Auszug aus dem Protokoll des Stadtrats von Zürich

vom 31. Mai 2017

416.
Schriftliche Anfrage von Sven Sobernheim und Guido Hüni betreffend Ausfall der städtischen IT-Infrastruktur am 20. März 2017, Gründe für den Ausfall im Rechenzentrum Hagenholz sowie generelle Massnahmen zur Absicherung wichtiger Infrastrukturen

Am 22. März 2017 reichten Gemeinderäte Sven Sobernheim und Guido Hüni (beide GLP) folgende Schriftliche Anfrage, GR Nr. 2017/69, ein:

In der Nacht auf den 20. März 2017 kam es zu einem Ausfall zentraler Teile der IT Infrastruktur der Stadt Zürich. Die Auswirkungen zogen sich bis in den Abend hinein. Der Internetauftritt der Stadt war ausser Betrieb, betroffen waren IT-Arbeitsplätze sowie weitere Applikationen, beispielsweise im Gesundheitswesen. Ursache war laut Medienmitteilung der OIZ ein Defekt an einer zentralen Hardwarekomponente im Rechenzentrum Hagenholz. Das Ereignis reiht sich in eine Serie von Grossausfällen wichtiger Infrastrukturen (neben IT auch Stromversorgung und Verkehr) ein.

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

1. Was genau ist am 20. März im Rechenzentrum Hagenholz passiert?
2. Wie wäre es möglich gewesen diesen Ausfall vorauszusehen und welche Vorkehrungen hätte man dafür treffen müssen?
3. Sind Verbesserungen geplant, um eine Wiederholung des konkreten Ausfalls zu verhindern?
4. Welche generellen Massnahmen bestehen in der Stadtverwaltung um wichtige IT Infrastrukturen generell gegen Ausfälle abzusichern?
5. Wann hat die Stadt diese Massnahmen zum letzten Mal extern auditiert?
6. Zieht die Stadt aus dem Ausfall allgemeine Konsequenzen für die Absicherung wichtiger Infrastrukturen?
7. Wie sichert die Stadt generell wichtige Infrastrukturen (Energie, Telekommunikation, Verkehr) gegen Ausfälle und Angriffe von aussen ab?
8. Wie erfolgt die Zusammenarbeit mit unabhängigen Betreibern von Infrastruktur, welche auch auf Stadtgebiet tätig sind (z.B. SBB)?
9. Gibt es Statistiken zur Frage, ob die Stadt Zürich im Vergleich mit ähnlichen Gemeinwesen häufiger von derartigen Grossereignissen betroffen ist?

Der Stadtrat beantwortet die Anfrage wie folgt:

Zu Frage 1 («Was genau ist am 20. März im Rechenzentrum Hagenholz passiert?»):

Am Sonntag, 19. März 2017, trat um 23.05 Uhr im städtischen Rechenzentrum «Hagenholz» eine Störung aufgrund einer defekten Hardwarekomponente auf. Die defekte Hardwarekomponente war Teil eines Speichersystems, auf dem die Daten zahlreicher städtischer Applikationen und grundlegender IT-Basisdienste gespeichert werden. In den beiden städtischen Rechenzentren «Albis» und «Hagenholz» sind insgesamt sechs derartige Speichersysteme im produktiven Einsatz. Aufgrund der damit einhergehenden Wichtigkeit beinhaltet jedes einzelne Speichersystem redundante, d. h. mehrfach ausgelegte Einzelkomponenten, damit auch im Falle eines Einzeldefekts die Speicherfunktion ohne Unterbruch aufrechterhalten werden kann. Unter diese Einzelkomponenten fallen beispielsweise die einzelnen Speichermedien, die Stromversorgung, die Lüfter sowie das vom konkreten Hardwaredefekt betroffene Kommunikationsmodul, das u. a. die Schreib- und Lesevorgänge der ihm zugeordneten Speichermedien steuert.

