XXIV.GP.-NR
2657 /J
- 9. Juli 2009

Anfrage

der Abgeordneten Herbert, Mag. Stefan, Dr. Hübner
und weiterer Abgeordneter

an den Bundesminister für europäische und internationale Angelegenheiten
betreffend des Internetprojektes „Google Street View" und Datenübermittlung in die USA

In der Sitzung des Datenschutzrates vom 5. Juni 2009 wurde das Thema Google-Stree-View auf die Tagesordnung gesetzt. Ein Vertreter des Internetkonzernes war ebenfalls geladen worden, um über datenschutzrechtliche Fragen den Mitgliedern des Datenschutzrates Rede und Antwort zu stehen. Probleme wie das Recht auf Privatsphäre, das Recht auf das eigene Bild und der Schutz öffentlicher Einrichtung wurde behandelt. Bei der Frage wie das Verfahren aussieht, um Bilder von einem selbst oder von seinem Grundstück oder Haus sowie Wohnung löschen lassen zu können, wurde vom Vertreter des Konzernes darauf hingewiesen, dass man nur eine Mail mit den entsprechenden Daten an Google-Konzern in den USA schicken brauche. Von dort aus wird die „Löschung" (das Bild wird nur vom Netz genommen) veranlasst.
Das Verfahren für die Versendung der Bilddaten wurde wie folgt vom Vertreter von Google beschrieben:

- Alle Aufnahmen werden auf Festplatten gespeichert
- Diese Festplatten werden in eigene Behältnisse verpackt
- Die Behältnisse werden schließlich in die USA verbracht
- In der USA wird von Google die Speicherung und Verwendung der Aufnahmen vorgenommen

Dieses Verfahren würde deshalb verwendet werden, da die Datenmenge viel zu hoch wäre, um sie über E-Mail bewältigen zu können. Die Begründung ist einleuchtend, steht aber in Konflikt mit den österreichischen Datenschutzbestimmungen.

Die Homeland Security ist die Oberste Behörde bei den Zollbehörden der USA. Eine staatliche Organisation, die sich um Datenschutzbestimmungen, die in den USA nicht so ausgeprägt sind wie in den EU-Mitgliedsstaaten, kein Sorgen machen braucht.
In einem Merkblatt (siehe Anlage) für Dienstreisende in das außereuropäische Ausland der Max-Planck-Gesellschaft wird folgendes vermerkt:
„(...) Zwei US-Behörden, die Aufgaben des Grenzschutzes und der Zollkontrolle wahrnehmen und beide dem US Department of Homeland Security unterstehen, dürfen seit dem 16.07.2008 ohne konkreten Anlass mobile Datenträger von jeder Person, die in die USA einreisen, auszureisen oder durchreisen möchte, durchsuchen. Laut den entsprechenden Richtlinien dürfen die Beamten Daten bzw. Kopien der Daten zur Überprüfung einbehalten. Eine Verschlüsselung der Daten bzw. der Datenträger, um diese vor einer potentiellen Auswertung zu schützen, ist nur bedingt hilfreich. Zwar ist es generell erlaubt, Verschlüsselungssoftware bei Einreise in die USA mit sich zu führen, die US-Behörden haben jedoch das Recht, die erlangten Daten an andere Regierungs- oder private Stellen zur Entschlüsselung weiterzuleiten. (...)"

Weiteres siehe Merkblatt:

HBRP

MAX-PLANCK-GESELLSCHAFT

Datenschutz und IT-Sicherheit

Merkblatt für Dienstreisende in das außereuropäische Ausland

Dieses Merkblatt soll Sie darüber aufklären, was zu beachten ist, wenn Sie sich auf eine Dienstreise in das außereuropäische Ausland begeben und einen oder mehrere mobile Datenträger bei sich führen.

Unter mobilen Datenträgern versteht man alle elektronischen Geräte, die flexibel und ortsungebunden einsetzbar sind und als Datenspeicher dienen. Beispiele hierfür sind: Notebook, Smartphone, PDA, Mobiltelefon, MP3-Player, CD-Rom, DVD, externe Festplatten, USB-Stick, Digitalkamera etc..

