| | | | |
|---|---|---|---|
| **Protokoll:** | **Verwaltungsausschuss des Gemeinderats der Landeshauptstadt Stuttgart** | **Niederschrift Nr.**<br>**TOP:** | 117<br>1 |
| | Verhandlung | **Drucksache:**<br>**GZ:** | 144/2015<br>OB 0413 |

| | |
|---|---|
| **Sitzungstermin:** | 22.04.2015 |
| **Sitzungsart:** | öffentlich |
| **Vorsitz:** | BM Wölfle |
| **Berichterstattung:** | Herr Hauber (AK/DSB) |
| **Protokollführung:** | Herr Häbe de |
| **Betreff:** | **Datenschutz und IT-Sicherheit bei der Stadtverwaltung Stuttgart - Bericht 2013/2014 -** |

Vorgang: Verwaltungsausschuss vom 25.03.2015, nicht öffentlich, Nr. 72

Ergebnis: Einbringung

Beratungsunterlage ist die Mitteilungsvorlage des Herrn Oberbürgermeisters vom 23.02.2015, GRDrs 144/2015.

BM Wölfle bedankt sich bei Herrn Hauber für dessen Bericht und die dort verwendete klare Sprache.

Der in seiner Einführung von BM Wölfle unterbreitete Vorschlag, dass der Datenschutzbeauftragte künftig seine Berichte vorab der Verwaltung zukommen lassen soll und diese dann, gegebenenfalls ergänzt um Anmerkungen der Verwaltung, dem Verwaltungsausschuss vorgelegt werden, bleibt im Rahmen der Erörterung des Tätigkeitsberichts ungeklärt.

In seinem Einführungsvortrag teilt Herr Hauber mit, mit dem Bericht 2013/2014 werde der 15. Bericht zum Datenschutz und zur IT-Sicherheit bei der Stadtverwaltung vorgelegt. Im Berichtsjahr sei die IT-Sicherheit deutlich stärker in den Fokus der Öffentlichkeit gerückt. Um Cyberangriffe auszuführen, müsse man kein Experte mehr sein. Methoden der Nachrichtendienste könnten im Internet kopiert werden.

Die Bedrohung wachse von daher nicht nur durch die Anzahl der Angriffsversuche, sondern auch durch die deutliche Zunahme der Angriffsqualität. Nach einer Studie des Computerverbandes BITCOM richteten Angriffe allein in Deutschland Schäden in Höhe von rund 51 Mrd. Euro an. Betroffen von Attacken sei bereits jedes zweite deutsche Unternehmen.

In der Folge stellt Herr Hauber die Frage in den Raum, kann überhaupt noch etwas unternommen werden, oder kann die Stadtverwaltung in Stuttgart annehmen, für Hacker kein attraktives Ziel zu sein? Die beunruhigende Antwort könne auf der Seite 53 des Berichtes gefunden werden. Auch die Stadt Stuttgart sei im Berichtsjahr erfolgreich angegriffen worden. Diesen Angriff habe die Verwaltung selbst nicht entdeckt, sondern das Bundeskriminalamt sei auf die Stadt mit dem Hinweis zugekommen, dass sich in einem vermeintlich sicheren Bereich, nämlich im Kellergeschoss des Rathauses, ein verseuchter Server befindet.

Nach der gemeinsam mit dem Innenministerium im Jahr 2013 organisierten Veranstaltung "Die Hacker kommen" sei bei vielen Mitarbeiterinnen und Mitarbeitern der Verwaltung das Bewusstsein gestiegen, wie gefährlich selbst Smartphones sein können. Besonders beeindruckend sei die Vorführung einer ungewollten Raumüberwachung mit einem Smartphone gewesen, gegen die nichts habe unternommen werden können. Die gesamte EDV abzuschalten und zum Papier zurückzukehren, könne daraus sicherlich nicht die richtige Konsequenz sein. Allerdings müsse erkannt werden, dass Sicherheit durch Technik immer weniger gewährleistet werden kann. Mit der marktüblichen Software und mit den städtischen IT-Spezialisten stehe die Stadt zwischenzeitlich auf verlorenem Posten. Erhöht werden könne die personelle Sicherheit. Benötigt werde also eine informierte Mitarbeiterschaft, die kritisch und informiert aufschlagenden Gefahren entgegentreten kann. Dies bedeute, in der gesamten Stadtverwaltung sei eine Sicherheitskultur, durch Schulung, Beratung und Überprüfung erforderlich. Ein Mosaikstein dazu werde die im kommenden Herbst für die gesamte Stadtverwaltung geplante Awarenesskampagne "Ich bin dabei - mIT Sicherheit" sein.