Am 19. März um 23.05 Uhr fand diese, im Speichersystem vorgesehene, unterbruchsfreie Umschaltung innerhalb der redundant ausgelegten Kommunikationsmodule jedoch nicht statt,

da das defekte Kommunikationsmodul nach wie vor einen aktiven Betriebszustand suggerierte, wodurch der softwareseitig gesteuerte Umschaltmechanismus auf die redundante Komponente blockiert wurde. Als Folge davon konnten ab diesem Zeitpunkt keine neuen Daten auf die betroffenen Speichermedien des Speichersystems geschrieben werden, wodurch neben zahlreichen Fachapplikationen u. a. teilweise auch die serverbasierende Arbeitsplatzinfrastruktur (sogenannte «Thin Clients»), die Druckdienste, die Telefonie, die eGovernment-Applikationen sowie der städtische Webauftritt beeinträchtigt wurden.

Mit dem Auftreten der Störung wurde eine automatische Alarmierung des Pikettdienstes der Organisation und Informatik (OIZ) ausgelöst. Um 23.15 Uhr erfolgte eine erste Fehleranalyse durch den OIZ-Pikettdienst mittels Fernzugriff auf das Speichersystem. Der Zugriff durch die Supportabteilung des Systemherstellers erfolgte um 23.57 Uhr. Daraufhin wurde einerseits ein Austausch des gemäss Herstellers defekten Kommunikationsmoduls eingeleitet. Andererseits wurde versucht, die Lastübernahme auf die redundante Komponente manuell auszulösen. Dieser Versuch schlug jedoch fehl, da der softwareseitig gesteuerte Umschaltmechanismus blockiert war.

Als sich abzeichnete, dass die Fehlerbehebung länger dauern würde, wurde am Montag, 20. März, um 2.05 Uhr der OIZ-Krisenstab einberufen und eine Taskforce des Systemherstellers, bestehend aus der bereits aktivierten Supportorganisation, dem in Irland ansässigen Engineering und der Entwicklung aus den USA gebildet. Um 3.35 Uhr wurde das betroffene Kommunikationsmodul durch den Systemlieferanten vor Ort ausgetauscht. Die nach dem Austausch notwendigen Prüfprozeduren zur Verhinderung eines Datenverlusts zogen sich dabei entgegen der vom Hersteller prognostizierten Stunde über insgesamt sechs Stunden hin. Die Ursache dieser zeitlichen Verzögerung ist Gegenstand einer laufenden Abklärung mit dem Systemhersteller.

Aufgrund der sich abzeichnenden Verzögerung bis zur Wiederinbetriebnahme des Speichersystems wurde die Arbeit im OIZ-Krisenstab in zwei Richtungen vorangetrieben. Einerseits wurden die Arbeiten des Lieferanten zur Wiederinbetriebnahme des Speichersystems unterstützt. Anderseits wurden die gemäss Service Level festgelegten, kritischen städtischen Applikationen vom Rechenzentrum «Hagenholz» in das zweite Rechenzentrum «Albis» migriert und wiederhergestellt. So konnten bis zum Mittag des 20. März 2017 sukzessive die wichtigsten Applikationen wiederhergestellt werden.

Der zwischenzeitlich vorgenommene Austausch des defekten Kommunikationsmoduls im Speichersystem führte nicht zum erwünschten Ergebnis, weshalb um 16.00 Uhr auch das übergeordnete Speicherlogikmodul durch den Systemhersteller ersetzt wurde. Diese Massnahme sowie ein nachfolgender partieller Neustart des Speichersystems führten zur Behebung der Störung, so dass letztlich am 20. März 2017 um 17.30 Uhr die Wiederinbetriebnahme des Speichersystems erfolgte. Im Anschluss an die Wiederinbetriebnahme koordinierte der OIZ-Krisenstab den gestaffelten Wiederanlauf und die Funktionstests der verbleibenden, vom Ausfall betroffenen Applikationen in der Reihenfolge ihrer Wichtigkeit. Diese Arbeiten dauerten bis Dienstag, 21. März 2017, 5.00 Uhr an. Ab diesem Zeitpunkt standen sämtliche von der Störung betroffenen Systeme und Applikationen wieder vollumfänglich zur Verfügung, woraufhin der OIZ-Krisenstab aufgelöst wurde.

