DATENSCHUTZ UND DATEN-SICHERHEIT IN SMART CITIES

In Smart Cities werden Daten und Informationen erhoben und weiterverarbeitet, um die Lebensqualität der Bevölkerung und die Wettbewerbsfähigkeit der ansässigen Wirtschaft zu erhöhen. Datenschutz und Datensicherheit sind dabei von zentraler Bedeutung.

→ VON VIKRAM BHATNAGAR

Städte werden digital. Die fortschrittliche Stadt ist «smart» und löst ihre Aufgaben durch den Einsatz neuer Technologien und die Einbindung verschiedener Anspruchsgruppen. Die Hivemind-IoT-Plattform fungiert dabei als zentrales Element, auf dem Städte und Unternehmen ihre IoT-Services und -Projekte aufbauen. Die Bevölkerung sowie die vor Ort ansässigen Unternehmen profitieren gleichermassen: Ressourcen werden eingespart und geschont, die Effizienz gesteigert und die Nachhaltigkeit verbessert. Durch die Vernetzung aller Akteure innerhalb einer Stadt entstehen neue Zusammenarbeitsformen. Die zunehmende Digitalisierung führt aber auch dazu, dass eine grosse Menge Daten erhoben, gespeichert und weiterverarbeitet werden. Dabei steht für alle Beteiligten fest: Der Zugang, die Verwendung sowie die Sicherung der Daten muss zwingend definiert und eindeutig geregelt werden.

In der Stadt Zürich wird beispielsweise der Umgang mit Daten bezüglich Eigentum, Verantwortung, Ablage, Verwendung, Weitergabe und Veränderung durch die Entwicklung einer stadtweit gültigen Governance geregelt. Dabei sollen sämtliche stadtinternen Identitäten durch den Aufbau eines umfassenden «Identity & Access Management»-Systems sicher verwaltet werden können.

OPEN DATA VERSUS SCHÜTZENSWERTE DATEN

Open Data ist Teil der Wissens-Philosophie, Daten ohne spezifische Schutzbedürfnisse der Bevölkerung zur freien Verwendung zur Verfügung zu stellen. Open Data befähigt dabei Dritte wie beispielsweise Forschungseinrichtungen, Start-ups und Unternehmen dazu, die Veränderungen innerhalb einer Stadt zu analysieren und aus den öffentlich verfügbaren Daten in Open-Innovation-Projekten neue Services abzuleiten (Thomas Riesenecker-Caba, Forschungs- und Beratungsstelle Arbeitswelt, «Smart Cities. Eine technologische und datenschutzrechtliche Einschätzung»). In diesem kollaborativen Ansatz zur Nutzung von städtischen Daten können Prozesse oder Vorgänge im Interesse der Gesellschaft verbessert sowie vereinfacht werden.

Die Frage, welche Daten geschützt werden sollen und welche Daten lizenzfrei publiziert werden können, ist hierbei allerdings auch eine Frage des Persönlichkeitsschutzes.

Zweifelsfrei sicher ist, dass Daten, die Rückschlüsse auf Einzelpersonen erlauben, immer schützenswert sind. Dies bedeutet, dass Städte den Schutz der Privatsphäre in Bezug auf die Erfassung und Verwendung von personenbezogenen Daten gewähren müssen, wenn sie die Stadtentwicklung positiv fördern und das Vertrauen der Bevölkerung und der Unternehmen für ihre Projekte gewinnen wollen.

Beispielhaft für die strikte Einhaltung der schweizerischen und europäischen Datenschutzbestimmungen hinsichtlich Privasphäre und Persönlichkeitsschutz ist die Stadt Carouge vor den Toren von Genf. Die von der Stadt entwickelte «Privacy App» erlaubt es der Bevölkerung, jederzeit einzusehen, welche Sensoren wo in der Stadt zu welchem Zweck eingesetzt werden. Mit dieser App ist es Carouge gelungen, Transparenz zu schaffen und das Vertrauen der Bevölkerung für die städtischen Smart-City-Initiativen zu gewinnen.

DIE RÜCKIDENTIFIKATION DER ERHOBENEN DATEN

Personenbezogene Daten und Informationen sollten in einer Smart City nur erhoben werden, wenn es zweckdienlich ist. Werden zum Beispiel Videokameras für die Verkehrsmessung zur Stauvermeidung installiert, so ist es nicht zielführend, Bildmaterial von Kontrollschildern und Gesichtern zu sammeln. Werden dennoch schützenswerte Daten erhoben, so sollten die gesammelten Datensätze via Rückidentifikationsmethode anonymisiert werden.

Zum Autor

Vikram Bhatnagar,
Digital Leader &
CEO.