Trotz zahlreicher Anfragen habe die Verwaltung im Berichtszeitraum keine Beanstandungen durch den Landesbeauftragten für den Datenschutz erhalten. Dies sei sicherlich erfreulich, aber kein Grund in den Anstrengungen nachzulassen. Es gelte, Datenschutz und IT-Sicherheit als Daueraufgaben zu begreifen. Erfreulich wäre, wenn der Gemeinderat die Arbeit von AK/DSB weiterhin kritisch und zugleich solidarisch begleitet.

Ihren Dank und Lob für den Bericht sprechen StR Dr. Reiners (CDU), StRin Deparnay-Grunenberg (90/GRÜNE), StR Pfeifer (SPD), StR Urbat (SÖS-LINKE-PluS), StRin von Stein (FW), StR Prof. Dr. Maier (AfD) und StR Dr. Oechsner (FDP) sowie für den Gesamtpersonalrat Herr Purz aus. Von Herrn Purz wird die Verwaltung für ihr Datenschutzbewusstsein gelobt. Zur Sicherung der städtischen Netze würden viele sinnvolle Maßnahmen ergriffen. Herr Reichert (HauptPersA) merkt an, als Leiter des Haupt- und Personalamtes, also des Amtes, das die entsprechenden Anwendungen betreibe, sei er sozusagen der Hauptbetroffene der Berichtsinhalte. Ausdrücklich wolle er der Datenschutzstelle für die sehr gute Zusammenarbeit danken. Gegenüber StR Dr. Reiners unterstreicht Herr Hauber die Notwendigkeit eines technischen Grundschutzes. Angesichts der steigenden Anzahl qualitativ

hochwertiger Angriffe reiche dies jedoch nicht mehr aus. Bedingt durch die heutigen Möglichkeiten, Viren zu verändern, würden die Hersteller von Virenschutzprogrammen der Realität hinterherhinken. Zwischenzeitlich gebe es im Gegensatz zur Vergangenheit eine steigende Anzahl verseuchter Clients. Trotz Firewall und Virenschutz schlage schädliche Software vermehrt im städtischen Netz auf. Davon betroffene Rechner müssten unter Umständen mit viel Aufwand neu aufgesetzt werden.

Die Stadt habe sich in der Vergangenheit nicht zuletzt durch einen hohen Mitteleinsatz sicher fühlen können. Angesichts der nun veränderten höheren Qualitäten von Angriffen, treffe dies nicht mehr zu. Die städtische Mitarbeiterschaft gehöre deshalb dahingehend sensibilisiert, dass das Öffnen von z.B. mit "dringend" deklarierten Mails unterlassen wird.

Zu der von StRin Deparnay-Grunenberg und Herrn Purz nachgefragten **Priorisierung von Handlungsbedarfen** informiert Herr Reichert, in der Stadtverwaltung gebe es das sogenannte IT-Sicherheitsmanagementteam. Dort bewerteten AK/DSB, das Haupt- und Personalamt sowie diverse Fachstellen IT-Sicherheitsrisiken der gesamten Stadtverwaltung nach ihrer Eintrittswahrscheinlichkeit und ihrer Schadenshöhe. Daraus resultiere ein Risikomanagement. Es handle sich um einen abgestimmten, strukturierten Prozess. Naturgemäß sei die dort erarbeitete Liste sehr lang. Aus den wichtigsten Themen habe die Verwaltung einen Personalbedarf abgeleitet. Da die Problematik darin liege, dass Datenschutz bei der Umsetzung von Anwendungen nicht zuletzt durch technische Unterstützung funktioniert, sei der Stellenbedarf nicht bei der Datenschutzstelle selbst angesiedelt. Benötigt werde spezielle Software und sehr fachspezifische technische Installationen. Dies münde in einem Stellenbedarf auch beim Haupt- und Personalamt. Dieser Personalbedarf sei theoretisch grenzenlos ausweitbar, im Stellenplanverfahren habe sich sein Amt für diesen Bereich auf die Nennung von drei Stellen mit unterschiedlichen Prioritäten beschränkt. Bei der Schaffung dieser Stellen könne also stufenweise vorgegangen werden.

