ELF PIRATEN FRAKTION

Eingang: 09.09.2013, 20.10 Uhr

A 419

09.09.2013

Anfrage der ELF Piraten Fraktion gemäß § 50 II Satz 5 HGO

Überwachung der städtischen Kommunikation durch Geheimdienste

Aktuelle Medienberichte legen die Überwachung der elektronischen Kommunikation durch die Geheimdienste der „Five Eyes Alliance" in ungeahnten Ausmaßen offen. Im Rahmen der bisher bekannt geworden Projekte PRISM, Tempora, Bullrun und Edgehill können u.a. der US-amerikanische Militärnachrichtendienst National Security Agency (NSA) sowie der britische Nachrichten- und Sicherheitsdienst Government Communications Headquarters (GCHQ) Zugriff auf nahezu jegliche elektronische Kommunikation erlangen, verschlüsselt oder nicht, insbesondere wenn sie über US-amerikanische oder britische Unternehmen abgewickelt wird. Auch Hersteller von Smartphones (z.B. Apple, Google/Motorola) und Smartphone-Betriebssystemen (z.B. Apple, Google, Microsoft) sowie Hersteller von Verschlüsselungs- und Sicherungssystemen unterliegen diesem Zugriff.

Die überproportional starke Präsenz von Unternehmen auf dem Markt der elektronischen Kommunikation, die eine Niederlassung in Großbritannien oder den USA unterhalten, sorgt dafür, dass faktisch alle Nutzerinnen und Nutzer von dieser Überwachung betroffen sind.

Aktuellen Berichten zufolge übertragen Geräte des kanadischen Herstellers Blackberry alle Passwörter zu E-Mail-Konten unverschlüsselt über US-amerikanische und britische Server.[1, 2] Smartphones mit dem Betriebssystem Android geben die gespeicherten Passwörter von WLAN-Netzwerken an den Hersteller Google weiter und ermöglichen, z.B. beim Einsatz von sogenanntem Single-Sign-On, Geheimdiensten den Zugriff.[3]

Microsoft hat laut einem Bericht der britischen Tageszeitung „The Guardian" dem US-Geheimdienst NSA aktiv geholfen, die Daten-Verschlüsselung bei Diensten wie Outlook.com, SkyDrive oder Skype zu umgehen.[4, 5] Weiteren Berichten zufolge können die meisten Verschlüsselungssysteme von Geheimdiensten entschlüsselt oder umgangen werden.[6]

Neben Bürgerinnen und Bürgern sowie privatwirtschaftlichen Unternehmen sind auch alle öffentlichen Stellen Nutzer digitaler Kommunikation, und damit der Magistrat und sämtliche Leitungsebenen der städtischen Verwaltung und der stadteigenen Betriebe. In allen Fällen müssen sich die Kommunikationsteilnehmenden auf die Vertraulichkeit ihrer Kommunikation verlassen können.

1. Magistrat
2. Wv. 12.12.2013

Dokumente und Kommunikation von Regierungen und anderen Verfassungsorganen gehören traditionell zu den begehrtesten Zielen ausländischer Geheimdienste. Berichten zufolge ist dabei besonders der Netzwerkknoten in Frankfurt am Main im Fokus. Das US-Generalkonsulat in Frankfurt unterhalte zudem einen eigenen Lauschposten im Rahmen des „Special Collection Service".

