**Eingelangt am 30.03.2012**


BM für Inneres

# Anfragebeantwortung

Frau
Präsidentin des Nationalrates
Mag.[a] Barbara Prammer
Parlament
1017 Wien

GZ: BMI-LR2220/0218-II/BK/5.2/2012

Wien, am . März 2012

Der Abgeordnete zum Nationalrat Mayerhofer und weitere Abgeordnete haben am 1. Februar 2012 unter der Zahl 10500/J an mich eine schriftliche parlamentarische Anfrage betreffend „Cyberkriminalität“ gerichtet.

Diese Anfrage beantworte ich nach den mir vorliegenden Informationen wie folgt:

**Zu Frage 1:**

Die Bekämpfung der Querschnittsmaterie „Cyber-Crime“ findet im Bundesministerium für Inneres auf mehreren organisatorischen Ebenen statt. Im High-Level Bereich sind im Bundeskriminalamt 26 Bedienstete für die Bekämpfung von Cyber-Crime eingesetzt.

Auf Ebene der Landeskriminalämter findet die Bekämpfung von Cyber-Crime in nahezu allen Ermittlungsbereichen und dem Assistenzbereich „Informationstechnologie-Beweissicherung“ statt. Derzeit umfasst die Mindestanzahl an Bediensteten in den schwerpunktmäßig am stärksten mit Cyber-Crime befassten Fachbereichen im Landeskriminalamt:

| | |
|---|---|
| Burgenland | 8 |
| Kärnten | 9 |
| Niederösterreich | 22 |
| Oberösterreich | 19 |
| Salzburg | 9 |
| Steiermark | 13 |
| Tirol | 12 |
| Vorarlberg | 9 |
| Wien | 36 |

Darüber hinaus wurden mit 162 Ermittlern aus allen Fachbereichen der Landeskriminalämter spezielle Cyber-Crime-Schulungen durchgeführt.

Im Bereich der Bezirks- und Stadtpolizeikommanden wurden in den Bundesländern Burgenland, Kärnten, Niederösterreich sowie Salzburg bereits 39 lokale Bezirks-IT-Ermittler implementiert.

In Bezug auf das Bundesamt für Verfassungsschutz und Terrorismusbekämpfung und die Landesämter für Verfassungsschutz und Terrorismusbekämpfung wird aus polizeitaktischen Gründen von der Nennung der Anzahl der mit der Bekämpfung von Cyber-Crime befassten Bediensteten Abstand genommen.

**Zu Frage 2:**

Im Rahmen des Umsetzungskonzeptes „Gesamtstrategie Cyber-Crime“ wird die sukzessive Implementierung von Bezirks-IT-Ermittlern weitergeführt, sodass in der Endausbauphase im Jahr 2014 alle Bundesländer über Bezirks-IT-Ermittler verfügen. Weiters sollen, abhängig von den laufenden Entwicklungen, zusätzliche Bedienstete mit bedarfsangepassten Spezialisierungsgraden den unterschiedlichen Organisationsebenen und Fachbereichen zugeführt werden.

**Zu Frage 3:**

Die Voraussetzung für ein Cyber-Crime-Competence Center (C4) wie die Einrichtung eines Referates Mobile Forensics, Planstellen für Techniker mit akademischem Abschluss und die Cyber-Crime-Meldestelle waren bereits mit Juli 2011 realisiert, weitere Maßnahmen waren bisher nicht erforderlich.

**Zu Frage 4:**

Im Cyber-Crime-Competence Center (C4) verrichteten mit Stichtag 1. Februar 2012 14 Mitarbeiter ihren Dienst.

**Zu Frage 5:**

- Technischer High Level Support für alle nachgeordneten Dienststellen;
- Technische Spezialisierungen und Grundsatzarbeit;
- Zentraler Betrieb von speziellen ermittlungsrelevanten Technologien;
- Zentraler Betrieb eines Referenzgeräte-Pools;
- Zentrale Durchführung von innovativen oder technisch aufwändigen Projekten;
- Zentraler Aufbau einer Hashwerte-Datenbank;
- Zentraler Aufbau einer Expertenplattform und Wissensdatenbank;
- Zentraler Betrieb der Cyber-Crime-Meldestelle mit technischem Support;
- Bearbeitung von ausgewählten Phänomenen und Delikten;
- Erkenntnisgewinnung für Schutzmaßnahmen und Prävention;
- Durchführung und Koordination von Ausbildungsmaßnahmen;
- Kooperation mit Wirtschaft und Wissenschaft;
- Entwicklung von nationalen und internationalen Bekämpfungsstrategien, Lagebildern, Berichten und Analysen sowie
- Marktbeobachtung und Technologiefolgenabschätzung inklusive Technologie-Radar.

