Dezernat I

Ressort Digitales & Kommunikation

Sitzungsvorlage 2021/454

CRAILSHEIM

Anfrage der GRÜNEN-Fraktion vom 28.10.2021 / Stadtrat Karg Cybersicherheit der Stadtverwaltung

Gremium	Termin	Beratungsfolge	Status
Gemeinderat	16.12.2021	Kenntnisnahme	öffentlich

Anlagen

Weitere beteiligte Ressorts

Sachverhalt und Begründung

Die Digitalisierung gehört zu den zentralen kommunalen Herausforderungen unserer Zeit. Mit dem Ausbau der elektronischen Vernetzung, einer zunehmenden IT-Unterstützung der kommunalen Strukturen und der damit verbundenen Abhängigkeit von diesen Systemen sind zwangsläufig Risiken verbunden. Die Bedrohungslage durch Cyberangriffe hat sich in der jüngsten Vergangenheit durch verschiedene Faktoren in rasantem Tempo drastisch verschärft. Auch staatliche und öffentliche Institutionen sind ebenso wie Kommunalverwaltungen im Visier von kriminellen Hackergruppen.

Insbesondere Cyberangriffe mittels Ransomware haben in jüngster Vergangenheit massiv zugenommen. Hierbei handelt es sich um besonders gefährliche Schadsoftware, die häufig etwa über E-Mail-Anhänge verbreitet wird. Hier genügt ein unvorsichtiges Öffnen eines infizierten E-Mail-Anhangs. In der Folge können alle verfügbaren Daten des Netzwerks verschlüsselt werden, wodurch im Zweifel die gesamte IT-Infrastruktur nicht mehr genutzt werden kann. Die Angreifer fordern dann zumeist ein Lösegeld für die Wiederherstellung der unbrauchbar gemachten Daten. Durch die Verschlüsselung kann es im Zweifel zu einem mehrwöchigen oder gar mehrmonatigen Verwaltungsausfall kommen, denn die elektronische Datenverarbeitung ist heute die fundamentale Arbeitsgrundlage – auch der Stadtverwaltung Crailsheim.

Es ist aus Sicht der Verwaltung gerade in Anbetracht der akuten Bedrohungslage unbedingt erforderlich, den digitalen Wandel mit ganzheitlichen, vorausschauenden und gleichzeitig effizienten Cybersicherheitsmaßnahmen zu begleiten, um die weiter fortschreitende kommunale Digitalisierung auf ein tragfähiges und stets in Stand gehaltenes Fundament zu stellen. Im Spannungsfeld der öffentlichen Aufgabenwahrnehmung, einer immer komplexer werdenden Umwelt und dem gestiegenen Erwartungsdruck Dritter bedarf es eines konsequenten Vorgehens, das gleichzeitig jederzeit offen genug ist, um organisationales Lernen und die Wahrnehmung neuer Risiken und Sicherheitsmöglichkeiten zu ermöglichen.

Dem Cybersicherheitskonzept der Stadtverwaltung sind zwei Dimensionen inhärent, die präventive und reaktive Maßnahmen enthalten. Zum präventiven Bereich gehören umfangreiche technische Maßnahmen auf neuestem Niveau, etwa eine redundant aufgestellte Firewall, Viren- und Angriffsschutz, Spamfilter und Patchmanagement. Das Ressort Digitales & Kommunikation arbeitet bei der technischen

Prävention mit verschiedensten Partnern zusammen – aus dem privaten wie dem öffentlich-rechtlichen Bereich. Im landesweiten Verbund des Kommunalen Verwaltungsnetzes sowie des Landesverwaltungsnetzes ist das kommunale Rechenzentrum Komm.ONE, an dem die Stadt Crailsheim über den Zweckverband 4IT mittelbar beteiligt ist, engster öffentlich-rechtlicher Partner.

Zu den Präventionsmaßnahmen zählen auch nicht-technische Vorkehrungen wie beispielsweise organisatorische Vorgaben zur Nutzung dienstlicher IT-Infrastruktur sowie die Fortbildung und Sensibilisierung der Mitarbeiterinnen und Mitarbeiter der Verwaltung. Cybersicherheit und der Schutz personenbezogener Daten greifen hierbei Hand in Hand. So werden zum Beispiel bei der Stadtverwaltung regelmäßig fingierte Phishing-Mails an alle Mitarbeitenden versandt, um einerseits gezielt zu sensibilisieren und andererseits zu eruieren, inwieweit diese Form des Angriffsrisikos im Bewusstsein der Belegschaft verankert ist.

Reaktive Maßnahmen umfassen ebenso technische wie organisatorische Maßnahmen. So setzt die Stadtverwaltung unter anderem seit diesem Jahr eine neuartige Sicherheitssoftware ein, die gestützt auf Künstliche Intelligenz die gesamte IT-Infrastruktur der Verwaltung zu jeder Zeit genauestens beobachtet und etwaige Anomalien umgehend erkennt. Sollte es also trotz aller präventiven Vorkehrungen tatsächlich zu einem schädlichen Vorfall kommen, kann hierauf zügig reagiert werden, mit dem Ziel, den möglichen Schaden so gering wie möglich zu halten. Zusätzlich hat das Ressort Digitales & Kommunikation ein schlagkräftiges Unternehmen vertraglich gebunden, das im Schadensfall unter anderem forensische Untersuchungen durchführt, um festzustellen, welche Gründe zu dem Vorfall führten und wie nun angemessen zu reagieren ist, um die IT-Infrastruktur schnellstmöglich wieder produktiv nutzen zu können.

Im Ergebnis muss klar sein, dass es keine absolute Sicherheit für IT-Infrastrukturen geben kann und es das Thema Cybersicherheit erfordert, laufend die bestehenden und geplanten Maßnahmen auf deren Angemessenheit kritisch zu hinterfragen. Dennoch sieht sich die Verwaltung zeitgemäß aufgestellt, um etwaige Bedrohungen abzuwenden und nötigenfalls angemessen auf Vorfälle reagieren zu können, damit die Arbeitsfähigkeit der Stadtverwaltung zuverlässig aufrechterhalten werden kann.