Landtag von Sachsen-Anhalt

Drucksache 6/382
08.09.2011

Antwort der Landesregierung auf eine Kleine Anfrage zur schriftlichen Beantwortung

Abgeordneter Sebastian Striegel (BÜNDNIS 90/DIE GRÜNEN)

Unbefugter Zugriff auf Datenbestände des LKA Sachsen-Anhalt

Kleine Anfrage - **KA 6/7140**

Vorbemerkung des Fragestellenden:

Anfang Juli 2011 drangen nach Medienberichten Hacker in geschützte Netzwerke des deutschen Zolls und einiger Landeskriminalämter ein. Sie entwendeten dabei Daten aus unzureichend geschützten Datenbanken und veröffentlichten diese (auszugsweise) im Internet.

Antwort der Landesregierung erstellt vom Ministerium des Innern

Namens der Landesregierung beantworte ich die Kleine Anfrage wie folgt:

1. Nutzt auch das Landeskriminalamt Sachsen-Anhalt das von Hackern beeinträchtigte Peil- und Ortungssystem „Patras“?

Das Landeskriminalamt Sachsen-Anhalt (LKA) nutzte bis zum 11. Juli 2011 einen so genannten virtuellen Paip Tracking-Server (PATRAS), der sich physisch im Technischen Polizeiamt befindet. Unmittelbar nach Bekanntwerden des Hackerangriffs wurde der entsprechende Server vom Netz getrennt.

2. War auch das Landeskriminalamt Sachsen-Anhalt durch den Hackerangriff auf das System „Patras“ betroffen und wenn ja, in welcher Form?

Im Ergebnis der forensischen Untersuchung des Servers sowie der mit diesem System in Verbindung stehenden IT-Systeme konnten keine Anhaltspunkte für das Vorhandensein von Schadsoftware festgestellt werden. Somit liegt kein Anfangsverdacht einer strafbaren Handlung vor.

(Ausgegeben am 12.09.2011)

3. Wird bei den vermuteten Straftatbeständen durch die Landesregierung eine politische oder nicht-politische Motivation unterstellt?

In mehreren betroffenen Bundesländern werden Ermittlungsverfahren wegen des Verdachts des Ausspähens von Daten (§ 202a Strafgesetzbuch) und des Verdachts der Datenveränderung in Verbindung mit Computersabotage (§§ 303a und 303b StGB) geführt. Da im Land Sachsen-Anhalt ein entsprechender Anfangsverdacht nicht vorliegt und keine Ermittlungsverfahren zu den Hackerangriffen geführt werden, können auch keine Aussagen über die Motivation der Beschuldigten getroffen werden.

4. Wenn das Landeskriminalamt betroffen war, auf welche konkreten Datenbestände bezog sich der Hackerangriff? Bitte den genauen Zeitraum der betroffenen Datenbestände angeben.

Entfällt.

5. Sollten Behörden Sachsen-Anhalts oder Ermittlungsvorgänge in Sachsen-Anhalt betroffen sein, bitte ich um Mitteilung, welche Datensätze im Internet veröffentlicht wurden.

Entfällt.

6. Sind personenbezogene Daten betroffen? Wenn ja, von wie vielen Personen wurden personenbezogene Daten durch die Hacker ausgelesen?

Entfällt.

7. Beeinträchtigt der Datenklau etwaige Ermittlungen des Landeskriminalamts Sachsen-Anhalt? In welcher Form?

Entfällt.

8. Gab es in der Vergangenheit bereits andere (erfolgreiche) Hackerangriffe, bei denen Daten aus geschützten Netzwerken des sachsen-anhaltischen Landeskriminalamts oder von anderen Polizeidienststellen entwendet wurden? Bitte ggf. nach Datum sowie der Art der entwendeten Daten aufschlüsseln.

Es sind keine Angriffe bekannt, bei denen Daten aus geschützten Netzwerken der Polizei entwendet wurden.

9. Welche konkreten Vorkehrungen haben das Landeskriminalamt und die Polizeidienststellen des Landes getroffen, um zukünftige Hackerangriffe und den unbefugten Zugriff auf Datenbestände der Sicherheitsbehörden zu verhindern?

Die Kommunikation der Polizei erfolgt innerhalb einer geschlossenen Benutzergruppe (Virtual Private Network - VPN) im Informationstechnischen Netz des Landes Sachsen-Anhalt (ITN LSA). Der Betrieb, die Administration und die Überwachung dieses VPN obliegen, ebenso wie beim ITN LSA mit seinen

Übergängen in Fremdnetze, dem Technischen Polizeiamt des Landes Sachsen-Anhalt (TPA).

Dort kommen hoch komplexe Firewall-Systeme (High Level Firewalls) zum Einsatz. Sie verhindern im Zusammenhang mit eingesetzten Proxy-Servern einen direkten Zugriff aus den Fremdnetzen in das VPN. Zur Überwachung dieser Schutzmaßnahmen werden regelmäßig Penetrationstests durchgeführt.

Ein entscheidender Faktor für die Sicherheit der polizeilichen Netze und Daten des Landes Sachsen-Anhalt ist der zentrale Betrieb durch das TPA. Somit wird eine einheitliche Strategie für die Informationssicherheit durchgesetzt. Es werden alle Maßnahmen zum Schutz der Informationen abgestimmt.

10. Sind die oben genannten Vorkehrungen Teil einer Strategie, die gesamten Datenbestände des Landes gegen unbefugte Zugriffe zu sichern?

Bereits seit Bestehen des Landesdatennetzes wird eine besonders auf die IT-Sicherheit abgestimmte Strategie praktiziert. Grundsatz ist der zuverlässige Schutz sämtlicher Übergänge vom Netz der Polizei und des Landesdatennetzes zu Fremdnetzen. Hierfür ist der Netzbetreiber TPA mit seinem zentralen Security-Management verantwortlich.

Seit mehreren Jahren gibt es einen etablierten IT-Sicherheitsprozess sowohl im Landesdatennetz ITN LSA als auch bei der Polizei. Das Landesdatennetz wurde in der Vergangenheit regelmäßig von unabhängigen Auditoren zertifiziert.

Zusätzlich ist die Polizei des Landes Sachsen-Anhalt mit ihrer gesamten IT-Umgebung im bundesweiten IT-Sicherheitsprozess der Polizeien des Bundes und der Länder nach den Vorgaben des Bundesamtes für Sicherheit in der Informationstechnik (BSI) integriert. Jährlich werden dazu wechselseitige Audits zwischen den Polizeien der Bundesländer durchgeführt.

Dieser ständige Analyse- und Abstimmungsprozess unterstützt das Erkennen und Schließen von möglichen Schwachstellen im IT-System.