Deutscher Bundestag **Drucksache 14/1149**
14. Wahlperiode

16. 06. 99

Antwort
der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Angela Marquardt, Rolf Kutzmutz und der Fraktion der PDS
— Drucksache 14/1057 —

Standpunkt der Bundesregierung zu Kryptographie und zur Einführung kryptographischer Software mit Key-Recovery-System bei der Bundeswehr

Die Enquete-Kommission „Zukunft der Medien in Wirtschaft und Gesellschaft – Deutschlands Weg in die Informationsgesellschaft“ hat sich in ihrem vierten Zwischenbericht zum Thema „Sicherheit und Schutz im Netz“ gegen eine Regulierung kryptographischer Verfahren ausgesprochen. Key-Recovery-Systeme, bei denen ein Schlüssel für Kontrollbehörden zugänglich hinterlegt wird, hat die Enquete-Kommission eindeutig abgelehnt. Dem „Tagesspiegel“ vom 24. Januar 1999 zufolge wurde die Bundeswehrverwaltung mit der Krypto-Software „Lotus Notes“ des Herstellers IBM ausgestattet. IBM ist jedoch Mitglied der „Key Recovery Allianz“ in den USA.

1. Welche Folgerungen zieht die Bundesregierung aus der Position der Enquete-Kommission, Kryptographie uneingeschränkt und ohne Key Recovery zuzulassen?

Die Bundesregierung hat nicht die Absicht, die Nutzung der Kryptographie einzuschränken.

2. Wann wird sich die Bundesregierung offiziell zur sogenannten Krypto-Debatte äußern?

Die Bundesregierung hat in der Kabinettsitzung am 2. Juni 1999 die „Eckpunkte der deutschen Kryptopolitik“ beschlossen. Sie hat damit ihre Position eindeutig dargelegt und die Grundlage für eine sachorientierte Behandlung des Themas in der Zukunft geschaffen.

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums für Wirtschaft und Technologie vom 15. Juni 1999 übermittelt.

Die Drucksache enthält zusätzlich – in kleinerer Schrifttype – den Fragetext.

3. Gibt es unterschiedliche Bewertungen der Kryptographie im Bundesministerium des Innern und im Bundesministerium für Wirtschaft und Technologie?

Nein.

4. Wenn ja, ist dies der Grund dafür, daß eine Stellungnahme der neuen Bundesregierung zur Regelung der Kryptographie bisher unterblieben ist?

Siehe Antwort zu Frage 3.

5. Welche Maßnahmen plant die Bundesregierung, um die Entwicklung starker Verschlüsselungsprogramme in Deutschland zu fördern?

6. Welche Maßnahmen plant die Bundesregierung, um die massenhafte Anwendung von Verschlüsselungsprogrammen durch die Wirtschaft und die das Internet nutzende Bevölkerung zu unterstützen?

Das Bundeskabinett hat am 2. Juni den Bundesminister für Wirtschaft und Technologie und den Bundesminister des Innern beauftragt, auf der Basis der vorliegenden Eckpunkte ein Konzept zur Ausgestaltung der deutschen Kryptopolitik zu entwickeln. Dieses Konzept wird auch die Förderung der Entwicklung und der Verbreitung starker Verschlüsselung in Deutschland zum Gegenstand haben. Im übrigen hat die Bundesregierung mit der im März d. J. vorgestellten Initiative für „Sicherheit im Internet“ bereits begonnen, gerade den privaten Anwender über sicherheitsrelevante Fragen bei der Benutzung des Internet zu informieren.

7. Stimmt es, daß die Bundeswehrverwaltung mit der Software „Lotus Notes“ ausgestattet wurde?

Die Bundeswehr setzt Lotus Notes seit 1994 ein. Dieses Produkt wird z. Zt. an ca. 20 000 Arbeitsplätzen genutzt.

8. Wenn ja, weshalb wurde sich für „Lotus Notes“ entschieden?

Der Entscheidung für das Produkt Lotus Notes liegt das Ergebnis einer Studie aus dem Jahre 1993 zu Grunde. Im Rahmen der Studie wurden verschiedene Produkte untersucht, getestet und bewertet, die außer einer reinen Mailfunktion auch sogenannte Workflow-Systeme zur elektronischen Abbildung von Arbeitsabläufen in der täglichen Arbeit enthalten.

Die Studie empfiehlt den Einsatz von Lotus Notes aus folgenden Gründen:

– Erfüllung aller organisatorischen und technischen Bedingungen des IT-Rahmenkonzeptes BMVg,

– Interoperabilität mit anderen Mailsystemen,
– sehr gutes Preis-Leistungsverhältnis.

9. Wer hat diese Entscheidung getroffen?

Das Bundesministerium der Verteidigung.

10. Welche Schlüssellänge in Bit hat die Lotus-Notes-Verschlüsselung?

In Lotus Notes sind verschiedene umfassende Sicherheitsmechanismen integriert, die technischen Parameter sind in der Anlage erläutert. Da Lotus Notes in der Bundeswehr zur Übertragung offener Informationen und Informationen des Schutzbereichs 1 (VS NfD und Personen-bezogene Daten des Schutzbereichs 1) genutzt wird, ist i. d. R. der Mailverkehr nicht verschlüsselt. Abweichende Regelungen existieren z. T. in einzelnen Organisationsbereichen auf Grundlage von Vorgaben der zuständigen IT-Sicherheitsbeauftragten.

11. Ist eine Key-Recovery-Funktion in diese Software implementiert?

Es handelt sich nicht um eine Key-Recovery-Funktion im technischen Sinne. Vielmehr werden aufgrund der Funktion „Workfactor Reduction for International Releases“ bei der Generierung eines 64 Bit-Blocks zum Verschlüsseln des Mail-Inhaltes die obersten 24 Bit des Schlüssels mit dem Öffentlichen Schlüssel (Public-Key) der National Security Agency (NSA) verschlüsselt, so daß die NSA, die den passenden Privaten Schlüssel (Private Key) dazu besitzt, letztendlich nur 40 Bit entschlüsseln muß. Potentielle Angreifer müßten dagegen die vollen 64 Bit entschlüsseln.

12. Wenn ja, wie erklärt die Bundesregierung, daß in staatlichen Institutionen Verschlüsselungsprogramme mit Key Recovery eingesetzt werden, während Key Recovery eigentlich abgelehnt wird?

13. Teilt die Bundesregierung die Auffassung, daß die offizielle Anschaffung von Key Recovery unterstützender Krypto-Software den Empfehlungen der Enquete-Kommission „Zukunft der Medien“ entgegensteht?

Entfällt aufgrund Beantwortung zu Frage 11.

14. Welche Rolle spielt der Bericht der Enquete-Kommission „Zukunft der Medien“ für die Bundesregierung bei der Bewertung der Krypto-Debatte?

Der Bericht der Enquete-Kommission „Zukunft der Medien“ ist von der Bundesregierung bei der Festlegung ihrer Eckpunkte gewürdigt worden.