DIE BUNDESMINISTERIN
FÜR JUSTIZ

BMJ-Pr7000/0254-Pr 1/2010

XXIV. GP.-NR
6524 /AB
14. Dez. 2010
zu 6597/J

An die

Frau Präsidentin des Nationalrates

Wien

zur Zahl 6597/J-NR/2010

Der Abgeordnete zum Nationalrat Harald Vilimsky und weitere Abgeordnete haben an mich eine schriftliche Anfrage betreffend „Datensicherheit" gerichtet.

Ich beantworte diese Anfrage wie folgt:

Zu 1, 2 und 6 bis 9:
Das Bundesministerium für Justiz hat die Bundesrechenzentrum-GmbH (BRZ-GmbH) vertraglich dazu verpflichtet, ein Informationssicherheits-Managementsystem (ISMS) nach der internationalen Sicherheitsnorm ISO27001 zu führen. Für die Rezertifizierung (die im März 2011 erforderlich wird) ist das ISMS kontinuierlich weiter zu entwickeln und zu verbessern. Dazu gehören das Überarbeiten des Sicherheitsregelwerks (das mit 10. Oktober 2010 in Kraft gesetzt wurde) und die Einführung eines E-Learning Systems für alle Mitarbeiter zur Ausbildung in Informationssicherheit. Die laufende Durchführung von Audits zur Prüfung der Einhaltung der Sicherheitsregeln wird nach dem von der Geschäftsführung der BRZ-GmbH verfügten Auditplan vorgenommen.

Bis dato gab es meinen Informationen zu Folge keinerlei „Cyberattacken" auf die IKT-Systeme des Justizressorts.

Zu 3:
Ich gehe davon aus, dass sich alle mit Informations- und Kommunikationstechnologie (IKT) befassten Organisationseinheiten mit dem Thema Datensicherheit und folglich mit der Abwehr von Angriffen auf IKT-Systeme auseinander zu setzen haben. Die technische Abwehr von derartigen Attacken fällt

freilich nicht in meinen Wirkungsbereich. Soweit die legislative Seite der Thematik angesprochen ist, darf ich auf meine Antwort zu Fragepunkt 12 verweisen.

Zu 4 und 5:
Ja, das Justizressort arbeitet hier etwa – koordiniert mit anderen Ressorts – mit dem Gremium „Digitales Österreich IKT Bund" zusammen.

Zu 10 und 11 sowie 13 und 14:
Das Bundesministerium für Justiz lässt von der BRZ-GmbH zur Sicherung seiner Daten, seiner Anwendungen und seines Netzwerkes folgende Systeme betreiben:

- Ein Intrusion Detection/Intrusion Prevention-System zur Erkennung und Verhinderung von Angriffen auf das Netzwerk und einzelne Server. Dabei sind die einzelnen Netzsegmente in der BRZ-GmbH auch einzeln geschützt (Mehrdimensionalität des Systems);
- einen Webfilter, der schadhafte bzw. manipulierte Seiten selbständig erkennt und deren Zugriff auf das Netzwerk der Justiz verhindert;
- einen Webfilter zur Sperre von gefährlichen Seiten;
- ein Patch-System; die Betriebssysteme werden regelmäßig über sogenannte Sicherheits-Patches auf den neuesten Sicherheitsstandard gehoben. Dringende Patches werden nach einer kurzen Testphase von etwa ein bis zwei Tagen eingespielt; kritische Security Patches werden sofort eingespielt;
- einen laufend aktualisierter Spamfilter für das E-Mailsystem;
- ein tagaktuelles und am letzten Stand der Technik operierendes Antivirensystem;
- ein Netzwerk mit sicherheitstechnisch kontrollierten Zugriffen („demilitarized zone" oder DMZ) und Firewalls zwischen den Netzsegmenten.

Dieser digitale Schutzschild war nach bisherigen Erfahrungen ausreichend. Er wird aber – wie bereits ausgeführt – laufend aktualisiert, weiterentwickelt und auf Lücken geprüft. Dabei arbeitet die Justiz eng mit den Experten der BRZ-GmbH zusammen.

Zu 12:
Die (technische) Planung, Ausarbeitung und Umsetzung von IKT-Sicherheitskonzepten im Bereich der öffentlichen Verwaltung fällt nicht in den Wirkungsbereich der Bundesministerin für Justiz.

In legislativer Hinsicht hat Österreich auf die mit der technischen Entwicklung einhergehende Möglichkeit der kriminellen Nutzung moderner Technologie schon vor zwei Jahrzehnten durch Anpassungen des materiellen Strafrechts reagiert. Durch das Strafrechtsänderungsgesetz 1987 wurden die Strafbestimmungen gegen Sachbeschädigung (durch ein Verbot der vorsätzlichen Beschädigung automationsunterstützt gespeicherter oder übermittelter Daten und Programme: § 126a StGB, „Datenbeschädigung") und die Strafbestimmungen gegen Betrug (zur Erfassung von Fällen, in denen – ohne Täuschung eines Menschen – mit Bereicherungsvorsatz das Ergebnis einer automationsunterstützten Datenverarbeitung beeinflusst wird: § 148a StGB, „Betrügerischer Datenverarbeitungsmissbrauch") ergänzt.

Am 23. November 2001 hat Österreich – gemeinsam mit 29 anderen Staaten – die Cyber-Crime-Konvention des Europarats, ETS Nr. 185 (CCC), unterzeichnet, welche am 1. Juli 2004 in Kraft trat. Die Konvention enthält eine Reihe materieller Straftatbestände. Diese unterteilen sich im Wesentlichen in vier Kategorien:

- unerlaubte Angriffe auf Computersysteme,
- strafbare Handlungen mit Hilfe von Computersystemen,
- Verbreitung strafbarer Inhalte über Computersysteme sowie
- Urheberrechtsverletzungen.

