

Kleine Anfrage

der Abgeordneten Gisela Piltz, Sabine Leutheusser-Schnarrenberger, Jörg van Essen, Dr. Max Stadler, Christian Ahrendt, Daniel Bahr (Münster), Uwe Barth, Rainer Brüderle, Angelika Brunkhorst, Ernst Burgbacher, Patrick Döring, Mechthild Dyckmans, Ulrike Flach, Otto Fricke, Horst Friedrich (Bayreuth), Dr. Edmund Peter Geisen, Hans-Michael Goldmann, Miriam Gruß, Joachim Günther (Plauen), Dr. Christel Happach-Kasan, Heinz-Peter Haustein, Elke Hoff, Birgit Homburger, Dr. Werner Hoyer, Michael Kauch, Gudrun Kopp, Jürgen Koppelin, Heinz Lanfermann, Sibylle Laurischk, Harald Leibrecht, Ina Lenke, Michael Link (Heilbronn), Markus Löning, Horst Meierhofer, Patrick Meinhardt, Burkhard Müller-Sönksen, Hans-Joachim Otto (Frankfurt), Detlef Parr, Cornelia Pieper, Jörg Rohde, Frank Schäffler, Marina Schuster, Dr. Hermann Otto Solms, Dr. Rainer Stinner, Carl-Ludwig Thiele, Christoph Waitz, Dr. Claudia Winterstein, Dr. Volker Wissing, Hartfrid Wolff (Rems-Murr), Martin Zeil, Dr. Guido Westerwelle und der Fraktion der FDP

Online-Durchsuchungen

Im Rahmen der Feststellung des Haushaltsplanes für das Haushaltsjahr 2007 wurde im Geschäftsbereich des Bundesministeriums des Innern das Programm zur Stärkung der Inneren Sicherheit (PSIS) mit der Mehrheit der Regierungskoalition von CDU, CSU und SPD beschlossen. Im Rahmen dieses Programms wurden Mittel vorgesehen, um Möglichkeiten zu entwickeln, „entfernte PCs“ auf „verfahrensrelevante Inhalte hin“ zu durchsuchen, „ohne tatsächlich am Standort des Geräts anwesend zu sein“.

Diese Vorgehensweise wurde als „Online-Durchsuchung“ bekannt. Der Bundesgerichtshof hat mit Beschluss vom 25. November 2006 festgestellt, dass für ein derartiges Vorgehen keine Rechtsgrundlage besteht.

Der Bundesminister des Innern, Dr. Wolfgang Schäuble, kündigte daraufhin in einer Pressemitteilung am 5. Februar 2007 an, nun eine Rechtsgrundlage für die Online-Durchsuchungen schaffen zu wollen. In einem Interview mit dem „Kölner Stadt-Anzeiger“ vom 8. Februar 2007, welches auch auf der Homepage des Bundesministeriums des Innern eingestellt ist, spricht er sich zudem dafür aus, die Online-Durchsuchungen sowohl der Polizei als auch dem Verfassungsschutz zu ermöglichen.

Wir fragen die Bundesregierung:

1. Werden die im PSIS vorgesehenen Forschungen und Entwicklungen zur Online-Durchsuchung aktuell weiterverfolgt?
2. Wenn nein, was geschieht mit den dafür vorgesehenen Mitteln, und wird der Plan, Online-Durchsuchungen zu erreichen, vollständig aufgegeben, bzw. wie soll dieser Plan unter der aktuellen Rechtslage weiterverfolgt werden?

3. Welche Planungen bestehen innerhalb des Bundesministeriums des Innern und innerhalb der Bundesregierung zur Schaffung einer Rechtsgrundlage für Online-Durchsuchungen?

4. Welche technische Lösung wird bzw. wurde bei der Online-Durchsuchung verfolgt?

Werden sich selbst installierende Programme entwickelt, um so genannte Schadsoftware bzw. Trojaner – in den Medien „Bundestrojaner“ genannt – in PCs einzuschleusen, und/oder werden Absprachen mit den Softwareherstellern angestrebt mit dem Ziel, dass diese gezielt Sicherheitslücken in ihrer Softwarearchitektur offenlassen, um den Ermittlungsbehörden den Zugriff auf die im Internet angeschlossenen PCs zu ermöglichen?

Welche Vor- und Nachteile sieht die Bundesregierung in den verschiedenen Möglichkeiten?

5. Wenn Sicherheitslücken in der Software für Online-Durchsuchungen genutzt werden sollen/sollten, wie will/wollte die Bundesregierung dem Problem begegnen, dass auch Kriminelle sich diese Lücken zunutze machen könnte und wie will/wollte die Bundesregierung dem Problem begegnen, dass Software international identisch ist und daher eine international einheitliche Sicherheitslücke angestrebt und mit allen anderen betroffenen Staaten abgesprochen werden müsste und daher auch fremde Geheimdienste und ggf. andere fremde Behörden Zugriff auf die in Deutschland befindliche an das Internet angeschlossenen PCs erhielten, und wie soll verhindert werden, dass beispielsweise auch eine von deutschen Behörden kryptografisch abgesicherte Software zur heimlichen Online-Durchsuchung von PCs Kriminellen, Terroristen und gegnerischen Geheimdiensten in die Hände fällt?

