Abgeordnetenhaus BERLIN

Drucksache 17 / 10 380
Kleine Anfrage

17. Wahlperiode

Kleine Anfrage

des Abgeordneten Christopher Lauer (PIRATEN)

vom 25. März 2012 (Eingang beim Abgeordnetenhaus am 28. März 2012) und **Antwort**

Quellen-Kommunikationsüberwachung (Quellen-TKÜ) in Berlin

Im Namen des Senats von Berlin beantworte ich Ihre Kleine Anfrage wie folgt:

1: Ist es in Berlin mittlerweile zu einem Einsatz der Software zur Quellen-TKÜ der Firma Syborg (Auftragsnummer 62035795) gekommen?

Zu 1.:Wie schon in der Kleinen Anfrage 17/10287 erläutert, war die Beschaffung der Quellen-Telekommunikationsüberwachungs-Software (Quellen-TKÜ-Software) ein eigenständiger Vorgang und hängt nicht zusammen mit dem Auftrag zur Erweiterung der TKÜ-Anlage der Berliner Polizei (Auftragsnummer 62035795).

Die Berliner Polizei hat bisher noch keine Quellen-TKÜ-Maßnahme durchgeführt.

2. Wird/Wurde die Software der Firma Syborg zur Quellen-TKÜ (Auftragsnummer 62035795) vor ihrem Einsatz in Berlin hinsichtlich ihrer Recht- und Verfassungsmäßigkeit geprüft?
a) Wenn ja, von wem und wie?
(Bitte detaillierte Beschreibung eines etwaigen Prüfverfahrens.)
b) Was spricht gegen eine Prüfung durch eine unabhängige Expertenkommisson?
c) Was spricht – auch ohne eine rechtliche Verpflichtung – dagegen, den Datenschutzbeauftragten des Landes in die Prüfung miteinzubeziehen?

Zu 2.: Das bei der Polizei Berlin vorhandene Quellen-TKÜ-System wurde im Rahmen der Beschaffung umfangreichen Tests durch die zuständige Dienststelle unterzogen.

Gegen die Einbeziehung Dritter spricht, dass durch das Bekanntwerden der technischen Möglichkeiten und der genauen Arbeitsweise der Lösung zukünftige Ermittlungen erschwert oder unmöglich gemacht werden könnten.

Die Polizei hat den Berliner Datenschutzbeauftragten bei der Erstellung des Datenschutzkonzeptes hinzugezogen.

Zur weiteren Beantwortung dieser Frage verweisen wir auf die Nummer 1 der Beantwortung Ihrer Kleinen Anfrage 17/10287.

3. Wurde von der Firma Syborg eine Zusicherung gefordert, dass verfassungswidrige Eingriffe mithilfe der Software nicht möglich sind?
a) Wenn ja, hat die Firma Syborg diese abgegeben?
b) Wenn nicht, warum soll diese Software dennoch eingesetzt werden bzw. wurde sie schon eingesetzt?

Zu 3.: Eine solche Zusicherung des Herstellers wurde und wird auch zukünftig nicht gefordert. Kein Hersteller eines Ermittlungswerkzeugs/Einsatzmittels kann garantieren, dass dieses ausschließlich gesetzmäßig eingesetzt wird. Hierfür zu sorgen, ist vielmehr Aufgabe der Sicherheitsbehörden selbst.

4. Durch welche technischen Vorkehrungen wird sichergestellt, dass das Sicherheitsniveau dieses „Trojaners“ besser ist, als das des vom Chaos Computer Club analysierten „Trojaners“?

Zu 4.: Die Vertraulichkeit der übermittelten Daten wird durch die Implementierung eines hybriden Verschlüsselungssystems sichergestellt.

5. Wurde geprüft, ob die Software die infiltrierten Rechner für weitere Angriffe von außen, die mit der Überwachung nichts zu tun haben, anfälliger macht?
a) Wenn ja, wie wurde das geprüft und durch wen?
(Bitte detallierte Beschreibung des etwaigen Prüfverfahrens.)
b) Wenn nein, warum nicht?

Die Drucksachen des Abgeordnetenhauses sind bei der Kulturbuch-Verlag GmbH zu beziehen.
Hausanschrift: Sprosserweg 3, 12351 Berlin-Buckow · Postanschrift: Postfach 47 04 49, 12313 Berlin, Telefon: 6 61 84 84; Telefax: 6 61 78 28.

Zu 5.: Eine Überprüfung im Vorhinein ist objektiv nicht möglich. Eine derartige Prüfung könnte erst erfolgen, wenn hinreichende Informationen über das Zielsystem bekannt sind und gilt dann auch nur für genau dieses Zielsystem.

