



DER BUNDESMINISTER
FÜR JUSTIZ

XXII. GP.-NR

281 /AB

2003 -05- 26

7020/1-Pr 1/2003

zu 288 /J

An den

Herrn Präsidenten des Nationalrates

W i e n

zur Zahl 288/J-NR/2003

Die Abgeordneten zum Nationalrat Mag. Johann Maier, Kolleginnen und Kollegen haben an mich eine schriftliche Anfrage betreffend „Datensicherheitsmaßnahmen im Zusammenhang mit der Verwendung von Microsoft-Produkten – Schutz von personenbezogenen Daten und anderer sensibler oder geheimer Daten, über die Bundesbehörden verfügen“ gerichtet.

Ich beantworte diese Anfrage wie folgt:

Zu 1 und 2:

Die vom Bundesministerium für Justiz ermittelten und mithilfe der EDV verarbeiteten und/oder gespeicherten, personenbezogenen Daten sind in den Meldungen an das Datenverarbeitungsregister enthalten. Darin sind die verarbeiteten Datenarten einzeln aufgezählt. Die im Ressort verarbeiteten sensiblen Daten sind den öffentlich und für jedermann zugänglichen Registrierungen im Datenverarbeitungsregister zu entnehmen, das zu diesem Einsichtszweck geführt wird. In der jeweiligen Registrierung ist auch die Rechtsgrundlage ersichtlich und angeführt, an welche Übermittlungsempfänger die einzelnen Datenarten übermittelt werden bzw. werden dürfen.

Zu 3 und 4:

Dieses Programm ist dem Bundesministerium für Justiz nicht bekannt.

Zu 5 und 6:

Das Bundesministerium für Justiz hat keinen „kontrollierten Zugriff“ auf den Quellcode des Betriebssystems von Microsoft Windows.

Zu 7:

Die Justiz sichert jeden Rechner mittels Benutzerkennung und Passwort ab. Es ist nicht möglich, von außen auf die Rechner der Justiz zuzugreifen. Was die Datenübermittlung via E-Mail betrifft, so ist das hiefür eingesetzte Lotus Notes in der Lage, E-Mail zu verschlüsseln und zu signieren. Die Justiz setzt sowohl eine sog. „Firewall“ ein, die Attacken von außen abwehrt, als auch VirensScanner, die sowohl am Server als auch auf den Arbeitsplatz-PCs kontinuierlich Virenkontrollen durchführen. Sämtliche Daten werden - soweit sie auf dem Server gespeichert wurden - regelmäßig auf Bänder gesichert. Schließlich haben die Benutzer nur beschränkte Zugriffsrechte innerhalb des Netzwerks.

Zu 8:

Daten werden grundsätzlich nicht verschlüsselt, weil sich die interne Datenübermittlung in einem nach außen vollkommen abgeschlossenen Netzwerk bewegt.

Zu 9:

Die Verschlüsselung des E-Mail-Verkehrs liegt im Ermessen des Benutzers.

Zu 10 bis 12:

Die Zusammenarbeit mit ausländischen Behörden erfolgt grundsätzlich auf konventionellem Weg. In Auslieferungssachen werden mit der Mehrzahl der EU-Staaten Informationen über ein besonders gesichertes Telefaxgerät übermittelt, das eine Verschlüsselung von Daten ermöglicht.

Ausländischen Behörden stehen – wie jedermann – die öffentlich zugänglichen Daten aus Grund- und Firmenbuch sowie der Ediktsdatei zur Verfügung.

Zu 13 bis 16:

Diese Einrichtung ist dem Bundesministerium für Justiz nicht näher bekannt.

Zu 17:

Die Justiz setzt derzeit das Betriebssystem Windows NT ein und auf einem verhältnismäßig geringen Anteil der Arbeitsplatz-PCs Microsoft Office. Im Strafvollzug wird überdies in jeder Justizanstalt für das sogenannte Notsystem ein SQL-Server eingesetzt. Es ist beabsichtigt im Laufe des Jahres 2004 auf das Betriebssystem Windows 2000 zu migrieren.

Zu 18 und 19:

So weit mir bekannt ist, gibt es keine unbeabsichtigte Datenübertragung von den im Justizressort eingesetzten Microsoft Produkten zu Microsoft. Microsoft Windows XP wird in der Justiz nicht eingesetzt.

Zu 20:

Durch die enge Beziehung zur BundesrechenzentrumGmbH ist das Bundesministerium für Justiz in alle deren Sicherheitsmaßnahmen indirekt eingebunden.

26. Mai 2003

(Dr. Dieter Böhmdorfer)