6. Wenn „Trojaner“ genutzt werden sollen/sollten, auf welchem Weg sollen/sollten diese auf den zu durchsuchenden Festplatten installiert werden: durch täuschungsbedingte Selbstinstallation durch den Benutzer der Festplatte und/oder soll physisch in die Räumlichkeiten bis zum PC vorgedrungen werden, um eine solche Software aufzuspielen, oder auf welche andere Weise?

7. Wenn „Trojaner“ genutzt werden sollen/sollten, wie soll/sollte dem Problem begegnet werden, dass Kriminelle einen erkannten „Bundestrojaner“ kopieren und benutzen, und wie soll/sollte dem Problem begegnet werden, dass die Softwareindustrie Antivirenprogramme und „Firewalls“ auf die Bedrohung durch diese „Trojaner“ hin entwickelt bzw. verbessert?

8. Sieht die Bundesregierung die Gefahr eines digitalen Wettrüstens, wenn Kriminelle einen „Bundestrojaner“ oder eine bewusste Sicherheitslücke in der Software entdecken und die Software daraufhin angepasst werden muss und neue „Bundestrojaner“ bzw. Sicherheitslücken geschaffen werden müssen, welche wiederum von Kriminellen entdeckt werden usw., und wie schätzt die Bundesregierung die Folgekosten eines solchen Wettrüstens ein?

9. Hält es die Bundesregierung für vereinbar, dem Bundesamt für Sicherheit in der Informationstechnik (BSI) auf der einen Seite die Aufgabe der technischen Prüfung der technologischen Sicherheit und Zuverlässigkeit und auf der anderen Seite die Aufgabe der Entwicklung von technischen Möglichkeiten zur Überwindung der technischen Sicherheitsarchitektur in der Informationstechnologie zuzuweisen?

Inwieweit sieht die Bundesregierung eine Gefahr, das Vertrauen in das BSI durch die Übertragung der Aufgabe der Entwicklung von technischen Möglichkeiten zur Online-Durchsuchung zu beschädigen?

10. Wie weit sind die Möglichkeiten der Ermittlungsbehörden des Bundes nach dem aktuellen technischen und wissenschaftlichen Stand der Computerforensik und auch im Hinblick auf den Ausbildungsstand der Mitarbeiter gegeben, auch gelöschte Daten auf Festplatten und die letzten Internetverbindungsdaten, welche sich auf der Festplatte befanden, wiederherzustellen?

11. Wie schätzt die Bundesregierung das Entwicklungspotential der Computerforensik in dieser Hinsicht ein?
12. Wo liegen nach Ansicht der Bundesregierung die Erkenntnis- und Beweisvorteile einer Online-Durchsuchung auf der einen Seite gegenüber einer Präsenzdurchsuchung mit Beschlagnahme der entsprechenden Datenträger und der Überwachung der elektronischen Post im Rahmen der Telekommunikationsüberwachung auf der anderen Seite?
13. Inwieweit können anhand der absehbaren Fortschritte in der Computerforensik in Zukunft im Nachgang einer Beschlagnahme von Datenträgern nach Einschätzung der Bundesregierung dieselben Daten beweisfähig gesichert werden, welche nach heutigem Erkenntnisstand nur bei einer Online-Durchsuchung beweissicher erlangt werden können?
14. Inwieweit handelt es sich nach Ansicht der Bundesregierung in dem Fall, dass über die Online-Durchsuchung mittels Auffinden entsprechender „Cookies“ oder auf andere Weise herausgefunden werden soll, ob jemand inkriminierte Online-Kommunikation getätigt hat oder ob anderweitige inkriminierte Daten auf der Festplatte vorhanden sind, von einer herkömmlichen Durchsuchung mit Beschlagnahme der Festplatte aber wegen dem warnenden Effekt bzw. der für einen Durchsuchungsbeschluss nicht ausreichenden Beweislage abgesehen wird, um Ermittlungen ohne konkreten Anfangsverdacht?
15. Sind diese Ermittlungen aus Sicht der Bundesregierung gerechtfertigt und/oder wünschenswert, und welche Anlassschwelle muss nach Ansicht der Bundesregierung für eine Online-Durchsuchung überschritten sein?
16. Wenn der Online-Zugriff auf die Festplatte erfolgreich ist, wie sollen/sollten die gesuchten Daten auf der Festplatte aufgefunden werden, und wie soll/sollte vermieden werden, dass dabei auch Daten aus dem geschützten höchstpersönlichen Lebensbereich des Benutzers der Festplatte erfasst werden?
17. Soweit bei der Erfassung der Daten während einer Online-Durchsuchung mit Schlagwörtern gearbeitet werden soll/sollte, wie soll/sollte dem Problem begegnet werden, dass nur Menschen, nicht aber Software eine „moralische“ – bzw. eine die rechtlich zutreffende Abwägung widerspiegelnde – Auswahl hinsichtlich der gesuchten und der – weil dem geschützten höchstpersönlichen Lebensbereich zugehörig – nicht zu erfassenden Daten treffen können?
18. Soweit nicht mit Schlagwörtern gearbeitet werden soll/sollte, welche intelligenten Filter sollen/sollten verwendet werden?
19. Inwieweit soll/sollte bei der Online-Durchsuchung vorher feststehen, dass sich der zu durchsuchende Datenträger in Deutschland befindet und damit der deutschen Rechtsordnung unterliegt?
Wie soll/sollten die Erkenntnisse über den Standort des Datenträgers erlangt werden?
20. Sollen/sollten Abkommen mit anderen Staaten getroffen werden, welche einen Eingriff in die Souveränität dieser Staaten bei der Online-Durchsuchung von in diesen Staaten befindlichen Datenträgern gestatten?
21. Wenn nein, wie soll/sollte dem Problem der Berührung fremder Staatssouveränität bei der Online-Durchsuchung von nicht körperlich in Deutschland befindlichen Datenträgern begegnet werden?
22. Sollen/Sollten die Staaten, in denen sich (wie es zur Verschleierung des Absenders durch mehrere zumeist in verschiedenen Staaten befindliche, jeweils mit einer neuen IP-Adresse im Internet auftretende Server gängige Methode ist) „zwischengeschaltete“ PCs befinden, bei einer Ermittlung des Absenders – also dem Nachverfolgen von IP-Adressen zum Auffinden des ursprünglichen Absender-PCs über in fremden Staaten befindliche Datenträger – informiert werden, wenn ja, auf welchem Weg, wenn nein, warum (im Hinblick auf die Feststellung der auf in diesem Staat befindlichen Datenträgern gespeicherten IP-Adressen und den damit verbundenen Eingriff in die Souveränität dieses fremden Staats) nicht?

