Kritische Infrastrukturen im kommunalen Bereich

Hacker-Angriff auf die Smart City?

Die Digitalisierung kommunaler Infrastrukturen ist einer der ersten Schritte in Richtung Smart City. Um die Risiken zu mindern, müssen ein effektiver Datenschutz durchgesetzt und kritische digitale Infrastrukturen abgesichert werden.

> Ulrich Greveler

Aspekte von Datenschutz und Datensicherheit sollten von Beginn an in der Konzeption von Smart-City-Projekten berücksichtigt werden. Es ist in der Kommunalverwaltung leider nicht unüblich, DatenschützerInnen und Sicherheitsverantwortlichen die mangelnde Effizienz und Fehleranfälligkeit eines Systems anzulasten: sie sollen zum Start einer Pilotphase oder Einführung eines neuen Systems die Freigabe erteilen und damit eine oft nebulös bleibende Unbedenklichkeit bescheinigen. Dies führt in der Praxis zu überbordenden Auflagen und bürokratischen Hemmnissen, da die Verantwortlichen sich gegenüber einer politischen Haftung absichern wollen.

Steht die Software-Architektur eines Projekts bereits fest und ist für den Testbetrieb einsatzbereit, kommen Datenschutz- und Sicherheitsbedenken aber ohnehin zu spät: Umfangreiche Änderungen der Architektur würden nun Kosten- und Zeitrahmen sprengen. Es sind meist nur noch überschaubare Anpassungen möglich, die wie Flicken auf eine technische Lösung aufgebracht werden und sich nicht mehr harmonisch in den Designentwurf einfügen. Dies ist für das Image der Freigabeinstanz nicht förderlich, da sie in die Rolle eines Buhmanns gerät: „Unser System könnte so schön funktionieren, wenn der Datenschutz nicht gefragt worden wäre."

Datenschutz und Funktionsfähigkeit: Das geht!

Allen Unkenrufen zum Trotz bleibt aber festzuhalten: Tatsächlich kollidieren Interessen von Datenschutz und Datensicherheit nicht mit der Gebrauchstauglichkeit und der Funktionsfähigkeit von digitalen Infrastrukturen! Es bedarf auch hier – wie in vielen politischen Entscheidungsprozessen – eines vorausschauenden Planes und dem wirksamen Einbinden der Interessen. Die Sicherheitstechnik der folgenden Beispiele aktueller Smart-City-Anwendungen sollte besonders unter die Lupe genommen werden.

Beispiel: Mängelmelder und Bürger-Apps

Mängelmelder oder Bürgeranliegen-Apps versetzen die BewohnerInnen einer Stadt in die Lage, mithilfe von Smartphones Mängel oder Anregungen zu dokumentieren – meist mit Foto, Ortskoordinaten und kurzer Beschreibung – und den Verlauf der Bearbeitung zu verfolgen. Neuartige Lösungen bereichern diese Vorgänge um Transparenzfunktionen ähnlich sozialer Netze: Die Meldungen sind allgemein sichtbar und können gemeinsam verfolgt und kommentiert werden. Es entsteht eine lebendige Kommunikation zwischen Verwaltung und Bürgerschaft.

Solche Projekte sollten bereits zu Beginn wichtige Parameter hinsichtlich Datenschutz und Datensicherheit festlegen: Setzt die Meldung zwingend voraus, dass personenbezogene Daten, etwa Name und Anschrift, zum Fall übermittelt werden, oder kann das System auch anonym oder mit Pseudonymen genutzt werden? Pseudonyme erleichtern kollaborative Funktionen, zum Beispiel Nachfragen zu beantworten, die durch Anonymität verhindert werden. Liegen die zu speichernden Daten auf einem Server des kommunalen Rechenzentrums oder speichert der Dienstleister sie mithilfe von außereuropäischen Clouddiensten? Gibt es eine Funktionalität, Rechtsverstöße oder Verletzungen der Privatsphäre aufgrund von hochgeladenen Bildern zu melden, diese Meldungen effizient zu bearbeiten und den Vorgang nachvollziehbar darzustellen?

Diese Fragen machen deutlich, dass es zum Ende des Projektes viel zu spät wäre, nach Antworten zu suchen. Denn dann sind nur noch Notlösungen möglich, zum Beispiel die nachträgliche Anonymisierung von Datensätzen aufgrund von Beschwerden.