Zum Unternehmen:
Hivemind ist ein führendes Schweizer IoT-Unternehmen, das durch den Aufbau umfassender IoT-Ökosysteme Unternehmen und Städte in der digitalen Transformation unterstützt. Mit der von Hivemind entwickelten IoT-Plattform können Städte, Unternehmen, Integratoren und Service Provider Internet-of-Things-Anwendungen schnell und einfach entwickeln und implementieren. Die Hivemind-IoT-Plattform erfüllt höchste Datenschutzstandards sowie modernste Sicherheitsmechanismen und wird als einer der ersten IoT-Stacks auf dem neuen Microsoft Datencenter in der Schweiz laufen. Durch die enge Zusammenarbeit mit Microsoft kann Hivemind Unternehmen und Städte die Möglichkeit anbieten, ihre Daten in naher Zukunft sicher und lokal in der Schweiz abzuspeichern.

Mehr Informationen:
www.hivemind.ch

HIVEMIND

Bild: Hivemind AG, Zurich

Hivemind-Team mit Smart-Building-3D-Modell

Dies geschieht durch das Entfernen von Details wie Gesichtern, dem Namen, der persönlichen Identifikationsnummer, E-Mail-Adressen und der Anschrift sowie grundlegenden Informationen wie Alter, Geschlecht und Beruf.

WO SOLLEN DIE ERHOBENEN DATEN GESPEICHERT WERDEN?

Insbesondere für Städte stellt sich bei der Nutzung von IoT die entscheidende Frage, wo die erhobenen Daten prozessiert und gespeichert werden, sodass den steigenden Datenschutzanforderungen nachgekommen werden kann. Eigene Rechenzentren zu betreiben, ist unterhalts- und entsprechend kostenintensiv. Aus diesem Grund setzen nicht nur Unternehmen, sondern vermehrt auch Städte auf skalierbare Cloud-Lösungen vertrauenswürdiger Cloud-Anbieter. Aufgrund der starken inländischen Datenschutzbestimmungen gilt die Schweiz laut Experten als eines der besten Länder für den Betrieb eines sicheren Rechenzentrums. Schweizer Städte, die Gerichtsstand und gesetzliche Grundlagen wählen möchten, sollten demnach auf Schweizer oder zumindest europäische Cloud-Dienste setzen.

Doch wie sicher sind Daten in der Cloud und was sollte bei der Wahl einer geeigneten Cloud-Lösung beachtet werden?

DATENSICHERHEIT IN DER CLOUD

Bei der Wahl des richtigen Cloud-Anbieters sollte berücksichtigt werden, dass die Daten verschlüsselt in der Cloud gesichert werden und eine Transportverschlüsselung bei der Datenübertragung zwischen zwei Geräten vorliegt. Grosse Cloud-Anbieter wie beispielsweise Microsoft & Co. nehmen den Datenschutz sowie die Datensicherheit sehr ernst und setzen auf höchste, vertraglich geregelte Datensicherheits- und Verschlüsselungsstandards. Die Wahrscheinlichkeit, dass solche Clouds gehackt werden, ist demnach äusserst gering. Städte und Unternehmen können bei diesen Cloud-Anbietern auch den Standort des Rechenzentrums wählen. Dies ermöglicht den Städten und Unternehmen, den teilweise engen, gesetzlichen Vorgaben zu entsprechen.

FAZIT

Um das Leben von Bürgern und Unternehmen zu verbessern und die Mehrheit der Bürger für Smart-City-Initiativen begeistern zu können, müssen Smart Cities Datenschutz- und Datensicherheitsanforderungen nachkommen und sich als vertrauenswürdig erweisen: Um das Vertrauen der Bevölkerung in diese neuen Technologien zu gewinnen, sind Städte und Unternehmen gleichermassen gefordert, die Einhaltung der Richtlinien und Gesetze offen und proaktiv zu kommunizieren. Nur so können sie den Bürgern glaubhaft beweisen, dass der Schutz ihrer Privatsphäre umfangreich gewährleistet ist und sämtliche IoT-Initiativen zur Verbesserung des Lebens sowie Arbeitens in der Smart City lanciert werden. IoT funktioniert sowohl auf der technischen als auch auf der menschlichen Ebene nur gemeinsam. Genau daher sollte das oberste Gebot für die Implementierung von IoT-Lösungen Transparenz sein, um die Bürger positiv abzuholen und vom Nutzen der Lösungen zu überzeugen. ←

Dieser Beitrag wurde von der **Hivemind AG** zur Verfügung gestellt und stellt die Sicht des Unternehmens dar. Computerworld übernimmt für dessen Inhalt keine Verantwortung.