Winterthur, 4. Juni 2014
GGR-Nr. 2013/112

An den Grossen Gemeinderat

W i n t e r t h u r

Beantwortung der Interpellation betreffend Sicherheit der Bürgerdaten auf Polizei-iPads, eingereicht von Gemeinderat M. Wäckerlin (PP)

Am 9. Dezember 2013 reichte Gemeinderat Marc Wäckerlin namens der GLP/PP-Fraktion mit 14 Mitunterzeichnerinnen und Mitunterzeichnern folgende Interpellation ein:

"Die Stadtpolizei setzt im Dienst iPads ein, basierend auf einem System der Kantonspolizei. Seit den Enthüllungen über den amerikanischen Geheimdienst NSA durch Edward Snowden gilt als bekannt, dass unter anderen die Firma Apple, welche die iPads baut und das Betriebssystem iOS dazu entwickelt, direkt mit der NSA zusammenarbeitet und Daten in grossem Umfang liefert. Gemäss meiner Nachfrage ist die Polizei zwar der Meinung, sie würde ihre Geräte ausreichend absichern, aber sie hat letztlich keinerlei Kontrolle über die tatsächlich installierte Software und allfällige Hintertüren, da sie die Software nicht in Quellform untersuchen kann. Nun ist ebenfalls dank Snowdens Enthüllungen bekannt, dass Softwareanbieter auf Geheiss der NSA absichtlich Sicherheitslücken, sogenannte Hintertüren, in ihre Programme einbauen. Gerade bei Sicherheitssoftware ist dies verstärkt der Fall, rühmt sich die NSA doch, fast jede Verschlüsselung durch Hintertüren knacken zu können. Die einzige einigermassen sichere Lösung wäre die ausschliessliche Verwendung von OpenSource, inklusive des Betriebssystems (auch auf dem Pad selbst), namentlich Linux, wenn der Code unabhängig und alles aus den Quellen kompiliert wird (z.B. selbst ein kompiliertes Android, Firefox OS, Ubuntu, ...), oder aber wenn durch einen Vertrag mit allen beteiligten Softwareherstellern Zugang zum Quellcode, deren Sicherheitsprüfung durch eigene Experten, sowie die eigene Kompilierung aus den Quellen sichergestellt wird.

Das heisst, die Daten der Bürger, welche von der Polizei erfasst werden, sind nicht sicher.

Dasselbe Problem mit möglichen Hintertüren und fehlender Kontrollmöglichkeit besteht nicht nur bei den iPads der Polizei, sondern auf sämtlichen Servern und Clients der Verwaltung, insbesondere wenn proprietäre, nicht quelloffene Software installiert ist. Weitere Firmen, von denen berichtet wurde, dass sie mit der NSA zusammenarbeiten, sind unter anderen Microsoft, Google, Facebook, Yahoo, PalTalk, YouTube, Skype und AOL. Dienste und Software der betroffenen Firmen dürften unter keinen Umständen mehr in der öffentlichen Verwaltung eingesetzt werden. Ansonsten können die Rechte der Bürger potentiell verletzt, ihre Daten nicht wirksam geschützt werden.

Fragen:

- *Verwendet die Stadt oder die Stadtpolizei Software oder Dienste betroffener Firmen?*
- *Welche Bürgerdaten sind betroffen?*
- *Sind die Behörden verpflichtet, die Daten ihrer Bürger zu schützen, auch gegen Zugriff fremder Geheimdienste?*
- *Welche Massnahmen werden getroffen, um die Bürger künftig zu schützen?"*

Der Stadtrat erteilt folgende Antwort:

Die Informationssicherheit ist dem Stadtrat seit jeher – und nicht erst seit den Enthüllungen über angebliche Praktiken von Geheimdiensten und Softwareherstellern – ein wichtiges Anliegen, welchem er zusammen mit den Informatikdiensten (IDW) bei der Erneuerung bzw. Beschaffung neuer Informatikprodukte stets Rechnung trägt. Der Sicherheitsaspekt spielte auch eine zentrale Rolle bei der Anschaffung der iPads für die Stadtpolizei, die unter Federführung der Kantonspolizei erfolgte. Es wurden in einem aufwändigen Verfahren verschiedene Tablets evaluiert, letztlich jedoch das iPad des Herstellers Apple als das für die polizeilichen Zwecke geeignetste befunden. Das Produkt wurde eingehend geprüft und es hat die hohen Sicherheitsanforderungen der Polizeikorps erfüllt. Zur Überprüfung der organisatorischen und technischen Massnahmen zum Schutz der bearbeiteten Daten wurden zudem die Datenschutzbeauftragten des Kantons Zürich und der Stadt Winterthur beigezogen.

Die Information, dass diese Geräte und die Software der genannten Hersteller absichtliche Sicherheitslücken, so genannte „Hintertüren“, enthalten sollen, geht auf die Enthüllungen des ehemaligen NSA-Mitarbeiters Edward Snowden zurück. Diese Behauptungen sind zwar sehr ernst zu nehmen, dennoch konnten sie bis jetzt nicht verifiziert werden. Die Interpellanten schlagen vor, in der Stadtverwaltung inskünftig ausschliesslich OpenSource-Produkte zu verwenden, damit mittels Untersuchung der Quellform solche Lücken ausgeschlossen werden können. Der kürzlich bekannt gewordene Fall mit dem "Heartbleed"-Bug, einem schwer wiegenden Programmfehler, der in der OpenSource-Anwendung "OpenSSL" den unbefugten Zugang zu privaten Daten ermöglichte, hat jedoch gezeigt, dass auch OpenSource-Produkte gravierende Sicherheitsmängel aufweisen können. Eine umfassende Kontrolle der städtischen IT auf alle möglichen Lücken der Informationssicherheit wäre für die Stadt zudem kaum zu bewältigen, da ihr sowohl die personellen wie auch die finanziellen Ressourcen für ausgedehnte Sicherheitsprüfungen der verwendeten Produkte fehlen. Ausserdem hat der "Heartbleed"-Bug gezeigt, dass auch die OpenSource-Projekte über genügend personelle und finanzielle Ressourcen verfügen müssten, damit solche Fehler in der Entwicklung und Programmierung vermieden werden können. Darauf hat die Stadt jedoch keinen Einfluss.