Zu Frage 2 («Wie wäre es möglich gewesen diesen Ausfall vorauszusehen und welche Vorkehrungen hätte man dafür treffen müssen?»):

Beim vorliegenden Hardwaredefekt im Speichersystem handelt es sich nicht um Verschleissteile. Insofern konnte der Ausfall nicht mittels vorgängigen Wartungsarbeiten erkannt und proaktiv verhindert werden. Anhand der internen Systemaufzeichnungen zum Betriebszustand konnte keine Voraussage des bevorstehenden Ausfalls abgeleitet werden, da bis zum Ausfallzeitpunkt keine entsprechenden Hinweise auftraten.

Die präventiven Massnahmen zur Verhinderung derartiger Ausfälle liegen primär in der fehlertoleranten Ausstattung des Speichersystems. OIZ setzt entsprechend sogenannte High-End-Systeme eines renommierten Herstellers ein, deren Einsatzbereich in grossen Unternehmen mit kritischen Applikationen liegen. Wie in der Antwort zu Frage 1 erläutert, sind diese Systeme bereits in sich selbst hochredundant gebaut, so dass Defekte einzelner Systemkomponenten üblicherweise nicht zum Ausfall führen. Zudem wird der vom Ausfall betroffene Speichersystemtyp gemäss Herstellerangaben weltweit in grossen Stückzahlen eingesetzt. Der vorliegende Fehler trat in dieser Ausprägung bisher an keinem anderen installierten System auf. Somit war der Ausfall vom 20. März 2017 auch herstellerseitig nicht voraussehbar.

Im Bereich der reaktiven Massnahmen, die die schnellstmögliche Erkennung und Behebung eines Ausfalls adressieren, hat die vorausgehende und automatisch durch das Speichersystem initiierte Alarmierung des OIZ-Pikettdienstes einwandfrei funktioniert. Die daraufhin erbrachten Leistungen des Systemherstellers, die in Form eines Service Level Agreements vereinbart wurden, konnten im vorliegenden Ausfall OIZ-seitig abgerufen werden. Sie umfassen insbesondere die Einhaltung einer sehr kurz bemessenen Reaktionszeit von 30 Minuten sowie den Hardwareersatz vor Ort innert vier Stunden.

Zu Frage 3 («Sind Verbesserungen geplant, um eine Wiederholung des konkreten Ausfalls zu verhindern?»):

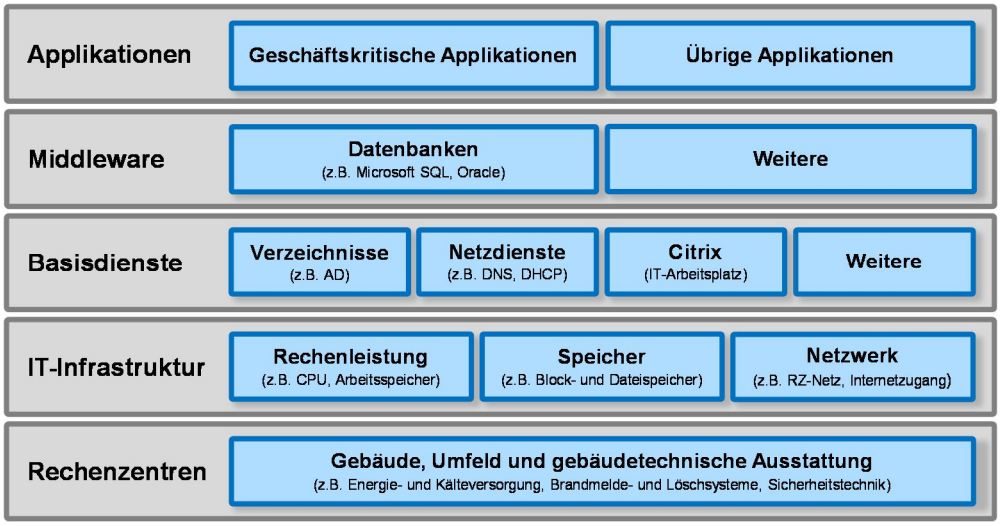
Die Softwarekomponente, die fälschlicherweise einen aktiven Betriebszustand suggerierte und somit ein automatisches Umschalten auf die redundante Komponente verhinderte, wurde zwischenzeitlich durch den Hersteller verbessert. Dies erfolgte mittels eines neuen Softwarereleases. Sämtliche Speichersysteme des betreffenden Typs wurden entsprechend durch die OIZ am 4. und 5. April 2017 auf den neuen Softwarestand aktualisiert. Im Zusammenhang mit dieser Aktualisierung wurden auch die Redundanzmechanismen pro Speichersystem durch manuelle Interventionen erfolgreich getestet.

