

NIKOLAUS BERLAKOVICH  
Bundesminister



Lebensministerium

An die  
Frau Präsidentin  
des Nationalrates  
Mag.<sup>a</sup> Barbara Prammer

Parlament  
1017 Wien

XXIV.GP.-NR  
634 /AB

11. März 2009

zu 637 /J

ZI. LE.4.2.4/0004 -I 3/2009

Wien, am 10. MRZ. 2009

Gegenstand: Schriftl. parl. Anfr. d. Abg. z. NR Karl Öllinger, Kolleginnen und Kollegen vom 15. Jänner 2009, Nr. 637/J, betreffend Datenverluste und Datensicherheit 2008

Auf die schriftliche parlamentarische Anfrage der Abgeordneten Karl Öllinger, Kolleginnen und Kollegen vom 15. Jänner 2009, Nr. 637/J, teile ich Folgendes mit:

Zu Frage 1:

Im Jahr 2008 wurden in der Zentralstelle bzw. den nachgeordneten Dienststellen des Bundesministeriums für Land- und Forstwirtschaft, Umwelt und Wasserwirtschaft (BMLFUW) 3.293 stationäre Computer eingesetzt.

Zu Frage 2:

Im Jahr 2008 wurden in der Zentralstelle bzw. den nachgeordneten Dienststellen des BMLFUW 673 tragbare Computer eingesetzt.

Zu Frage 3:

Im Jahr 2008 wurden in der Zentralstelle bzw. den nachgeordneten Dienststellen des BMLFUW 935 Handys (Mobilfunkgeräte) eingesetzt.



Zu Frage 4:

Im Jahr 2008 wurden in der Zentralstelle bzw. den nachgeordneten Dienststellen des BMLFUW 42 dienstliche Taschencomputer eingesetzt.

Zu Frage 5:

- a) Es wurden zwei der unter 1) bis 4) abgefragten Geräte als unauffindbar gemeldet.
- b) Es wurde 1 Notebook in einer nachgeordneten Dienststelle als gestohlen gemeldet. Weiters wurden 4 Mobilfunktelefone als gestohlen gemeldet.

Zu Frage 6:

Es wurden in allen Fällen polizeiliche Anzeigen erstattet. Bei den Mobilfunkgeräten wurde die SIM-Karte gleichzeitig inaktiv geschaltet.

Zu Frage 7:

Es wurden 4 Memory-Sticks als unauffindbar gemeldet.

Zu Frage 8:

Auf diesen Trägern befanden sich dienstliche Daten der jeweiligen Tätigkeit des Nutzers.

Zu Frage 9:

Es befanden sich keine geheimen bzw. vertraulichen Daten im Sinne des Informationssicherheitsgesetzes auf den abgefragten Geräten bzw. Datenträgern.

Zu Frage 10:

Der Sachwert der als gestohlen gemeldeten Geräte beträgt € 914,40.

Zu Frage 11:

Es wurden keine Zugriffe von Geräten, die als gestohlen oder unauffindbar gemeldet wurden, protokolliert.

Zu Frage 12:

Die Erfassung erfolgt zentral durch die inventarisierende Stelle.

Zu Frage 13:

Der Schutz erfolgt durch jeweils geeignete technische und organisatorische Sicherheitsmaßnahmen.

Zu Frage 14:

In der Zentralstelle bzw. den nachgeordneten Dienststellen des BMLFUW gab es im Jahr 2008 bei den unter 1) bis 4) genannten Geräten mehrmals „Virenalarm“, jedoch wurden nur 3 Computer im Bereich der Verwaltung und ca. 50 Computer im Bereich der Pädagogik verseucht. Durch den Einsatz geeigneter Tools (Viren- und Malwarescanner) wurden die Geräte gesäubert bzw. konnten diese Gefahren erfolgreich abgewehrt und somit ein Eindringen in die Systeme verhindert werden.

Derartige Ereignisse werden sowohl im Bereich der Zentraleitung als auch in den nachgeordneten Dienststellen protokolliert.

Zu Frage 15:Richtlinien/Erlässe/VorkehrungenRichtlinien:

- Österreichisches Informationssicherheitshandbuch
- IKT-Interne Richtlinie für „Backup und Archivierung“
- IKT-Interne Richtlinie für die „Verbringung von Datenträgern“
- WLAN-Richtlinie
- Ressortweite Benutzerrichtlinie für Computerarbeitsplätze im BMLFUW für die Nutzung von internen/externen Netzen und Diensten sowie E-Mail.

Erlass:

- Ressortweite Datensicherheitsvorschrift (Seit April 2007)

Sonstige Vorkehrungen innerhalb der IKT:

- Security Policy der IKT-Abteilung
- Backup und Sicherung aller relevanten Daten und Informationen
- Auslagerung der Sicherungsbänder
- Verschlüsselung von Daten auf Datenträgern (Notebooks, USB-Sticks)
- Absicherung mobiler Geräte und Datenträger mittels Pin und Passwort
- Awareness-Schulungen der Mitarbeiter und Mitarbeiterinnen
- Sicherheitsteam innerhalb der IKT für Störfälle

Für die nachgeordneten Dienststellen gelten die Ressortvorgaben betreffend "Datensicherheitsvorschrift und Benutzerrichtlinie" und "WLAN-Richtlinie", darüber hinausgehend gibt es bei den Dienststellen den Gegebenheiten entsprechend individuelle Vorschriften basierend auf dem „Österreichischen Informationssicherheits-Handbuch“.

Zu Frage 16:

Zusätzliche Vorkehrungen sind:

- Sicheres Löschen von Datenträgern nach DOD 5220
- mechanische und thermische Vernichtung von Datenträgern

Zu Frage 17:

Geplant sind vermehrt personenbezogene Zuteilung von elektronischen Geräten und Datenträgern sowie die Übertragung der persönlichen Verantwortung im Rahmen der Übernahme. Darüber hinaus wird laufend beobachtet, welche Entwicklungen bzw. Verbesserungen sich am Sicherheitssektor ergeben.

Der Bundesminister:

