DIE LINKE.
FRAKTION IM RAT DER STADT KÖLN

Haus Neuerburg
Gülichplatz 1-3 · 50667 Köln
Postanschrift:
Postfach 103564 · 50475 Köln
Tel: 0221/221-27840 · Fax: 0221/221-27841
E-mail: DieLinke@stadt-koeln.de
Fraktionsvorstand

Eingang beim Amt des Oberbürgermeisters: 09.08.2013

AN/0990/2013

Anfrage gem. § 4 der Geschäftsordnung des Rates

Gremium	Datum der Sitzung
Ausschuss Allgemeine Verwaltung und Rechtsfragen / Vergabe / Internationales	23.09.2013

Der internationale Überwachungsskandal und die Datensicherheit bei der Stadt Köln

In den vergangenen Monaten haben Aussagen und Dokumente von Edward Snowden, bis dahin Mitarbeiter der US-Geheimdienste CIA und NSA, eine permanente, umfassende und weltweite Überwachung digitaler Kommunikation und Ausspähung persönlicher Daten durch US- und britische Geheimdienste bestätigt.

Das Projekt **Prism** ermöglicht im Zusammenspiel mit anderen Programmen dem US-Geheimdienst den Zugriff auf die Daten von Onlineunternehmen – insbesondere auf die Online-Dienste (auch Cloud-Dienste) von Microsoft, Yahoo, Google, Facebook, PalTalk, AOL, Skype, YouTube und Apple. Ziel ist zudem die Überwachung digitaler Kommunikation und die Speicherung und Auswertung von Verbindungsdaten der Telekommunikation. Aus diesen „Metadaten“ sind individuelles Kommunikationsverhalten und persönliche Netzwerke ablesbar.
Mit seinem Pendant zum US-Projekt, **Tempora**, versucht Großbritannien, eine möglichst umfassende Überwachung des Internets und der Telekommunikation zu erreichen und übertrifft darin offenbar sogar das US-Programm.

Die Überwachung digitaler Kommunikation wird komplettiert und perfektioniert im neueren System **XKeyscore**, das Inhalte, Verbindungsdaten und Aktivitätenprotokolle des Mailverkehrs, von Online-Chats, Logins sowie die Browserhistorie umfassend speichert und durchsucht *[Glenn Greenwald: XKeyscore: NSA tool collects 'nearly everything a user does on the internet'; Onlineausgabe des Guardian, eingestellt am 31.07.2013]*. Dieses System wird von US- und britischen Geheimdiensten eingesetzt und vom BND und vom BfV zumindest getestet *[Verfassungsschutz testet NSA-Programm; Onlineausgabe der Zeit, eingestellt am 21.07.2013].*

Gegen die umfassende und flächendeckende Überwachung ist aus der Bevölkerung ein breiter Protest erwachsen. Zivilgesellschaftliche Organisationen und Mitglieder mancher Parteien rufen unter dem Motto **„Stop watching us!“** für den 31.08.2013 zu deutschlandweiten Protesten auf.
Die Bundesregierung stellt sich jedoch bislang auf den Standpunkt, dass Datenschutz eine Aufgabe des einzelnen Bürgers sei. So forderte Bundesinnenminister Friedrich die Bürger dazu auf, ihre elektronischen Daten selber zu schützen *[Friedrich fordert Deutsche zu besserem Datenschutz auf; Onlineausgabe der Zeit, eingestellt am 16.07.2013]*.

Auch regierungsnahe Sicherheitspolitiker bestreiten die Möglichkeit gesetzlich gegen die Verletzung des Datenschutzes vorzugehen und fordern die Bürger zur Verschlüsselung ihrer digitalen Kommunikation auf. Da zum Beispiel ein Mailverkehr auch dann über die USA laufen kann, wenn Sender und Empfänger in Deutschland sind, könne die deutsche Gesetzgebung hier keinen Schutz bieten. *[„Die Regierung kann deine Daten nicht schützen"; Interview mit Hans Peter Uhl, Onlineausgabe der FAZ, eingestellt am 17.07.2013]*

Der Bundesdatenschutzbeauftragte Peter Schaar dagegen sieht die Politik in der Pflicht, die Verschlüsselung digitaler Kommunikation aktiv zu fördern. Eine weitverbreitete Verschlüsselung verhindere nach seiner Einschätzung die Durchsuchung von Massen von Kommunikationsdaten. Eine Entschlüsselung und damit Überwachung werde dann aufgrund des Aufwandes auf tatsächliche Verdachtsfälle begrenzt. *[Schaar für mehr verschlüsselte Kommunikation; Pressemeldung auf dem Onlineauftritt von Bayern 2 / radioWelt, Stand vom 27.6.2013]*

Neben der Überwachung und Ausspähung von Privatpersonen ist nach Einschätzung von Experten auch Wirtschaftsspionage ein Ziel der umfassenden Überwachung und Ausspähung digitaler Kommunikation *[Constanze Kurz: Das prächtige neue Gewand der guten alten Wirtschaftsspionage; Onlineausgabe der FAZ, eingestellt am 14.06.2013]*.

