Stadt Zürich
Stadtrat

# Beschluss des Stadtrats

vom 30. Oktober 2024

GR Nr. 2024/417

## Nr. 3292/2024
## Schriftliche Anfrage von Flurin Capaul und Roger Suter betreffend Systemausfälle als Folge eines Updates der Software CrowdStrike, Verwendung von Cloud-Diensten durch die Stadt, Prüfung der Risiken hinsichtlich eines ausfallsicheren Betriebs und Beurteilung der Abhängigkeit kritischer IT-Systeme zu Drittanbietern

Am 4. September 2024 reichten die Mitglieder des Gemeinderats Flurin Capaul und Roger Suter (beide FDP) folgende Schriftliche Anfrage, GR Nr. 2024/417, ein:

Mitte Juli führte ein Update der CrowdStrike Software zu weltweiten Ausfällen von Medienanstalten, Flughäfen- und Fluglinien, Zahlungssystem und weiteren kritischen Systemen. Microsoft schätzte, dass 8.5 Mio Systeme betroffen waren.

Eine kurze Analyse der CrowdStrike AGB durch einen Experten für Recht im digitalen Raum, zeigte dass darin kritische Passagen enthalten waren:

«Die CrowdStrike-Angebote und CrowdStrike-Tools sind nicht fehlertolerant und nicht für den Einsatz in gefährlichen Umgebungen ausgelegt oder vorgesehen, die eine ausfallsichere Leistung oder einen ausfallsicheren Betrieb erfordern.»

In diesem Zusammenhang bitten wir den Stadtrat um die Beantwortung der folgenden Fragen:

1. Verwendet die Stadt Zürich Cloud Dienste im Allgemeinen und/oder für kritische Applikationen? Wenn ja, welche externen Cloud Dienste werden häufig verwendet?
2. Werden die AGB von Cloud Diensten geprüft und hinsichtlich Risiken für ausfallsicheren Betrieb geprüft? Falls ja, von wem?
3. Beinhalten die AGBs von Cloud Diensten weitere vergleichbare/ ähnliche Klauseln, welche die Stadt Zürich im Betrieb ihrer Applikationen einschränkt?
4. Wie beurteilt der Stadtrat i.A. die Abhängigkeit kritischer IT-Systeme zu Drittanbieter? Was für Risiken für die Stadt ergeben sich daraus?

Der Stadtrat beantwortet die Anfrage wie folgt:

### Frage 1
### Verwendet die Stadt Zürich Cloud Dienste im Allgemeinen und/oder für kritische Applikationen? Wenn ja, welche externen Cloud Dienste werden häufig verwendet?

Im Zeitraum 2014 bis September 2024 wurden der Organisation und Informatik (OIZ) über 600 Cloud-Vorhaben gemeldet und in Bezug auf Informationssicherheit, Datenschutz und strategischer Konformität beurteilt. Die Meldungen erfolgten aus über sechzig verschiedenen Organisationseinheiten (Dienstabteilungen, Fachstellen, Departementssekretariate). Entsprechend erstreckt sich der stadtweite Einsatz von Cloud-Diensten über ein breit gefasstes Einsatzspektrum.

Bei der überwiegenden Mehrheit handelt es sich dabei um Anwendungen mit kleiner Nutzerzahl und unkritischen Diensten. Mit achtunddreissig Prozent der gemeldeten Vorhaben entsprechen Cloud-Dienste für dienstabteilungsspezifische Fachapplikationen dabei dem grössten Anteil. Weitere häufige Einsatzbereiche von Cloud-Diensten bilden die Bereiche «Online-Beratung, Übersetzung, Kommunikation» (15 Prozent), «Finanzen und HR» (10 Prozent), «Business Intelligence» (7 Prozent), «Microsoft-Anwendungen und -Dienste» (6 Prozent) und «Umfragen» (5 Prozent).

Am häufigsten verwendet werden aktuell «Microsoft 365» (Office-Plattform mit Microsoft Teams-Phone-System) und «SAP Success Factors» (stadtweite Personalmanagementprozesse).

**Fragen 2**
**Werden die AGB von Cloud Diensten geprüft und hinsichtlich Risiken für ausfallsicheren Betrieb geprüft? Falls ja, von wem?**

Grundsätzlich werden für Informatik-Verträge der Stadt die Allgemeinen Geschäftsbedingungen (AGB) der Schweizerischen Informatikkonferenz (neu «Digitale Schweiz») angewendet. Wenn sich diese gar nicht oder nur mit Abweichungen durchsetzen lassen, prüft der Rechtsdienst der OIZ die AGB der von ihr beauftragten Cloud-Lieferfirmen genau gleich, wie sie jegliche AGB ihrer Lieferfirmen in solchen Fällen einer Prüfung unterzieht.

