Deutscher Bundestag **Drucksache 17/6849**

17. Wahlperiode 24. 08. 2011

Kleine Anfrage

der Abgeordneten Dr. Konstantin von Notz, Wolfgang Wieland, Memet Kilic, Josef Philip Winkler, Volker Beck (Köln) und der Fraktion BÜNDNIS 90/DIE GRÜNEN

Datensicherheit und Datenschutz bei Zoll und Bundespolizei

Anfang Juli dieses Jahres wurde bekannt, dass ein Hacker-Angriff auf Server des Zolls erfolgte. Eine Gruppe mit Namen „No-Name-Crew“ war dabei offenbar in den Besitz von Daten des Zolls gelangt und hatte diese anschließend im Internet veröffentlicht. Zu den veröffentlichten Daten sollen Klarnamen von Fahndern und observierten Tatverdächtigen, Kraftfahrzeugkennzeichen ausgespähter Fahrzeuge und die Passwörter von Peilsendern der Ermittler zählen. Auch Daten des Zielverfolgungssystems Patras sollen von den Veröffentlichungen betroffen gewesen sein. Zwischenzeitlich liegen dazu weitere, teilweise widersprüchliche Medienberichte vor. „FOCUS Online“ zitiert am 16. Juli 2011 aus internen Untersuchungsberichten des Bundesamtes für Sicherheit in der Informationstechnik (BSI) sowie des Zolls, wonach Angriffe der Hackergruppe auf Server der Bundespolizei bereits vor ca. einem Jahr erfolgt seien. Das BSI geht davon aus, dass alle für den Betrieb von Patras bei den unterschiedlichsten Dienststellen unterhaltenen Server kompromittiert seien. Es seien „Trojaner“ auf die nur unzureichend abgesicherten Rechner der Bundespolizei eingeschleust worden, welche das Patras-System als verantwortlicher Dienstleisterin für andere Behörden betreibt. Ferner sei die von der Bundespolizei den Partnerbehörden zur Verfügung gestellte Software zur Absicherung der Server für die Erfüllung dieses Zweckes ungeeignet. Auch die Handlungsanweisungen für den Betrieb der Patras-Datenbank sollen in keinster Weise gängigen Sicherheitsstandards entsprochen haben. Das Ausmaß der erlangten Daten und Informationen aus dem Zuständigkeitsbereich sowohl von Bundespolizei, Bundeskriminalamt und Zoll ist somit bis heute weitgehend ungeklärt. Zwischenzeitlich wurde gemeldet, es seien zwei von drei bereits identifizierten Tatverdächtigen festgenommen worden, einer sei geständig (sueddeutsche.de vom 18. Juli 2011). Laut Meldungen vom 9. August 2011 (unter anderen SPIEGEL ONLINE) soll bereits vor zwei Jahren der private Rechner eines Zollbeamten mit einem Trojaner infiziert worden sein. Dieser habe eine dauerhafte Mailumleitung von seiner dienstlichen Adresse auf seine private Mailadresse vorgenommen, so dass sämtliche dienstlich erhaltenen Informationen dem Zugriff durch Unbefugte offenstanden.

Wir fragen die Bundesregierung:

1. Wie viele sicherheitsrelevante Zwischenfälle bei Bundespolizei-, Zoll- und Sicherheitsbehörden kann die Bundesregierung für die zurückliegenden drei Jahre bis heute bestätigen, bei denen nicht ausgeschlossen werden kann, dass personenbezogene und/oder sicherheitsrelevante Daten und Informationen aus dem Bereich dieser Stellen für den Zugriff unbefugter Dritter offenstanden?

2. Welche Stellen des Bundes und/oder der Länder waren bzw. sind von den oben genannten, jüngsten Angriffen konkret betroffen?
3. Seit wann ist der Bundesregierung bzw. den zuständigen Stellen bekannt, dass ein entsprechender Einbruch in das System stattgefunden hat bzw. die Möglichkeit dazu bestand?
4. Hinsichtlich welcher konkreten Daten und Informationen aus dem Bereich dieser Behörden kann bestätigt bzw. nicht ausgeschlossen werden, dass diese, wenn auch nur vorübergehend, dem Zugriff der Angreifer offenstanden?
5. Hinsichtlich welcher konkreten Daten und Informationen kann bestätigt werden, dass diese, wenn auch gegebenenfalls nur vorübergehend, im Internet zum Abruf zur Verfügung standen?
6. Auf welche Weise hat sich nach Auffassung der Bundesregierung der Angriff auf Server des Zolls und der Bundespolizei zugetragen?
7. Welche Behörde bzw. welches Bundesministerium zeichnet für die Ausermittlung der jüngst gemeldeten Angriffe auf Server des Zolls sowie der Bundespolizei verantwortlich?
8. Zu welchem Zeitpunkt und mit welcher konkreten Aufgabenstellung bzw. mit welchem konkreten Ziel wurde das neu geschaffene Cyber-Abwehrzentrum eingeschaltet?

