INSTITUT FÜR INNOVATION UND TECHNIK

DStGB Deutscher Städte- und Gemeindebund

PRESSEERKLÄRUNG

Berlin, 25.03.2025

Zukunftsradar 2024
Gemeinsamer. Digitaler. Sicherer.

Über 1.000 Kommunen senden ein klares Signal in Richtung Bund und Länder: Wenn wir die Chancen der Digitalisierung zum Wohle der Gesellschaft nutzen wollen, müssen Arbeitsstrukturen beschleunigt und verschlankt werden. Der heute veröffentlichte Zukunftsradar von DStGB und Institut für Innovation und Technik (iit) liefert aussagekräftige Daten zur Kooperationsbereitschaft der Städte und Gemeinden: 94 Prozent der befragten Kommunen würden es begrüßen, wenn eine verbindliche, föderale IT-Infrastruktur mit einheitlichen Schnittstellen und zentralen Basisdiensten zur Verfügung stehen würde.

„Städte und Gemeinden sind nicht lediglich Außenstellen von Bund und Ländern. Wenn es bei digitalen Prozessen, wie etwa bei der Kfz-Zulassung, nur darum geht, Leistungen zu erbringen, bei denen es kein Ermessen vor Ort gibt, sollten diese auch zentral von Bund und Ländern erbracht werden. Gleiches gilt für Leistungen wie Meldewesen, Wohngeld oder weitere Bundesleistungen. Wir müssen jetzt schnell ins Handeln kommen. In einem ersten Schritt sollte ein für alle Kommunen nutzbares Softwareangebot bereitgestellt werden. Die Daten aus dem Zukunftsradar unterlegen eindrücklich, dass die Kommunen startklar sind für ein dringend erforderliches Update der föderalen Kooperationen in der Digitalisierung,“ formuliert **DStGB-Hauptgeschäftsführer Dr. André Berghegger**.

Auch im Bereich der Cybersicherheit müssen wir unsere Strukturen überdenken und eine stärker auf Vernetzung und Zusammenarbeit ausgerichtete Sicherheitsarchitektur etablieren. *„Cybersicherheit geht nur gemeinsam. Eine immer differenziertere digitale*

Deutscher Städte- und Gemeindebund

Marienstraße 6
12207 Berlin

Alexander Handschuh
Pressesprecher

Telefon 030.773 07.253
E-Mail:
alexander.handschuh@dstgb.de

Institut für Innovation und Technik (iit):

Lorenz Hornbostel

Telefon: 030. 310078.4079
E-Mail:
hornbostel@iit-berlin.de

Bedrohungslage macht auch vor Städten und Gemeinden nicht Halt. Rund ein Viertel der Kommunen war laut Zukunftsradar in den vergangenen zwei Jahren Ziel einer Cyber-Attacke. Das dürfen wir nicht einfach so stehen lassen. Um Bürgerinnen und Bürger, unsere Demokratie und unsere Werte besser vor Spionage, Desinformation und Destabilisierung zu schützen, müssen wir in Zukunft stärker auf Zusammenarbeit setzen. Ohne substanzielle Investitionen in die IT-Infrastruktur werden wir unsere Systeme auf Dauer nicht schützen können", sagt **Dr. Werner Wilke, Geschäftsführer des Instituts für Innovation und Technik (iit) in der VDI/VDE Innovation + Technik GmbH.**

„Mehr Informationsaustausch, stabile Kooperationen, Standards und harmonisierte Meldeketten bei Sicherheitsvorfällen müssen Teil einer gesamtstaatlichen Strategie gegen hybride Bedrohungen sein. Der Vorstoß, die Lockerung der Schuldenbremse für sicherheitspolitische Ausgaben auch auf den Bereich Cybersicherheit auszuweiten, ist die richtige und notwendige Schlussfolgerung, um ein Mehr an Cybersicherheit auch finanziell zu hinterlegen. Daneben gehören jetzt aber auch die derzeitigen Strukturen und Zuständigkeiten auf den Prüfstand: Wir können es uns nicht länger leisten, dass zentrale Stellen auf Bundesebene, die wie Bundeswehr, Polizei, Nachrichtendienste und BSI, die alle mit Sicherheitsfragen befasst sind, nicht deutlich vernetzter agieren und reagieren. Die Kommune als kleinste Einheit im Staatsgefüge ist zwingend auf die Zusammenarbeit und den Informationsaustausch mit den nationalen Akteuren angewiesen", unterstreicht **Berghegger.**

Bund, Länder und Kommunen müssen technisch, organisatorisch, finanziell und personell in die Lage versetzen, sich präventiv und reaktiv auf Cyberangriffe einzustellen. Bund und Länder stehen hier in der Verantwortung für ein möglichst hohes Maß an Sicherheit auf der kommunalen Ebene zu sorgen. Dies wird aus Sicht der Kommunen aber nur unzureichend gelingen können, wenn die Kompetenzen des BSI nicht deutlich ausgeweitet werden und in seiner Funktion für ein einheitliches Mindestniveau der Cyberresilienz verantwortlich zeichnet.

„Die Schaffung von Cybersicherheit wird zusätzliche und fortlaufend steigende Kosten mit sich bringen. Hier besteht kein Spielraum für Abstriche oder Kompromisse. Denn Digitalisierung und Sicherheit sind von herausragender Bedeutung für einen funktionierenden, effizienten und verlässlichen Staat", unterstreichen **Berghegger und Wilke** abschließend.