Zu Frage 4 («Welche generellen Massnahmen bestehen in der Stadtverwaltung um wichtige IT Infrastrukturen generell gegen Ausfälle abzusichern?»):

Die Absicherung wichtiger IT-Infrastrukturen gegen Ausfälle erfolgt generell durch sogenannte «Redundanzmassnahmen». Diese verfolgen das Ziel, die Daten vor Verlust zu schützen und auch beim Ausfall einer technischen Komponente eine aus Benutzersicht hohe Verfügbarkeit der jeweiligen Applikationen zu gewährleisten.

Eine zentrale Massnahme zur Absicherung gegen Ausfälle ist die Datensicherung. Diese schützt nicht nur bei hardwarebedingten Defekten, sondern auch bei Anwenderfehlern oder Attacken mittels Schadsoftware, indem die Daten auf einem separaten Datenträger gespeichert werden. Die Limitationen der Datensicherung bestehen darin, dass nur der Datenbestand bis zur letzten Sicherung geschützt ist und die Wiederherstellung der Daten vergleichsweise viel Zeit benötigt. Um den zwischenzeitlichen Datenverlust und die Ausfallsdauer bei technischen Defekten zu reduzieren, werden deshalb bei geschäftskritischen Applikationen weitere Redundanzmassnahmen ergriffen, wie z. B. die Onlinespiegelung der Daten, die Zuhilfenahme redundanter Serversysteme oder den Einsatz hochverfügbarer Datenbanken.

Die folgende Abbildung zeigt eine stark vereinfachte schematische Übersicht der städtischen IT-Landschaft. Dabei sind die übergeordneten Bestandteile (z. B. die geschäftskritischen Applikationen) von den darunterliegenden Bestandteilen (z. B. den Datenbanken) abhängig.



Im Folgenden werden einige zentrale Absicherungsmassnahmen innerhalb der städtischen IT-Landschaft aufgeführt.

– Die beiden Rechenzentren «Albis» und «Hagenholz» mit ihren gebäudetechnischen Ausstattungen sind vollständig redundant ausgelegt.
– Die gesamte Netzwerkinfrastruktur der Rechenzentren ist redundant aufgebaut und mit zwei unabhängigen Redundanzmechanismen abgesichert.
– Die dezentralen städtischen Verwaltungsstandorte werden aufgrund definierter Kriterien (mehr als 100 Anwenderinnen und Anwender, geschäftskritische Applikationen usw.) redundant angeschlossen. Diese Kriterien gewährleisten, dass alle wichtigen Standorte redundant vernetzt sind.
– Sämtliche entsprechend klassifizierten Daten der Stadt Zürich werden gesichert. Die entsprechenden Sicherungskopien werden zudem in beiden städtischen Rechenzentren aufbewahrt.
– Bei den geschäftskritischen Applikationen und wichtigen Basisdiensten kommen zusätzlich redundante Komponenten für Rechenleistung und Speicher sowie hochverfügbare Datenbanken zum Einsatz. Die Ausgestaltung der Redundanz einzelner Applikationen ist von deren Architektur abhängig und wird im Einzelfall konzipiert.

Die verschiedenen Redundanzmassnahmen auf den unterschiedlichen Ebenen der städtischen IT-Landschaft bezwecken ein fehlertolerantes und robustes Verhalten der Gesamtlandschaft. Die Ausgestaltung dieser Massnahmen erfolgt dabei in Abhängigkeit zur Kritikalität und geschäftlicher Relevanz der darüber liegenden Applikationen. So wird eine wirtschaftliche und den Risiken entsprechende Auslegung der IT-Infrastruktur gewährleistet.

