

Antwort
der Landesregierung

auf die Kleine Anfrage 1138
des Abgeordneten Ludwig Burkardt
CDU-Fraktion
Drucksache 5/2914

Wurm im Finanzministerium – Sicherheitslücken in der Landesverwaltung?

Wortlaut der Kleinen Anfrage 1138 vom 14.03.2011:

Ende Februar mussten im Brandenburger Finanzministerium nach der Entdeckung eines Computerwurms alle Computer abgeschaltet und überprüft werden. Die Ursache hierfür war nach Presseberichten offenbar ein veralteter Virenschutz. Nach der Darstellung der Pressesprecherin konnte der Wurm auf dem Weg zum Server abgefangen worden, so dass keine Daten in Mitleidenschaft gezogen worden seien.

Ich frage die Landesregierung:

1. Welche Schadsoftware ist wann und auf welche Weise entdeckt worden und wie konnte diese gelöscht werden?
2. Welche Sicherheitslücken sind die Ursache für diesen Vorfall?
3. Ist es zutreffend, dass der Computerwurm aufgrund eines veralteten Virenschutzes eindringen konnte und wenn ja, wer trägt hierfür die Verantwortung?
4. Ist die Darstellung des ZIT-Sprechers richtig, dass die Sicherheitslücken aufgetreten sind, weil das Ministerium dem IT-Dienstleister den Zugang zu einigen Servern nicht ermöglicht hat?
5. Ist die Aussage der MdF-Sprecherin zutreffend, dass am 21.02.2011 sämtliche Rechner im Finanzministerium nicht genutzt werden konnten?
6. In welchem Zeitraum verfügten welche Teile der Landesverwaltung über keinen aktuellen Virenschutz?
7. Aufgrund welcher Prüfungen kann das MdF ausschließen, dass hausinterne Daten oder besonders schützenswerte Steuerdaten entwendet worden sind?
8. Welche Prüfungen erfolgten in dieser Hinsicht in den anderen betroffenen Teilen der Landesverwaltung und mit welchem Ergebnis?
9. Welche besonderen Sicherheitsvorkehrungen trifft das Finanzministerium, um das Steuergeheimnis im IT-Bereich zu schützen?
10. Welche rechtlichen Vorschriften regeln die IT-Sicherheit in der Landesverwaltung und welche Maßnahmen sind vorgesehen, wenn die definierten Sicherheitsstandards nicht eingehalten werden?
11. Wann ist die Datenschutzbeauftragte des Landes über den Vorfall unterrichtet worden und wie bewertet sie den Sachverhalt gemäß den Bestimmungen des Datenschutzgesetzes?

Namens der Landesregierung beantwortet der Minister der Finanzen die Kleine Anfrage wie folgt:

Frage 1:

Welche Schadsoftware ist wann und auf welche Weise entdeckt worden und wie konnte diese gelöscht werden?

zu Frage 1:

Am 19.02.2011 wurde im Rahmen von planmäßigen Wartungsarbeiten des Brandenburgischen IT-Dienstleisters (ZIT-BB) bei einigen Rechnern des Ministeriums der Finanzen (MdF) der Befall mit dem Conficker-Wurm festgestellt. Die betroffenen Rechner wurden vom Conficker-Wurm durch entsprechende technische Mittel gesäubert.

Frage 2:

Welche Sicherheitslücken sind die Ursache für diesen Vorfall?

zu Frage 2:

Die Ursache hierfür war ein veralteter Stand der Virenschutzprogramme und der Softwareupdates des Betriebssystems.

Frage 3:

Ist es zutreffend, dass der Computerwurm aufgrund eines veralteten Virenschutzes eindringen konnte und wenn ja, wer trägt hierfür die Verantwortung?

zu Frage 3:

Ja. Im Rahmen der Bündelung der IT-Infrastruktur des Landes beim ZIT-BB wurde auch die Informationstechnik des MdF übertragen. Die Übernahme der IT-Infrastruktur war in diesem Fall verbunden mit einer Umstellung der Virenvorsorge auf die technischen Gegebenheiten des Dienstleisters und einem Wechsel der Virenschutzsoftware. Nach der Übernahme wurde der Virenschutz sukzessive aktualisiert. Hierbei wurden jedoch Geräte, die sich vorwiegend im mobilen Einsatz befinden, über das Netzwerk nicht erreicht, wodurch eine zeitnahe Aktualisierung unterblieb.

Frage 4:

Ist die Darstellung des ZIT-Sprechers richtig, dass die Sicherheitslücken aufgetreten sind, weil das Ministerium dem IT-Dienstleister den Zugang zu einigen Servern nicht ermöglicht hat?

zu Frage 4:

Nein. Die Presseberichte geben den Sachverhalt nicht korrekt wieder.

