Auszug aus dem Protokoll des Regierungsrates des Kantons Zürich

KR-Nr. 308/2010

Sitzung vom 15. Dezember 2010

1807. Anfrage (Schutz und Massnahmen vor Cyber-Angriffen)

Kantonsrat Jean-Philippe Pinto, Volketswil, hat am 4. Oktober 2010 folgende Anfrage eingereicht:

Es liest sich wie in einem Krimi. Offenbar hat der Computer-Schädling Stuxnet im Iran Rechner des AKW Buschehr infiziert. Nach Presseberichten über die Verbreitung von Stuxnet sagte der Buchautor Arne Schönbohm der Zeitschrift «WirtschaftsWoche»: «Der Cyberspace wird mittlerweile als fünftes militärisches Schlachtfeld neben dem Boden, der Luft, dem Wasser und dem Weltraum gesehen.»

Als hochindustrialisiertes Land ist die Schweiz und insbesondere auch der Kanton Zürich von Cyberattacken auf Industrieanlagen und Infrastruktur besonders gefährdet. Beim Schutz der Infrastruktur für Kommunikation, Strom und Wasser vor elektronischen Angriffen gebe es noch «erheblichen Nachholbedarf», sagt Schönbohm.

Auch in der Schweiz ist die Bedrohung erkannt worden. Armeechef Andre Blattman bezeichnete Cyber-Angriffe vor kurzem als «grösste Bedrohung für die Schweiz». Gemäss Andre Blattmann ist die Schweiz für Cyber-Angriffe ein leichtes Opfer.

Es stellen sich verschiedene Fragen betreffend Sicherheit vor Cyber-Angriffen im Kanton Zürich.

1. Ist das Thema Cyber-Angriff vom Regierungsrat thematisiert worden? Wenn nein, warum nicht?
2. Wie beurteilt der Regierungsrat den derzeitigen Schutz von Industrieanlagen und Infrastruktur durch Cyber-Angriffe im Kanton Zürich? Wo sieht die Regierung die grössten Risiken für den Kanton Zürich?
3. Wo sieht der Regierungsrat Handlungsbedarf? Wie beabsichtigt die Regierung allfällige Verbesserungsmassnahmen in die Wege zu leiten?
4. Hat der Regierungsrat hierfür eine Arbeitsgruppe eingesetzt? Arbeitet der Kanton Zürich auch mit privaten Unternehmen zusammen? Wie funktioniert die diesbezügliche Zusammenarbeit mit dem Bund? Wie werden die Gemeinden miteinbezogen?
5. Gibt es spezielle Bestimmungen und Kontrollen bei der Anstellung von Personen in hochsensitiven Bereichen?

6. Wie nimmt der Regierungsrat Einfluss auf Sicherheitsbestimmungen der verselbständigten Anstalten wie ZKB, USZ, EKZ etc.?
7. Bestehen gesetzliche Grundlagen für wirksame Massnahmen zur Sicherung und Verteidigung von Datennetzwerken im Kanton Zürich?

Auf Antrag der Direktion der Justiz und des Innern

beschliesst der Regierungsrat:

I. Die Anfrage Jean-Philippe Pinto, Volketswil, wird wie folgt beantwortet:

Zu Frage 1:

Die Thematik der Cyber-Angriffe (gezielte elektronische Angriffe auf Computernetze) stellt einen Teilaspekt der sogenannten Internetkriminalität dar. Mit Beschluss vom 1. Juli 2009 hat der Regierungsrat die Bekämpfung der Internetkriminalität zu einem der Schwerpunkte der Tätigkeit der Strafverfolgungsbehörden für die Legislaturperiode 2009–2012 erklärt (RRB Nr. 1068/2009). Im Verbund mit Nutzerinnen und Nutzern sowie Betreiberinnen und Betreibern des Internets soll nach Lösungen gesucht werden, wie kriminelle Machenschaften im Bereiche der Internetkriminalität unterbunden werden können. Seit August 2009 ist in diesem Zusammenhang auch ein aus Vertretungen der Erwachsenenstrafverfolgung, der Jugendstrafverfolgung, der Kantonspolizei, der Stadtpolizei Zürich und Unternehmen der Privatwirtschaft zusammengesetztes Projektteam daran, verschiedene Fragen zur Bekämpfung der Internetkriminalität zu bearbeiten.

Zu Frage 2:

Eine zentrale Überwachung des Internets ist nicht möglich. Unternehmen oder Verwaltungseinheiten schützen sich vor Cyber-Angriffen mit entsprechenden Sicherheitssystemen. Diese bestehen beispielsweise aus ganzen Sets moderner Firewallsysteme und zusätzlichen Schutzmechanismen.

