REPUBLIK ÖSTERREICH

Die Bundesministerin
für auswärtige Angelegenheiten

Dr. Benita Ferrero-Waldner

XXII. GP.-NR
302/AB
2003 -05- 30
zu 284 /J

Herrn Präsidenten
des Nationalrates
Univ.-Prof. Dr. Andreas KHOL
Parlament
1017 Wien

27. Mai 2003

GZ 850.00.18/3e-I.9/2003

Die Abgeordneten zum Nationalrat Mag. Johann Maier, Kolleginnen und Kollegen, haben am 2. April 2003 unter der Nummer 284/J-NR/2003 eine schriftliche parlamentarische Anfrage betreffend Datensicherheitsmaßnahmen im Zusammenhang mit der Verwendung von Microsoft-Produkten – Schutz von personenbezogenen Daten und anderer sensibler oder geheimer Daten an mich gerichtet.

Diese Anfrage beantworte ich wie folgt:

Zu den Fragen 1 und 2:

In den Meldungen der im Wirkungsbereich des Bundesministeriums für auswärtige Angelegenheiten durchgeführten Datenverarbeitungen an das Datenverarbeitungsregister sind die verarbeiteten Datenarten einzeln aufgezählt. Die im Ressort verarbeiteten sensiblen Daten sind somit den öffentlich und für jedermann zugänglichen Registrierungen im Datenverarbeitungsregister zu entnehmen, das eben zu diesem Einsichtszweck geführt wird. In der jeweiligen Registrierung ist auch angegeben, an welche Übermittlungsempfänger die einzelnen Datenarten übermittelt werden bzw. werden dürfen.

Zu Frage 3:

Die für IT-Security im Bund zuständige IKT-Stabsstelle ist im permanenten Dialog mit Microsoft. Der „Beginn eines Government Security Programs" mit Microsoft ist daher nicht erforderlich.

Zu Frage 4:

Fragen der IT-Security werden für den Bund im IKT-Board, dem alle Bundesministerien angehören, gemeinsam behandelt.

Zu den Fragen 5 und 6:

Die für IT-Security zuständigen Stellen des Bundes haben den im Rahmen des Bedarfes der Bundesverwaltung notwendigen mittelbaren Zugriff auf die Quellcodes des Betriebssystems Microsoft Windows.

Zu Frage 7:

Das Bundesministerium für auswärtige Angelegenheiten sieht die gemäß Datenschutzgesetz 2000 erforderlichen Maßnahmen vor.

Zu den Fragen 8 und 9:

Bei Daten, die in bestimmten Verarbeitungen mit sehr hohem Geheimhaltungsgrad enthalten sind, ist die verschlüsselte Speicherung vorgesehen. Eine verschlüsselte Übermittlung von Daten in offenen Netzen erfolgt dann, wenn dies aufgrund einer Vereinbarung zwischen den Kommunikationspartnern möglich ist.

Zu Frage 10:

Ja.

Zu den Fragen 11 und 12:

Diese Fragen können aus verwaltungsökonomischen Gründen nicht beantwortet werden.

Zu den Fragen 13 bis 16:

Nein.

Zu Frage 17:

Windows NT 4.0
Windows 2000 Server 5.0
Microsoft Windows Internet Explorer 5.5
SMS
Microsoft Visual Studio Common\IDE\IDE98 Microfot
Entwicklungsumgebung 6.0 Windows Media Player
Windows 2000 Server
Windows Scripting Host (SSH)
Exchange 5.5
Exchange 2000
Active Directory Connector (ADC)
Proxy
System Management Server (SMS)
DNS
DHCP
DFS
Internet Information Server (IIS)
Terminal Service
Windows 2000 Professional

Windows 2000 Professional Multi-Language User Interface (MUI)
Office 2000 Standard
Office 2000 Multi-Language User Interface (MUI)
Agent
SMS
Active Sync.

Zu Frage 18:

Durch eine entsprechende Netzwerkabsicherung (Firewalls u.a.) kann ausgeschlossen werden, dass die Daten an Microsoft übertragen werden.

Zu Frage 19:

Ja.

Zu Frage 20:

Im e-Government-Projekt der Bundesregierung ist die Einhaltung höchster Datensicherheit ein durchgehendes und vorrangiges Prinzip.