   Welche konkreten Ergebnisse hat die Einbeziehung des Cyber-Abwehrzentrums bei der Aufklärung der Vorfälle ergeben?
9. Zu welchem Zeitpunkt fanden erstmalig Angriffe auf Server bundesdeutscher Behörden statt, die der Gruppe „No-Name-Crew“ zugerechnet werden?
10. Zu welchem Zeitpunkt fand der Angriff statt, der den oben bezeichneten Zugriff auf das sogenannte Patras-System ermöglichte?
11. Kann die Bundesregierung ausschließen, dass bei den eingangs beschriebenen Vorgängen auch Daten und Informationen, die nachvollziehbare personenbeziehbare Hinweise auf verdeckt durchgeführte Ermittlungsvorgänge gegen Tatverdächtige im Rahmen des Einsatzes von Patras enthalten, für Unbefugte zugänglich geworden sind?

    Wenn nein, mussten bereits entsprechende Konsequenzen beobachtet werden oder selbst gezogen werden, wie z. B. die Aufhebung der Tarnung von Ermittlern oder der Abbruch von Ermittlungen, zum Schutz von verdeckt tätigen Mitarbeitern?
12. Ist es zutreffend, dass das gesamte Peil- und Ortungssystem Patras aufgrund des Angriffs und des unklaren Ausmaßes der Betroffenheit der IT-Systeme vorübergehend abgeschaltet werden musste?

    Wenn ja, für welchen Zeitraum und mit welchen konkreten Konsequenzen für die ermittelnden Behörden bzw. die einzelnen zu diesem Zeitpunkt über das System laufenden Vorgänge bzw. Ermittlungen?
13. Auf welche Weise und durch welche Stellen wurde nach Bekanntwerden versucht, den Tathergang aufzuklären, und ist dies nach Ansicht der Bundesregierung inzwischen in einem zufriedenstellenden Ausmaß gelungen?
14. Welchen Anteil an der Aufklärung hat das Geständnis des 23-jährigen, vorübergehend festgenommenen mutmaßlichen Täters?
15. Waren nach Einschätzung der Bundesregierung für die Tatausführung überdurchschnittliche Fähigkeiten und/oder Erfahrungen erforderlich, oder genügten angesichts der von den Tätern angetroffenen Sicherheitsvorkehrun-

gen im Wesentlichen durchschnittliche Kenntnisse, wie sie beispielsweise in einschlägigen Foren etc. vermittelt werden?

16. Wird der Bericht des Bundesamtes für Sicherheit in der Informationstechnik über den Hergang in dem dafür erforderlichen Umfang zur Information der Öffentlichkeit zur Verfügung gestellt?

    Wenn nein, weshalb nicht?

17. Teilt die Bundesregierung die Auffassung, dass auch öffentliche Stellen, wie es etwa der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, Peter Schaar, kürzlich forderte und es jüngst in Schleswig-Holstein gesetzlich geregelt wurde, einer Informationspflicht bei Sicherheitsvorfällen zumindest gegenüber den Datenschutzbehörden unterliegen sollten?

    Wenn nein, was spricht aus Sicht der Bundesregierung gegen eine auf diese Weise mögliche unabhängige Drittkontrolle der vorgenommenen Sicherheitsvorkehrungen verantwortlicher Stellen?

18. Auf welche Weise ist das Zielinformationssystem Patras informationstechnisch in die IT-Infrastruktur integriert?

    Welche Behörden haben auf welcher Rechtsgrundlage Zugriffs- bzw. Nutzungsrechte?

19. Wer ist die datenschutzrechtlich verantwortliche Stelle für den Betrieb des Patras-Systems, und in welchem Umfang werden welche Arten von personenbezogenen Daten in Patras bzw. der dafür geschaffenen Infrastruktur gespeichert?

    Ist es zutreffend, dass die Bundespolizei datenschutzrechtlich im Sinne eines Auftragnehmers einer Auftragsdatenverarbeitung tätig wird?

20. Welche Verantwortlichkeiten für IT-Sicherheit und Datenschutz beim Einsatz des Patras-Systems treffen nach Auffassung der Bundesregierung die ebenfalls mitnutzenden Landeskriminalämter (LKA), das Bundeskriminalamt sowie den Zoll bzw. das Zollkriminalamt?

    Sind nach Auffassung der Bundesregierung insoweit alle das System einsetzenden Stellen den Vorgaben entsprechend ordnungsgemäß vorgegangen?