Zum Thema **Port Security** führt StR Urbat aus, bei deren Einführung seien größere Umstände zu befürchten. Darauf sei er bereits im Reform- und Strukturausschuss eingegangen. So könnten dann keine USB-Sticks mehr in Laptops gesteckt werden. Für die Nutzer wären größere Benutzungsschwierigkeiten die Folge. Geklärt gehöre dann ebenfalls, inwieweit man dann noch mit Dockingstations zu Rande kommt. Zudem sei hier relevant, dass die wenigsten Laptop-Nutzer ihre Geräte, auch wenn sie diese nicht benötigten, herunterfahren. Wenn diese Geräte in Betrieb seien, bestehe die Möglichkeit des Einstöpselns über FireWire. Dann könnten Daten aus dem Arbeitsspeicher (RAM) gezogen werden. Dieses stelle einen sehr gefährlichen Angriffssektor dar. Durch Herrn Hauber, der die von Herrn Reichert beschriebene ressourcenbedingte Priorisierung bestätigt, bezeichnet das Thema Port Security als wichtig. Hier werde entsprechend der Priorisierung im Rathaus begonnen. Das Rathaus in Stuttgart sei ein offenes Rathaus. Es gehe hierbei um die Absicherung öffentlich zugänglicher Netzdosen. Jeder Besucher könne sich theoretisch an einer solchen Netzdose im Rathaus einstöpseln. Damit befinde man sich bereits im städtischen Netz (hinter der Firewall); Angriffe, die vom Inneren eines Netzes ausgingen, seien deutlich gefährlicher. Ein Projekt, um dieses abzusichern, laufe bereits. Die dabei erforderlichen Schritte seien sehr aufwendig und müssten stadtweit angelegt sein. In verschiedenen Ämtern sei dieses bereits geschehen, bei den Laptops der

Ratsmitglieder allerdings noch nicht. USB-Sticks würden dann noch funktionieren, aber die FireWire-Schnittstelle, die in der Verwaltung nicht erforderlich sei, werde dadurch geschlossen. Das FireWire-Angriffsszenario werde damit also ausgeschlossen.

Den für den Datenschutz gesehenen **Personalbedarf** hinterfragen StRin Deparnay-Grunenberg und Herr Purz. Angemerkt wird dazu von StR Urbat, üblicherweise werde die Aufgabe "Beauftragter für Informationsfreiheit" zusätzlich dem Datenschutzbeauftragten angedient. Im Auge müsse behalten werden, dass sich hieraus weiterer zusätzlicher Stellenbedarf ergibt. Nach Information von Herrn Hauber gibt es für den Bereich Datenschutzbeauftragter und IT-Sicherheit vier Stellen verteilt auf fünf Mitarbeiter. Er benötige keine weiteren Stellen; bundesweit gebe es keinen städtischen Datenschutzbeauftragten, der über eine solch gute Stellenausstattung wie er verfügt. Es sei aber natürlich nicht weiterführend, und hier unterstützt er den Leiter des Haupt- und Personalamts, dass vom IT-Sicherheitsteam als erforderlich angesehene Maßnahme vor Ort personell nicht umsetzbar sind. Das Haupt- und Personalamt sei hier in erster Linie betroffen und entsprechend hoch sei dort der Bedarf. Bei diesem Amt liefen aufgrund dessen Zuständigkeiten sehr viele Projekte und kritische Äußerungen seitens des Datenschutzes zu Projekten richteten sich in erster Linie an dieses Amt. Seine Anmerkungen dürften jedoch nicht so verstanden werden, dass die Projekte schlecht laufen, sondern er trete hier als Mahner auf. Er wolle zum Ausdruck bringen, dass Manches besser hätte gemacht werden können. Es gebe zwischen seinem Bereich und der restlichen Verwaltung einen ständigen Austausch.

Generell gebe es für die Zukunft in der Verwaltung in Sachen Datenschutz steigende Bedarfe. Nun müsse qualifiziertes Personal eingestellt werden, um vor Ort die Datensicherheit zu bearbeiten. Beispielsweise sei es nicht zielführend, darauf zu drängen, laufend Updates einzuspielen, wenn Server nicht gepflegt werden. Vor Ort müsse etwas passieren und dazu würden Finanzen und Stellen benötigt. BM Wölfle weist auf die im Rahmen der Stellenplanberatungen zu treffenden Entscheidungen hin.

