Anfrage

des Abgeordneten Vilimsky
und weiterer Abgeordneter
an die Bundesministerin für Inneres
betreffend Cyber-Krieg

Die Presse vom 02.10.2010 berichtete folgendes:

„Experte: „Österreich nicht besonders gut geschützt"

Digitale Verwaltung ist anfällig für Cyber-Attacken.

Wien. Cyber-Krieg-Experte Alexander Klimburg, er berät das Bundeskanzleramt in Sachen Computersicherheit, warnt davor, dass Österreichs Systeme „nicht besonders gut geschützt sind. Wir stehen da wirklich am Anfang."

Nach Meinung des Experten sei nun „rasches Handeln" erforderlich: Immerhin sei Österreich nach einer Untersuchung des Consultingunternehmens Capgemini auf Platz eins in der EU, was die Vernetzung der Verwaltung betrifft, auch international liegt Österreich hier auf den vordersten Plätzen. Die wichtige Rolle, die Österreichs Banken auch international einnehmen, deutet zudem auf eine Verwundbarkeit des österreichischen Bankenwesens hin. „Dabei sind unsere Cyber-Schutzmechanismen sehr niedrig und waren vor ein paar Jahren nicht einmal existent. Wir haben noch einen weiten Weg vor uns", sagt der Experte am Österreichischen Institut für Internationale Politik (oiip).

Zugute käme Österreich, „dass wir über ungeheure Ressourcen verfügen. Und zwar nicht nur in der öffentlichen Verwaltung, sondern auch in der Privatwirtschaft und der Zivilgesellschaft. Auf die könnte man im Falle eines Cyber-Angriffs zurückgreifen."

Klimburg bringt ein Beispiel: Als im Jahr 2009 der heimtückische Computerwurm mit dem unanständigen Namen „Conficker" Rechner der Kärntner Landesregierung und Spitalscomputer lahmlegte, begann im Verwaltungsbereich eine beispiellose Mobilmachung von IT-Personal: Fast 4000 vom „Conficker"-Computerwurm befallene Computer mussten wieder zum Laufen gebracht werden. „Solche Maßnahmen können reiche Staaten setzen, Länder wie der Iran, die Türkei oder Indien aber auch China verfügen über viel weniger Ressourcen in diesem Bereich und sind somit auch mehr gefährdet", sagt Klimburg.

Der Cyberwar-Experte am Österreichischen Institut für Internationale Politik (oiip) schätzt aber trotz der Bedrohung die Gefahr für Österreich, direktes Angriffsziel einer Cyber-Attacke zu werden, als „eher gering" ein. „Aber wir werden ins Cyber-Kreuzfeuer geraten", sagt Klimburg. Zwar ist Stuxnet, die derzeit kursierende Cyber-Waffe eher zielgerichtet (siehe auch Seite 2), aber theoretisch könnte der Code in hunderten Systemen, die in so unterschiedlichen Anlagen wie Verkehrsleitsystemen oder Molkereien installiert sind, enormen Schaden anrichten.

Stuxnet sorgt daher seit seinem ersten Auftreten vor drei Monaten für erhebliche Besorgnis in den Zirkeln jener Experten, die sich mit der Sicherheit von Computersystemen beschäftigen.

„In den Code wurden mehrere tausend Stunden Arbeit hineingesteckt. Jede Ingenieursstunde ist mindestens 500 bis 1000 Euro wert. Das ist eindeutig ein paar Schuhnummern zu groß für eine Gruppe von Hackern, die der Welt etwas beweisen wollen. Computerkriminelle scheiden ebenfalls aus, weil es sozusagen nichts zu gewinnen gibt. Die Cyber-Mafia ist viel mehr am Ausspionieren von Passwörtern, dem Plündern von Konten oder Computerbetrug interessiert. Als Täter oder Auftraggeber kommt wohl nur ein staatlicher Geheimdienst infrage." Nicht zuletzt auf-

grund dieser neuesten Eskalation im mysteriösen und weithin unsichtbaren Krieg der Computer hat nun eine von Kanzleramt sowie dem Innen- und Verteidigungsministerium in Baden organisierte Fachtagung, bei der es um einen besseren Schutz der sogenannten „Strategischen Infrastrukturen" gehen soll, besonders an Aktualität gewonnen.

Ultimativer asymmetrischer Krieg
Cyber-Krieg ist, so Klimburg, der ultimative asymmetrische Krieg: „Jenes Land, das weniger von Computersystemen abhängig ist, dessen Militär weniger von IT abhängig ist, ist deutlich im Vorteil."
Das Land, das einer Cyber-Attacke ausgesetzt ist, weiß – zumindest zu Beginn – vielleicht gar nichts davon, dass ihm eine andere Macht den Cyber-Krieg erklärt hat. Und wenn dann die Computersysteme verrückt spielen, dann lässt sich oft nicht zweifelsfrei feststellen, wer der Angreifer ist.
Andererseits seien auch jene Länder – wie etwa die USA, EU-Länder oder Israel – im Vorteil, die auf mächtige Serverfarmen zurückgreifen können und die mit ihren Heerscharen an gewieften Programmierern eine größere Cyber-Schlagkraft entwickeln können. Bislang kannte man den Cyber-Krieg nur aus James Bond „Tomorrow Never Dies" oder „Terminator". Was bisher die Domäne Hollywoods war, scheint nun Realität."

In diesem Zusammenhang richten die unterfertigten Abgeordneten an die Bundesministerin für Inneres folgende

Anfrage:

1. Wer ist in Ihrem Ressort zur Bekämpfung von „Cyber-Attacken" zuständig?
2. Wie viele Personen arbeiten in diesem Bereich in Ihrem Ressort?
3. Welche Stellen in Österreich beschäftigen sich noch mit der Bekämpfung von Cyber-Attacken und der Sicherheit der digitalen Verwaltung?
4. Gibt es in diesem Bereich eine Zusammenarbeit mit anderen Stellen?
5. Wenn ja, mit wem?
6. Wie viele derartige Angriffe auf Einrichtungen Ihres Ressorts gab es in den letzten drei Jahren?
7. Welcher Schaden ist dadurch entstanden?
8. Konnte man die Angreifer lokalisieren?
9. Wenn ja, wer war verantwortlich?
10. Warum sind die österreichischen Systeme nicht besser geschützt?
11. Was planen Sie zur Verbesserung des Schutzes Ihres Ressorts?
12. Was ist auf Regierungsebene dazu geplant?
13. Arbeiten Sie in diesem Zusammenhang mit externen Experten zusammen?
14. Wenn ja, mit wem?
15. Wo und in welcher Art und Weise werden besonders wichtige Daten in Ihrem Haus gespeichert?
16. Gibt es externe Sicherheitsspeicher?
17. Wenn ja, wo?