21. Ist es zutreffend, dass in der Bundespolizeikaserne Swisstal-Heimerzheim ein zentraler Server für den Betrieb von Patras steht, welcher über das Internet mit den weiteren, das System einsetzenden Behörden (LKA, BKA, Zoll) verbunden ist?

    Wurde nach Kenntnis der Bundesregierung auch dieser Server durch Trojaner befallen, und wenn ja, zu welchem Zeitpunkt?

22. Welche Sicherheitsvorkehrungen sieht die Bundespolizei generell für den Schutz ihrer Netzwerke vor Angriffen aus dem Internet vor?

23. Welche Systeme werden über das Internet mit anderen Behörden verbunden, und welche Sicherheitsvorgaben bestehen für die Anbindung über das Internet?

24. Bestehen bei Bundespolizei, Zoll und Bundeskriminalamt Sicherheitsvorgaben für die Inbetriebnahme eines Programmes wie Patras?

    Wenn ja, welche?

25. Wurden für Patras Vorabkontrollen und/oder Erlaubnisverfahren durch das BSI und den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit durchgeführt?

    Wenn nein, weshalb nicht?

26. Hat es in der Vergangenheit bereits unabhängige Prüfungen des Wirkbetriebes von Patras seitens des BSI und/oder des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit gegeben?

    Ist jetzt eine entsprechende Prüfung vorgesehen?

27. Wie konnten aus Sicht der Bundesregierung die entsprechenden Schadprogramme die Schutzvorkehrungen bei der Bundespolizei bzw. den angeschlossenen Behörden überwinden?

28. Hat die Bundespolizei verantwortlich Sicherheitssoftware für den Betrieb von Patras an die beteiligten Behörden ausgeliefert, und wenn ja, welche?

    Handelte es sich dabei um das in diesem Zusammenhang von mehreren Quellen unter anderem auch im Internet unabhängig voneinander erwähnte Programm XAMP?

29. Wie bewertet die Bundesregierung die Tatsache, dass die Bundespolizei dieses Programm zum Einsatz brachte bzw. den beteiligten Behörden zur Absicherung empfahl, dass selbst von Zollbeamten und der Bundesnetzagentur für diesen Zweck für ungeeignet gehalten wird?

30. Lagen konkrete Handlungsanweisungen für den Einsatz von Patras durch Behörden seitens der Bundespolizei vor?

    Wenn ja, wurde dort die datenbankmäßige Speicherung von Passwörtern im Klartext nahegelegt?

    Sollte dies der Fall gewesen sein, wie bewertet die Bundesregierung eine derartige Vorgabe?

31. Seit wann ist der Bundesregierung bzw. den zuständigen Stellen bekannt, dass aufgrund einer Mailumleitung auf den Privatrechner eines Zollmitarbeiters dienstliche Informationen für unbefugte Dritte zugänglich waren?

32. Für welchen Gesamtzeitraum kann nicht ausgeschlossen werden, dass Daten und Informationen dieser Stellen für den Zugriff unbefugter Dritter offenstanden?

33. Ist es zutreffend, dass aufgrund des genannten Falles eines Zollmitarbeiters, welcher eine Mailumleitung von seinem dienstlichen auf seinen privaten Rechner vorgenommen hatte, nunmehr einzelne Landeskriminalämter per Dienstanweisung entsprechende Mailumleitungen untersagt haben?

    Wenn ja, um welches LKA handelt es sich?

34. Sind entsprechende Mailumleitungen auch bei anderen polizeilichen Bundesbehörden technisch möglich?

    Welche Regelungen bestehen zu Mailumleitungen auf Bundesebene bei den betroffenen Behörden Bundeskriminalamt, Zoll und Bundespolizei?

35. Liegt nach Auffassung der Bundesregierung in den vorliegend geschilderten Sachverhalten vorwerfbares Fehlverhalten vor?

    Wer trägt, soweit die geschilderten Sicherheitslücken zutreffen sollten, die Verantwortung dafür, und welche Konsequenzen zieht die Bundesregierung aus diesen Vorgängen?

Berlin, den 24. August 2011

Renate Künast, Jürgen Trittin und Fraktion

Gesamtherstellung: H. Heenemann GmbH & Co., Buch- und Offsetdruckerei, Bessemerstraße 83–91, 12103 Berlin, www.heenemann-druck.de
Vertrieb: Bundesanzeiger Verlagsgesellschaft mbH, Postfach 10 05 34, 50445 Köln, Telefon (02 21) 97 66 83 40, Fax (02 21) 97 66 83 44, www.betrifft-gesetze.de
ISSN 0722-8333