Frage 5:

Ist die Aussage der MdF-Sprecherin zutreffend, dass am 21.02.2011 sämtliche Rechner im Finanzministerium nicht genutzt werden konnten?

zu Frage 5:

Am 21.02.2011 war eine begrenzte Anzahl von Arbeitsplätzen im MdF für einige Stunden nicht arbeitsfähig. Die in der Fragestellung suggerierte Aussage, dass am 21.02.2011 die Computerarbeitsplätze des MdF ganztägig nicht einsatzfähig gewesen wären, ist falsch und wurde von der Pressesprecherin des MdF so nie bekannt gegeben.

Frage 6:

In welchem Zeitraum verfügten welche Teile der Landesverwaltung über keinen aktuellen Virenschutz?

zu Frage 6:

Hinweise auf einen nicht aktuellen Virenschutz in Dienststellen der Landesverwaltung liegen der Landesregierung – bis auf den genannten Virenbefall - nicht vor.

Frage 7:

Aufgrund welcher Prüfungen kann das MdF ausschließen, dass hausinterne Daten oder besonders schützenswerte Steuerdaten entwendet worden sind?

zu Frage 7:

Tiefgehende Analysen des ZIT-BB haben keinerlei Hinweise auf einen Verlust von Vertraulichkeit oder Integrität der Daten ergeben. Aufgrund der physischen und logischen Trennung der Netze der allgemeinen Verwaltung und der Steuerverwaltung waren Steuerdaten zu keinem Zeitpunkt betroffen.

Frage 8:

Welche Prüfungen erfolgten in dieser Hinsicht in den anderen betroffenen Teilen der Landesverwaltung und mit welchem Ergebnis?

zu Frage 8:

Die Landesverwaltung betreibt eine zentrale Netzüberwachung. Es wurden keine Hinweise auf einen Virenbefall außerhalb des MdF gefunden.

Frage 9:

Welche besonderen Sicherheitsvorkehrungen trifft das Finanzministerium, um das Steuergeheimnis im IT-Bereich zu schützen?

zu Frage 9:

Die Daten der Steuerverwaltung werden in einem zentralen Fachrechenzentrum in Cottbus bearbeitet, welches physisch und logisch abgeschottet zum Netz der allgemeinen Verwaltung betrieben wird.

Frage 10:

Welche rechtlichen Vorschriften regeln die IT-Sicherheit in der Landesverwaltung und welche Maßnahmen sind vorgesehen, wenn die definierten Sicherheitsstandards nicht eingehalten werden?

zu Frage 10:

Durch den Runderlass der Landesregierung zur Gewährleistung der IT-Sicherheit in der Landesverwaltung Brandenburg (IT-Sicherheitsleitlinie) vom 22.09.2009 wird die Gewährleistung der IT-Sicherheit in der Landesverwaltung geregelt. Werden Verstöße gegen die Vorgaben der IT-Sicherheitsleitlinie oder Sicherheitsverletzungen festgestellt, so wird die betreffende Dienststelle über den zuständigen IT-Sicherheitsbeauftragten des Ressorts aufgefordert, in einer angemessenen Frist die Sicherheitsverletzungen zu beheben beziehungsweise die Vorgaben der IT-Sicherheitsleitlinie umzusetzen. Bei anhaltenden Verstößen gegen die Vorgaben der IT-Sicherheitsleitlinie oder bei anhaltenden Sicherheitsverletzungen informiert der IT-Sicherheitsmanager der Landesverwaltung den Ausschuss der Ressortbeauftragten für IT und E-Government (RIO-Ausschuss). Dieser kann bindende Maßnahmen zur Gewährleistung der IT-Sicherheit im Landesverwaltungsnetz beschließen.

Frage 11:

Wann ist die Datenschutzbeauftragte des Landes über den Vorfall unterrichtet worden und wie bewertet sie den Sachverhalt gemäß den Bestimmungen des Datenschutzgesetzes?

zu Frage 11:

Eine Unterrichtung der Landesbeauftragten für den Datenschutz und das Recht auf Akteneinsicht (LDA) erfolgt nur, wenn personenbezogene Daten betroffen sind oder sein könnten. Nach den Erkenntnissen des MdF und des ZIT-BB war dies nicht der Fall.

Gleichwohl wurde die LDA ihrem Wunsch entsprechend am 04.03.2011 durch das MdF über den Vorfall unterrichtet.

Informationen über die Bewertung des Vorfalls durch die Datenschutzbeauftragte des Landes liegen der Landesregierung derzeit nicht vor.