Stadt Zug

Stadt Zug
Stadtrat

Stadthaus, Gubelstrasse 22
6301 Zug
www.stadtzug.ch

Nr. 2859

Grosser Gemeinderat, Vorlage

Postulat der SP-Fraktion vom 14. Juni 2023 betreffend «IT-Sicherheitstest der Stadtverwaltung».

Bericht und Antrag des Stadtrats Nr. 2859 vom 30. Januar 2024

Sehr geehrter Herr Präsident
Sehr geehrte Damen und Herren

Am 14. Juni 2023 hat die SP-Fraktion die Motion für einen umfassenden IT-Sicherheitstest der Stadtverwaltung eingereicht. Sie verlangt eine spezialisierte IT-Sicherheitsfirma zu beauftragen, um einen umfassenden Penetrationstest durchzuführen. Dieser Test soll sowohl die technischen Infrastrukturen – inklusive Netzwerke und Software – als auch das Sicherheitsbewusstsein und -Praktiken der Mitarbeitenden umfassen.

Die Begründung des Vorstosses ist aus dem vollständigen Postulatstext im Anhang ersichtlich.

An seiner Sitzung vom 4. Juli 2023 hat der Grosse Gemeinderat die Motion in ein Postulat umgewandelt und dem Stadtrat zum schriftlichen Bericht und Antrag überwiesen.

Wir erstatten Ihnen hierzu den folgenden Bericht:

I. Ausgangslage

Die IT-Infrastruktur der Stadt Zug ist täglich von Cyberattacken betroffen. Die Cyberangriffe konnten jeweils erfolgreich mit den technischen Abwehrmechanismen von Kanton und Stadt abgewehrt werden. Die am häufigsten attackierten Systeme sind Mail Server, WEB Server und Extranet Server (DMZ). Vielfältige Sicherheitsvorkehrungen verhindern, dass solche Angriffe erfolgreich sind. Ohne aus Sicherheitsgründen auf Details einzugehen, kann der Stadtrat die Anfrage aber nachfolgend wie folgt beantworten: Die Abteilung Informatik der Stadt Zug wie auch der Stadtrat sind sich deshalb der Notwendigkeit einer umfassenden und guten IT-Sicherheit sehr bewusst. In vielen verschiedenen Bereichen, wie zum Beispiel E-Mail- oder Internetzugang (und -eingang), ist die städtische Informatik verbunden mit dem Netzwerk des Kantons Zug. Sicherheitsmassnahmen und weitere Aktionen werden von der Stadt Zug und dem Kanton Zug deshalb gemeinsam realisiert. Sämtliche IT-Systeme der öffentlichen Hand im Kanton Zug sind untereinander vernetzt und bilden letztlich ein eigenes, autarkes System. Bildlich gesprochen sind sie eine Festung mit lebendigem "Innenleben", das gegen aussen mit starken Mauern und weiteren Sicherheitseinrichtungen gegen Angriffe geschützt ist. Der Kanton Zug sichert die Zugänge mit mehrstufig geschalteten Firewalls, dahinter geschalteten speziellen Gateways (Mail, Web, etc.) und wenn immer möglich mit einer Zwei-Faktor-Anmeldung ab, d.h. Benutzername und Passwort, sowie einem zusätzlich generierten Code auf dem Smartphone (ähnlich dem e-Banking der Zuger Kantonalbank). Zusätzlich setzt die Stadt Zug als weiteren Sicherheitsfaktor eine eigene Firewall ein. Ein hundertprozentiger Schutz von Informatik-Infrastruktur und -Systemen kann in der heutigen Zeit allerdings nicht gewährleistet werden. Informatik-Systeme können durch technische und organisatorische Massnahmen "sicherer" gemacht werden; dies wird vom Kanton Zug und den

