Stadt Zug
Stadtrat

Nr. 2459

Grosser Gemeinderat, Vorlage

Interpellation Stefan W. Huber und David Meyer, beide glp, vom 15. Mai 2017 betreffend Cybersicherheit

Antwort des Stadtrats vom 7. Juli 2017

Sehr geehrter Herr Präsident
Sehr geehrte Damen und Herren

Am 15. Mai 2017 haben Stefan W. Huber und David Meyer, beide glp, die Interpellation „Cybersicherheit“ eingereicht. Sie stellen darin dem Stadtrat eine Reihe von Fragen. Wortlaut und Begründung des Vorstosses sind aus dem vollständigen Interpellationstext im Anhang ersichtlich.

Frage 1
Hat der Stadtrat Kenntnis von sicherheitsrelevanten Vorkommnissen im Bereich der Cyberkriminalität in städtischen Behörden und Institutionen in den letzten Jahren?

Antwort
Ja, der Stadtrat hat Kenntnis von Cyberangriffen in den letzten Jahren. Die Cyberangriffe konnten wir jeweils erfolgreich mit den technischen Abwehrmechanismen abwehren. Die Stadtverwaltung Zug hatte in den vergangenen Jahren zwei PC's mit Virenbefall. Diese Viren waren aber nie sicherheitsrelevant für das Gesamtsystem der Informatik. Von Viren befallene PC's werden automatisch durch den Virenscanner der Informatikabteilung gemeldet und die befallene Arbeitsstation wird vom Netzwerk getrennt, damit sich der Virus nicht weiter ausbreiten kann.

Frage 2
Wie gross schätzt der Stadtrat die Wahrscheinlichkeit eines erfolgreichen Angriffes auf die Informatiksysteme ihrer Behörden und Institutionen heute und in naher Zukunft ein? (Diebstahl, Manipulation, Verschlüsselung und Löschung von Systemen und Daten)

Antwort
Angriffe auf die Informatiksysteme der Stadt Zug oder des Kantons Zug erfolgen mehrmals täglich. Die am häufigsten attackierten Systeme sind Mail Server, WEB Server und Extranet Server. Vielfältige Sicherheitsvorkehrungen verhindern, dass solche Angriffe erfolgreich sind.

Zu den Systemen und Servern des Kantons Zug und der Zuger Gemeinden gibt es nur eine redundant geführte Eintrittsstelle für Daten aus dem Internet. 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. Diese Eintrittspunkte befinden sich bei der kantonalen Verwaltung Zug. 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 der Informatik-Infrastruktur und -Systeme kann in der heutigen Zeit 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.
Der Mensch kann jedoch, trotz hoher Sensibilisierung auf Sicherheitsverhalten, immer wieder irrational oder ungeschickt handeln und dadurch einen Schaden am gesamten Informatiksystem verursachen. Durch ständiges Schulen der Mitarbeitenden und laufende Informationen über das Intranet erreichen wir eine höhere Sensibilität der Anwenderinnen und Anwender. Bei erhöhtem Risiko, ausgelöst zum Beispiel durch eine Warnung von MELANI (Melde- und Analysestelle Informationssicherheit des Bundes), informiert die Informatikabteilung über die aktuelle Bedrohungslage ebenfalls via Intranet-News. Dadurch sind alle Mitarbeitenden sensibilisiert.

Frage 3
Gibt es ein für die Stadt Zug und deren Institutionen verbindliches Konzept/Vorgehen im Falle eines erfolgreichen Angriffes durch Cyberkriminelle?

Antwort
Verfahrensweise und Verhalten sind abhängig von der jeweiligen Bedrohungslage. Grundsätzlich orientiert sich das Verhalten an den bewährten Information Technology Infrastructure Library (ITIL) Prozessen in der Handhabung von Störungen (Incident Prozess). Sobald die technischen Systeme wie Virenschutz einen Alarm absetzen – dies kommt ein bis zweimal jährlich vor – 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 Reaktionen 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 Cyber Spezialisten (siehe Beitrag "Betrügern auf der Spur") 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 MELANI des Bundes verfügt.

Das Amt für Informatik und Organisation (AIO) hat im Rahmen der ISO 27001 Zertifizierung 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 ISO 27001. Dadurch ist die Stadt Zug Teil des Prozesses des Kantons Zug.

