



REPUBLIK ÖSTERREICH  
BUNDESMINISTERIN FÜR INNERES

Frau  
Präsidentin des Nationalrates  
Mag.<sup>a</sup> Barbara Prammer  
Parlament  
1017 Wien

MAG.<sup>a</sup> JOHANNA MIKL-LEITNER  
HERRENGASSE 7  
1014 WIEN  
POSTFACH 100  
TEL +43-1 53126-2352  
FAX +43-1 53126-2191  
ministerbuero@bmi.gv.at

GZ: BMI-LR2220/0992-II/2013

Wien, am 16. Jänner 2014

Die Abgeordneten zum Nationalrat Mag. Stefan, Vilimsky und weitere Abgeordnete haben am 20. November 2013 unter der Zahl 46/J an mich eine schriftliche parlamentarische Anfrage betreffend „Schaden für die österreichische Wirtschaft durch Spionage“ gerichtet.

Diese Anfrage beantworte ich nach den mir vorliegenden Informationen wie folgt:

**Zu den Fragen 1 und 2:**

Es liegen keine konkreten Zahlen vor. Die im Jahr 2010 durchgeführte Studie, datiert mit 16. November 2010, zur Betroffenheit der österreichischen Unternehmen von Wirtschafts- und Industriespionage lieferte erstmals Zahlen bezüglich Schadenshöhe, Betroffenheit, Täterprofile, Bekanntheitsgrad der zuständigen Behörden, etc. Diese Studie wurde auch auf der Homepage des Bundesministeriums für Inneres veröffentlicht ([http://www.bmi.gv.at/cms/BMI\\_Verfassungsschutz/wis/start.aspx](http://www.bmi.gv.at/cms/BMI_Verfassungsschutz/wis/start.aspx)).

**Zur Frage 3:**

Meinungen und Einschätzungen sind nicht Gegenstand des parlamentarischen Interpellationsrechtes.

**Zu den Fragen 4 bis 6:**

Auf Basis der im Frühjahr 2013 von der österreichischen Bundesregierung verabschiedeten Cyber-Sicherheitsstrategie werden derzeit interministeriell Maßnahmen getroffen, um erkannte Defizite ausgleichen zu können.

Derzeit laufen intensive Planungs- und Umsetzungsbemühungen für die Einrichtung eines bundesweit zentralen „Cyber Security Incident Coordination Centers“ samt allen dazu gehörenden Teilbereichen, wie beispielsweise

- Einrichtung sektor- bzw. bereichsspezifischer Meldestellen,
- Schaffung eines zentralen Koordinationszentrums für operative Leistungen im Schadensfall,
- Implementierung und Betrieb eines (Echtzeit-)Lagezentrums,
- Beschreibung und Implementierung eines Cyber-Krisenbewältigungs-Management-Prozesses einschließlich aller dazu gehörenden funktionalen Einrichtungen,
- Bereitstellung und Betrieb einer sicheren Kommunikations- und Meldeplattform.

**Zu den Fragen 7 und 8:**

Zu der Frage der Schaffung sicherer europäischer Kommunikationsinfrastrukturen sind keine konkreten Vorschläge auf EU-Ebene bekannt. Betreffend die Meldeverpflichtung in Bezug auf Cyber-Vorfälle wird auf EU-Ebene derzeit im Rahmen der Verhandlungen über einen Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über Maßnahmen zur Gewährleistung einer hohen gemeinsamen Netz- und Informationssicherheit in der Union („NIS-Richtlinie“) beraten. Der Vorschlag über die „NIS-Richtlinie“ sieht eine Meldeverpflichtung von Cyber-Sicherheitsvorfällen vor. Österreich unterstützt die Meldepflicht von Betreibern kritischer Infrastrukturen bei schweren Cyber-Vorfällen.