Bei Reisen in das außereuropäische Ausland – insbesondere in sicherheitskritische Staaten, wie China und Russland, aber auch in die USA – müssen Sie mit folgenden Einschränkungen rechnen.

DURCHSUCHUNG UND AUSWERTUNG MOBILER DATENTRÄGER

Zwei US-Behörden, die Aufgaben des Grenzschutzes und der Zollkontrolle wahrnehmen und beide dem US Department of Homeland Security unterstehen, dürfen seit dem 16.07.2008 ohne konkreten Anlass mobile Datenträger von jeder Person, die in die USA einreisen, auszureisen oder durchreisen möchte, durchsuchen. Laut den entsprechenden Richtlinien dürfen die Beamten Daten bzw. Kopien der Daten zur Überprüfung einbehalten.

Eine Verschlüsselung der Daten bzw. der Datenträger, um diese vor einer potentiellen Auswertung zu schützen, ist nur bedingt hilfreich. Zwar ist es generell erlaubt, Verschlüsselungssoftware bei Einreise in die USA mit sich zu führen, die US-Behörden haben jedoch das Recht, die erlangten Daten an andere Regierungs- oder private Stellen zur Entschlüsselung weiterzuleiten.

Entsprechende Regularien gibt es auch in anderen Ländern. So haben z.B. Indien und Australien Gesetze, die eine Pflicht des Inhabers zur Entschlüsselung seiner Daten statuieren.

EINFUHRVERBOTE FÜR VERSCHLÜSSELUNGS-SOFTWARE

Etliche Länder, wie z.B. China, Russland, Kasachstan, Ukraine oder Weißrussland sehen Einfuhrbeschränkungen für Verschlüsselungs-Software vor. Verschlüsselungs-Software darf nur eingeführt werden, wenn eine entsprechende Lizenz des jeweiligen Staates vorliegt. Derartige Bestimmungen kommen damit einem Einfuhrverbot für in westlichen Ländern üblicherweise eingesetzte Verschlüsselungs-Software gleich.

Diese Beschränkungen bzw. Verbote gelten bereits für das bloße Vorhandensein von derartiger Software auf Datenträgern. Es ist nicht notwendig, dass die Software an Dritte weitergegeben wird.

Lediglich ausgenommen ist solche Software, die als „Nebenfunktion" eine Verschlüsselungskomponente enthält, wie z.B. Webbrowser (diese können verschlüsselte Verbindungen zu Webseiten aufbauen) oder Mobiltelefone (diese verschlüsseln typisch die Kommunikation auf Funkstrecke).

Wird gegen Einfuhrverbote verstoßen, so muss mit Konsequenzen wie Beschlagnahme des Datenträgers, Einreiseverbot bis hin zur persönlichen Konfrontation mit den jeweiligen Behörden gerechnet werden.

EMPFEHLUNGEN

Vor Dienstreisen in das außereuropäische Ausland, insbesondere in oben erwähnte Staaten sollten Sie folgende Punkte beachten.

1. Führen Sie weder private Daten noch private mobile Datenträger mit sich.
2. Nehmen Sie nicht Ihre üblichen Arbeitsgeräte mit, sondern lassen Sie sich von Ihrer EDV-Abteilung ein neu vorkonfiguriertes Gerät geben.
3. Installieren Sie keine zusätzliche Software, insbesondere keine Verschlüsselungs-Software.
4. Nehmen Sie nur diejenigen Daten mit, die Sie unbedingt benötigen und bei denen eine Kenntnisnahme durch ausländische staatliche Stellen nicht zur negativen Konsequenzen für die MPG führen kann.
5. Vertrauliche und sensible Daten sollten auf einem Server der MPG oder in einem Web-Mail-Account ihres Instituts gespeichert werden, der verschlüsselt via Webbrowser per https über das Netz abrufbar ist.
6. Lassen Sie Ihre mobilen Geräte nicht unbeaufsichtigt. Dies gilt auch für Hotelzimmer und Konferenzräume. Auch Safes in Hotels bieten hier keine Sicherheit.
7. Melden Sie etwaige Kontrollen unmittelbar nach Ihrer Rückkehr Ihrer Institutsleitung.
8. Übergeben Sie die mobilen Geräte – unabhängig von etwaigen Kontrollen – Ihrer EDV-Abteilung, damit die Geräte untersucht und ggfs. neu konfiguriert werden können.