Zusätzlich zu den technischen Vorkehrungen existieren verschiedene organisatorische Massnahmen, die die Eintretenswahrscheinlichkeit eines Ausfalls reduzieren bzw. bei einem Ausfall eine rasche und koordinierte Reaktion sicherstellen. So unterliegen beispielsweise Änderungen an produktiven IT-Systemen einem strukturierten Risikobeurteilungs- und Bewilligungsprozess. Die bei Störungen ausserhalb der Büroarbeitszeiten aktivierte Pikett- und Krisenstabsorganisation der OIZ wird anhand definierter Kriterien aufgeboten. Die dazu erforderlichen Abläufe werden regelmässig trainiert und sind Gegenstand externer Audits. Im Nachgang zu IT-bedingten Ausfällen erfolgt zudem eine systematische Aufarbeitung der zugrundeliegenden Ursachen.

Zu Frage 5 («Wann hat die Stadt diese Massnahmen zum letzten Mal extern auditiert?»):

Die externe Auditierung der technischen und organisatorischen Massnahmen zur Sicherstellung der physischen Sicherheit der beiden städtischen Rechenzentren «Albis» und «Hagenholz» wird bei OIZ im 2-Jahres-Intervall gemäss der Prüfungsgrundlage TÜViT Trusted Site Infrastructure durchgeführt. Sie beinhaltet die Auditbereiche Umfeld, Baukonstruktion, Brandschutz, Melde- und Löschtechnik, Sicherheitssysteme und -organisation, Energieversorgung, Raumlufttechnische Anlagen, Organisation und Dokumentation. Die Auditierung erfolgte letztmals im Mai 2015. In den entsprechenden Prüfberichten wurden sieben Auflagen formuliert, welche im Sinne einer betrieblichen, kontinuierlichen Verbesserung umgesetzt werden.

Die externe Auditierung der organisatorischen und prozessualen Massnahmen im Bereich der Informationssicherheit, die u. a. auch das Risikomanagement und die Verfügbarkeit von informationsverarbeitenden Einrichtungen beinhaltet, wird bei der OIZ im Jahresintervall gemäss der Normgrundlage ISO/IEC 27001:2013 durchgeführt. Die Auditierung erfolgte letztmals im Mai 2016 und führte zum Ergebnis, dass die überprüften Normanforderungen ohne sogenannte Haupt- oder Nebenabweichungen erfüllt werden.

Die externe Auditierung der organisatorischen und prozessualen Massnahmen im Bereich der Störungsbehebung und nachhaltiger Problemlösung wird bei der OIZ im Jahresintervall gemäss der Normgrundlage ISO/IEC 20000-1:2011 durchgeführt. Die Auditierung erfolgte letztmals im Februar 2017 und führte zum Ergebnis, dass die überprüften Normanforderungen ohne Haupt- oder Nebenabweichungen erfüllt werden.

Ergänzend zu diesen externen Prüfungen im Auditverfahren wurde bei der OIZ im Herbst 2015 eine externe Maturitätsmessung im Bereich Business Continuity Management (BCM) vorgenommen. Das dabei angewendete BCM-Maturitätsmodell orientiert sich an internationalen Standards und adressiert die Bereiche Business, BCM-Organisation, Informatik und Logistik / Infrastruktur. Die OIZ erreichte innerhalb einer Maturitätsskala von 0 (nicht vorhandenes BCM) bis 5 (exzellentes BCM) einen Gesamtwert von 4,1.

Abschliessend sei erwähnt, dass die dem Ausfall zugrundeliegende Speicherinfrastruktur der OIZ im Dezember 2014 in Form einer externen Studie verifiziert wurde. Im Rahmen dieser Studie wurde sowohl das Einsatzkonzept als auch die Gesamtarchitektur geprüft und deren Angemessenheit in Bezug auf die städtischen Anforderungen bestätigt.