Der Datenschutzbeauftragte des Landes NRW, Ulrich Lepper, erklärt „Spätestens jetzt sollten alle Warnsignale leuchten." und empfiehlt mit Blick auf die Aktivitäten der US- und britischen Geheimdienste „allen Behörden des Landes und der Kommunen in NRW, zu überprüfen, ob die Konzepte für die Datensicherheit den Gefährdungsszenarien standhalten, die aktuell vorstellbar sind" *["PRISM", "XKeyscore" und die Folgen: Landes- und Kommunalbehörden müssen ihre Datensicherheit überprüfen; Internetauftritt des Landesbeauftragten für Datenschutz und Informationsfreiheit unter www.ldi.nrw.de/]*

Die Verwaltung der **Stadt Köln** verfügt über eine Vielzahl von Daten über Privatpersonen und Wirtschaftsunternehmen. Sie steht im elektronischen Austausch mit Kölner Einwohnern, mit anderen öffentlichen Stellen und mit Wirtschaftsunternehmen. Mitarbeiter der Kölner Verwaltung nutzen für ihre tägliche Arbeit das Internet und auch Onlinedienste der oben genannten Unternehmen. Die Stadt unterhält Internetauftritte, die von einer Vielzahl von Menschen genutzt werden.
Viele solcher digitalen Aktivitäten, an denen die Stadt Köln in der einen oder anderen Weise beteiligt ist, werden nach dem aktuellen Kenntnisstand mit den oben genannten Projekten überwacht, gespeichert und ausgewertet.

In diesem Zusammenhang stellt die Fraktion DIE LINKE die folgenden Fragen:

1. Beschäftigt sich die Verwaltung mit den Auswirkungen der Überwachungsskandale auf die Datensicherheit der Stadt Köln und auf das Recht auf informationelle Selbstbestimmung von Einwohnern und Mitarbeitern der Stadt Köln?
   Was sind die bisherigen Aktivitäten und welche Dienststellen sind daran beteiligt?
2. In welchen Hinsichten sieht die Verwaltung datenschutzrechtliche Belange und das Recht auf informationelle Selbstbestimmung im Verantwortungsbereich der Stadt Köln, bei Aktivitäten der städtischen Mitarbeiter im Internet, in der Kommunikation der Stadt zu anderen öffentlichen Stellen, in der Kommunikation zu Privatpersonen und bei der Nutzung städtischer Onlineangebote und der Köln-App durch Privatpersonen betroffen?
3. Welche Maßnahmen hält die Verwaltung für vorstellbar, um den nun bekannten Gefahren für die Datensicherheit und das Recht auf informationelle Selbstbestimmung zu begegnen und den Schutz von Daten in Bezug auf die unter 2. genannten Bereiche zu erhöhen?
4. Wie schätzt die Verwaltung in diesem Zusammenhang die folgenden Maßnahmen ein:
   a. Erreichbarkeit aller Seiten der Domain stadt-koeln.de, der Domain koeln.de und cologne.de über HTTPS und eventuell die komplette Umstellung dieser Domains auf HTTPS,
   b. Unterstützung von Perfect Forward Secrecy auf den HTTPS-unterstützenden Seiten der Domains stadt-koeln.de und koeln.de,
   c. Verwendung von SMTP TLS (Transport Layer Security) auf den Mail-Servern der Stadt Köln, von koeln.de und von cologne.de,

d. Möglichkeit, auf Wunsch mit Mitgliedern der Stadtverwaltung mittels PGP-verschlüsselter E-Mails zu kommunizieren,
e. die Verwendung anonymisierender Browser in der Stadtverwaltung,
f. einen Verzicht auf gefährdete Online-Dienste,
g. einen Verzicht auf Software der oben genannten Unternehmen und den Einsatz von Software mit offenem Quellcode?

Mit freundlichen Grüßen

Gez.

Jörg Detjen
Fraktionssprecher

Gez.

Gisela Stahlhofen
Fraktionssprecherin