BM.I REPUBLIK ÖSTERREICH
BUNDESMINISTERIN FÜR INNERES

XXIV. GP.-NR
14324 /AB
26. Juni 2013
zu 14568 /J

Frau
Präsidentin des Nationalrates
Mag.ª Barbara Prammer
Parlament
1017 Wien

MAG.ª 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-LR2220/0466-IV/8/2013

Wien, am 4. Juni 2013

Der Abgeordnete zum Nationalrat Vilimsky und weitere Abgeordnete haben am 26. April 2013 unter der Zahl 14568/J an mich eine schriftliche parlamentarische Anfrage betreffend „Datenleck BMI" gerichtet.

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

Zu den Fragen 1 und 2:

Die IKT-Sicherheitsstrukturen wurden nicht kompromittiert, sondern die Benutzerkennung eines BM.I-Mitarbeiters ausspioniert. Mit dieser Benutzerkennung erfolgte ein unrechtmäßiger Zugriff auf die Informationen seines Postfachs.

Zu Frage 3:

Seitens des BM.I wird versucht nach dem Stand der Technik die ressortinternen Daten zu schützen und es ist kein Umstand bekannt, dass die IKT-Sicherheitsstrukturen ihre Aufgabe nicht erfüllen. Der Umstand, dass ein Benutzeraccount kompromittiert wurde ist Gegenstand von Ermittlungen des Bundesamts für Verfassungsschutz und Terrorismusbekämpfung. Das Ausspähen eines Benutzeraccounts mit einer unzureichenden Absicherung von Unternehmensdaten gleichzusetzen stellt keinen folgerichtigen Schluss dar.

Zu Frage 4:

Es handelt sich bei diesen technischen Informationen um schutzwürdige Daten für die unternehmensinterne Kommunikation. Erst durch das unrechtmäßige Ausspähen einer

Benutzerkennung und dem Zugriff auf ein ebenso schutzwürdiges Postfach eines Mitarbeiters der IKT-Abteilung wurden diese Informationen kompromittiert.

Zu Frage 5:

Bei den Informationen handelt es sich um übliche Kommunikationsinhalte eines IKT-Mitarbeiters in der unternehmensinternen Kommunikation.

Zu den Fragen 6 und 7:

In der internen Kommunikation des Ressorts ist es unvermeidbar zur Erfüllung einer Aufgabe Informationen zwischen Speziallisten auszutauschen. Aus gegebenem Anlass erfolgte eine Sensibilisierung der Mitarbeiter und es wurden für derartige Informationsübermittlungen weitergehende organisatorische und technische Vorsorgen getroffen.

Zu Frage 8:

Wir bemühen uns im BM.I die IKT-Sicherheit permanent auf dem Stand der Technik zu halten, um den hohen Sicherheitsanforderungen gerecht zu werden. Dafür ist es notwendig, neben laufender technischer Adaptionen und Investitionen in die IKT-Sicherheitsstrukturen wiederkehrende organisatorische Maßnahmen (Schulungen, Awarenessmaßnahmen etc.) zu setzen.