299/AB XXII. GP

Eingelangt am 30.05.2003

Anfragebeantwortung

BM FÜR LANDESVERTEIDIGUNG

Die Abgeordneten zum Nationalrat Mag. Maier, Genossinnen und Genossen haben am 2. April 2003 unter der Nr. 289/J an mich eine schriftliche parlamentarische 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. Diese Anfrage beantworte ich wie folgt:

Zu l und 2:

Das Bundesministerium für Landesverteidigung ermittelt, verarbeitet und speichert in seinem Wirkungsbereich Daten von Dienstnehmern und Wehrpflichtigen. In den Meldungen dieser Datenverarbeitungen an das Datenverarbeitungsregister sind die verarbeiteten Datenarten einzeln aufgezählt. Die 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 3:

Die für IT-Sicherheit im Bund zuständige IKT-Stabsstelle (IKT-Board), der alle Bundesministerien angehören, steht in permanentem Kontakt mit Microsoft. Der „Beginn eines Government Security Program" ist daher nicht erforderlich.

Zu 4:

Fragen der IT-Sicherheit werden für den Bund im IKT-Board gemeinsam behandelt. Im Zuständigkeitsbereich des Bundesministeriums für Landesverteidigung, in dem Sicherheitsaspekte besondere Bedeutung haben, wird das seit Jahren bestehende Sicherheitskonzept weiterhin umgesetzt.

Zu 5:

Nein, ein derartiger Bedarf hat sich auf Grund der beim Bundesministerium für Landesverteidigung bestehenden Sicherheitsarchitektur (physikalische Trennung des internen Netzes von allen anderen Netzen) bisher nicht gestellt.

Zu 6:

Entfällt.

Zu 7:

Datenzugriffe sind nur durch berechtigte Personen mit definierten Benutzerprofilen möglich. Die Zugriffe werden durch ein Chipkarten-Sicherheitssystem gesteuert und protokolliert. Externe Zugriffe sind infolge der physikalischen Trennung der Netze nicht möglich.

Zu 8 und 9:

Es werden alle Daten, die von den Benutzern in dafür definierten Verzeichnissen abgelegt werden, sowie alle Datenübermittlungen, die über eine einzelne Liegenschaft hinausgehen (WAN), verschlüsselt. Bei den - mit dem ressortinternen Netz nicht verbundenen - Stand Alone-Geräten (insbesondere E-Mail-Anschlüsse) obliegt die Verschlüsselung den Anwendern.

Zu 10 bis 12:

Kontakte mit ausländischen Behörden, in deren Rahmen Daten angefragt werden, bestehen selbstverständlich, soweit dafür rechtliche Grundlagen vorliegen. Eine detaillierte Auflistung im Sinne der Fragestellung kann aus verwaltungsökonomischen Gründen bzw. aus Gründen der militärischen Geheimhaltung nicht bekannt gegeben werden. Ich bitte daher

um Verständnis, dass ich von einer detaillierten Beantwortung dieser Fragen Abstand nehme.

Zu 13:

Nein.

Zu 14 bis 16:

Entfällt.

Zu 17:

Neben dem Betriebssystem Windows (hauptsächlich NT, in Einzelfällen auch 2000 bzw. XP pro) werden vor allem die Produkte Office XP sowie auch Visio, Project, VisualStudio, Exchange, WindowsServer, SQL-Server, Frontpage und Autoroute eingesetzt.

Zu 18:

Das Bundesministerium für Landesverteidigung verwendet sog. Corporate-Versionen der Programme, für die eine Registrierung über Telefon oder Internet nicht erforderlich ist. Durch die physikalische Trennung des internen IT-Netzes sind Übertragungen von Daten nicht möglich. Im Bereich der - nicht mit dem internen Netz verbundenen - Stand Alone-Geräte ist die Speicherung von personenbezogenen Daten nicht vorgesehen.

Zu 19:

Ja, ein derartiges Sicherheitskonzept wird im Bundesministerium für Landesverteidigung bereits seit Einführung der automationsunterstützten Datenverarbeitung angewandt und weiterentwickelt.

Zu 20:

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