Zuger Gemeinden mit grossem zeitlichem Aufwand täglich gemacht. Zuständig für die übergeordnete Sicherheitsstrategie ist das Amt für Informatik und Organisation (AIO) des Kantons Zug. Diese Strategie gilt auch für die Stadt Zug. Vor einigen Jahren wurde beim AIO eine neue Stelle eines Sicherheitsbeauftragten geschaffen, der sich ausschliesslich mit den Sicherheitsfragen rund um die Cyber-Kriminalität befasst. Zusätzlich werden auch die Benutzerinnen und Benutzer immer wieder auf ihre Sensibilität geschult. Seit drei Jahren macht die Informatik regelmässig mit den Mitarbeitenden Phishing Awareness und Schulungen im Bereich IT-Sicherheit.
Die Informatikabteilungen der Stadt Zug und des Kantons Zug haben somit mehrere Massnahmen für die Sicherheit ihrer Infrastruktur im Einsatz und weitere sind auch in Zukunft geplant. 2023 wurde eine Bug Bounty (ein Bug-Bounty-Programm, ist eine Crowdsourcing-Initiative, die Einzelpersonen für die Entdeckung und Meldung von Sicherheitslücken belohnt) durchgeführt, um zu sehen, ob (und wie) es für Hacker möglich wäre in die städtische Infrastruktur zu gelangen. Ab 2024 wird dies regelmässig geschehen und auch interne Penetration Tests werden durchgeführt.
2022 wurde beschlossen, einen gemeinsamen Fachbereich SOC (Security Operations Center) für den Kanton Zug und die Zuger Gemeinden aufzubauen. Die Stelle wurde im Jahr 2023 ausgeschrieben und zum Teil schon besetzt; dies auch im Zusammenhang mit dem Projekt «Zugkunft» Auslagerung der Informatik in eine selbständige Betriebsorganisation für die Erbringung von Informatik-Dienstleistungen. Dieses Projekt sieht vor, dass alle übergreifenden ICT-Dienstleistungen für die Stadt Zug, die Zuger Gemeinden sowie den Kanton Zug künftig durch eine unabhängige, gemeinsame ausgelagerte Organisation erfolgt. Sie nimmt dabei eine Vorreiterrolle in der Erbringung von ICT-Dienstleistungen für die Verwaltungs- und die Schulorganisation basierend auf aktuellen und fortschrittlichen Technologien ein. Die beteiligten Institutionen der öffentlichen Hand sind als Kundinnen und Kunden und Nutzniesserinnen und Nutzniesser zu hundert Prozent Eigentümerinnen und Eigentümer der Organisation, entscheiden über deren strategische Ausrichtung und sind zur Abnahme der ICT-Dienstleistungen aus dem definierten Dienstleistungskatalog verpflichtet.

