Abgeordnetenhaus BERLIN

Drucksache 17 / 12 393
Kleine Anfrage

17. Wahlperiode

Kleine Anfrage

des Abgeordneten Stefan Gelbhaar (GRÜNE)

vom 02. Juli 2013 (Eingang beim Abgeordnetenhaus am 05. Juli 2013) und **Antwort**

Spionage à la Prism und Tempora - Schlussfolgerungen für Berliner Behördenkommunikation?

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

1. Hat der Senat in Hinblick auf die Kommunikation zwischen bzw. in den Berliner Behörden Schlussfolgerungen aus dem Bekanntwerden von Prism und Tempora gezogen und wenn ja, welche? Wenn nein, soll eine solche Auswertung noch erfolgen, und wenn ja, durch wen, bis wann und in welcher Form“?

Zu 1.: In der Berliner Verwaltung wird zur Kommunikation zwischen den Behörden grundsätzlich das vom zentralen IT-Dienstleister des Landes Berlin, dem IT-Dienstleistungszentrum Berlin (ITDZ) betriebene landeseigene Übertragungsnetz (Berliner Landesnetz) genutzt.

Für das Berliner Landesnetz und den IT-Einsatz der Berliner Verwaltung insgesamt sind - auf Basis der Standards des Bundesamtes für Sicherheit in der Informationstechnik (BSI) zum IT-Grundschutz - vielfältige Maßnahmen zum anforderungsgerechten Schutz der Vertraulichkeit, Verfügbarkeit und Integrität der verarbeiteten Informationen umgesetzt.

Die Wirksamkeit der Maßnahmen wird in einem regelmäßigen Controllingprozess bewertet. In diesem Prozess werden - auch unter Berücksichtigung aktueller Ereignisse - neue Risiken und ihre Auswirkungen auf den IT-Einsatz in der Berliner Verwaltung insgesamt und speziell auf die IT-gestützte Kommunikation der Behörden analysiert. Aus dieser Analyse ergeben sich die Anforderungen an fortzuschreibende bzw. neue Maßnahmen und Regelungen, die dann schrittweise umgesetzt werden.

In diesen Prozess fließen auch die vorliegenden Informationen zu Prism und Tempora ein.

2. Ist aus Sicht des Senats ein Schaden denkbar, wenn die Berliner Behördenkommunikation durch staatliche Einheiten aus Drittländern ausgespäht wird? Wenn ja, welcher mögliche Schaden wird dabei bewertet?

Zu 2.: Verlust oder Beeinträchtigung der unter Tz. 1. angeführten Schutzziele (Vertraulichkeit, Verfügbarkeit und Integrität) können grundsätzlich zu entsprechenden Schäden für die Berliner Verwaltung führen.

Zur Bewertung möglicher Schäden werden die vom BSI bereitgestellten Klassifikationen in einer an die Berliner Verwaltung angepassten Form mit folgenden Schadenskategorien genutzt:

- Verstoß gegen Gesetze/Vorschriften/Verträge
- Beeinträchtigung des informationellen Selbstbestimmungsrechts
- Beeinträchtigung der persönlichen Unversehrtheit
- Beeinträchtigung der Aufgabenerfüllung
- Negative Innen- oder Außenwirkung.

3. Gab es in der Vergangenheit Spionage-Attacken auf Berliner Behörden und ihre Kommunikation über das Internet oder in anderer Form? Sind die VerursacherInnen bekannt geworden? Welche Bereiche waren betroffen?

Zu 3.: Gezielte, spezifisch auf bestimmte Behörden der Berliner Verwaltung ausgerichtete Angriffe sind in den letzten Jahren nicht festgestellt worden.

Angriffe von ausländischen staatlichen Stellen waren in der Vergangenheit nicht nachweisbar.

Andererseits ist die Berliner Verwaltung, wie alle anderen Nutzerinnen und Nutzer des Internet auch, tagtäglich einer Vielzahl ungezielter Angriffe ausgesetzt. Ungezielte Angriffe werden überwiegend automatisiert durchgeführt und betreffen jedes IT-System, das an das Internet angebunden ist. Diese automatisierten Angriffe werden durch die vorhandenen Sicherheitsmaßnahmen erkannt und wirksam verhindert.

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.

Die für die Berliner Verwaltung vorliegenden Analysen zeigen, dass ca. 10% der von außen eingehenden Kommunikationsversuche als solche ungezielten Angriffe anzusehen sind.

4. Welche vertrauliche (also über Amtsgeheimnis geschützte) Behördenkommunikation wird über das Internet, etwa per Mail, Internet-Telefonie etc., abgewickelt? Gibt es diesbezüglich Vorgaben zum Schutz, etwa zur Verschlüsselung der Daten, und wenn ja, welche? Bitte konkret ausführen.

