IT-Sicherheit

Feuerwehr und Firewall

[02.09.2024] Cyberattacken treffen immer öfter auch Verwaltungen. Um kommunale IT besser abzusichern, fordert Vitako eine Reihe von Maßnahmen: eine stärkere Vernetzung, mehr Mittel, den Ausbau des BSI zur Zentralstelle und die Schaffung eines regulativen Rahmens.

Die Bedrohung im Cyberraum ist so hoch wie nie zuvor. Dabei stehen nicht mehr nur zahlungskräftige Wirtschaftsunternehmen im Fokus der Angreifer, sondern zunehmend auch staatliche Institutionen und Kommunen. Für Verwaltung, Bürger und Wirtschaft entstehen im Angriffsfall enorme Schäden – unverzichtbare Verwaltungsleistungen stehen wochen- oder monatelang nicht zur Verfügung, mitunter gelangen auch persönliche Daten in die Hände Krimineller. Wie gravierend die Folgen erfolgreicher Cyberangriffe auf Kommunalverwaltungen und kommunale Betriebe sind, haben prominente Vorfälle im Landkreis Anhalt-Bitterfeld, im Rhein-Pfalz-Kreis (40164+wir berichteten), in der Stadt Potsdam (40808+wir berichteten) und zuletzt beim kommunalen IT-Zweckverband Südwestfalen-IT (44288+wir berichteten) gezeigt. Trotz dieser Bedrohungslage sind aber viele kommunale IT-Infrastrukturen nicht ausreichend abgesichert. **Frage nach angemessenem Schutz** Die Bundes-Arbeitsgemeinschaft der Kommunalen IT-Dienstleister, Vitako, stellte die Frage, wie ein angemessener Schutz für systemrelevante kommunale IT erzielt werden kann, in den Mittelpunkt eines parlamentarischen Abends. Im Juni hatte der Verband Expertinnen und Experten aus der Politik, aus der Verwaltung und von Seiten der kommunalen IT-Dienstleister zu einer Paneldiskussion ins Tagungszentrum im Haus der Bundespressekonferenz geladen und präsentierte außerdem sein Positionspapier zum Thema. Auf kommunaler Ebene gebe es derzeit keine bundesweit einheitlichen Vorgaben bezüglich Informationssicherheit, konstatierte Gerhard Schabhüser, der Vizepräsident des Bundesamts für Sicherheit in der Informationstechnik (BSI), in seiner Keynote. Das BSI könne Kommunen zwar dabei helfen, ihre Resilienz zu erhöhen und Cyberangriffe zu bewältigen, in der Rolle als Cybersicherheitsagentur des Bundes sei der Handlungsspielraum des BSI aber eingeschränkt: „Aufgrund der fehlenden Rechtsgrundlage sind wir in vielen Fällen auf das Mittel der Amtshilfe angewiesen. Die Bedrohungslage erfordert aber eine verstetigte, institutionalisierte Zusammenarbeit zwischen Bund, Ländern und Kommunen. Dazu muss der Rechtsrahmen geschaffen und das BSI zur Zentralstelle ausgebaut werden“, betonte der BSI-Vizepräsident. Derzeit, so räumte Schabhüser in der anschließenden Panel-Diskussion ein, finde diese Konzeption allerdings keine Mehrheit. **Ausbau zu einer interföderalen Zentralstelle** Auch Vitako fordert in ihrem Positionspapier den Ausbau des BSI zu einer interföderalen Zentralstelle und die Schaffung der entsprechenden Rechtsgrundlage. Die Kommunen und ihre IT-Dienstleister müssten vollumfänglichen Zugriff auf detaillierte, auf die Situation in Kommunen abgestellte Lage-Informationen des BSI erhalten und sowohl präventiv als auch bei einem IT-Sicherheitsvorfall umfassend vom BSI unterstützt werden. Gemeinsam mit den Ländern könne das BSI im Schadensfall dann etwa den Wiederanlauf der kommunalen IT unterstützen. Ähnlich wie bei der Verwaltungsdigitalisierung, bei der sich Bund, Länder und Kommunen zunehmend stärker vernetzen, sei auch der Schutz öffentlicher Verwaltungen eine Gemeinschaftsaufgabe über alle föderalen Ebenen hinweg, so der Verband. Zudem müssten Kommunen und kommunale IT-Dienstleister in einheitliche interföderale Vernetzungs- und Unterstützungsstrukturen – etwa Landes-CERTs – eingebunden werden, so Vitako. Die schon jetzt vielerorts stattfindenden Vernetzungsaktivitäten benötigten geregelte, einheitliche Informationsstrukturen und müssten flächendeckend erfolgen. Das Teilen von Informationen über Sicherheitsvorfälle und den Umgang damit führe letzten Endes dazu, dass

