcomputer Daten abgerufen haben sollen. Das berichtet der Spiegel und beruft sich dabei auf eine Umfrage unter den Datenschutzbeauftragten des Bundes und der Länder sowie in den Innenministerien. Auch in Großbritannien wurde allein im Jahr 2016 in mehr als 600 Datenmissbrauchsfälle ermittelt. Und ein Jahr später gab es bereits in den ersten 100 Tagen 176 Vorfälle.
Die Polizei steht mit ihrer Digitalstrategie also an einem Wendepunkt. Jetzt geht es darum, das Vertrauen der Öffentlichkeit nicht zu verspielen. Wichtig ist daher, dass die Beamten Schulungen im Umgang mit hochsensiblen Daten erhalten und dass die Polizei eine übergreifende und verbindliche Strategie für das Daten-Management etabliert. Nur dann kann sie auch in Zukunft wertvolle Informationen datenschutzkonform aus ihren Daten ableiten, damit Fälle lösen und geplante Verbrechen verhindern.

()

Stichwörter: Innere Sicherheit, Datenschutz, IT-Infrastruktur, IT-Sicherheit, Veritas