Die Prüfung der AGB erfolgt auch hinsichtlich der Verfügbarkeit der Systeme. Je nach Kritikalität der Systeme werden unterschiedliche Verfügbarkeitsanforderungen vertraglich vorgesehen, z. B. Serviceverfügbarkeit in Prozent, Serviceausfallzeit pro Jahr, maximale Ausfallzeit pro Ereignis, maximale Ereignisse pro Jahr. Bei Nichteinhaltung der Verfügbarkeitszusicherungen kommen je nach Kritikalität der Systeme Vertragsstrafen zur Anwendung.

**Frage 3**
**Beinhalten die AGBs von Cloud Diensten weitere vergleichbare/ ähnliche Klauseln, welche die Stadt Zürich im Betrieb ihrer Applikationen einschränkt?**

Generell gilt, dass IT-Anbietende weder eine 100-prozentige Verfügbarkeit noch eine Fehlerfreiheit ihrer Systeme zusichern. Dies wird von den Anbietenden in der Regel auch so in den AGB bzw. Verträgen festgehalten. Nebst den Überprüfungen von AGB- und Vertragsbestimmungen werden die für die Stadt Zürich bereitgestellten Dienste je nach Kritikalität der Systeme deshalb im Risikomanagement der OIZ u. a. nach Kriterien der Fehlertoleranz und Verwendung beurteilt und gemäss dieser Einschätzung mit Massnahmen versehen. Dies erfolgt unabhängig davon, ob es sich um durch die OIZ in den städtischen Rechenzentren («on premises») betriebene Systeme oder um Cloud-Dienste handelt. Nach allgemein gültiger Fachmeinung sind dabei Cloud-Dienste generell bezogen auf Fehlertoleranz und Eignung für den Einsatz in kritischen Umgebungen nicht weniger gut geeignet als vergleichbare on-premises-Lösungen.

**Frage 4**
**Wie beurteilt der Stadtrat i.A. die Abhängigkeit kritischer IT-Systeme zu Drittanbieter? Was für Risiken für die Stadt ergeben sich daraus?**

Risiken sind in der heutigen technologischen und digitalisierten Welt allgegenwärtig. Dies gilt auch für Städte, die zunehmend auf komplexe IT-Systeme angewiesen sind, um ihre Dienstleistungen für die Einwohnenden bereitzustellen. Da die Stadt ihre kritischen IT-Systeme zum allergrössten Teil von Drittanbietenden bezieht und nicht selbst entwickelt, besteht eine Abhängigkeit von diesen Anbietenden. Das gilt sowohl für «on premises»-Lösungen als auch für aus der Cloud bezogene Leistungen. Diese Abhängigkeit birgt verschiedene Risiken, beispielsweise in Bezug auf die Verfügbarkeit, die Sicherheit und den Datenschutz. Um diese Risiken zu minimieren, werden für kritische Systeme geeignete technische Massnahmen, wie z. B. ein redundanter Aufbau von Systemkomponenten eingesetzt, die im Falle eines Ausfalls die Betriebskontinuität gewährleisten. Redundanz bedeutet, dass wichtige Systemkomponenten doppelt vorhanden sind, sodass bei Ausfall einer Komponente die andere einspringen kann.

Das Risikomanagement der OIZ berücksichtigt zudem das Bedrohungsszenario «Supply Chain Attacks» (Angriffe über die Lieferkette). Supply Chain Attacks sind Cyberangriffe, die nicht direkt auf die Systeme der Stadt gerichtet sind, sondern auf die Systeme der Lieferfirmen, um über diese einen Zugang zu den Systemen der Stadt zu erlangen. Relevante Risiken aus dieser Bedrohung, wie beispielsweise die Kompromittierung von Software-Updates oder die Infiltration von Schadsoftware über Hardwarekomponenten, werden regelmässig bewertet und entsprechende, dem Risiko angemessene Massnahmen (z. B. Audits, kontinuierliche Überwachung der Systeme auf Anomalien, u. dgl.) ergriffen.

Im Namen des Stadtrats
Der Stadtschreiber
Thomas Bolleter