Diese Systeme bieten in der Regel einen angemessenen Schutz gegen gängige Cyber-Angriffe. Für die Sicherheit der kantonalen Informationstechnologien (IT) sind dabei verschiedene Konzepte vorhanden, die sich u. a. an der Informatiksicherheitsverordnung vom 17. Dezember 1997 (ISV; LS 170.8) ausrichten. Die kantonalen IT-Systeme sind nach diesen Vorgaben durch angemessene organisatorische und technische Massnahmen vor äusseren Einwirkungen und vor unbefugtem

Zugriff zu schützen und die Amtsstellen haben eine entsprechende Analyse der Gefahren und Risiken ihrer Informatiksysteme zu erstellen und Schutzziele festzulegen.

Ob die eingesetzten Sicherheitssysteme darüber hinaus einem gezielten Cyber-Angriff, beispielsweise von einem ausländischen Nachrichtendienst, standhalten würden, ist schwer zu sagen, zumal infolge der sich rasend schnell entwickelnden Technik davon ausgegangen werden muss, dass *kein* Sicherheitssystem unantastbar ist, das am Internet angeschlossen ist. Grösste Risiken wären wohl mit Angriffen auf die Infrastruktur wie Wasser- und Stromversorgung oder Kommunikationsnetze verbunden. Im Falle eines Angriffs hätten vorab die Spezialistinnen und Spezialisten der Kantonspolizei mit den betroffenen Informatikbetreibern den Fall zu bearbeiten. Zudem käme der Beizug der Melde- und Analysestelle für Informationssicherung (MELANI), die dem Eidgenössischen Departement für Verteidigung, Bevölkerung und Sport (VBS) angegliedert ist, in Betracht. MELANI gibt regelmässig auch Einschätzungen betreffend Schutz bzw. Bedrohung von Industrieanlagen und Infrastruktur für die Schweiz (und damit auch für den Kanton Zürich) sowie auch international ab (vgl. auch www.melani.ch).

Zu Frage 3:

Handlungsbedarf ergibt sich vor dem Hintergrund der raschen technischen Entwicklung bei der fortlaufenden Anpassung der Sicherheitskonzepte und der ständigen Aktualisierung der Sicherheitssysteme von Firmen und Verwaltung. Die fachlich zuständigen Sicherheitsexpertinnen und -experten befassen sich entsprechend laufend mit der Beurteilung möglicher Risiken, mutmasslicher Schadensausmasse und deren Eintretenswahrscheinlichkeit sowie der Konzeption der Gefahrenabwehr (vgl. im Übrigen auch die Ausführungen zu Frage 1).

Zu Frage 4:

Über das vom Regierungsrat eingesetzte Projektteam zur Verfolgung der Internetkriminalität wurde bereits in der Beantwortung der Frage 1 informiert. Die diesbezügliche Zusammenarbeit mit dem Bund (vgl. auch Frage 2) beschränkt sich nicht nur auf die erwähnte MELANI, sondern beschlägt auch die Bundesanwaltschaft und die Bundeskriminalpolizei. In diesem Zusammenhang kann auch auf die der Bundeskriminalpolizei (BKP) angegliederte Schweizerische Koordinationsstelle zur Bekämpfung der Internetkriminalität (KOBIK), verwiesen werden, die einerseits aktiv im Internet nach strafrechtlich relevanten Inhalten sucht und anderseits besorgt ist für eine vertiefte Analyse im Bereich der Internetkriminalität. Sie steht der Öffentlichkeit, den Behörden und den Internet-Providern als Kompetenzzentrum zur Verfügung. KOBIK

ist das Ergebnis einer Konkordatslösung der Kantone unter Beteiligung des Bundes. Als Ansprechstelle für Gemeinden wirkt schliesslich die Kantonspolizei. Sie verfügt über eigene Fachspezialistinnen und -spezialisten zur Analyse von Cyberangriffen. Staatsanwaltschaften und Polizei ziehen bei Bedarf auch externe Dienstleister und Fachkräfte als Sachverständige für die Aufklärung von Straftaten hinzu.

Was die verwaltungsinterne Erarbeitung von Sicherheitsverfahren und Nutzung von moderner adäquater Technologie anbelangt, so arbeiten die zuständigen Stellen in der kantonalen IT-Organisation auch mit privaten Unternehmungen zusammen. Dies geschieht auf der Grundlage einer fachlichen Zusammenarbeit; die Verantwortung liegt in allen Geschäftsbeziehungen bei den kantonalen Stellen. Auch mit Bundesstellen wird zusammengearbeitet. Es sind jeweils entsprechende Gremien für die spezifischen Anforderungen der Zusammenarbeit tätig. Diese regeln jeweils bilateral – und allenfalls in Absprache mit übergeordneten Stellen – Zuständigkeiten und Verantwortung in den fraglichen Umfeldern. Die meisten dieser Gremien sind in den Rahmen der Schweizerischen Informatikkonferenz (SIK; vgl. www.sik.ch) eingebettet. Ebenfalls besteht ein stetiger Informationsaustausch zwischen den Informatikorganisationen der Gemeinden bzw. der entsprechenden Dachorganisation (IG ICT; vgl. www.igict.ch) und den kantonalen Ämtern sowie dem Kantonalen IT-Team (KITT), das der Finanzdirektion angegliedert ist. Eine vierteljährliche gemeinsame Konferenz stellt diese Kontinuität sicher und delegiert allenfalls spezifische Aufgaben an bilaterale Arbeitsgruppen.