Wie jedes staatliche Handeln ist auch jede einzelne Maßnahme der Quellen-TKÜ jeweils neu hinsichtlich ihrer Verhältnismäßigkeit zu prüfen. Dies geschieht bei der Quellen-TKÜ naturgemäß bei den Strafverfolgungsbehörden im Rahmen der Antragstellung an den Ermittlungsrichter/in, im Rahmen der Prüfung dieses Antrages durch den Richter/in und fortlaufend im Rahmen der Umsetzung der Maßnahme.

Sollte bei der Vorbereitung oder während der Umsetzung/Durchführung einer Maßnahme der Quellen-TKÜ beispielsweise aufgrund der Gegebenheiten des Zielsystems die Einbringung der Software oder die Weiterführung einer bereits laufenden Maßnahme wegen einer konkreten Gefährdung der Sicherheit unverhältnismäßig erscheinen, kann die Maßnahme nach Rücksprache mit der zuständigen Staatsanwaltschaft und nach deren Entscheidung nicht umgesetzt werden.

6. Wie wird das Risiko der Manipulation der vermeintlich korrekt erhobenen Daten minimiert?

Zu 6.: Die auf dem überwachten System erhobenen Daten werden unverzüglich nach dem Rivest-Shamir-Adleman-Verfahren (RSA) signiert, gleiches gilt für alle Protokolldateien auf dem Zentralsystem. Der fehlerfreie und nicht manipulierte Datenbestand ist damit jederzeit nachweisbar.

7. Wie bewertet der Senat die sich zwangsläufig mit der Überwachung eines überwachten Kommunikationspartners ergebene inhaltliche Mitüberwachung des anderen, nicht überwachten Kommunikationspartners bei der Quellen-TKÜ?

8. Wie bewertet der Senat die Tatsache, dass durch den Einsatz der Trojaner-Software ohne Wissen der jeweils überwachten Person Daten Dritten zur Kenntnis gelangen, zu deren Geheimhaltung sich die überwachte Person verpflichtet hat (bspw. vertrauliche Geschäftsdaten)?

Zu 7. und 8.: Im Rahmen von Quellen-TKÜ-Maßnahmen besteht – wie bei jeder anderen Überwachung von Telekommunikation – die grundsätzliche Möglichkeit der Aufzeichnung von Telekommunikationsvorgängen mit Dritten.

Die Weiterleitung von Kommunikationsdaten an die Ermittlungsbehörden richtet sich auch bei einer "Quellen-Telekommunikationsüberwachung" nach § 100a Strafprozessordnung (stopp). Sie darf nur durch das Gericht, bei Gefahr im Verzug durch die Staatsanwaltschaft angeordnet werden, § 100b Abs. 1 Satz 1, 2 StPO.

§ 100a StPO ermöglicht – unter engen Voraussetzungen – die Überwachung und Aufzeichnung sämtlicher technischer Vorgänge des Aussendens, Übermittelns und auch des Empfangens von Nachrichten und damit auch eine "Mitüberwachung des anderen, nicht überwachten Kommunikationspartners". Dabei können den Ermittlungsbehörden auch Daten zur Kenntnis gelangen, "zu deren Geheimhaltung sich die überwachte Person verpflichtet hat". Das Interesse, diese Daten nicht zu offenbaren, tritt dann hinter das Interesse an der Aufklärung einer schweren Straftat zurück.

9. Wie wird sichergestellt, dass keine vertraulichen Daten aus Ermittlungsverfahren an den Eigentümer von Syborg (Verint) gelangen?

Zu 9.: Die Firma Syborg ist nicht Herstellerin des Quellen-TKÜ-Systems der Berliner Polizei.

Der Systemhersteller hat grundsätzlich keinen Zugang zum Quellen-TKÜ-System.

Sollte im Einzelfall, z.B. im Rahmen eines Releasewechsels eine Arbeit am Zentralsystem erforderlich sein, wird diese auf gespiegelter Hardware durchgeführt, auf der zwar die Systemsoftware installiert ist, die jedoch als reines Standby-System ohne Lizenz und Nutzdaten betrieben wird. Nach dem Abschluss dieser Arbeiten werden dann die Updates durch eigenes Personal vom Spiegelsystem auf das Wirksystem übertragen.

10. Wurde der Quellcode der Software analysiert?
a) Wenn ja, von wem?
b) Wenn nein, warum nicht?
c) Wenn Anwendungstests durchgeführt wurden, wie sahen diese aus?
(Bitte detaillierte Beschreibungen dieser Anwendungstests.)

Zu 10.: Zur Beantwortung dieser Frage verweisen wir auf die Nummer 2 der Beantwortung der Kleinen Anfrage 17/10287.

11. Weist die Software eine Aktualisierungsfunktion auf?
a) Wenn ja, wie wird sichergestellt, dass die Überwachungssoftware nicht nachträglich mit Funktionen versehen wird, die von der jeweiligen Anordnung nicht umfasst sind?
(Bitte genaue Beschreibung durch welche technischen und organisatorischen Maßnahmen das Vorgenannte sichergestellt wird.)