**Zu den Fragen 6 und 7:**

Für das Cyber-Crime-Competence Center (C4) sind insgesamt 49 Mitarbeiter projektiert. Die Verstärkung des Personalstandes wird dabei sukzessive, im Rahmen einer begleitenden Evaluierung, entsprechend dem aktuellen Umsetzungsstand, erfolgen.

**Zu den Fragen 8 bis 10:**

Derzeit stehen dem Cyber-Crime-Competence Center (C4) mit 309,47 m² ausreichende Raumflächen zur Verfügung. Der zusätzliche Raumbedarf für den Endausbau liegt erst nach Abschluss der derzeit laufenden Feinplanungsphase vor.

**Zu den Fragen 11 und 12:**

Der Auftrag zur Errichtung des Cyber-Crime-Competence Center (C4) wurde im Jahr 2011 erteilt, weshalb bisher noch keine Budgetmittel ausgewiesen wurden. Die für das Jahr 2012 verfügbaren Budgetmittel werden erst nach Abschluss der ressortinternen Budget-verteilungen feststehen.

**Zu den Fragen 13 und 14:**

Spezifische technische Aufgabenstellungen, wie beispielsweise technische Grundsatz- oder Projektarbeiten, sind nur für den Zuständigkeitsbereich des Cyber-Crime-Competence Center (C4) vorgesehen. Daher ist nur dort der Einsatz von Technikern mit einer Ausbildung in den Bereichen Informatik und Nachrichtentechnik geplant. Das Cyber-Crime-Competence Center (C4) verfügt derzeit über 3 Mitarbeiter mit einem einschlägigen akademischen Abschluss.

**Zu den Fragen 15 bis 18:**

Im Zuge des Umsetzungsplanes werden die konkreten Ausbildungsmodule für die Bediensteten der jeweiligen Fachbereiche der Landeskriminalämter und die Bezirks-IT-Ermittler bedarfsorientiert, basierend auf dem Projekt der „European Cyber-Crime Training & Education Group“, erarbeitet. Die Gesamtstrategie „Cyber-Crime“ wurde den Leitern der Abteilung 1 der Sicherheitsdirektionen und den Leitern der Landeskriminalämter zur Kenntnis gebracht. Derzeit ist die Ausbildung für den High-Level-Bereich in der Detailplanung.

**Zu Frage 19:**

Das „Kuratorium Sicheres Österreich“ (KSÖ).

**Zu Frage 20:**

Die Beantwortung dieser Frage fällt nicht in den Vollzugsbereich des Bundesministeriums für Inneres.

**Zu Frage 21:**

Am 27. September 2011 wurde im Rahmen eines EU-Projektes eine Übung durchgeführt.

**Zu den Fragen 22 und 23:**

Diese Übung wurde im Bereich Cyber Security, Informationstechnologie sowie Kommunikation durchgeführt. Die Übung zielte auf eine Evaluierung der Verfahren und Abläufe zur gemeinsamen Bewältigung einer eventuellen IT-Krise in Europa.

Es wurden die Verfahrens- und Kommunikationsabläufe, wie beispielsweise das Meldeverfahren, das vorgeschlagene Datenverschlüsselungsschema, die Rollen und Verantwortlichkeiten getestet und hierbei Verbesserungen ausgearbeitet. Dabei bewährte sich bei der Bewältigung der Aufgaben die langjährige Zusammenarbeit der Übungspartner, die für gegenseitiges Vertrauen sorgte und das Zusammenspiel erleichterte.

**Zu Frage 24:**

Vom Ergebnis der Übung wurden sowohl die Übungsteilnehmer als auch das Bundeskanzleramt (GovCERT) in Kenntnis gesetzt. Der Bericht wird in Kürze auf www.cert.at öffentlich zugänglich sein.

**Zu Frage 25:**

Derzeit findet die Planungsphase für Aktivitäten und Übungen im Jahr 2012 statt, welche im laufenden Jahr stattfinden werden.

**Zu Frage 26:**

Es wurden bisher acht öffentlichkeitswirksame Veranstaltungen mit Experten aus Politik, Wirtschaft, Wissenschaft bzw. IT abgehalten, eine Cyber-Risiko-Matrix erarbeitet und präsentiert. Ebenso fand eine Veranstaltung des Bundesministeriums für Inneres gemeinsam mit dem Kuratorium Sicheres Österreich zum Thema „Ausfallszenarien statt. Gemeinsam mit dem Kuratorium Sicheres Österreich erarbeitet das Bundesministerium für Inneres in einer Veranstaltungsreihe eine nationale Cyber-Security-Strategie.