

16. Wahlperiode

Nicht behandelte Mündliche Anfrage Nr. 12

des Abgeordneten Thomas Birk (Bündnis 90/Die Grünen)

aus der 78. Sitzung des Abgeordnetenhauses vom 03. März 2011 und **Antwort**

Ist die Berliner Verwaltung gerüstet gegen Cyber-Attacken?

Im Namen des Senats von Berlin beantworte ich Ihre nicht erledigte Mündliche Anfrage gemäß § 51 Abs. 5 der Geschäftsordnung des Abgeordnetenhauses wie folgt:

1. Sieht der Senat die Berliner Verwaltung ausreichend gerüstet gegen Angriffe durch Computerviren, wie im brandenburgischen Finanzministerium, angesichts der Tatsache, dass nur rund die Hälfte der Berliner Behörden über ein von der jeweiligen Leitung bestätigtes IT-Sicherheitskonzept verfügt?

Zu 1.: Die Berliner Verwaltung ist nach den derzeit erkennbaren Risiken ausreichend gerüstet gegen Angriffe durch Computerviren. In allen Behörden der Verwaltung sind Maßnahmen zum Virenschutz umgesetzt. In dem vom zentralen IT-Dienstleister des Landes, dem IT-Dienstleistungszentrum Berlin (ITDZ), betriebenen zentralen Übergang ins Internet sind entsprechende Sicherheitsmaßnahmen umgesetzt, um Schadsoftware rechtzeitig zu erkennen und abzuwehren.

Die Maßnahmen zum Virenschutz entsprechen den Standards des Bundesamtes für Sicherheit in der Informationstechnik (BSI).

Die Wirksamkeit und Umsetzung von IT-Sicherheitsmaßnahmen insgesamt und speziell auch zum Virenschutz wird durch einen jährlich von der Senatsverwaltung für Inneres und Sport erstellten verwaltungsinternen "Bericht zur Informationssicherheit" überprüft. Aus diesem Bericht ergibt sich, dass zwar noch nicht alle Behörden über ein vollständiges IT-Sicherheitskonzept verfügen, gleichwohl Maßnahmen zum Virenschutz (z. B. durch den Einsatz entsprechender Virenschutzprogramme) in allen Behörden realisiert sind. Durch fortlaufende Aktualisierungen ist gewährleistet, dass die von den Virenschutzprogrammen zum Erkennen von Schadsoftware benötigten Signaturen immer auf dem aktuellen Stand sind.

Die eingesetzte Virenschutzsoftware erkennt Schadsoftware zuverlässig, so dass trotz vorhandener Angriffe, denen auch die Berliner Verwaltung ausgesetzt ist, die Vertraulichkeit und Integrität der in der Berliner Verwaltung verarbeiteten Informationen gewährleistet ist.

2. Welche Maßnahmen wird der Senat ergreifen, um zeitnah endlich ein flächendeckendes IT-Sicherheitsmanagement in der Berliner Verwaltung durchzusetzen?

Zu 2.: Die Verantwortung für das Einrichten eines behördlichen IT-Sicherheitsmanagements obliegt - gemäß der grundsätzlichen dezentralen Umsetzungsverantwortung - den jeweiligen Behörden. Der aktuell für das Jahr 2010 erstellte "Bericht zur Informationssicherheit" zeigt auf, dass fast alle Behörden bereits die Rolle eines "IT-Sicherheitsbeauftragten" eingerichtet haben.

Der IT-Sicherheitsbeauftragte ist ein notwendiges Element des behördlichen IT-Sicherheitsmanagements. Gleichwohl muss dieses Element eingebettet sein in einen ganzheitlichen, von der Behördenleitung aktiv unterstützten Prozess, mit dem die Gewährleistung von IT-Sicherheit in der Behörde gesteuert wird. Dieser Prozess ist derzeit in der Hälfte aller Behörden vollständig etabliert.

Die Grundlagen für solch einen Prozess sind im Rahmen einer behördlichen "Leitlinie Informationssicherheit" festzulegen. Unter Federführung der Senatsverwaltung für Inneres und Sport wird derzeit auf Arbeitsebene eine Mustervorlage für eine solche Leitlinie erstellt. Damit sollen die Behörden bei ihrer dezentralen Umsetzungsverantwortung unterstützt werden.

Eine landesweite "Leitlinie für Informationssicherheit" liegt in Form der "IT-Sicherheitsgrundsätze" bereits seit vielen Jahren vor und bildet die Grundlage für die landesweite Steuerung bzgl. IT-Sicherheit.

Berlin, den 14. März 2011

Dr. Ehrhart Körting
Senator für Inneres und Sport

(Eingang beim Abgeordnetenhaus am 28. März 2011)