Für weitere Fragen wenden Sie sich bitte an den IT-Sicherheitsbeauftragten der Max-Planck-Gesellschaft, it-sicherheit@mpg.de, Tel. 089-2108-1317.

Vor diesem Hintergrund richten die unterfertigten Abgeordneten an den Bundesminister für europäische und internationale Angelegenheiten nachstehende

Anfrage:

1. Ist Ihnen der Umstand bekannt, dass zwei US-Behörden, die Aufgaben des Grenzschutzes und der Zollkontrolle wahrnehmen und beide dem US Department of Homeland Security unterstehen, seit dem 16.07.2008 ohne konkreten Anlass mobile Datenträger von jeder Person, die in die USA einreisen, ausreisen oder durchreisen möchte, durchsuchen und kopieren dürfen?

2. Wenn „Ja", warum ist es auf Ihrer Homepage nicht ersichtlich?

3. Haben Sie für österreichische Unternehmer, die ihre Mitarbeiter in die USA entsenden, eine Informationsplattform?

4. Wenn nein, wo können sich diese Unternehmer und ihre Mitarbeiter informieren?

5. Können Sie den Österreichern garantieren, dass ihre Daten, die an den Google-Konzern geschickt werden, nicht von der Homeland Security kopiert werden?

6. Wenn „Nein", welche rechtlichen oder politischen oder auch diplomatischen Schritte können Sie einleiten, um solche kopierten Daten auch löschen lassen zu können?

7. Stehen Sie dahingehend schon mit den zuständigen Behörden oder mit den politischen Verantwortungsträgern in den USA in Verbindung?

8. Gibt es für solche Fälle, und andere Fälle der Datenkopie durch die Homeland-Security, ein bilaterales Abkommen mit den USA?

9. Gibt es dafür ein multilaterales Abkommen?

10. Gibt es für solche Fälle der Datenkopie ein Abkommen mit den USA und der EU und ihren Mitgliedsstaaten?

11. Wenn es solche Abkommen nicht gibt, haben österreichische Staatsbürger die Möglichkeit eine Löschung von sichergestellten Daten durch die amerikanischen Behörden auf anderen Wegen einzufordern?

12. Wenn „nein", warum nicht?

13. An wen können sich österreichische Staatsbürger wenden, falls Sie vermuten, dass Daten von ihnen und Daten über sie von der Homeland-Security kopiert wurden?

HBRP

14. Was für rechtliche Möglichkeiten haben österreichische Staatsbürger, um eine Löschung von Daten, die von Google gespeichert werden und/oder von der Homeland-Security kopiert wurden, durchzusetzen?

15. An wen können sich österreichische Staatsbürger wenden, wenn sie erkennen müssen, dass diese gespeicherten bzw. die kopierten Daten dennoch verwendet werden?

16. Wie kann die österreichische Botschaft und wie können auch Sie den geschädigten Staatsbürgern helfen?

17. Haben sich schon österreichische Staatsbürger bei österreichischen Vertretungsbehörden in den USA bezüglich des Kopierens von Daten, die auf mobilen Datenträgern gespeichert waren, und der Sicherstellung von Datenträgern durch die US-Behörden beschwert?

18. Wie konnten Sie oder die österreichischen Vertretungsbehörden helfen?

19. Wenn Sie und die österreichischen Vertretungsbehörden nicht helfen konnten, warum nicht?

Wien am 8. JULI 2009

HBRP