Kritische Infrastrukturen im kommunalen Bereich

Daseinsvorsorge im Visier der Hacker?

Kommunen steuern ihre Energie-, Wasser- und Wärmeversorgung zunehmend digital, genauso wie Rettungsdienste, Krankenhäuser, ÖPNV und Müllentsorgung. Dass sie damit auch für Angriffe aus dem Netz verwundbar werden, dringt immer mehr ins Bewusstsein. Anhand dreier Bereiche stellt dieser Artikel vor, wo die Gefahren liegen und wie sich Verantwortliche darauf vorbereiten können.

> Ulrich Greveler

Digitale Innovation zieht sich durch sämtliche Bereiche der Daseinsvorsorge. Auch die öffentlichen Verwaltungen interagieren mit der Bevölkerung immer stärker über vernetzte Systeme. Die Informationswirtschaft der öffentlichen Hand bietet mit ihren medienbruchfreien digitalen Wegen zum Menschen und automatisierten Büroabläufen ein enormes Potenzial an Effizienz- und Effektivitätssteigerung.

Während die weitreichende Verbesserung der Leistungen für BürgerInnen, Wirtschaft und Gesellschaft zu begrüßen ist, birgt Digitalisierung auch spezifische Risiken: Die Abhängigkeit von digitalen Systemen, Informationstechnologien und Datenhaltungen nimmt zu. Die globale Vernetzung führt dazu, dass kommunale Daseinsvorsorge zum Ziel von Angriffen werden kann. Diese Risiken zu kennen und zu beherrschen, ist wesentlicher Teil einer erfolgreichen Digitalisierungsstrategie.

Krankenhäuser

Einige Fälle in den vergangenen Jahren haben gezeigt, dass etwa Krankenhäuser gleich mehrfach verwundbare Angriffsziele sind. Stand bisher die Vertraulichkeit der Patientendaten im Vordergrund, wird nun zunehmend spürbar, dass die Verfügbarkeit der medizinischen Dienste selbst gefährdet ist. Eine Studie der Unternehmensberatung Roland Berger ergab, dass fast zwei Drittel der deutschen Krankenhäuser schon einmal zum Opfer eines Hacker-Angriffs wurden. Der schlimmste Fall ist der Komplettausfall einer Klinik-IT, der dazu führt, dass Kranke in andere Häuser transportiert und Notfälle abgewiesen werden müssen. Letzteres war die Folge eines digitalen Angriffs auf das Klinikum Arnsberg im Jahre 2017.

Das IT-Sicherheitsgesetz des Bundes verpflichtet mittlerweile alle Krankenhäuser mit jährlich mehr als 30.000 vollstationären Behandlungsfällen zu Sicherheitsstandards bei Technik und Organisation. Doch auch diese Standards können nicht ausschließen, dass Angriffe Erfolg haben. Zudem sind Kliniken mit kommunalen Trägern oft kleiner ausgelegt und fallen nicht unter diese Vorschrift.

Neben technischen Eingriffen, wie der Abschottung der Netze nach außen, ist vor allem die Sensibilisierung des Personals gegenüber Risiken ein wichtiger Schritt in Richtung sichere Klinik-IT. Und es werden Notfallprozeduren gebraucht: Im Falle eines Versagens der IT-Infrastruktur muss es weiterhin möglich sein, auf eine „Zettelwirtschaft“ und nicht vernetzte Systeme zurückzufallen, die eine fachgerechte Behandlung der PatientInnen wie auch die Neuaufnahme von Notfällen erlauben.

ÖPNV

Busse und Straßenbahnen unterliegen einem digitalen Telematik- und Fuhrparkmanagement: Die Dienst- und Streckenplanerstellung, die Lenkzeitenüberwachung, Tankdatenerfassung und alle Abrechnungsvorgänge sowie das mobile Ticketing sind in den meisten kommunalen Verkehrsbetrieben durchgehend digitalisiert. Das spart nicht nur Kosten, sondern hilft, die Auslastung der Fahrzeuge zu optimieren, und bei einer flexiblen Routenplanung. Punkte, die zur Durchsetzung der Nachhaltigkeitsziele erheblich beitragen.

