1522/AB XXI.GP
Eingelangt am: 19-01-2001

Die Abgeordneten zum Nationalrat Egghart und Kollegen haben am 21. November 2000 unter der Nr. 1506/J an mich eine schriftliche parlamentarische Anfrage betreffend "Informationssicherheit im Bereich der Exekutive" gerichtet.

Diese Anfrage beantworte ich aufgrund der mir vorliegenden Informationen wie folgt:

Zu Frage 1:
Software
Das EKIS - System läuft auf dem Zentralen Rechnersystem der EDV - Zentrale unter dem Betriebssystem OS/390. Dieses Betriebssystem für Großrechner wird im kommerziellen und im ministeriellen Bereich (BMF, BMLV, BKA) eingesetzt und durch die Fa. IBM vertrieben. Die Wartung dieses Betriebssystems erfolgt durch Bedienstete des BMI.
Die Datenbanksoftware ist eine Eigenentwicklung durch Mitarbeiter der EDV - Zentrale und wird durch diese Mitarbeiter auch gewartet.
Als interne Datenbanksoftware ist das Produkt RACF eingesetzt, das sicherstellt, dass nur jene Mitarbeiter der EDV - Zentrale die Datenstrukturen sehen können, die sie zur Ausübung ihrer Tätigkeit brauchen
Hardware
Das EKIS - System läuft auf Hardware der Fa. IBM im CPU - Bereich, bei Plattenspeicher auf Hardware der Fa. IBM und Comparex.

Die Wartung wird ausschließlich von sicherheitstechnisch überprüften Technikern, unter Aufsicht der BMI - eigenen Operatoren und Systemprogrammierer durchgeführt.

Zu Frage 2:
Alle Firmen müssen vor Abschluss eines Liefer - bzw. Wartungsvertrages eine Sicherheitserklärung unterfertigen, bei der die Techniker auf Verschwiegenheit nachweislich verpflichtet werden.
Firmen, die zur Erfüllung ihrer Aufgaben eventuell auch Einblick in Datenbereiche erhalten können, werden von der zuständigen Abteilung im BMI sicherheitstechnisch überprüft und nur beschäftigt, wenn ein negatives Überprüfungsergebnis vorliegt.

Zu Frage 3:
Nein.

Zu Frage 4:
Es sind Firewall - Systeme installiert, welche gegenüber dem WWW auf höchste Sicherheitsstufe konfiguriert sind.
Weiters werden Spezialfirmen beauftragt, Angriffe gegen das Firewall - System des BMI durchzuführen um eventuell Schwachstellen festzustellen. Bei den bisher durchgeführten Angriffstests (simulierter Hackerangriff) auf das BMI - interne Netz war ein Eindringen nicht möglich und es wurden keine Schwachstellen festgestellt.

Zu Frage 5:
Im Internet finden von Zeit zu Zeit praktisch gegenüber allen vorhandenen Firewallsystemen Angriffe bzw. Angriffsversuche statt. Jene gegenüber dem BMI - Firewall - System waren jedoch nie erfolgreich und somit auch nicht feststellbar.

Zu Frage 6:
Die Systemadministration wird im Benutzerrechte - Bereich durch die Abt. IV/8 des BMI, die technische Systemadministration durch Bedienstete der EDV - Zentrale des BMI durchgeführt.

Zu Frage 7:
Die EKIS - Datensicherung im BMI erfolgt durch laufende Protokollierung aller Anfragen und Änderungsvorgänge (Protokollfile) sowie jeder technischen Ver - änderung der Datenbanken (Journalfile).
Die tägliche Sicherung der Protokoll - und Journalfile erfolgt auf Magnetbandkassetten in einem Bandrobotersystem, das getrennt vom Speichersystem in einem anderen

Objektteil aufgestellt ist. Diese Sicherungen werden dupliziert und in einem brand - hemmenden und zutrittsgesicherten Datensafe abgelegt.
Einmal monatlich werden alle EKIS - und Systemdaten gesichert und unter polizei - licher Bedeckung in den Zentralraum des Bundes (ZAS) ausgelagert.

Zu Frage 8:
Datensicherungen werden drei Monate, Protokolldaten werden drei Jahre aufbewahrt.

Zu Frage 9:
Die Datenvernichtung erfolgt in unterschiedlichen Formen, je nach Medium:
Magnetbänder/Kassetten: Die Datenträger werden mittels starken elektromagnetischen Feldern mit eigenen Löschgeräten gelöscht. Im Fall einer Wiederverwendung anschließend neu formatiert, oder unter Aufsicht der Abt. IV/8 vernichtet (verbrannt).
Magnetplatten: Nach Ausbau aus einem PC oder Server werden die Platten von Mitarbeitern der EDV - Zentrale physikalisch zerstört, da sich hier elektromagnetische Felder als zu schwach erwiesen haben.
Disketten/CD - ROM: Diese Datenträger werden durch Bedienstete der EDV - Zentrale mittels eigens dafür beschafften Schreddergerät physikalisch zerstört.

Zu Frage 10:
Wenn überhaupt, findet eine Wiederverwendung ausschließlich im Bereich der Gruppe EDV des BMI statt.

Zu Frage 11:
Der Zugriff auf die gesicherten Daten ist in der Datensicherheitsvorschrift geregelt. Werden Datensicherungen zur Dateifehlerbehebung oder technischen Wiederher - stellbarkeit benötigt, so erfolgt die Ausgabe im Vieraugen - Prinzip. Der Zugang zum Datenarchiv wird systemmäßig durch ein Zutrittskontrollsystem überwacht, durch den Archivar dokumentiert und von den zuständigen Fachvorgesetzten überprüft.
Weiters wird ein Zugriff auf gesicherte Daten vom Schichtleiter des rund um die Uhr besetzten Rechenzentrums der EDV - Zentrale des BMI im elektronischen Vorfall - protokoll zusätzlich dokumentiert.

Zu Frage 12:
Durch die strikte Trennung von Produktionsdaten und Testdaten für Entwicklung besteht für die Entwicklungsmannschaft keine unkontrollierte Zugriffsmöglichkeit auf Produktionsdaten.

Jeder Zugriff auf Echtdaten wird auch für interne Mitarbeiter protokolliert. Zusätzlich müssen diese für jeden Zugriff ein sogenanntes Datenschutzprotokoll ausfüllen in dem anzugeben ist, aus welchem dienstlichen Grund diese Datenabfrage getätigt wurde. Diese Angaben werden stichprobenartig von der Datenschutzabteilung IV/8 des BMI überprüft.