23. Wie soll/sollte hinsichtlich der heimlichen Online-Durchsuchungen gewährleistet sein, dass staatliches Handeln für den Bürger überprüfbar bleibt, und welche – wie durchsetzbare – Rechtsposition soll/sollte dem Bürger gegenüber der heimlichen Online-Durchsuchung eingeräumt werden?
24. Wie hoch schätzt die Bundesregierung den Bedarf an zusätzlichen personellen Ressourcen für die Auswertung des durch die Online-Durchsuchungen gewonnenen Datenmaterials ein, und wie soll/sollte dieser Bedarf gedeckt werden?
25. Sieht die Bundesregierung die Gefahr von erheblichen Schäden, wenn Kriminelle die bewusste Sicherheitslücke in der Software bzw. den „Bundestrojaner“ nutzen, um an Betriebsgeheimnisse von Unternehmen zu gelangen, um die digitale Steuerung beispielsweise von Produktionsanlagen, Video- und Schließanlagen oder Tresoren zu beeinflussen oder sich auf andere Art und Weise auf Kosten von Unternehmen zu bereichern, und wie beurteilt die Bundesregierung die Gefahr von Regressforderungen gegen die Bundesrepublik Deutschland aufgrund solcher Vorgänge?
26. Wie beurteilt die Bundesregierung diese Frage im Hinblick auf drohende Wirtschaftsspionage durch ausländische Geheimdienste?
27. Wie bewertet die Bundesregierung insbesondere im Hinblick auf die vom Bundesverfassungsgericht entwickelten Grundsätze zum Schutz des Kernbereichs der privaten Lebensführung den mit jeder Online-Durchsuchung verbundenen Eingriff in die digitale Privatsphäre der Benutzer der an das Internet angeschlossenen Datenträger in Abwägung zu den Beweissicherungsinteressen?
28. Wie bewertet die Bundesregierung den mit der Online-Durchsuchung ggf. verbundenen Eingriff in die digitale Privatsphäre unbeteiligter Dritter bzw. die Gefahr des Eingriffs bei ggf. der ermittelnden Behörde unbekanntem Mitgewahrsam unbeteiligter Dritter an dem zu durchsuchenden Datenträger bzw. weiterer in einem Netzwerk angeschlossener PCs unbeteiligter Dritter?
29. Inwieweit sieht die Bundesregierung die Verhältnismäßigkeit im Sinne des Subsidiaritätsprinzips bei heimlichen Online-Durchsuchungen im Vergleich zu offenen Ermittlungsmaßnahmen und der Überwachung der Telekommunikation gewahrt?
30. Inwieweit erwägt/erwog die Bundesregierung mehrfach bei demselben Benutzer weitere und/oder denselben Datenträger zu durchsuchen, ohne diesen schon nach der ersten Durchsuchung zu unterrichten?
31. Welche Bedeutung misst die Bundesregierung in der Beurteilung der Eingriffsschwere dem Unterschied bei, dass bei einer akustischen Wohnraumüberwachung diese auf die Gespräche und damit die Kommunikation zwischen mehreren Menschen abzielt, während die heimliche Online-Durchsuchung nicht aktuelle Kommunikation, sondern vielmehr gespeicherte Daten wie beispielsweise auch persönliche Aufzeichnungen erfasst?

Berlin, den 20. März 2007

Dr. Guido Westerwelle und Fraktion