LANDTAG NORDRHEIN-WESTFALEN
16. Wahlperiode

Drucksache **16/3690**

31.07.2013

Kleine Anfrage 1485

der Abgeordneten Lukas Lamla, Daniel Schwerd, Marc Olejak und Frank Herrmann PIRATEN

Haben ausländische Geheimdienste ihr Ohr an Diensthandys der nordrhein-westfälischen Regierung?

Aktuelle Medienberichte legen die Überwachung der elektronischen Kommunikation durchbritische und US-Geheimdienste in ungeahnten Ausmaßen offen. Im Rahmen des Projektes PRISM kann der US-amerikanische Militärnachrichtendienst National Security Agency (NSA) Zugriff auf nahezu jegliche elektronische Kommunikation erlangen, die über US-amerikanische Unternehmen abgewickelt wird. Auch Hersteller von Smartphones (bspw. Apple, Google/Motorola) und Smartphone-Betriebssystemen (bspw. 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 US-amerikanischer Jurisdiktion unterliegen, sorgt dafür, dass faktisch alle 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] Smartphones mit dem Betriebssystem Android geben die gespeicherten Passwörter von WLAN-Netzwerken an den Hersteller Google weiter und ermöglichen, bspw. beim Einsatz von sogenanntem Single-Sign-On, Geheimdiensten den Zugriff.[2]

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.[3]
Quellen:

[1]http://frank.geekheim.de/?p=2379 http://www.heise.de/newsticker/meldung/BlackBerry-spaeht-Mail-Login-aus-1919718.html
[2]http://www.heise.de/newsticker/meldung/Android-und-die-Passwoerter-Offene-Tueren-fuer-Spionage-1917386.html
[3] http://www.guardian.co.uk/world/2013/jul/11/microsoft-nsa-collaboration-user-data

Datum des Originals: 29.07.2013/Ausgegeben: 31.07.2013

Neben Bürgen und privatwirtschaftlichen Unternehmen sind auch alle öffentlichen Stellen, und damit die Regierungen und sämtliche Leitungsebenen der Ministerien und Landesbehörden, Nutzer digitaler Kommunikation. In allen Fällen müssen die Kommunikationsteilnehmer sich auf die Vertraulichkeit ihrer Kommunikation verlassen können.

Dokumente und Kommunikation von Regierungen und anderen Verfassungsorganen gehören traditionell zu den begehrtesten Zielen ausländischer Geheimdienste.

Wir fragen die Landesregierung:

1. Welche Mobiltelefone/Smartphones -- unter Angabe von Hersteller, Modell und Betriebssystem/Version -- werden von der Ministerpräsidentin, den Ministerinnen und Ministern, den Staatsekretärinnen und Staatssekretären, den Mitarbeiterinnen und Mitarbeitern der Ministerbüros sowie den Mitgliedern der mittleren Leitungsebene in den Ministerien (Abteilungs- und Unterabteilungsleiter und -leiterinnen) für dienstliche Zwecke genutzt?

2. Über welche Systeme zur Verschlüsselung und Sicherung von Gesprächen und Daten verfügen die Mobiltelefone/Smartphones der in Frage 1 genannten Personengruppen jeweils?

3. Welche Instant-Messaging-Dienste nutzen die in Frage 1 genannten Personengruppen auf dienstlichen Mobiltelefonen/Smartphones?

4. Über welche Dienstleister wird der dienstliche Mobilfunk der Ministerpräsidentin, der Ministerinnen und Minister, der Staatsekretärinnen und Staatssekretäre sowie der Mitarbeiterinnen und Mitarbeiter der Ministerien abgewickelt?

5. Wie wird die Vertraulichkeit der telefonischen Kommunikation der Landesregierung 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?

Lukas Lamla
Daniel Schwerd
Frank Herrmann
Marc Olejak