Zu Frage 6 («Zieht die Stadt aus dem Ausfall allgemeine Konsequenzen für die Absicherung wichtiger Infrastrukturen?»):

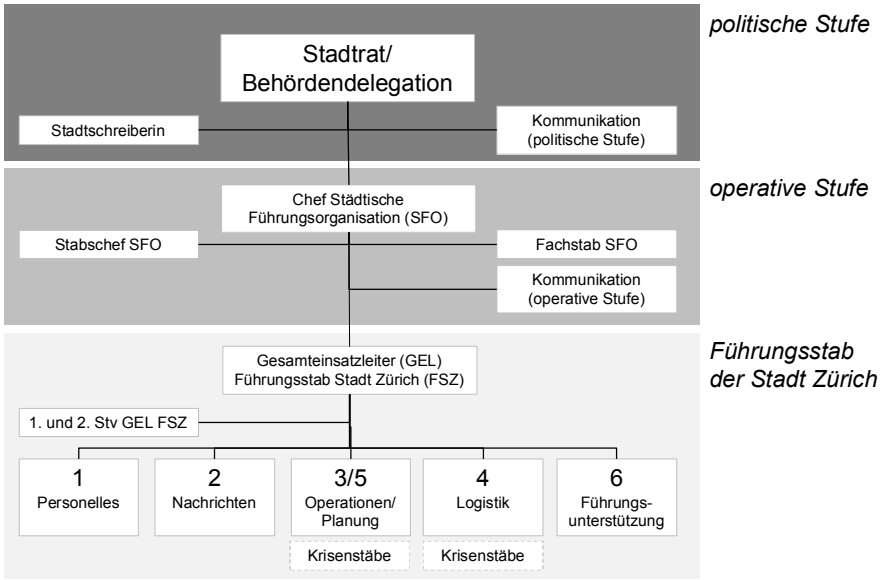
Die Stadt Zürich setzt sich in kontinuierlicher Weise mit dem Umgang von Grossausfällen wichtiger Infrastrukturen auseinander. Sie ist sich bewusst, dass derartige Ausfälle aufgrund der zunehmenden technologischen Vernetzung der heutigen Gesellschaft, der steigenden Abhängigkeiten von kritischen Infrastrukturen, der hohen Wertedichte sowie der wachsenden Bevölkerung zu immer grösseren Schäden führen kann. Entsprechend sind u. a. folgende Stadtratsbeschlüsse zum systematischen Umgang mit den sich stetig verändernden Gefährdungen und Risiken freigegeben worden, damit adäquate Massnahmen zur Risikoreduktion laufend geplant und umgesetzt werden können.

– STRB Nr. 1193/2006 betreffend «Vorbereitungen zur Bewältigung einer pandemischen Grippe»
– STRB Nr. 1587/2007 betreffend «Neues Risiko- und Versicherungskonzept Stadt Zürich (RVKZ), Genehmigung und Umsetzung»
– STRB Nr. 169/2008 betreffend «Struktur zur Führung in besonderen und ausserordentlichen Lagen in der Stadt Zürich (FIBAL)»

– STRB Nr. 435/2011 betreffend «Einführung eines Chancen- und Risikomanagements in der Stadtverwaltung Zürich, Neuerlass des Risiko- und Versicherungsreglements der Stadt Zürich»

– STRB Nr. 855/2016 betreffend «Führung in besonderen und ausserordentlichen Lagen in der Stadt Zürich (FIBAL)»

Insbesondere im Zusammenhang mit Führung in besonderen, ausserordentlichen Lagen (FIBAL), zu deren Bewältigung ein Zusammenwirken mehrerer Dienstabteilungen notwendig ist, hat der Stadtrat eine FIBAL-Führungsstruktur gemäss nachstehender Darstellung festgelegt. Die einzelnen Stufen dieser Führungsstruktur werden dabei je nach Lage (Alltag, Ereignisfall) aktiviert.



Um die Risiken in der Stadt Zürich auf ein vertretbares Mass zu verringern, werden durch die städtische FIBAL-Führungsstruktur Gefährdungen systematisch erfasst, bewertet und ihre Tragbarkeit beurteilt. Aufgrund dieser Risikobeurteilung werden auch vorsorgliche Massnahmen in Form von Ausbildungen und Übungen ergriffen. So konnte beispielsweise durch die Teilnahme der Stadt Zürich an der nationalen «Sicherheitsverbundübung 2014 (SVU14)» die FIBAL-Führungsstruktur entlang eines grossflächigen, langandauernden Stromausfalls, kombiniert mit einer Grippe-Pandemie, praktisch geprüft werden. Verschiedene der im Schlussbericht zur Übung (Schlussbericht SVU 14, Herausgegeben durch die Projektorganisation SVU 14, Abrufbar unter www.admin.ch) aufgeführten Verbesserungsmassnahmen wurden bereits umgesetzt.