Die Abbildung zeigt einen Prozessablauf aus dem Handbuch:

6. Notfall- und Krisenmanagement (KM)

In Abbildung 1 ist der schematische Ablauf einer Störung bzw. Notfall bzw. Krisen Bewältigung ersichtlich.

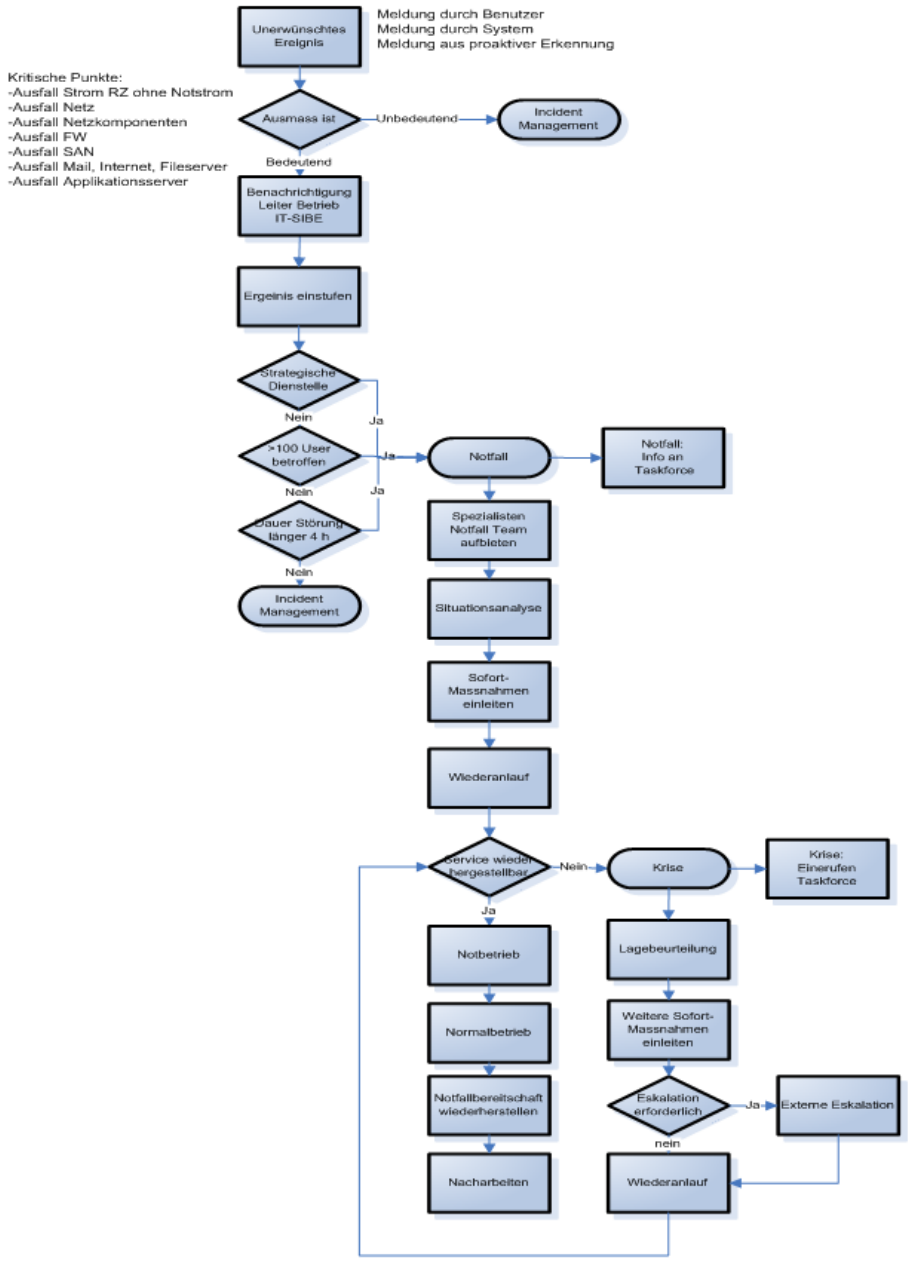

Abbildung 1: KM Prozessablauf AIO

Quelle: Kanton Zug

Das dargestellte Notfall- und Krisenmanagement (KM) des Kantons Zug käme bei Grossereignissen zum Einsatz. Ein solches Grossereignis ist bislang noch nie eingetreten. In der Task Force sind im Ernstfall neben Betroffenen Vertreter des Amts für Informatik und Organisation (AIO), der Interessensgemeinschaft Gemeindeinformatik Zug (IGI), die Zuger Polizei, externe Spezialisten sowie auch die IT Stadt Zug durch ihren Leiter vertreten. Der KM-Prozess umfasst auch die Mitwirkung der externen Meldestelle MELANI des Bundes sowie eines externen, spezialisierten Unternehmens, welches adhoc für Untersuchungen aufgeboten werden kann. Bis jetzt musste das spezialisierte Unternehmen noch nie aufgeboten werden, was auf einen guten und aktuellen Stand der Schutzmechanismen beim Kanton Zug und den angeschlossenen Gemeinden hinweist.

Frage 4
Was unternimmt die Stadt Zug, um den Herausforderungen der fortschreitenden Digitalisierung zu begegnen, ihrer Vorreiterrolle in diesem Bereich gerecht zu werden und das Vertrauen der Zugerinnen und Zuger in die digitale Sicherheit ihrer Daten sicherzustellen? (z.B. Sensibilisierung und Schulung des Personals)

Antwort
Die heutige Bedrohungslage verlangt eine vermehrte Zusammenarbeit mit anderen Informatikorganisationen. Diese Zusammenarbeit mit dem Kanton Zug sowie den Zuger Gemeinden untereinander wird durch die Vorstände der Organisationen wie die "Schweizerische Informatik Konferenz" (SIK) und die "Schweizerische Städte und Gemeinde Informatik" (SSGI) orchestriert. Daniel Truttmann, Leiter IT Stadt Zug, ist Vizepräsident der SSGI und Delegierter der SIK, wodurch die Stadt Zug direkt Einsitz in diesen wichtigen Gremien hat. Überdies arbeitet die Stadt Zug eng mit dem AIO zusammen. Die technische Infrastruktur der Stadt Zug – gemeint sind Storage