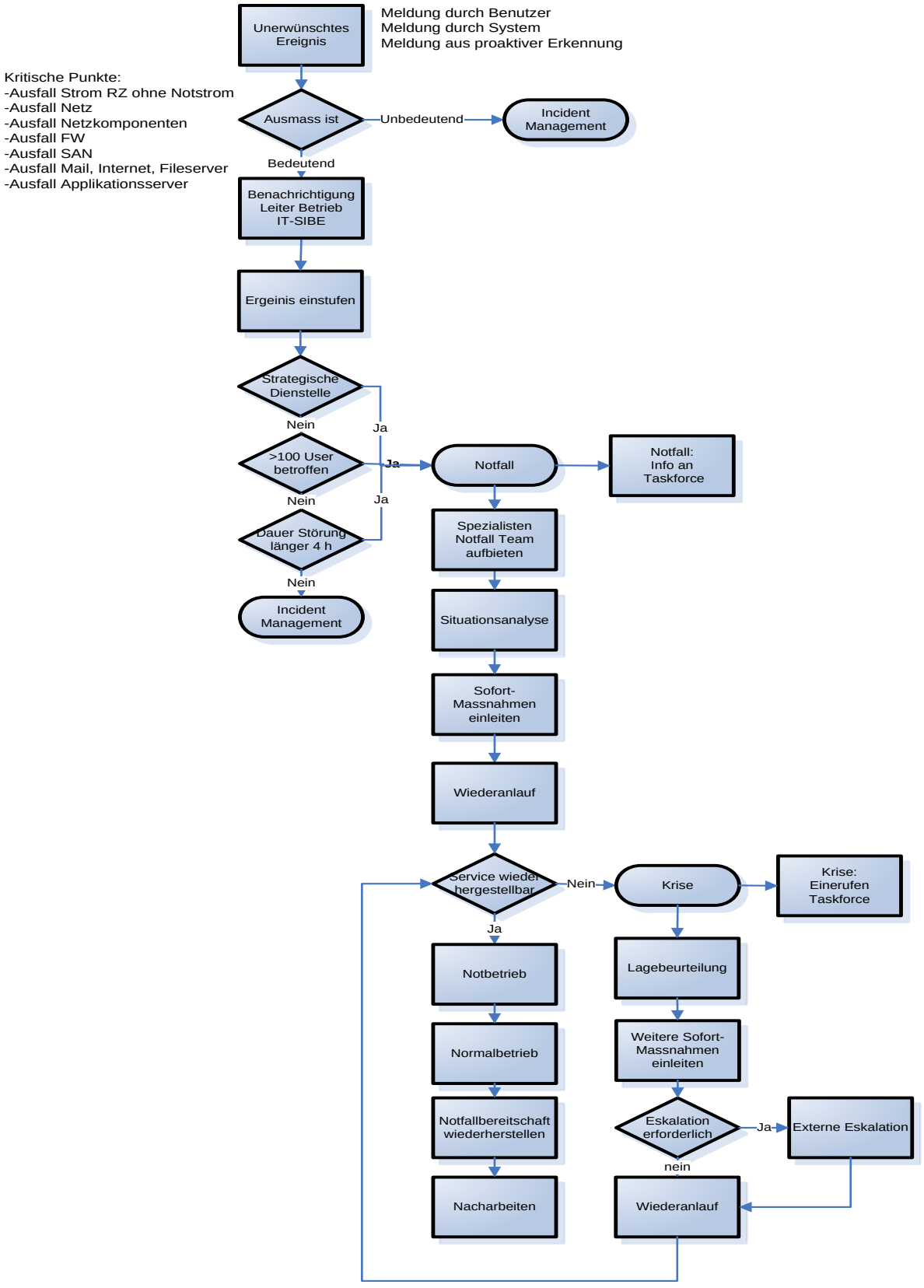
Die Stadt Zug hat im Falle eines erfolgreichen Cyberangriffs ein verbindliches Konzept. Sobald die technischen Systeme wie Virenschutz einen Alarm absetzen – dies kommt ein bis zweimal jährlich vor – wird der Prozess durch die Betriebsorganisation der Informatikabteilung angestossen und die notwendigen Massnahmen werden automatisch eingeleitet. Diese bestehen darin, den IT-Service für die Anwenderin und den Anwender so schnell wie möglich wiederherzustellen. Dabei wird das betroffene Gerät, dies kann ein Computer oder ein Mobiltelefongerät sein, isoliert und anschliessend neu installiert. Um eine schnelle Reaktion in der IT-Organisation der Stadt Zug sicherzustellen, existiert eine Pikettorganisation der Informatikabteilung. So ist 7 x 24 Stunden Erreichbarkeit eines Informatikmitarbeitenden garantiert. Verschiedene Überwachungssysteme melden Vorfälle automatisch direkt an die Pikettorganisation und den Leiter Informatik. Bei einem Vorfall werden Sofortmassnahmen ergriffen und je nach Ereignis Meldungen an den Kanton Zug (IT Security Verantwortlichen des AIO) und die Gemeinden (IGI Zug und IT-Leiter) abgesetzt. Bei Schadenfällen würde mittels Strafanzeige die Zuger Polizei involviert, welche über eigene Cyberspezialisten verfügt.

Im Kanton Zug sind sowohl auf Kantonsstufe wie auch in den Gemeinden Notorganisationen für unterschiedliche Gefährdungslagen definiert, die bei Bedarf entsprechend zum Einsatz kommen. Im Bereich Cyberkriminalität erfolgt die Koordination über die Zuger Polizei, welche über spezielle Kontakte zur Gefährdungsstelle National Cyber Security Centre (NCSC) des Bundes verfügt.

