ZfK Zeitung für kommunale Wirtschaft

IT

ZfK+ "Drei Themen der Cybersicherheitsstrategie 2021 sind von besonderem Interesse"

Thomas Schuster von der Kanzlei GvW Graf von Westphalen analysiert in der ZfK die neue Cybersicherheitsstrategie: Was bedeutet sie für Stadtwerke und wo gibt es noch Verbesserungspotenzial.

05.10.2021

"Nicht zuletzt ist auch die Verbesserung des Schutzes Kritischer Infrastrukturen ein prägendes Ziel der neuen Cybersicherheitsstrategie", sagt Rechtsanwalt Thomas Schuster.

Bild: © Graf von Westphalen

Herr Schuster, die Regierung hat die neue deutsche Cybersicherheitsstrategie verabschiedet, hat diese auch Auswirkungen auf Stadtwerke und Kommunen?

Thomas Schuster, Partner und Rechtsanwalt bei der Kanzlei GvW Graf von Westphalen: Ja, die Cybersicherheitsstrategie hat Auswirkungen auf Stadtwerke und Kommunen. Zwar ist die Strategie zunächst einmal eine solche der Bundesregierung. Sie bildet für die kommenden fünf Jahre aber das Korsett für das Handeln der Bundesregierung in Themen der Cybersicherheit und damit auch unter anderem für regulatorische Maßnahmen. Drei Punkte sind von besonderem Interesse:

Angesprochen sind Kommunen und Stadtwerke direkt und unmittelbar, wenn es um ihre eigene digitale Transformation geht. E-Government und OZG-Umsetzung erfordern durchweg eine belastbare Cyber- und Informationssicherheit. Ohne selbige können sich die Bürgerinnen und Bürger nicht frei und selbstbestimmt in einer digialisierten Umgebung bewegen. Fehlt es hieran, so wird dies mit einem Mangel von Vertrauen und Akzeptanz einhergehen. Bezogen auf die Stadtwerke als Dienstleister sind hier vor allem die Themenfelder aus dem Smart-City-Kontext und der Telekommunikation angesprochen. Verletzungen der Cybersicherheit in diesen sensiblen Bereichen gehen mit einem hohen Schadenspotential einher. Zu dem Themenfeld Digitalisierung im

öffentlichen Sektor wird es in der Zukunft neben den bestehenden Handlungsempfehlungen zur IT-Sicherheit in der öffentlichen IT dem Vernehmen nach weitere Konkretisierungen geben. Zu beobachten ist selbstverständlich auch die Bundesverordnung zu § 5 OZG, die einen wesentlichen Regelungsrahmen für die IT-Sicherheit in E-Government und Portalverbund bildet.

Zentral ist in der Cybersicherheitsstrategie, dass die deutsche digitale Wirtschaft gestärkt werden soll. Konkret steht die Erhöhung der IT-Sicherheit der Produkte beziehungsweise die Schaffung von Produkten zur Erhöhung der IT-Sicherheit in bestimmten Wirtschaftszweigen im Vordergrund: Bezogen auf Kommunen und Stadtwerke sind das insbesondere energiewirtschaftliche wie auch Smart-City-Themen. Hinsichtlich der Energiewirtschaft ist in der Strategie besonders die Smart-Metering-Public-Key-Infrastructure (PKI) als zentrale Infrastrukturkomponente für die Digitalisierung der Energiewende angesprochen.

Flankierend nimmt die Roadmap des Bundeswirtschaftsministeriums und des Bundesamts für Sicherheit in der Informationstechnik (BSI) zur Entwicklung technischer Eckpunkte für die Einsatzbereiche Smart Grid, Smart Mobility und Smart- beziehungsweise Sub-Metering im Rahmen mehrerer Standardisierungsprojekte Gestalt an. Im Bereich der Smart Cities werden bestehende kommunale IoT-Infrastrukturen analysiert und hieraus Handlungsempfehlungen der Zukunft abgeleitet. Zudem werden Technische Richtlinien und weitere Standards für den cyber- und informations-sicheren Betrieb von Smart-City-Lösungen entwickelt.

