Interview

Basis schaffen für resiliente Systeme

[03.05.2023] Der Schutz Kritischer Infrastrukturen rückt durch die veränderte Sicherheitslage in Europa immer mehr in den Fokus. stadt+werk sprach mit Manuel Atug, Sprecher der AG KRITIS, über resiliente Energiesysteme und die Gefahren durch Cyber-Angriffe.

Herr Atug, welche Aufgaben und Ziele hat sich die Arbeitsgruppe KRITIS gesetzt?

Die Arbeitsgruppe KRITIS ist eine unabhängige Interessengemeinschaft, die sich dem Schutz Kritischer Infrastrukturen verschrieben hat. Derzeit besteht sie aus 42 Fachleuten, die an der Planung, dem Bau und der Prüfung dieser Infrastrukturen beteiligt sind. Unser Ziel ist es, Kritische Infrastrukturen angemessen zu schützen und im Falle einer Störung reaktiv zu handeln. Dabei arbeiten wir unabhängig von Staat und Wirtschaft, um unsere Expertise und Erfahrung bestmöglich für die Sicherheit der Bevölkerung einzusetzen.

Derzeit ist viel von Resilienz die Rede. Was heißt das im Zusammenhang mit Kritischen Infrastrukturen?

Resilienz bezeichnet die Fähigkeit eines Systems, sich auf unvorhergesehene Ereignisse einzustellen und so widerstandsfähig gegen diese zu sein. Kritische Infrastrukturen, wie beispielsweise das Energiesystem, sind besonders anfällig für Störungen, die zu schwerwiegenden Folgen führen können. Doch durch geeignete Reaktionen und Vorkehrungen können Krisen und Katastrophen vermieden werden. Eine schnelle und effektive Reaktion auf Störungen kann dazu beitragen, dass diese nicht in einer Krise eskalieren. In diesem Sinne sind Störungen in Ordnung, solange sie angemessen gehandhabt werden.

Die Digitalisierung des Energiesystems ist eine Voraussetzung für das Gelingen der Energiewende. Was ist dabei zu beachten?

Eine schlecht umgesetzte Digitalisierung kann das Risiko von Cyber-Sicherheitsvorfällen erhöhen. Besonders bei der Digitalisierung des Energiesystems ist es wichtig, Security by Design und Privacy by Design zu berücksichtigen. Wenn dies vernachlässigt wird, führt das langfristig zu Sicherheitsproblemen. Komponenten wie etwa Smart Meter haben eine lange Lebensdauer von Jahrzehnten. Entscheidungen und Maßnahmen in der IT-Sicherheit und beim Datenschutz können langfristige Auswirkungen haben. Nur wenn wir jetzt die richtigen Entscheidungen treffen, können wir eine sichere und nachhaltige Zukunft für uns und kommende Generationen schaffen.

Worauf kommt es also an?

Wir müssen erkennen, dass mangelnde IT-Sicherheit nicht nur die digitale Welt betrifft, sondern auch Auswirkungen hat auf die physische Welt und damit auf uns Menschen. Die Bedeutung der IT-Sicherheit für den Schutz zukünftiger Generationen wird heute leider oft unterschätzt. Würden wir uns bewusst machen, dass Datenschutz und IT-Sicherheit nicht nur aktuell wichtig sind, sondern auch langfristig nachhaltige Lösungen bieten, hätten diese Themen einen anderen Stellenwert.

Wie können Stadtwerke zum Erfolg der Energiewende beitragen?

Um die Energiewende langfristig erfolgreich umzusetzen, müssen auf Bundes- und Landesebene strategische Entscheidungen getroffen werden, wie die Umstellung auf erneuerbare Energien grundsätzlich ausgerichtet werden soll. Stadtwerke können solche Entscheidungen nicht treffen, aber einfordern. Die Vergangenheit hat allerdings gezeigt, dass politische Entscheidungen nicht immer sinnvoll sind. Ganze Branchen wurden durch falsche Regulierungen fehlgeleitet, und es gibt immer noch Stimmen, die Atomkraftwerke weiterlaufen lassen wollen. Aus KRITIS-Sicht sind zentrale Kraftwerke anfälliger für Angriffe. Angesichts des russischen Angriffskriegs gegen die Ukraine müssen wir die Sicherheit des Energiesystems ernsthaft in Betracht ziehen. Das können Stadtwerke nicht alleine tun. Es bedarf einer Zusammenarbeit zwischen verschiedenen Akteuren, um Kritische Infrastrukturen abzusichern.

Ist es positiv zu bewerten, dass die Resilienz des Gesamtsystems durch die Dezentralität und die damit verbundene Nutzung vieler unterschiedlicher Systeme erhöht wird?