Zu Frage 5:

Solche Kontrollen werden durchgeführt. Sie beziehen sich nicht nur auf kantonale Mitarbeitende, sondern auch auf Mitarbeitende von externen Unternehmen (z. B. Abraxas AG), mit denen der Kanton zusammenarbeitet. Diese Massnahmen werden nötigenfalls auch auf ihre Tauglichkeit überprüft und die Kontrollen werden periodisch wiederholt.

Zu Frage 6:

Was die Informationssicherheit betrifft, so entscheidet die verantwortliche Stelle über die Angemessenheit der zu treffenden organisatorischen und technischen Massnahmen (beispielsweise mehrstufiges Firewall-System, automatische Verteilung von Patches, regelmässiger Audit des Datenschutzbeauftragen, verbindliche Weisungen zur Nutzung von IT-Mitteln usw.). Soweit selbstständige öffentlich-rechtliche Anstalten wie z. B. das Universitätsspital (USZ) oder die Elektrizitätswerke des Kantons Zürich (EKZ) dem Gesetz über die Information und den

Datenschutz (IDG, LS 170.4) unterstehen, richten sich die Zielsetzungen zum Schutz der Informationssicherheit dabei grundsätzlich nach § 7 IDG. Welche Massnahmen in Bezug auf die Informationssicherheit im Gesamten und der dazu notwendigen Infrastruktur im Besonderen getroffen und implementiert werden müssen, richtet sich entsprechend dieser Bestimmung nach Art der Information, dem Zweck der Verwendung und dem jeweiligen Stand der Technik. Der Kantonsrat oder die Verwaltung können bei solchen Anstalten allenfalls (indirekt) über ihre jeweilige gesetzliche Aufsichtstätigkeit oder im Rahmen von Verwaltungsratsmandaten Einfluss nehmen. Seitens der Verwaltung bestehen Vertretungen insbesondere bei den EKZ (Verwaltungsrat) oder im Spitalrat des Universitätsspitals bzw. des Kantonsspitals Winterthur. Der Kantonsrat übt u. a. die Oberaufsicht aus bei der Zürcher Kantonalbank, den EKZ, dem Universitätsspital und Kantonsspital Winterthur (§ 11 Abs. 1 Kantonalbankgesetz vom 28. September 1997 [LS 951.1], § 9 Abs. 1 EKZ-Gesetz vom 19. Juni 1982 [LS 732.1], § 8 Ziff. 1 Gesetz über das Universitätsspital vom 19. September 2005 [LS 813.15], § 7 Ziff. 1 Gesetz über das Kantonsspital Winterthur vom 19. September 2005 [LS 813.16]).

Bei ausgewählten Verwaltungseinheiten (z. B. auch bei Spitälern und Kliniken, Berufs-, Mittel- und Fachhochschulen) sowie Gemeinden überprüft sodann der Datenschutzbeauftragte getroffene Massnahmen im Rahmen seines jährlichen Kontrollplans und erlässt Hinweise und Bemerkungen. Er stützt sich dabei auf den Grundschutzkatalog und den Standard zur erweiterten Risikoanalyse BSI 100-3 des deutschen Bundesamtes für Sicherheit in der Informationstechnik (BSI) in Bonn (vgl. www.bsi.de). Der Datenschutzbeauftragte berichtet im Rahmen seiner Tätigkeitsberichte regelmässig über den Stand und die im Rahmen dieser Umsetzung auftretenden Probleme (vgl. www.datenschutz.ch).

Zu Frage 7:

Neben dem IDG und der zugehörigen Verordnung vom 28. Mai 2008 (IDV, LS 170.41), sind die Rahmenbedingungen der Informatiksicherheitsverordnung vom 17. Dezember 1997 (ISV, LS 170.8) für den Schutz von Informatiksystemen (Netzwerke, Server, Clients, Daten usw.) verbindlich. Organisatorische Regelungen zur direktionsübergreifenden Informatik in der kantonalen Verwaltung – einschliesslich der unselbstständigen Anstalten – finden sich in der Verordnung über die direktionsübergreifende Informatik vom 14. Dezember 2005 (KITT-Verordnung, LS 170.7).

Strafbarkeit und Strafverfolgung richten sich nach den einschlägigen Normen des Bundesrechts und damit insbesondere nach dem Strafgesetzbuch (StGB, SR 311.0).

II. Mitteilung an die Mitglieder des Kantonsrates und des Regierungsrates sowie an die Direktion der Justiz und des Innern.

Vor dem Regierungsrat
Der Staatsschreiber:
Husi