die kommunale Gemeinschaft insgesamt resilienter dastehe, sagte Schabhüser – auch wenn Betroffene dieser Art des Sharings zunächst eher skeptisch gegenüberstünden. **Einstufung der kommunalen IT als KRITIS** Vitako fordert schon seit Langem, dass kommunale IT als Kritische Infrastruktur (KRITIS) eingestuft wird, damit die Sicherheit der kommunalen Verwaltungs-IT verbindlich und einheitlich festgelegt werden kann. Diese Position bekräftigte der Verband auch während seiner Veranstaltung – deren Termin noch vor dem Beschluss des Bundeskabinetts zum NIS2-Umsetzungsgesetz lag – und in dem vorgelegten Paper. Zudem müssten Bund und Länder sicherstellen, dass die Kommunen finanzielle Mittel erhalten, um notwendige Schutzmaßnahmen umzusetzen. Nur so könne für die kommunale Verwaltungs-IT ein verbindliches und einheitliches Sicherheitsniveau geschaffen werden, betonte der Komm.ONE-Chef und stellvertretende Vitako-Vorstandsvorsitzende William Schmitt während der Diskussion. Dies müsse bei der Umsetzung der NIS2-Richtlinie in nationales Recht berücksichtigt werden. Inzwischen – am 24. Juli 2024 – hat das Bundeskabinett den von Bundesinnenministerin Nancy Faeser vorgelegten Entwurf für ein Gesetz zur Stärkung der Cybersicherheit beschlossen, mit dem die zweite EU-Richtlinie zur Netzwerk- und Informationssicherheit (NIS2) umgesetzt wird. Länder und Kommunen sind vom NIS2-Umsetzungsgesetz nicht explizit benannt. **Einigkeit über regulativen Rahmen** Bei den Diskutanden des Vitako-Empfangs im Juni herrschte Einigkeit darüber, dass ein regulativer Rahmen unumgänglich ist, um die Cybersicherheit von Kommunen zu stärken. Wenn dies nicht über das NIS2-Umsetzungsgesetz erfolge, die kommunale IT als KRITIS klassifiziere, müsse dieser Rahmen auf andere Weise geschaffen werden, betonte Gerhard Schabhüser. Dass ein solcher Rahmen fehle, obwohl die Kommunen die Mehrheit der öffentlichen Leistungen erbrächten, habe konkrete Folgen: Es fehle sowohl an Konzepten wie auch an Mitteln, sagte Jens Zimmermann, Obmann im Ausschuss für Digitales im Bundestag. Man müsse dahinkommen, dass kommunale Räte nicht nur Feuerwehrautos, sondern auch Firewalls selbstverständlich finanzieren könnten. Lars Hoppmann, Geschäftsleiter beim IT-Zweckverband Ostwestfalen-Lippe-IT (OWL-IT) und stellvertretender Vitako-Vorstandsvorsitzender, betonte noch einmal die Wichtigkeit verbindlicher Richtlinien. Mehr Mittel seien gut, so Hoppmann, doch dies sei nicht ausreichend: Auch die Strukturen müssten sich dringend ändern. Potsdam war im Januar 2020 und im Dezember 2022 von Cybersicherheits-Vorfällen betroffen und hatte jeweils präventiv die IT-Systeme vom Netz genommen. Melitta Kühnlein, die in der Landeshauptstadt den Bereich IT-Strategie leitet, berichtet von „Danach“: Als Kommune sei man bei einem solchen Angriff allein. So sei von drei Amtshilfeanträgen nur einer erfolgreich gewesen, die Zusammenarbeit mit unterstützenden IT-Dienstleistern indes war reibungslos. Allerdings, betonte Kühnlein, sei Potsdam finanziell recht gut ausgestattet und daher nicht repräsentativ für alle Kommunen. Ein umfassender Plan fehle und werde dringend benötigt.

()

Dieser Beitrag ist in der Ausgabe September 2024 von Kommune21 im Schwerpunkt IT-Sicherheit erschienen. Hier können Sie ein Exemplar bestellen oder die Zeitschrift abonnieren.

Stichwörter: IT-Sicherheit, KRITIS, Vitako