Darüber hinaus sieht die Konvention eine Reihe von Regelungen im Strafprozess- bzw. Rechtshilfebereich vor. An der Ratifizierung dieser Konvention wird derzeit gearbeitet, wobei die Einleitung des Ratifikationsprozesses noch in diesem Jahr geplant ist.

Das Strafrechtsänderungsgesetz 2002 diente unter anderem der Umsetzung der Cyber-Crime-Konvention in einem Teilbereich, wobei vorerst die eigentlichen Computerdelikte, d.h. die unerlaubten Angriffe auf Computersysteme sowie die Begehung herkömmlicher strafbarer Taten mit Hilfe von Computersystemen, in das Gesetz Eingang gefunden haben. Dabei wurden zum Teil neue Delikte geschaffen, die zum Teil bestehenden Strafbestimmungen gegen Missbrauch etc. von Computern im weitesten Sinn angepasst wurden (neu: „Widerrechtlicher Zugriff auf ein Computersystem" - § 118a StGB; „Missbräuchliches Abfangen von Daten" - § 119a StGB; „Störung der Funktionsfähigkeit eines Computersystems" - § 126b StGB;

„Missbrauch von Computerprogrammen oder Zugangsdaten" - § 126c; „Datenfälschung" - § 225a StGB).

Auf EU-Ebene wurde am 24. Februar 2005 der Rahmenbeschluss 2005/222/JI des Rates über Angriffe auf Informationssysteme (Amtsblatt Nr. L 069 vom 16/03/2005 S. 0067 - 0071) formell angenommen, in dem der rechtswidrige Zugang zu Informationssystemen (Art. 2), der rechtswidrige Systemeingriff (Art. 3) sowie der rechtswidrige Eingriff in Daten (Art. 4) unter gerichtliche Strafe gestellt werden soll. Aufgrund dieses Rahmenbeschlusses war nur ein geringfügiger Anpassungsbedarf gegeben, weil die CCC bereits ins innerstaatliche Recht umgesetzt wurde. Es musste daher kein neuer Straftatbestand zur Umsetzung des Rahmenbeschlusses eingeführt werden.

Ein weiterer aktueller Schritt wurde auf EU-Ebene im Bereich der Computerkriminalität unternommen, indem am 30. September 2010 von der Europäischen Kommission eine Richtlinie über Angriffe auf Computersysteme vorgelegt wurde, die den oben zitierten Rahmenbeschluss einerseits ersetzen soll und andererseits neue Kriminalisierungsverpflichtungen, wie etwa die kriminelle Nutzung von sogenannten „Botnets" bzw. „Botnetzen"[1], vorschlägt.

Zusammenfassend sollen die Mitgliedsstaaten zur Kriminalisierung folgender Verhaltensweisen verpflichtet werden:

- Herstellen, Verkaufen, Beschaffen zwecks Gebrauchs, Einführen, Verbreiten oder anderweitiges Verfügbarmachen von Vorrichtungen/Instrumenten, die zur Begehung der betreffenden Straftaten genutzt werden;
- rechtswidriges Abfangen von Daten;
- Der Einsatz von „Botnetzen" oder ähnlichen Instrumenten (Cyber-Großangriff) bei der Begehung von Straftaten, die von der Richtlinie erfasst sind, sowie die Verschleierung der wahren Identität des Täters bei Cyberangriffen, wenn dadurch der rechtmäßige Identitätseigentümer geschädigt wird, sollen erschwerende Umstände darstellen.

[1] Ein **Botnet** oder **Botnetz** ist eine Gruppe von Software-Bots. Die Bots laufen auf vernetzten Rechnern, deren Netzwerkanbindung sowie lokale Ressourcen und Daten ihnen zur Verfügung stehen. Betreiber illegaler Botnetze installieren die Bots ohne Wissen der Inhaber auf Computern und nutzen sie für ihre Zwecke. Die meisten Bots können von einem Botnetz-Operator (auch Bot-Master oder Bot-Herder genannt) über einen Kommunikationskanal überwacht werden und Befehle empfangen. Dieser wird in der Fachsprache zutreffend als Command-and-Control-Server bezeichnet; Kurzform: C&C (Quelle: wikipedia).

Die Verhandlungen zu diesem Vorschlag wurden im Rat noch nicht aufgenommen; es ist aber beabsichtigt, im Zuge der Verhandlungen auch die Experten des Bundesministeriums für Inneres einzubinden, um auch die praktischen Erfahrungen über die aktuellen Erscheinungsformen der Computerkriminalität effizient in den Verhandlungsprozess einzubringen.

Zu 15:
Hochsensible bzw. geheime Daten im Sinne des Informationssicherheitsgesetzes werden auf einem eigenen, vom Netzwerk getrennten (Offline-) Rechner in einem abgesperrten Raum mit strengem Zugriffsberechtigungskonzept gespeichert. Sonstige Daten werden im Regelfall im Elektronischen Aktensystem des Bundes (ELAK im Bund) ausfallssicher abgelegt und archiviert.

Zu 16 und 17:
Externe Sicherungen werden im Bundesrechenzentrum, in einem Parallelrechenzentrum und in einem Zentralen Ausweichsystem (in einer Zero Risk Umgebung) abgelegt.

29 November 2010

(Mag. Claudia Bandion-Ortner)