Ein dezentrales Energienetz mit vielen kleinen Einspeisern ist natürlich schwieriger anzugreifen als wenige große Kraftwerke. Wenn allerdings alle Anlagen über die Cloud verbunden sind, reicht es, die zentrale Steuerung anzugreifen. Eine Lösung wäre ein Netz mit vielen dezentralen Kraftwerken, die durch Batteriespeicher als Puffer stabilisiert werden. Solche Szenarien im Energienetz sind noch nicht ausreichend erforscht, da der Fokus offenbar lieber auf Glitzer-Technologien wie künstliche Intelligenz und Blockchain gelegt wird, die jedoch wieder Zentralität und damit weniger Resilienz bedeuten können. Inselnetzwerke könnten eine Alternative bieten, sind jedoch kaum vorhanden und werden weder angeboten noch staatlich gefördert.

Es heißt, der bisherige Schwerpunkt der klassischen IT-Sicherheit müsse zu einem ganzheitlichen Ansatz der Cyber-Sicherheit weiterentwickelt werden. Was bedeutet das?

Die IT-Sicherheit war lange Zeit ein rein technisches Thema, bei dem die IT-Abteilung für die Sicherheit der Systeme zuständig war. Doch diese Herangehensweise reicht heutzutage nicht mehr aus, da neue Bedrohungen wie Phishing aufkommen und IT-Systeme nicht in der Lage sind, solche Angriffe zu verhindern. Deshalb müssen nicht nur die Anwender geschult werden, sondern auch die Hersteller müssen ihre Systeme so gestalten, dass sie vor Angriffen geschützt sind. Um IT-Systeme zu schützen, sind auch organisatorische Maßnahmen wie Richtlinien und Anpassungen der Arbeitsabläufe notwendig, um Sicherheits-Know-how in alle Bereiche zu bringen. Die Verantwortung für die IT-Sicherheit liegt also nicht allein bei der IT-Abteilung, sondern auch die Geschäftsführung ist gefordert, entsprechende Maßnahmen zu ergreifen.

„Einem KRITIS-Betreiber kann es völlig egal sein, wer der Täter ist.“
Die Häufigkeit und Schwere von Cyber-Angriffen auf die IT-Infrastrukturen von Stadtwerken haben zugenommen. Was können kommunale Versorger konkret tun, um ihre IT-Systeme zu schützen?

Die Stadtwerke müssen zunächst erkennen, dass die IT-Sicherheit alle Mitarbeiterinnen und Mitarbeiter betrifft. Die Geschäftsleitung muss den Willen haben, Cyber-Sicherheit umzusetzen und ganzheitlich zu betrachten. Die Mitarbeitenden müssen geschult werden, wie Sicherheitsrisiken minimiert werden können. Und es muss eine positive Fehlerkultur etabliert werden.

Für wie wahrscheinlich halten Sie es, dass ein Cyber-Angriff zu einem Blackout in Deutschland führt?

Ein Blackout ist sehr unwahrscheinlich, ob durch einen Cyber-Angriff oder andere Ereignisse. Dies könnte sich in Zukunft durch eine schlechte Digitalisierung des Energiesystems ändern. Ein Beispiel ist die Fernwartung von Energieanlagen. Ich habe mir das als KRITIS-Auditor angeschaut und muss sagen, es

sieht sicherheitstechnisch düster aus. Anstatt die Fernwartung sicher zu machen, wird den KRITIS-Betreibern vorgeschrieben, dass sie Angriffserkennungssysteme einführen müssen. Das kann man machen, wenn man eine sichere Umgebung hat und keine offenen Scheunentore wie bei der Fernwartung. Aber heute ist es einfacher, einen Blackout durch physische Maßnahmen herbeizuführen als durch einen Cyber-Angriff.

War Russlands Krieg gegen die Ukraine hierzulande ein Weckruf für mehr Cyber-Sicherheit?

Im Moment sehe ich keinen Weckruf, außer vielleicht für die Rüstungsindustrie. Im Bereich der Cyber-Sicherheit geht es bei uns darum, wer der Täter war und wie das Lagebild aussieht. Einem KRITIS-Betreiber kann es aber völlig egal sein, wer der Täter ist. Ich kann nur sagen: Egal, ob es eine Ransomware-Bande, ein Cyber-Hooligan oder ein Geheimdienst war, ihr müsst ein Back-up haben. Also: Kümmert euch nicht um Täter oder Lagebilder, sondern schafft die Basis-Infrastruktur für sichere, resiliente IT-Systeme.

()

Dieser Beitrag ist im Schwerpunkt IT-Sicherheit der Ausgabe März/April 2023 von stadt+werk erschienen. Hier können Sie ein Exemplar bestellen oder die Zeitschrift abonnieren.

Stichwörter: Informationstechnik, AG KRITIS, IT-Sicherheit