Die bereits heute zur Verfügung stehenden und stadtweit eingesetzten Führungsstrukturen, Prozesse und Verfahren sind geeignet, um die im Zusammenhang mit dem konkreten IT-Ausfall eruierten Massnahmen im Sinne einer kontinuierlichen Verbesserung umzusetzen. Diese Massnahmen beinhalten einerseits Verbesserungen hinsichtlich der logischen Verteilung der städtischen Applikationen auf den zugrundeliegenden Server- und Speichersystemen, als auch Verbesserungen hinsichtlich der prozessualen und kommunikativen Aktivitäten zur Bewältigung derartiger IT-Ausfälle.

Zu Frage 7 («Wie sichert die Stadt generell wichtige Infrastrukturen (Energie, Telekommunikation, Verkehr) gegen Ausfälle und Angriffe von aussen ab?»):

Die Ableitung von Massnahmen zur Absicherung wichtiger städtischer Infrastrukturen erfolgt generell auf der Basis von Gefährdungen, damit einhergehenden Szenarien und daraus abgeleiteten Risikobewertungen. Die zur Risikominderung umgesetzten Massnahmen lassen

sich weiter in präventive Massnahmen zur Notfallvorsorge und reaktive Massnahmen zur Notfallbewältigung unterteilen.

Im Bereich der Energieversorgung wurde beispielsweise das städtische Rechenzentrum «Albis» präventiv an zwei unterschiedliche Unterwerke des Elektrizitätswerks (ewz) angebunden, um das Ausfallrisiko zu reduzieren. Ergänzende, dieselbetriebene Notstromaggregate, die eine Energieautonomie während 48 Stunden sicherstellen, führen zu einer weiteren Risikoverminderung.

Im Bereich der städtischen Telekommunikationsinfrastruktur «Züri-Netz» sind heute über 50 städtische Einrichtungen georedundant mit den beiden städtischen Rechenzentren verbunden. Darunter fallen beispielsweise das Verwaltungszentrum Werd, das VBZ-Zentrum an der Luggwegstrasse oder die Einsatzleitzentrale von Schutz und Rettung beim Flughafen Zürich.

Diese eher technischen Massnahmen zur Notfallvorsorge werden durch verschiedene organisatorische Massnahmen zur Notfallbewältigung komplettiert. So sind derzeit in der Stadtverwaltung spezifische Krisenstäbe (z. B. «Krisenstab GUD» im Gesundheits- und Umweltdepartement, «KATA TAZ» im Tiefbauamt, «Bereitschaftsdienst ewz» beim städtischen Elektrizitätswerk, «Krisenstab OIZ» im Finanzdepartement) installiert, die je nach Schweregrad eines Ereignisses eine autonome Krisenbewältigung sicherstellen oder der städtischen FIBAL-Führungsstruktur untergeordnet werden.

Zu Frage 8 («Wie erfolgt die Zusammenarbeit mit unabhängigen Betreibern von Infrastruktur, welche auch auf Stadtgebiet tätig sind (z.B. SBB)?»):

Im Führungsstab der Stadt Zürich wird die Zusammenarbeit mit unabhängigen Betreibern von Infrastrukturen geübt. So waren im Jahr 2013 die Sihltal Zürich Uetliberg Bahn (SZU) in der Übung «INITIO» integriert und im Jahr 2014 die SBB in der «Sicherheitsverbundübung 2014». Die beiden genannten Partner, wie auch weitere, sind derzeit auch in die laufende Erarbeitung des «Verkehrs- und Mobilitätskonzepts bei einer Strommangellage» eingebunden.