Zu 4.: Bei der Kommunikation über das Internet muss der anforderungsgerechte Schutz der Vertraulichkeit gewährleistet sein. Abhängig vom Schutzbedarf der Informationen werden dazu auch entsprechende Verschlüsselungslösungen genutzt. Insbesondere werden sensible Daten von Bürgerinnen und Bürgern grundsätzlich über verschlüsselte Verbindungen übertragen.

Im Bereich der Sprachkommunikation bietet das ITDZ u. a. mobile Telefone an, die mit besonderer Verschlüsselung arbeiten.

Gemäß den IT-Sicherheitsgrundsätzen der Berliner Verwaltung muss bei besonderem Schutzbedarf der verarbeiteten Daten auf Basis einer ergänzenden Risikoanalyse geprüft werden, ob und welche zusätzlichen Sicherheitsmaßnahmen ggf. erforderlich sind. Dies gilt in besonderem Maße für die Kommunikation über das Internet.

Wird der Schutzbedarf der Daten als so hoch eingeschätzt, dass hieraus ein nicht tragbares Risiko entsteht, ist in diesen Bereichen auf die Nutzung des Internet zu verzichten.

In der Gemeinsamen Geschäftsordnung der Berliner Verwaltung – Allgemeiner Teil – (GGO I) ist ebenso festgelegt, dass bei Schriftstücken, deren Inhalt in besonderem Maße schutzbedürftig ist, eine Übermittlung mit elektronischer Post nur möglich ist, wenn durch geeignete Sicherheitsmaßnahmen eine den gesetzlichen und sonstigen Anforderungen entsprechende Vertraulichkeit der Schriftstücke gewährleistet ist.

Die Kommunikation der Verfassungsschutzbehörde, soweit sie über das Internet erfolgt und Verschlusssachen betrifft, unterliegt einer besonders gesicherten und durch das BSI (Bundesamt für Sicherheit in der Informationstechnik) geprüften Verschlüsselung.

5. Wie bewertet der Senat die Wirksamkeit dieser Schutzmaßnahmen insbesondere in Hinblick auf Spähprogramme wie Prism und Tempora sowie die dahinter stehenden Organisationen?

Zu 5.: Die in der Berliner Verwaltung umgesetzten IT-Sicherheitsmaßnahmen bilden nach bisherigen Erkenntnissen einen wirksamen Schutz, um Vertraulichkeit, Verfügbarkeit und Integrität der verarbeiteten Informationen in dem erforderlichen Maße unter Berücksichtigung des jeweiligen Schutzbedarfes zu gewährleisten. Durch das regelmäßige Anpassen dieser Sicherheitsmaßnahmen an neue Risiken, z. B. durch die regelmäßige Aktualisierung der eingesetzten Schutzprogramme oder das Einspielen von Sicherheitsupdates wird dieser Schutz ständig auf dem erforderlichen Niveau gehalten und auch zielgerichtet weiter verbessert.

Wie unter Tz. 4 bereits dargestellt, ist bei besonderem Schutzbedarf der Daten eine gesonderte Risikobewertung erforderlich, die ggf. zum Verzicht auf den IT-Einsatz bzw. die Nutzung des Internet führen kann.

Wie unter Tz. 1 dargestellt, fließen die vorliegenden Informationen zu Prism und Tempora in den Controllingprozess, mit dem die Wirksamkeit der IT-Sicherheitsmaßnahmen bewertet wird, ein.

6. Wer ist zuständig in der Berliner Verwaltung und wie findet ggf. die Koordination statt?

Zu 6.: Der Senatsverwaltung für Inneres und Sport obliegt die Aufgabe, die notwendigen landesweiten Regelungen bzgl. IT-Sicherheit zu erstellen und fortzuschreiben und die behördenübergreifenden Prozesse zu koordinieren.

Die Umsetzung der notwendigen Maßnahmen in den Behörden liegt gemäß der dezentralen Fach- und Ressourcenverantwortung in Verantwortung der einzelnen Senats- und Bezirksverwaltungen.

In einer regelmäßig tagenden behördenübergreifenden Arbeitsgruppe (AG IT-Sicherheit) werden unter Federführung der Senatsverwaltung für Inneres und Sport aktuelle Themen der Informationssicherheit erörtert, neue Risiken bewertet und entsprechende Maßnahmenvorschläge erarbeitet.

Berlin, den 18. Juli 2013

In Vertretung

Bernd Krömer
Senatsverwaltung für Inneres und Sport

(Eingang beim Abgeordnetenhaus am 06. Aug. 2013)