Eine Schattenseite des digitalen ÖPNV ist, dass auch hier Angriffsflächen entstehen: Ohne Vernetzung der Systeme ist so ein Nahverkehr nicht denkbar. Schaffen es Angreifer jedoch, in die Systemlandschaft einzudringen oder Ausfälle zu provozieren, kann das zu Chaos im Fahrbetrieb führen. Die Zahl der potenziell Betroffenen ist dabei sehr hoch, zudem gibt es Auswirkungen auf Wirtschaft und Gemeinwesen, wenn Beschäftigte massenhaft nicht rechtzeitig zum Arbeitsplatz gelangen.

Auch hier ist der zentrale Lösungsansatz, Rückfall-Prozesse zu schaffen. Ein Ausfall der Anzeigeelemente im und am Bus und der Abfahrtsmonitore ist zwar ein Ärgernis, aber wohl noch zu verschmerzen, wenn papierbasierte Fahrhefte für die Streckenführung bei einem vollständigen IT-Ausfall zur Verfügung stehen: Die Fahrzeuge bedienen dann weiterhin die Strecken, so dass nur erhöhte Aufwände beim Nachverbuchen von Fahrscheinen beziehungsweise Einnahmeausfälle bei mobilen Tickets entstehen.

Foto: Jefferson Santos / Unsplash

Stromnetze und erneuerbare Energien

Stromnetze entwickeln sich zu Smart Grids. Diese vereinen Konzepte der Energie- mit denen der Informationstechnik und schaffen so ein intelligentes Netz, das die elektrische Abnahme steuert. Sie kann volatile erneuerbare Energiequellen, insbesondere Windkraft und Solarenergie, gezielt einbinden, um Lastspitzen zu dämpfen und kurzfristig überschüssige Energie zu verwenden. Dies soll die Effizienz des Energienetzes steigern und damit Kraftwerkskapazitäten mit CO_2-Ausstoß einsparen. Kommunale Energieversorger, darunter Stadtwerke, und Netzbetreiber haben vielfältige Pilotprojekte initiiert, um das Zusammenwirken der Komponenten zu testen und Erfahrungen zu gewinnen.

Die Integration von IT-Systemen in das Stromnetz, die dafür nötig ist, schafft eine neue Angriffsfläche: Sicherheitslücken in den Systemen, wie wir sie von Internetservern kennen, gefährden nicht nur die Integrität der Daten, sodass am Ende vielleicht ein falscher Stromverbrauch angezeigt wird. Sie können auch dazu führen, dass ein Angriff über das Datennetz ein Versagen des Energienetzes und damit einen flächigen Stromausfall verursacht. Der plötzliche Ausfall eines einzelnen Netzsegmentes kann sich zudem kaskadierend auf benachbarte Segmente auswirken, dann sitzt die Bevölkerung auch überregional im Dunkeln.

Betreiber von Strom- und Gasnetzen müssen unabhängig von der Größe des Unternehmens nach Vorgaben des Energiewirtschaftsgesetzes ein funktionierendes Informationssicherheits-Managementsystem aufbauen, extern zertifizieren lassen und kontinuierlich überprüfen. Die strengen Vorgaben sind berechtigt: So berichtete die Süddeutsche Zeitung im Mai 2018, dass mutmaßlich russische Hacker in das Netz einer Tochter des EnBW-Konzerns eingedrungen sind. Steuerungssysteme des Stromnetzes waren dabei glücklicherweise nicht betroffen. Anders war es im Dezember 2016 kurz vor Mitternacht in Kiew: Stromausfall. Hacker übernahmen die Systeme von mehreren Strombetreibern und ließen die Stadt für mehrere Stunden stromlos.

Risiken minimieren

Das Internet der Dinge und lokal vernetzte Systeme zeigen das enorme Potenzial des digitalen Wandels. Diese Neuerungen gehen mit einem Zuwachs an Sicherheitsrisiken einher. Öffentliche Infrastruktur wird immer verletzlicher.

Das stellt den Nutzen einer modernen Kommune allgemein nicht infrage. Der Gewinn an Effizienz und neue Services für die Bevölkerung rechtfertigen ein Fortschreiten der Digitalisierung trotz eventueller Gefahren. Die genannten Risiken zu betrachten, zu bewerten und – soweit möglich – zu vermeiden, ist jedoch als unverzichtbarer Teil einer kommunalen Digitalisierungsstrategie vorzusehen.

Betreiber kritischer Infrastrukturen sind Angriffsziele mit besonders hohem Schadpotenzial in Bezug auf die Gesellschaft. Daraus ergibt sich eine besondere politische Verantwortung bei EntscheiderInnen in Gremien und Verwaltungsvorständen.

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