Zu Frage 9 («Gibt es Statistiken zur Frage, ob die Stadt Zürich im Vergleich mit ähnlichen Gemeinwesen häufiger von derartigen Grossereignissen betroffen ist?»):

Die vom Bundesamt für Bevölkerungsschutz im Rahmen der Arbeiten zur nationalen Gefährdungsanalyse bereitgestellten Publikationen (Katastrophen und Notlagen Schweiz – Technischer Risikobericht 2015, Herausgegeben durch das Bundesamt für Bevölkerungsschutz [BABS], 3003 Bern, Abrufbar unter www.risk-ch.ch. Nationale Plattform Naturgewalten [PLANAT], Bereitgestellt durch das Bundesamt für Umwelt [BAFU], Abrufbar unter www.planat.ch) beschreiben derartige Grossereignisse umfassend in Form von 33 Szenarien. Diese werden in natur-, gesellschafts- und technikbedingte Ereignisse gruppiert und beinhalten u. a. Ereignisse wie Hochwasser, Erdbeben, Epidemien, Strommangellagen oder den Ausfall der Informations- und Kommunikationstechnik (IKT). Die Szenarien werden dabei hinsichtlich ihrer Häufigkeit und Eintrittswahrscheinlichkeit eingestuft, wobei diese Einstufung nicht auf regionaler Ebene, sondern im gesamtschweizerischen oder weltweiten Kontext erfolgt und somit keinen Vergleich für die Stadt Zürich zulassen.

Demgegenüber existieren zu einzelnen Themen weiterführende Statistiken, Datensammlungen und Berichte, die zu Teilen eine Gegenüberstellung der regionalen Häufigkeiten ermöglichen:

– *Informationen zu elementarbedingten Grossereignissen*

  Nationale Plattform Naturgewalten (PLANAT), Bereitgestellt durch das Bundesamt für Umwelt (BAFU), Abrufbar unter www.planat.ch.

  Unwetterschadens-Datenbank der Schweiz, Bereitgestellt durch die Eidg. Forschungsanstalt für Wald, Schnee und Landschaft (WSL), Abrufbar unter www.wsl.ch.

– *Informationen zur Stromversorgungssicherheit*

  Stromversorgungsqualität 2015, Herausgegeben durch die Eidgenössische Elektrizitätskommission ElCom, Abrufbar unter www.elcom.admin.ch.

– *Informationen zur Sicherheit im öffentlichen Verkehr*

  BAV Sicherheitsbericht 2016, Herausgegeben durch das Bundesamt für Verkehr, Abrufbar unter www.bav.admin.ch.

– *Informationen zu Ereignissen in der Zivilluftfahrt*

  Swiss civil aviation 2015, Bereitgestellt durch Bundesamt für Statistik, Abrufbar unter www.bfs.admin.ch.

– *Informationen zu Vorkommnissen in Schweizer Kernanlagen*

  Meldepflichtige Vorkommnisse in Schweizer Kernanlagen, Bereitgestellt durch das eidgenössische Nuklearsicherheitsinspektorat (ENSI), Abrufbar unter www.ensi.ch.

– *Informationen zu Epidemien und Pandemien*

  Ausbrüche, Epidemien und Pandemien, Bereitgestellt durch das Bundesamt für Gesundheit (BAG), Abrufbar unter www.bag.admin.ch.

– *Informationen zu Tierseuchen*

  Informationssystem Seuchenmeldungen (InfoSM), Bereitgestellt durch das Bundesamt für Lebensmittelsicherheit und Veterinärwesen (BLV), Abrufbar unter www.infosm.blv.admin.ch.

– *Informationen zur Sicherheit von Computersystemen, des Internets sowie kritischer Infrastrukturen*

  Halbjahresbericht 2016/2 zu den wichtigsten Cybervorfällen im In- und Ausland, Herausgegeben durch die Melde- und Analysestelle Informationssicherung MELANI Abrufbar unter www.melani.admin.ch.

Abschliessend ist zu erwähnen, dass der Vorsteher des Finanzdepartements in Absprache mit der städtischen IT-Delegation einen Auftrag zur Prüfung weiterer Fragen zum Ausfall erteilt hat. Er wird nach Vorliegen der Ergebnisse die zuständigen gemeinderätlichen Kommissionen entsprechend informieren.

Vor dem Stadtrat

die Stadtschreiberin

Dr. Claudia Cuche-Curti