Zu 11.: Das Quellen-TKÜ-System verfügt über eine Aktualisierungsfunktion, über die Updates und mögliche Fehlerkorrekturen eingespielt werden können.

Wie bereits zu Frage 6 ausgeführt, werden alle am System vorgenommenen Tätigkeiten und Veränderungen

von Einstellungen und Konfigurationsänderungen protokolliert. Die Protokolldateien werden digital signiert, jegliche Manipulationsversuche können damit nachvollzogen und durch das Gericht überprüft werden.

12. Sind bei der Firma Syborg über die Aktualisierungsfunktion hinausgehende Funktionserweiterungen in Auftrag gegeben worden?

a) Wenn ja, über welchen Server wäre ein solches Nachladen möglich?

b) Wie wird der entsprechende Server vor den Zugriffen Dritter geschützt?

Zu 12.: Die Firma Syborg ist nicht Herstellerin des Quellen-TKÜ-Systems der Berliner Polizei.

Es wurden keine Aufträge zur Funktionserweiterung vergeben.

13. Wie wird kontrolliert, dass der Kernbereich privater Lebensgestaltung von der Quellen-TKÜ ausgenommen wird?

a) Wenn Daten aus diesem Bereich gewonnen werden, wie wird sichergestellt bzw. kontrolliert, dass diese unverzüglich gelöscht werden?

Zu 13.: Im Rahmen von Quellen-TKÜ-Maßnahmen besteht – wie bei jeder anderen Überwachung von Telekommunikation – die grundsätzliche Möglichkeit der Aufzeichnung von Telekommunikationsinhalten, die im Einzelfall zum Kernbereich privater Lebensgestaltung zählen könnten.

Liegen tatsächliche Anhaltspunkte für die Annahme vor, durch eine Maßnahme der Telekommunikationsüberwachung würden allein Erkenntnisse aus dem Kernbereich privater Lebensgestaltung erhoben, ist diese nach § 100a Abs. 4 Satz 1 StPO unzulässig. Liegen diese Voraussetzungen nicht vor, kann die Telekommunikationsüberwachung durchgeführt werden, auch wenn die potentielle Möglichkeit besteht, im Einzelfall auch Erkenntnisse aus dem Kernbereich privater Lebensgestaltung zu erheben.

Im Rahmen der Auswertung der jeweiligen Überwachungsmaßnahmen können dem Kernbereichsschutz unterfallende Inhalte erkannt und unverzüglich nach § 100a Abs. 4 Satz 3 StPO i.Vm. der „Gemeinsamen Leitlinie der Generalstaatsanwälte zur Bestimmung kernbereichsrelevanter Telekommunikation und zur Benachrichtigung von Telekommunikationsüberwachungsmaßnahmen Betroffener“ gelöscht werden. Die Löschung wird aktenkundig gemacht.

14. Wodurch könnten etwaige Manipulationen von außen sichtbar bzw. nachgewiesen werden?

Zu 14.: Siehe Antwort zu Frage 6.

15. Nimmt die Behörde (z.B. LKA), die die Quellen-TKÜ vornimmt, die für den konkreten Einzelfall erforderliche Konfiguration der Software selbst vor?

a) Wenn ja, wie werden die Personen kontrolliert, die diese Konfiguration vornehmen?

Zu 15.: Maßnahmen der Quellen-TKÜ erfordern aufgrund ihrer Abstimmung auf das Zielsystem umfassende Ermittlungen im Vorfeld. Bereits im Rahmen der Prüfung einer Quellen-TKÜ-Maßnahme würden daher regelmäßig Einzelfallanordnungen beantragt, die den Besonderheiten des jeweiligen Vorgangs und dessen Anforderungen entsprechen müssten.

Sofern der zuständige Ermittlungsrichter/in dem Antrag stattgegeben und einen entsprechend ausgestalteten Beschluss zur Telekommunikationsüberwachung erlassen würde, würden die darin enthaltenen Vorgaben und Beschränkungen entsprechend im Quellen-TKÜ-System abgebildet und die Maßnahme umgesetzt.

Aufgrund der Protokollierung und der Signierung der dabei entstehenden Protokolldateien wäre für jede einzelne Überwachungsmaßnahme jederzeit nachvollziehbar, welche Einstellungen bei der Einrichtung der Maßnahme vorgenommen und ggfs. während der Laufzeit der Maßnahme verändert wurden.

Das Quellen-TKÜ-System stellt zur Prüfung der Integrität der genannten Protokolldateien ein geeignetes einfaches Werkzeug zur Verfügung (z.B. für Richter/innen).

Berlin, den 24. Mai 2012

Frank Henkel
Senator für Inneres und Sport

(Eingang beim Abgeordnetenhaus am 12. Juni 2012)