Nicht zuletzt ist auch die Verbesserung des Schutzes Kritischer Infrastrukturen ein prägendes Ziel der neuen Cybersicherheitsstrategie. Nach den jetzt bereits bestehenden gesetzlichen Vorgaben müssen die Betreiber Kritischer Infrastrukturen wie Energie, Telekommunikation, Wasser und Mobilität – damit stehen die Stadtwerke hier mit an vorderster Front – dem BSI regelmäßig Nachweise über ihre technischen und organisatorischen Maßnahmen zur Wahrung der IT-Sicherheit vorlegen. Zentral hierbei ist der Stand der Technik für die verschiedenen Branchen. In diesem Themenbereich sind drei strategische Ziele besonders zu erwähnen: zum einen sollen die Möglichkeiten und Befugnisse des BSI für Vor-Ort-Prüfungen ausgeweitet werden, zum weiteren soll der Stand der Technik für weitere KRITIS-Sektoren fortentwickelt werden und zuletzt ist in den Blick genommen, dass durch das Vorhalten eines umfassenden Cyberbedrohungslagebildes eine Möglichkeit geschaffen werden soll, etwaige Cyberangriffe auf KRITIS-Betreiber im Vorfeld erkennen und entsprechend abwehren zu können.

Stark kritisiert wird auch, dass es – nicht erst durch die neue Cybersicherheitsstrategie – Einfallstore für den Verfassungsschutz wie die Polizei- und Strafverfolgungsbehörden gibt. Zum einen soll zukünftig auch verschlüsselte Kommunikation für diese einsehbar sein, des Weiteren sollen Zero-Day-Schwachstellen auch für die staatliche Strafverfolgung eingesetzt werden können. Kritiker sehen darin gleichfalls auch ein Einfallstor für kriminelle Hacker und weniger einen Beitrag zur Cybersicherheit. Wie bewerten Sie diese Entwicklungen und betrifft das Zero-Day-Risiko auch Betreiber Kritischer Infrastrukturen?
Die Lage bei Zero-Day-Schwachstellen ist diffus, sowohl rechtlich wie in praktischer Hinsicht. Cyber- und Informationssicherheit bietet – vereinfacht gesprochen – Schutz für die Nutzerinnen und Nutzer von IT-Produkten und großen, vernetzten IT-Systemen mit dem Ziel der Verhinderung von Informationsverlusten und Cyberangriffen. Von diesem Schutz profitieren freilich auch Menschen mit unlauteren Motiven: Sie suchen sich Informations- und Kommunikationswege, in welchen sie ihre Absicht hinreichend vor den Sicherheitsbehörden geheim halten können. Haben IT-Systeme nun Sicherheitslücken in Gestalt von Zero-Day-Schwachstellen, so sind selbige selbstverständlich auch ein willkommenes Ziel für staatliche Ermittlungsmaßnahmen, wenn die gesetzlichen Voraussetzungen vorliegen. Zero-Day-Schwachstellen sind solche, die den Herstellern von Soft- und Hardware noch unbekannt sind. Dadurch entsteht ein kaum aufzulösendes Dilemma: Einerseits soll der Staat Cybersicherheit möglichst bestmöglich gewährleisten, auf der anderen Seite benötigen Sicherheitsbehörden auch Zugriffsmöglichkeiten auf ansonsten ohne Zero-Day-Schwachstellen zum Eindringen kaum geeignete Systeme. Ein sofortiger Bericht an den Hersteller könnte damit die Ermittlungs- und Gefahrenabwehrmöglichkeiten verringern.

In der neuen Cybersicherheitsstrategie 2021 bekommt der „verantwortungsvolle Umgang mit Zero-Day-Schwachstellen und Exploits“ ein eigenes Handlungsfeld. Das eben beschriebene Dilemma ist innerhalb der gesetzlichen Rahmenbedingungen und unter Wahrung des größtmöglichen Schutzes für alle betroffenen Rechtsgüter im Wege praktischer Konkordanz aufzulösen. Die

Cybersicherheitsstrategie 2021 möchte dieses Dilemma weitestgehend dadurch auflösen, dass die durch die bestehenden Gesetze in der Lage befindlichen Sicherheitsbehörden durch eine „ausgewogene behördenübergreifende Strategie“ des Umgangs mit Zero-Day-Schwachstellen die Interessen der Cyber- und Informationssicherheit sowie der Sicherheitsbehörden in einen angemessenen Ausgleich bringen. Als Mittel der Wahl sind standardisierte Prozesse vorgesehen, die im Ergebnis zu einem verbindlichen Vorgehen in der Praxis führen.

Besonderes Feuer hat die Diskussion durch einen jüngst im Juni 2021 ergangenen Beschluss des Ersten Senats des Bundesverfassungsgerichts erhalten: Danach muss der Gesetzgeber selbst den Umgang der Sicherheitsbehörden mit Zero-Day-Schwachstellen regeln. Das folge aus der bestehenden staatlichen Schutzpflicht. Bereits aus Gründen des Verfassungsrechts genügt die Herangehensweise in der Cybersicherheitsstrategie nicht mehr. Eine behördeninterne Abstimmung nebst untergesetzlichen Prozessen wird den Grundrechten nicht gerecht.