Zu der von StR Urbat nachgefragten Anzahl städtischer Datenschutzbeauftragter berichtet Herr Reichert, in jedem Amt gebe es einen Datenschutzbeauftragten mit festen Stellenanteilen (mehr oder weniger hauptamtlich). Konkretisiert wird von Herrn Hauber, letztlich entschieden die Amtsleitungen über den Stellenanteil des/der Datenschutzbeauftragten in ihrem Amt. Es gebe durchaus Ämter/Eigenbetriebe, die von der Ausweisung solcher Stellenanteile für die Arbeit ihrer/s Datenschutzbeauftragten abgesehen haben. Diese Datenschutzbeauftragten seien gezwungen, diese Aufgabe nebenher auszuüben. Und in der Stadtverwaltung sei ihm kein/e Datenschutzbeauftragte/r bekannt, die/der ihre/seine Stelle ausschließlich für Datenschutzaufgaben einsetzen darf.

An StR Urbat gewandt erläutert Herr Hauber zur **Festplattenverschlüsselung**, Rechner könnten verschiedenartig abgesichert werden. Beim Jugendamt könnten sich beispielsweise sensible Daten auf Rechnern befinden. Bei den mobilen Rechnern der Ratsmitglieder seien keine zwingenden Festplattenverschlüsselungen erforderlich. Die Ratsmitglieder seien bekanntlich angehalten, auf den Festplatten ihrer Geräte selbst keine Daten zu speichern. Abgespeichert werden solle aus-

schließlich im Netz. Diese Absicherung habe vielleicht nicht die erste Priorität, sondern Priorität zwei oder drei. Mit solchen Abstufungen werde versucht, Arbeitsplätze ohne sich mehrfach anmelden zu müssen, arbeitsfähig zu halten.

Angesichts der sensiblen Gemengenlage wertet StR Pfeifer, dass es keine Beanstandungen des **Landesdatenschutzbeauftragten** gegeben hat, als positives Zeichen. In diesem Zusammenhang begrüßt BM Wölfle die Mitarbeiterin von Herrn Hauber, Frau Pfleiderer. Frau Pfleiderer sei derzeit auch noch beim Land beschäftigt. Daher sei ihr die Arbeitsweise des Landesdatenschutzbeauftragten bekannt. Laut Herrn Hauber gab es seitens des Landesdatenschutzbeauftragten durchaus viele Anfragen/Nachfragen. Dies hänge sicherlich damit zusammen, dass die Landeshauptstadt bei vielen Themen anders aufgestellt ist, als kleinere Kommunen. So mach beispielsweise die Einführung einer Online-Beteiligung viele Missbrauchsabsicherungen erforderlich und solche Anwendungen führten durchaus auch zu Kritik.

Für StR Urbat ist angesichts der Enthüllungen von Edward Snowden die Frustration bei Datenschützern nachvollziehbar. Danach betont Herr Hauber, er habe bewusst davon abgesehen, davon zu sprechen, dass er das städtische Netz als Angriffsziel der **NSA** (National Security Agency/Größter Auslandsgeheimdienst der USA) betrachte. Problematisch sei, dass durch die für nachrichtendienstliche Zwecke entwickelte Technik mittlerweile im Internet abrufbar ist; Hacker hätten somit bessere Angriffsmöglichkeiten als noch vor drei, vier Jahren.

StR Urbat sieht sich durch den Datenschutzbericht in seiner Annahme, dass seitens der Verwaltung Auskünfte verweigert werden, in dem man sich zu Unrecht auf den Datenschutz bezieht, bestätigt. Er nimmt dabei Bezug auf eine von ihm gestellte Anfrage zur Einsichtnahme in Denkmalschutzlisten. Das Thema **"Denkmalschutzlisten"**, so Herr Hauber, sei bereits im letzten Bericht behandelt worden. Hier gehe es um eine Abwägungsfrage (Veröffentlichung ja/nein). Er selbst sei ein Anhänger für die Veröffentlichung dieser Listen. Dazu gebe es aber durchaus andere Rechtsmeinungen, auch innerhalb der Stadtverwaltung (Rechtsamt). Die Gegner einer Veröffentlichung argumentierten, dass solche Listen personenbezogene Daten enthalten und für deren Veröffentlichung gebe es in Baden-Württemberg keine Rechtsgrundlage. Beide Positionen seien nachvollziehbar.

Zum **Informationsfreiheitsgesetz** würden ihm, so Herr Hauber zu einer weiteren Wortmeldung von StR Urbat, andere Informationen vorliegen. Der Entwurf dieses Gesetzes sei ihm vorgelegt worden und er habe dazu bereits einen Kommentar abgegeben. Er erachtet es als vorstellbar, dass dieses Gesetz kommt. Sollte dies der Fall sein, könnte bei der Stadt angesichts der dann großen Anzahl von Anfragen, zentral ein Stellenbedarf entstehen.