Dies vorausgeschickt, fragen wir den Magistrat:

1. Ist der Magistrat der Auffassung, dass derartige Zugriffe von Nachrichtendiensten auf vertrauliche Kommunikation von öffentlichen Stellen, Bürgerinnen und Bürgern sowie Unternehmen geeignet sind, die Sicherheit und Ordnung zu beeinträchtigen? Wenn ja, hat der Magistrat die Generalkonsulate insbesondere der USA und Großbritanniens zu Stellungnahmen aufgefordert?
2. Verwenden die Stadt Frankfurt am Main sowie stadteigene Betriebe Möglichkeiten zur Verschlüsselung ihrer elektronischen Kommunikation? Wenn ja, warum sind sie auf diesem Wege nicht für die Bevölkerung erreichbar?
3. Welche IKT-Dienstleister nutzen der Magistrat, die Stadtverwaltung und die stadteigenen Betriebe seit dem Jahr 2010 zur Abwicklung ihrer elektronischen Kommunikation (E-Mail, Telefon, VoIP, Video- und Audiokonferenz, Hosting, Installation der Infrastruktur, Anbindung ans Netz etc.)? Wo sind die Standorte und Serverstandorte dieser Firmen? Bitte schlüsseln Sie die Dienstleistung nach Behörde, des in Anspruch genommenen Dienstes und Zeitraum der Inanspruchnahme auf.
4. Bei welchen der in Anspruch genommen Dienste ist dem Magistrat bekannt oder ist anzunehmen, dass ein Zugriff auf Daten durch Geheimdienste oder andere Dritte erfolgt?
5. Welche Dokumente und Datensätze, die personenbezogene Daten (Personalakten, Zeugnisse, dienstliche Beurteilungen, arbeitsmedizinische Bescheinigungen, Entgeltabrechnungen, eGovernment etc.) enthalten, werden von den Behörden regelmäßig in elektronischer Form empfangen, versendet oder sind maschinell abrufbar? Über welche Kommunikationswege und Dienstleister/ Ketten von Dienstleistern geschieht dies jeweils?
6. Welche dieser Datenübertragungen von und zu Servern der Stadt Frankfurt erfolgen verschlüsselt und welche unverschlüsselt? Welche Verschlüsselungsmethoden von welchen Anbietern/ nach welchen Standards werden dazu genutzt?
7. Wie bewertet der Magistrat unverschlüsselte Datenübertragung über Server, die nicht in der direkten physischen Kontrolle der Stadt Frankfurt am Main sind, insbesondere unter Berücksichtigung der Erkenntnisse der letzten Wochen über die Aktivitäten verschiedenster Geheimdienste, unverschlüsselte Kommunikation in großem Umfang abzuhören?
8. Welche Maßnahmen unternimmt der Magistrat, um sichere, verschlüsselte Datenübertragung zum Standard behördlichen Handelns werden zu lassen? Falls es dazu ein IKT-Sicherheitskonzept gibt, bitten wir um Anlage im Wortlaut. Falls es keines gibt, warum nicht?