und Server (Hardware) sowie die diversen Programme (Software) – ist örtlich getrennt und redundant ausgelegt. Dies dient der Speicherung und dem Schutz der Systeme und Daten. Die Zugriffe auf die Systeme und Daten der städtischen Infrastruktur unterliegen einem mehrstufigen Schutz. Mitarbeitende der Stadt Zug, welche von ausserhalb via Internet auf ihre Daten zugreifen müssen, arbeiten mit sogenannten virtuellen Desktops. Der Zugriff ist verschlüsselt und mittels einer Zwei-Faktor-Anmeldung, d.h. Benutzername und Passwort, sowie einem zusätzlich generierten Code auf dem Smartphone (ähnlich dem e-Banking der Zuger Kantonalbank) gesichert. Das bedeutet, dass sämtliche Anwendungen und deren Daten sich jederzeit zentral im Rechenzentrum befinden und so optimal gegen äussere Zugriffe geschützt sind. Auf den verwendeten Geräten, sprich den Computern der Mitarbeitenden am Arbeitsplatz, werden keine Daten und Anwendungen installiert bzw. gespeichert. Solche werden lediglich für den Aufbau einer gesicherten Verbindung ins Verwaltungsnetz verwendet. Die zentrale Speicherung und Überwachung von Daten, wie sie die Stadt Zug handhabt, vermindert das Risiko, von Cyber-Attacken überrascht zu werden um ein Mehrfaches. Anhänge von E-Mails werden gefiltert und angehängte Dokumente mit möglichem ausführbarem Code werden sogar gesperrt. Zudem verfolgt die Informatik der Stadt Zug laufend die Bedrohungslage und warnt bei neu auftretenden Attacken die Mitarbeitenden der städtischen Verwaltung über das Intranet und die Mailbenachrichtigung.

Dank der Nutzung von Synergieeffekten im Kanton Zug befinden sich viele Daten der Zugerinnen und Zuger auf Systemen des Kantons Zug. So sind alle Steuer-, Finanz-, Einwohnerkontroll-, Sozialbereichs-, Schul-, Objekt- wie Strassenverkehrsamt, Bau- und Immobilien-daten auf Systemen des Kantons Zug gespeichert, ebenso das zentrale Personenregister. Die Sicherheitsvorkehrungen des Kantons Zug entsprechen dem neusten Stand der Technik und Organisation. Das Amt für Informatik und Organisation (AIO) ist nach ISO 9001, ISO 20000 und auch ISO 27001 zertifiziert.