Für ein Beibehalten der **Zustellung von städtischen Postsendungen** durch Stadtboten spricht sich StR Urbat aus. Gewerblichen Zustellunternehmen könne nicht mehr vertraut werden. Diese würden Absender- und Empfängerfelder scannen. Um das Erfassen von Verbindungsdaten zu verhindern, wird von ihm angeraten, Postsendungen nicht mehr mit Absendern zu versehen.

Von Herrn Hauber erhält Herr Urbat zum Thema SAP/cloud (Speichern von Daten in einem entfernten Rechenzentrum, aber auch Ausführung von Programmen, die nicht auf den lokalen Rechner installiert sind, sondern eben nur in einer (metaphorischen) Wolke)) ebenfalls am "Hinterherrennen". Das Thema Cloud verbreite sich immer mehr in der Verwaltung. Es sei nicht immer eine freie Entscheidung möglich. So habe eine Firma gegenüber der Stadt erklärt, wenn künftig ihre IT-Produkte eingesetzt würden, gehe dies nur im Zusammenhang mit einer Lösung, welche automatisch in die Cloud speichert. Die Wahl zwischen einer Cloud-Lösung und einer zentralen Speicherung sei somit nicht mehr möglich. Sollte die Stadt als Anwender die Cloud-Speicherung abtrennen, würde das Ganze nach 2, 3 Wochen abgeschaltet.

Weiter an StR Urbat gerichtet, teilt Herr Hauber mit, in Lotus Notes sei das Verschlüsseln einzelner **E-Mails** aber auch aller E-Mails über die Grundeinstellung möglich. Sollte jedoch der Mail-Empfänger nicht über Lotus Notes verfügen, funktioniere diese einfache Verschlüsselung nicht. Möglich sei ebenfalls über die sogenannte virtuelle Poststelle beim KDRS Mails auch mit großen Anhängen auszutauschen. Desweiteren könnten Dateien gezippt verschlüsselt werden. Bei Bedarf nehme seine Stelle gerne eine Beratung vor. Beim Baurechtsamt habe sich dadurch eine Gefahrenquelle eröffnet, in dem Kunden erklärt worden sei, wenn eine Baurechtsakte eingesehen werden möchte, müsse dieses Anliegen per Mail geltend gemacht werden. Eine Verschlüsselung seitens des Baurechtsamtes sei allerdings nicht angeboten worden. Dies habe er als bedenklich angesehen.

StR Prof. Dr. Maier berichtet, die **Wettbewerbszentrale** habe nicht nur den Auftrag, den Wettbewerb zu sichern, sondern diese Einrichtung müsse sich satzungsgemäß ebenfalls um den Verbraucherschutz kümmern. Von daher werde von dort mit den Verbraucherzentralen seit Jahrzehnten eng zusammen gearbeitet. Er könne deshalb die vom Datenschutzbeauftragten geäußerte Verwunderung über die Post von dieser Einrichtung nicht nachvollziehen. Vermutlich seien auch die Eigenbetriebe angeschrieben worden, als deren AGBs durchleuchtet worden seien. Überzeugt ist er davon, dass man sich mit dieser Thematik in Zukunft weiterbeschäftigen muss. Er rät Herrn Hauber an, mit der Wettbewerbszentrale über den konkreten Anlass hinaus Kontakt aufzunehmen, um eine Zusammenarbeit zu vereinbaren. Von Herrn Hauber wird dazu angemerkt, er begreife sich eigentlich als Datenschutzbeauftragter des Stadtkonzerns Stuttgart. Formell sei er lediglich für die Stadtverwaltung bestellt. Theoretisch müssten alle städtischen Eigenbetriebe selbst schauen, wie sie das Thema Datenschutz in Griff bekommen. Seine Stelle versuche jedoch auch diesen Bereich abzudecken. So müsse bei in.Stuttgart das Bundesdatenschutzgesetz angewendet werden.

Im Verlauf der Aussprache wird zwischen StR Urbat und der Verwaltung besprochen, weitere von diesem Ratsmitglied angesprochene Punkte bilateral zu klären (z.B. device watch, Aufwand für die Einführung von Smartcards, Sozialdaten/Umgang mit Speicherfristen, Bericht Seite 22 / Jahreszahlen von Wahlen).

Zum Abschluss dieses Tagesordnungspunktes bittet BM Wölfle Herrn Hauber, den Dank des Ausschusses auch an seine Mitarbeiter/innen mitzunehmen.

Danach stellt der Bürgermeister fest:

Der Verwaltungsausschuss hat von der GRDrs 144/2015 Kenntnis genommen.

zum Seitenanfang