Das Amt für Informatik und Organisation (AIO) hat einen entsprechenden Prozess etabliert. Dieser Prozess definiert das Vorgehen, die Zuständigkeiten und Kompetenzen im Notfall- und Krisenmanagement (KM). Da der Kanton Zug und die Zuger Gemeinden ein gemeinsames Netzwerk betreiben,

gelten für die Stadt Zug die ausgearbeiteten Prozesse aus dem Handbuch. Dadurch ist die Stadt Zug Teil des Prozesses des Kantons Zug.
Die Abbildung zeigt einen Prozessablauf aus dem Handbuch:

Business Continuity Planning und Notfall-Krisenmanagement (BCP-KM-Umsetzungskonzept)



Quelle: Kanton Zug

II. Ausblick

Die Abteilung Informatik ist sich bewusst, dass im Sicherheitsbereich in Zukunft noch mehr finanzielle Ressourcen für Personal und technische Infrastruktur erforderlich sind. Dies zeigt alleine schon der Blick auf das Budget: 2023 wurden CHF 75'000.00 und im 2024 CHF 165'000.00 budgetiert. Es zeigt sich aber, dass es mehr braucht, weshalb für das Jahr 2025 die Informatikabteilung eine Teilzeitstelle für einen CISO (Chief Information Security Officer) beantragen wird, welche von den bei der Stadt Zug angeschlossenen Gemeinden mitfinanziert wird. Diese Stelle soll als Kontrollorgan der IT-Sicherheit die Fachgruppe SOC komplementieren und hat folgende Hauptaufgaben:

- Etablierung eines Managementsystems zur Informationssicherheit (ISMS)
- Bedrohungs- und Risikoanalysen durchführen
- Beratung bei Sicherheitsrelevanten Informatikprojekten
- Ausarbeitung, Anpassung von Sicherheitsrichtlinien, Schutzzielen und Sicherheitsvorgaben
- Auditierung von Infrastruktur und Personal zum Thema Informationssicherheit
- Awareness-Kampagnen und E-Learnings erarbeiten und durchführen
- Sicherstellung der Einhaltung des Datenschutzgesetzes

Die notwendigen Sicherheitssysteme werden immer komplexer. Daher nutzt die Stadt Zug Synergien mit dem Kanton Zug und namhaften Organisationen wie der SIK (Schweizerische Informatik Konferenz) oder bei der SSGI (Schweizerische Städte und Gemeinde Informatik).

III. Fazit

Der Stadtrat ist sich bewusst, dass die IT-Sicherheit eine sehr schnelländernde und immer wichtiger werdende Aufgabe ist. Durch die bereits erfolgten Massnahmen, ist es nicht notwendig, eine externe IT-Sicherheitsfirma für einen Penetrationstest zu beauftragen. Dies bedeutet, dass die internen Mitarbeitenden und die Informatik eng, flexibel und schnell zusammenarbeiten müssen. Mit der für 2025 geplanten Teilzeitstelle für einen CISO (Chief Information Security Officer) wird die noch vorhandene Lücke mit internen Mitarbeitenden gefüllt.

IV. Antrag

Wir beantragen Ihnen,

- den Bericht des Stadtrats zur Kenntnis zu nehmen,
- das Postulat der SP-Fraktion vom 14. Juni 2023 für einen umfassenden IT-Sicherheitstest der Stadtverwaltung als erledigt von der Geschäftskontrolle abzuschreiben.

Zug, 30. Januar 2024

André Wicki
Stadtpräsident

Martin Würmli
Stadtschreiber

Beilage
– Vorstoss vom 14. Juni 2023

Die Vorlage wurde vom Finanzdepartement verfasst. Weitere Auskünfte erteilt Ihnen gerne Stadtrat Urs Raschle, Departementsvorsteher, Tel. 058 728 92 01.