ISO 27001 umfasst die gesamten Sicherheitsanforderungen im ICT Bereich, welche laufend durch den Sicherheitsbeauftragten des Kantons Zug nach den neusten Gegebenheiten aktualisiert werden.

Neue Systeme und Projekte wie z.B. Einwohnerkontrolle, Sozialwesen und Baubewilligung werden vermehrt in Zusammenarbeit mit anderen Gemeinden und dem Kanton Zug aufgesetzt. Dabei wird der Sicherheit jeweils höchste Aufmerksamkeit geschenkt. Dazu gehört, dass die Fachämter ihre neuen Anwendungen auf Schwachstellen prüfen lassen (IT-Audit). Das neue, aktuell publizierte ZUGLOGIN für Einwohnerinnen und Einwohner des Kantons Zug garantiert den Einwohnerinnen und Einwohner, aber auch juristischen Personen einen sicheren Zugang zu Behördengeschäften. Das AIO des Kantons Zug belegte mit dem Projekt „Benutzerkonto (ZUGLOGIN)“ in der Kategorie „Bestes Infrastrukturprojekt 2017“ des eGovernment-Wettbewerbes den hervorragenden zweiten Platz. Dieser Wettbewerb ist seit vielen Jahren der anerkannte Gradmesser für eGovernment-Aktivitäten der Verwaltungen in Deutschland, Österreich und der Schweiz.

Zusammenfassung
Die Stadt Zug hat keine Kenntnisse von grösseren sicherheitsrelevanten Vorkommnissen im Bereich Cyberkriminalität. Kleinere Vorfälle auf dedizierten Systemen konnten sehr speditiv und ohne Schaden behoben werden.
Angriffe auf die Verwaltungssysteme des Kantons Zug und der Stadt Zug erfolgen mehrmals täglich. Durch sehr hohe und mehrstufig geschaltete Abwehrsysteme sind wir gegenüber Cyberkriminalität gut geschützt. Eine hundertprozentige Sicherheit wird es aber nie geben. Gezielte Angriffe von kriminellen Organisationen sind vermehrt auf international tätige Firmen, Suchmaschinen wie Google oder Yahoo und Anbieter von sozialen Netzwerken gerichtet. Da die Bedrohung in den letzten Jahren stark gestiegen ist, setzt die Verwaltung des Kantons Zug wie auch der Stadt Zug auch proaktiv vermehrt Personalressourcen für die Netzsicherheit ein und verbessert kontinuierlich ihre Prozesse. Allein die Stadt Zug hat diese Personalressourcen für Sicherheit in den letzten zehn Jahren von praktisch Null auf insgesamt etwa eine Vollzeitstelle ausgebaut.
Je nach Bedrohungslage gibt es unterschiedliche Abläufe, die eng mit dem Kanton Zug, AIO, abgestimmt sind. Für die laufende Überprüfung der Prozesse bestehen ISO Zertifizierungen wie ISO 27001 (Informationssicherheit-Managementsystem) und ISO 9001 (Qualitätsmanagement).
Die notwendigen und geforderten Sicherheitssysteme werden immer komplexer, daher sucht 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). In beiden Organisationen ist die Stadtverwaltung Zug Delegierte des Kantons Zug oder sogar in deren Vorstand. Insbesondere dank dem zentralen Netzwerk des Kantons Zug und der Zuger Gemeinden ist die Stadt Zug generell gut gegen Cyberangriffe geschützt. Mit entscheidend ist, dass das gesamte Zuger Netzwerk nur durch eine mit vielfachen Sicherheitsmechanismen versehene Eintrittsstelle für Daten aus dem Internet ausgestattet ist.

Antrag
Wir beantragen Ihnen
– die Antwort des Stadtrats zur Kenntnis zu nehmen.

Zug, 7. Juli 2017

Dolfi Müller	Martin Würmli
Stadtpräsident	Stadtschreiber

Beilagen:
1. Interpellation Stefan W. Huber und David Meyer, beide glp, vom 15. Mai 2017 betreffend Cybersicherheit
2. Auszug aus der Personalzeitung des kantonalen Personals vom April 2017.

Die Vorlage wurde vom Finanzdepartement verfasst. Weitere Auskünfte erteilt Ihnen gerne Stadtrat, Karl Kobelt, Departementsvorsteher, Tel. 041 728 21 21.