Zur Frage bezüglich Verwendung von OpenSource in der Stadtverwaltung wird zur Vermeidung von Wiederholungen auf die stadträtliche Beantwortung der Schriftlichen Anfrage „betreffend OpenSource in der Verwaltung, von München lernen“ vom 14. August 2013 (GGR-Nr. 2013/071) verwiesen. Speziell zu erwähnen ist hier lediglich, dass zwei grosse öffentliche Institutionen, die Kantone Aargau und Solothurn, Projekte zum Einsatz von OpenSource in der Verwaltung inzwischen wieder abgebrochen haben. Die Stadt Winterthur setzt im Übrigen bereits heute OpenSource-Produkte ein; die aktuelle städtische IT-Strategie orientiert sich am Grundsatz: "Microsoft wo nötig, OpenSource-Software wo möglich". Im Übrigen wäre es derzeit nicht möglich, sämtliche städtischen Anwendungen durch eine den vielfältigen Anforderungen genügende OpenSource-Lösung zu ersetzen.

Zu den einzelnen Fragen:

Zur Frage 1:

"Verwendet die Stadt oder die Stadtpolizei Software oder Dienste betroffener Firmen?"

Wie bereits in der Antwort auf die genannte Schriftliche Anfrage erwähnt, verwendet die Stadt (einschliesslich die Stadtpolizei) proprietäre Software. Verschiedene Bereiche der Stadtverwaltung unterhalten auch ein eigenes Facebook-Profil. Dafür, dass in der verwendeten Software „Hintertüren“ vorhanden sein könnten, bestehen bisher keine Anhaltspunkte.

Zur Frage 2:

"Welche Bürgerdaten sind betroffen?"

Die verschiedenen Verwaltungsabteilungen der Stadt Winterthur bearbeiten im Rahmen ihrer gesetzlichen Aufgaben verschiedene Informationen (einschliesslich Personendaten). Um welche Informationen es sich dabei konkret handelt, ist aus dem öffentlich zugänglichen Verzeichnis der Informationsbestände ersichtlich, das zur Umsetzung des gesetzlich vorgegebenen Öffentlichkeitsprinzips erstellt wurde. Das Verzeichnis kann unter folgendem Link aufgerufen werden: http://kommunikation.winterthur.ch/oeffentlichkeitsprinzip/.
Die Bearbeitung von Informationen und Daten richtet sich nach den datenschutzrechtlichen Bestimmungen. Konkrete Hinweise darauf, dass unautorisierte Zugriffe auf diese Informationsbestände erfolgt sein könnten, bestehen keine.

Zur Frage 3:

"Sind die Behörden verpflichtet, die Daten ihrer Bürger zu schützen, auch gegen den Zugriff fremder Geheimdienste?"

Die Behörden sind verpflichtet, die von ihnen bearbeiteten Informationen und Daten durch angemessene organisatorische und technische Massnahmen zu schützen (§ 7 Abs. 1 des Gesetzes über die Information und den Datenschutz, IDG; LS 170.4). Details dazu sind in der Informatiksicherheitsverordnung vom 17. Dezember 1997 (ISV; LS 170.8) geregelt. Die von den Behörden zu treffenden Massnahmen müssen sodann verhältnismässig sein (§ 7 Abs. 3 IDG). Das bedeutet, dass die Massnahmen der Art der Daten und Informationen anzupassen sind; je sensibler also die Daten, desto höher sind die Anforderungen an die Sicherheitsvorkehren. Zudem sind solche Massnahmen periodisch zu überprüfen und dem jeweiligen Stand der Technik anzupassen. Zu beachten ist aber auch, dass eine absolute Sicherheit nie gewährleistet werden kann (vgl. Bruno Baeriswyl, in: Praxiskommentar zum Informations- und Datenschutzgesetz des Kantons Zürich, Zürich 2012, § 7 N. 17). Die IDW treffen laufend alle nötigen Vorkehrungen, damit die städtischen Systeme die relevanten Sicherheitskriterien jederzeit erfüllen. Gemäss bundesrechtlicher Vorgabe gelten übrigens die gleichen Kriterien auch für alle Privaten, welche Personendaten bearbeiten.

Zur Frage 4:

"Welche Massnahmen werden getroffen, um die Bürger künftig zu schützen?"

Neben den oben erwähnten Vorkehrungen sieht der Stadtrat den Schutz hauptsächlich darin, dass man sich allfälliger Unzulänglichkeiten von Informatiksystemen bewusst ist und dementsprechend sorgsam mit sensiblen Informationen umgeht. Daneben werden in Winterthur die Entwicklungen im IT-Bereich unter Federführung der IDW aufmerksam verfolgt, Strategien wo nötig angepasst und die Systeme entsprechend den dargelegten Grundsätzen in Sicherheitsbelangen kontinuierlich aktualisiert.

Die Berichterstattung im Grossen Gemeinderat ist der Vorsteherin des Departements Sicherheit und Umwelt übertragen.

Vor dem Stadtrat

Der Stadtpräsident:

M. Künzle

Der Stadtschreiber:

A. Frauenfelder