Beispiel: Parkleitfunktionen und optische Überwachung

Bei Lösungen mit Parkleitfunktionen, Verkehrszählungs-Sensoren und optischer Überwachung – zum Beispiel um festzustellen, wieviele Parkplätze belegt sind – sollte frühzeitig spezifiziert werden, dass keine personenbezogenen Daten anfallen. Hier gilt der Grundsatz: Daten, die nicht erhoben werden, braucht man nicht schützen. So sollten Dienste keine Kennzeichen erfassen oder – wenn das kurzfristig notwendig ist, um das Passieren eines Bereiches festzustellen – nach Beendigung des Zählvorgangs zumindest nicht speichern. Falls Bilddaten aufgezeichnet werden, müssen bereits vor dem Speichervorgang Gesichter und Kennzeichen unkenntlich gemacht worden sein. Abrechnungsdaten, die oft Kontoverbindungen enthal-

Foto: Matthew Henry / unsplash.com

ten, sind von einem getrennten Server zu verwalten, so dass jeweilige Systemverantwortliche diese Daten nicht zusammenführen können.

Alle diese Techniken sind mit geringem Aufwand umsetzbar. Sie kollidieren nicht mit nützlichen Funktionen, sofern sie bereits in der Software-Architektur berücksichtigt sind.

Kritische Infrastruktur vor Angriffen schützen

Bei Systemen, die Anlagen steuern, den ÖPNV unterstützen, die Umwelt überwachen oder die Energieverteilung regeln, wie zum Beispiel Telematiklösungen oder Photovoltaik-Grids, kommt dem Versorgungssicherheitsaspekt besondere Bedeutung zu. Hier können bei Störungen, Hackerangriffen oder Viren-Befall buchstäblich die Lichter ausgehen.

In der **Planungsphase** ist daher die IT-Sicherheit in den Vordergrund zu stellen: Trennung von Netzen, Abschottung von Übergangspunkten, Auswahl sicherer Plattformen. Für den **Betrieb** sind auch Verantwortlichkeiten zu klären. Wer ist zuständig, die Software zu aktualisieren, auf Sicherheitsvorfälle zu reagieren und Systemzustände zu überwachen? Und nicht zuletzt: Gibt es einen Plan für den Fall, dass eine Komponente ungeplant ausfällt oder gehackt wurde? Dabei sind auch Fallback-Szenarien zu betrachten, damit aus einem Cyber-Incident kein Desaster-Fall wird: zum Beispiel ein Notbetrieb ohne Steuerungsfunktion oder ein Rückfall auf analoge Komponenten. Smarte Systeme sollen sich auch bei Angriffen und Störungen smart verhalten!

Zu uninteressant für Kriminelle?

Eine Betrachtung von Risiken in Bezug auf Datenschutz und Datensicherheit bei Smart-City-Projekten ist keineswegs mit Technologiefeindlichkeit oder Alarmismus zu verwechseln. Im Gegenteil: Smarte Lösungen berücksichtigen potenzielle Risiken und weisen in ihrer Architektur bereits risikomindernde Aspekte auf. Mit dem Internet verbundene Systeme sind ständigen Attacken ausgesetzt. Dies geschieht automatisch, da alle IP-Adressen weltweit von Angreifern gescannt werden. Niemand sollte leichtsinnigerweise davon ausgehen, dass das eigene Projekt zu uninteressant für Kriminelle ist.

Kommunalpolitische Akteure können bei der Risikoabwehr mitwirken, indem sie bei Entscheidungsvorlagen darauf achten, dass nicht nur Funktionalitäten, zum Beispiel in Lastenheften beschrieben sind, sondern bereits Planungsdokumente vorhanden sind, die eine sichere Gestaltung der smarten Infrastruktur abbilden. Soll ein System von Grund auf neu entworfen und implementiert werden, ist die Sicherheitstechnik als wesentliches und früh zu spezifizierendes Element der Architektur vorzusehen. MandatsträgerInnen können sich dann Zwischenergebnisse oder die Bewertung durch externe Sachverständige vorlegen lassen, denn eine Korrektur ist nur in frühen Projektphasen sinnvoll möglich.

> Ulrich Greveler ist Professor für angewandte Informatik, insbesondere IT-Sicherheit an der Hochschule Rhein-Waal und lehrt im Studiengang E-Government in Kamp-Lintfort, NRW.