9. Wie bewertet der Magistrat in diesem Zusammenhang die Eignung des nicht Ende-zu-Ende verschlüsselten Systems De-Mail?
10. Über welche Schnittstellen zu Dritten verfügt das Verbindungsnetz der öffentlichen Verwaltungen (DOI-Netz)? Befindet sich die gesamte Infrastruktur in öffentlicher Hand, oder werden dazu Knotenpunkte wie beispielsweise die von DE-CIX oder ECIX sowie Glasfasernetze privater Anbieter genutzt? Wenn ja, welche an welchen Standorten?
11. Erfolgt die elektronische Kommunikation in der Stadtverwaltung und städtischen Eigenbetrieben ausschließlich über das DOI-Netz?
12. Nachdem nicht einmal mehr das Bankennetzwerk Swift vor der NSA sicher ist,[7] glaubt der Magistrat weiterhin an die Sicherheit des DOI-Netzes? Wenn ja, was veranlasst ihn zu diesem Glauben?
13. Wie bewertet der Magistrat den Einsatz von System- und Anwendungs-Software US-amerikanischer Hersteller (z.B. Microsoft Windows, Microsoft Office) in städtischen Behörden und Eigenbetrieben angesichts der oben genannten Berichte, dass diese Unternehmen mit US-Geheimdiensten kooperieren und z.B. Sicherheitslücken zunächst an diese weitergeben?
14. Welche Vorschriften und Regelungen gelten für die Speicherung und elektronische Übermittlung (incl. Fax) von personenbezogenen medizinischen Daten, Patientenakten und Befunden? Nehmen Sie insbesondere Stellung zu der Frage, welche Formen und Stärken von Verschlüsselung angemessen sind.
15. Welche Sanktionen sind vorgesehen, wenn personenbezogene medizinische Daten, Patientenakten und Befunde nicht ausreichend geschützt gespeichert oder übermittelt werden?
16. Hält der Magistrat die derzeitigen Regelungen zum Schutz personenbezogener medizinischer Daten, Patientenakten und Befunde angesichts des Ausmaßes der Kompromittierung von Nachrichtenübermittlungs- und Datenspeichersystemen durch Geheimdienste für ausreichend? Nehmen Sie insbesondere dazu Stellung, ob Systeme US-amerikanischer Herkunft für diesen Zweck als vertrauenswürdig genug eingestuft werden können.
17. Plant der Magistrat Maßnahmen, den Schutz von personenbezogenen medizinischen Daten, Patientenakten und Befunden auf Datenspeicherungs- und Nachrichtenübermittlungssystemen zu stärken?
18. Welche Mobiltelefone/Smartphones – unter Angabe von Hersteller, Modell und Betriebssystem/ Version – werden vom Oberbürgermeister, dem Bürgermeister, den Dezernentinnen und Dezernenten, den Mitarbeiterinnen und Mitarbeitern der Magistratsbüros, sowie den Mitgliedern der höheren und mittleren Leitungsebenen in der Verwaltung bzw. den stadteigenen Betrieben für dienstliche Zwecke genutzt?
19. Über welche Systeme zur Verschlüsselung und Sicherung von Gesprächen und Daten verfügen die Mobiltelefone/ Smartphones der in Frage 18 genannten Personengruppen jeweils?

20. Welche Instant-Messaging-Dienste nutzen die in Frage 18 genannten Personengruppen auf dienstlichen Mobiltelefonen/ Smartphones?
21. Über welche Dienstleister wird der dienstliche Mobilfunk des Oberbürgermeisters, des Bürgermeisters, der Dezernentinnen und Dezernenten sowie der Mitarbeiterinnen und Mitarbeiter der Verwaltung und der stadteigenen Betriebe abgewickelt?
22. Wie wird die Vertraulichkeit der telefonischen Kommunikation des Magistrats gewährleistet vor dem Hintergrund der in den letzten Wochen öffentlich gewordenen Abhörmöglichkeiten ausländischer Geheimdienste sowie der berichteten Sicherheitslücken und Backdoors bei Android- und Blackberry-Mobiltelefonen?
23. Aufgrund welcher Datensätze bzw. Unterlagen wurden vorstehende Fragen beantwortet? Sind diese Quellen im Internet abrufbar? Falls ja, unter welchen Adressen? Wäre es möglich, diese auf frankfurt.de bzw. dem zukünftigen Open Data-Portal der Stadt einzustellen und fortlaufend zu aktualisieren?

Quellen:

1. http://frank.geekheim.de/?p=2379
2. http://www.heise.de/newsticker/meldung/BlackBerry-spaeht-Mail-Login-aus-1919718.html
3. http://www.heise.de/newsticker/meldung/Android-und-die-Passwoerter-Offene-Tueren-fuer-Spionage-1917386.html
4. http://www.guardian.co.uk/world/2013/jul/11/microsoft-nsa-collaboration-user-data
5. http://www.bloomberg.com/news/2013-06-14/u-s-agencies-said-to-swap-data-with-thousands-of-firms.html
6. http://www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html
7. http://www.zeit.de/digital/internet/2013-09/nsa-brasilien-snowden-swift-google-petrobas

Anfragesteller:

Stv. Martin Kliehm
Stv. Herbert Förster
Stv. Luigi Brillante
ELF Piraten Fraktion

gez. Martin Kliehm, Fraktionsvorsitzender