Der Gesetzgeber ist damit aufgerufen, hier zu handeln und den Umgang mit Zero-Day-Schwachstellen für die Sicherheitsbehörden gesetzlich zu regeln. Ein einschränkungsloser Vorrang für die Sicherheitsbehörden wird keinesfalls zu dulden sein. Letztendlich führen Zero-Day-Schwachstellen zu weitreichenden Angriffsmöglichkeiten mit hoher Schadensneigung gerade auch für Betreiber Kritischer Infrastrukturen. Das Bundesverfassungsgericht hat jedoch andererseits auch deutlich gemacht, dass einerseits kein grundrechtlicher Anspruch besteht, jede unerkannte IT-Sicherheitslücke sofort und unmittelbar an den Betreiber der IT-Infrastruktur zu melden. Es wäre zu wünschen, dass der Gesetzgeber hier schnell eine praxistaugliche Lösung findet und eine sinnvolle und grundrechtskonforme Abschichtung zwischen den bestehenden Interessen findet.

Worin sehen Sie Verbesserungen bei der neuen Cybersicherheitsstrategie und was könnte man noch verbessern?
Eine der Hauptherausforderungen der Gewährleistung von Cybersicherheit ist der Umgang mit Cyberangriffen. Hier ist positiv zu erkennen, dass sich die Cybersicherheitsstrategie sich einem besseren Informationsaustausch zwischen Staat, Wirtschaft, Wissenschaft und Gesellschaft verschreibt. In der Strategie ist nunmehr festgehalten, dass alle an der Cyberabwehr beteiligten Organisationen aus ihren jeweiligen Verantwortungsbereich so weit Informationen beitragen, wie dies der Geheimnisschutz und der Datenschutz erlauben. Letztendlich soll eine Kommunikationsplattform geschaffen werden, die einen effizienten Informationsaustausch ermöglicht. Soweit dies technisch und rechtlich möglich ist, sollen diese Informationen auch automatisiert geteilt werden. Das ist in jedem Falle begrüßenswert. Auf der anderen Seite steht aber ein kaum mehr zu durchdringendes Dickicht an staatlichen Stellen und anderen, staatsnahen Organisationen, die jede für sich eine Rolle in der „Cybersicherheitsarchitektur“ innehaben. Hier wäre dringend eine Verschlankung und Konzentrierung des Gesamtapparates auf wenige zentrale Stellen geboten, gerne mit einer entspre-chenden gesetzlichen Flankierung.

Begrüßenswert ist aus Sicht der Kommunen und Stadtwerke sicherlich auch die Aufnahme und verstärkte Herausbildung des „Security-by-Design“-Ansatzes, der an mehreren Stellen Eingang in die Strategie gefunden hat. Wie bereits der VKU in seiner Stellungnahme aus dem März 2021 zu den damaligen Eckpunkten der neuen Cybersicherheitsstrategie betont hat, ist es aus der Sicht der kommunalen Unternehmen ein zentrales Anliegen, dass hier die Hersteller von Hard- und Software noch stärker in die Verantwortung genommen werden.

Zuletzt sind die stärkere Einbettung der Bundesrepublik in das europäische Netzwerk der Cybersicherheitsakteure und die Vermeidung von Doppelregulierungen von großer Bedeutung, da letztlich ein Staat wie die Bundesrepublik Deutschland in Sachen Cybersicherheit mit einem rein nationalen Ansatz nicht weiterkommen kann. Andererseits ist im Blick zu halten, dass eine Regulierung auch immer die mitgliedstaatlichen Besonderheiten beachten sollte. Gerade die starke Rolle der kommunalen Wirtschaft mit ihren Unternehmen als Akteur im Bereich der öffentlichen Versorgung ist eine deutsche Besonderheit, die stellenweise bei der Fassung entsprechender Regulierungsmaßnahmen mitgedacht werden sollte.

Zusammenfassend ist die neue Cybersicherheitsstrategie 2021 ein wichtiges Instrument der Fortentwicklung von Recht und Regulierung in Cyber- und Informationssicherheit, nicht aber der große Wurf. Am Ende wird es auf die konkrete Umsetzung in Praxis und Recht ankommen.

Die Fragen stellte Stephanie Gust

Mehr zum Thema

Bild: @ PwC

IT

PwC baut Partnerschaft mit Powercloud aus

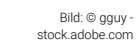

Bild: © gguy - stock.adobe.com

IT

Microsoft mit Notausschalter für Exchange Server

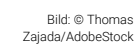

Bild: © Thomas Zajada/AdobeStock

IT

Hacker greift Stadtwerke Wismar an