

4382/AB XXII. GP

Eingelangt am 14.08.2006

Dieser Text wurde elektronisch übermittelt. Abweichungen vom Original sind möglich.

BM für Finanzen

Anfragebeantwortung

GZ. BMF-310205/0063-I/4/2006

Herrn Präsidenten
des Nationalrates

Dr. Andreas Khol

Parlament
1017 Wien

Sehr geehrter Herr Präsident!

Auf die schriftliche parlamentarische Anfrage Nr. 4369/J vom 14. Juni 2006 der Abgeordneten Mag. Johann Maier, Kolleginnen und Kollegen, betreffend Entsorgung von Festplatten in den Bundesministerien, beehe ich mich Folgendes mitzuteilen:

Einleitend möchte ich darauf hinweisen, dass das Bundesministerium für Finanzen einer der größten Informationstechnologie (IT)-Anwender Österreichs ist und seit Jahrzehnten in diesem Bereich eine enge Zusammenarbeit mit der Bundesrechenzentrum (BRZ) GmbH - ehemals Bundesrechenamt (BRA) - besteht.

Als führender IT-Dienstleister des Bundes verfügt die BRZ GmbH über eines der größten Rechenzentren, in dem höchst sensible Daten verarbeitet werden und daher der bestmögliche Schutz dieser Daten gewährleistet sein muss. Um diese Sicherheit zu gewährleisten, wird das Informationssicherheitssystem seit 2005 zertifiziert.

Im Mai letzten Jahres wurde die BRZ GmbH durch das Zertifizierungsunternehmen CIS GmbH einem umfangreichen Security-Audit unterzogen und hat diesen mit ausgezeichnetem Erfolg bestanden. Damit wurde die erstmalige Zertifizierung des Informationssicherheits-Managementsystems (ISMS) nach ÖNORM A 7799 bzw. BS 7799 erreicht.

Zum Jahresende 2005 wurde der neue ISO-Standard IS 27001 veröffentlicht, der die Sicherheitsnorm auf den aktuellen Stand der Technik adaptiert. Gleichzeitig wurde die Gültigkeit aller bestehenden Zertifikate nach älteren Normen bis zum 15. April 2007 begrenzt. Das BRZ war daher aufgerufen, ein Upgrade des bestehenden Zertifikats nach ÖNORM A 7799 auf den neuen ISO-Standard durchzuführen.

Von 24. bis 26. April dieses Jahres wurde das Sicherheitswesen des Unternehmens in der jährlich durchzuführenden Überprüfung neuerlich auditiert. Das Ziel war der Nachweis zur Erfüllung der Anforderungen der ÖNORM A 7799 nach der die BRZ GmbH im vergangenen Jahr geprüft wurde. Im Zuge des dreitägigen Verlaufs wurde die Normkonformität des ISMS der BRZ nach den Vorgaben von A 7799 bestätigt.

Darüber hinaus haben die CIS-Mitarbeiter den bereits vorhandenen Erfüllungsgrad in Bezug auf die neue Sicherheitsnorm ISO 27001 begutachtet. Das am 23. Mai 2005 erreichte Zertifikat nach der ÖNORM A 7799 wurde mit 11. Mai 2006 auf den aktuellen Standard 27001 erweitert. Dieses Zertifikat gilt bis 23. Mai 2008. Damit das nun erreichte höchste Sicherheitsniveau gewahrt bleibt, finden jährliche Überprüfungen statt. Dabei wird die Weiterentwicklung des Konzepts nachzuweisen sein, denn Security bedeutet nicht punktuelle Anstrengung, sondern ist ein laufender, sich ständig entwickelnder Prozess.

Das BRZ ist mit diesem Ergebnis wieder im Spitzenfeld bei der Bewertung des Sicherheitskonzepts und hat den Nachweis erbracht, dass das Sicherheitssystem dem aktuellen internationalen Standard entspricht.

Weiters möchte ich hinsichtlich der vorliegenden Anfrage grundsätzlich festhalten, dass der Regelfall nicht die Entsorgung, sondern das Ausscheiden von Geräten mit Festplatten nach Ablauf des Nutzungszeitraumes ist. Vor dem Ausscheiden werden die Festplatten jedenfalls mit einer Spezialsoftware gelöscht (Punkt 3 der folgenden Beantwortung).

Im Fehlerfall werden Festplatten entweder an die Lieferfirma (im Garantiefall) oder an die Wartungsfirma zur vertragskonformen Behandlung übergeben.

Hinsichtlich der echten Entsorgung/Vernichtung von Datenträgern (z.B. Magnetbändern) möchte ich auf die Darstellung unter den Punkten 4 und 6 hinweisen.

Zu 1.:

Ja, es gibt eine Sicherheitsrichtlinie für das Ausscheidung bzw. die Entsorgung der Hardware, in der u.a. geregelt wird, dass Datenträger oder andere Bausteine, die klassifizierte Informationen enthalten, vor dem Ausscheiden oder der Übergabe an ein Wartungs- bzw. Entsorgungsunternehmen zu löschen bzw. zu vernichten sind.

Zu 2.:

Im Zeitraum von 2000 bis 2005 wurde folgende Anzahl an Geräten ausgeschieden:

2000: 2534

2001: 5536

2002: 3409

2003: 5189

2004: 3132

2005: 3853

Zu 3.:

Ja, die Daten werden vor der Entsorgung bzw. dem Ausscheiden mit einer Spezialsoftware gelöscht.

Zu 4.:

Der Auftrag an die Entsorgungsfirma lautet:

Abholung der in versperrten Containern gelagerten Datenträger, Abtransport und ordnungsgemäße Entsorgung von Elektronikschrott.

Zu 5.:

Die Datenlöschung erfolgt soweit als möglich intern.

Wie bereits in der Einleitung dargelegt, ist nicht die Entsorgung sondern das Ausscheiden von Geräten der Regelfall. Es ist daher auch zu keiner Ausschreibung der Entsorgung gekommen, da aufgrund des geringen Auftragsvolumens eine Ausschreibung nicht erforderlich war.

Die Entscheidungskriterien für die Auswahl der Entsorgungsfirma waren insbesondere die Einhaltung des vorgegebenen sicheren Verfahrens und der Preis.

Zu 6.:

Die Kontrolle der ordnungsgemäßen Durchführung der Entsorgung wird durch Begleitung der Transporte und Überwachung der Vernichtung realisiert. Außerdem wird ein Vernichtungsprotokoll angefertigt.

Zu 7.:

Spezielle Sanktionen sind nicht vorgesehen. Bei einer Vertragsverletzung würden die üblichen zivilrechtlichen Wege beschritten werden.

Zu 8.:

Bisher sind keine Probleme bekannt geworden.

Zu 9.:

Eine vertragswidrige Verwendung kann nie gänzlich ausgeschlossen werden, weil auch kriminelle Handlungen durch im Prozess involvierte Personen nie restlos ausgeschlossen werden können. Es wurden jedoch alle als notwendig erachteten Maßnahmen ergriffen, um eine solche Möglichkeit weitestgehend zu verhindern.

Zu 10.:

Nein, diesbezüglich wird kein legitimer Handlungsbedarf gesehen.

Mit freundlichen Grüßen