



Präsentation einer Cyber-Risikomatrix: KSÖ-Generalsekretär Christian Kunstmann, Innenministerin Johanna Mikl-Leitner, Sicherheitsexperte Richard Clarke.

# Nationale Cybersecurity-Strategie

Das Innenministerium will Betreiber kritischer Infrastruktur in die staatliche Sicherheitspolitik einbinden. Auftakt war eine Konferenz, an der 90 Entscheidungsträger aus der Wirtschaft teilnahmen.

Cyber-Angriffe finden zwar virtuell statt, haben aber höchst reale Auswirkungen. Und die Anzahl der Angriffe steigt rasant. Dennoch werden die damit verbundenen Gefahren oft noch stark unterschätzt“, sagte Innenministerin Mag. Johanna Mikl-Leitner bei der Cybersecurity-Konferenz am 20. September 2011 im Innenministerium. „Nur mit vereinten Kräften und durch einen Schulterschluss zwischen Politik, Verwaltung, Wirtschaft und Wissenschaft können wir uns wirkungsvoll dagegen schützen. Cybersecurity ist damit zum Top-Thema geworden, das uns alle etwas angeht“, betonte Mikl-Leitner.

Mit dem *Kuratorium Sicheres Österreich (KSÖ)* will das Bundesministerium für Inneres das Bewusstsein der Verantwortungsträger schärfen und die Möglichkeit dafür schaffen, strategisch relevante Betreiber kritischer Infrastruktur in die gesamtstaatliche Sicherheitspolitik einzubinden. Die Cy-

bersecurity-Konferenz, an der rund 90 Entscheidungsträger aus der Wirtschaft teilnahmen, war Auftakt dazu. Außerdem soll eine nationale Cyber-Strategie erarbeitet werden – als Teil der österreichischen Sicherheitsstrategie.

**Cyber-Risikomatrix.** Um das bestehende Bedrohungsszenario zu verdeutlichen, hat das KSÖ im Vorfeld der Konferenz von Experten das Risikopotenzial von Cyber-Gefahren für Österreich analysieren lassen. Das Ergebnis ist eine Cyber-Risikomatrix, die auch in die Erstellung der nationalen Cybersecurity-Strategie einfließen soll.

„Wie uns die Cyber-Risikomatrix zeigt, besteht akuter Handlungsbedarf. Daher habe ich als Sicherheitsministerin gemeinsam mit dem KSÖ bereits die Schritte für den weiteren Prozess definiert. Dazu gehören eine Ausbildungsoffensive, um auch die Forschung in diesem Bereich voranzutreiben, die Einrichtung einer Cyber-Platt-

form zum institutionalisierten Austausch zwischen Behörden, Wirtschaft und Politik und die Durchführung eigener Cyber-Sicherheitsübungen mit besonderem Fokus auf verschiedene Bereiche kritischer Infrastruktur“, erläuterte Mikl-Leitner.

Cybersecurity- und Antiterror-Experte Richard Clarke (USA) unterstrich als Gastsprecher der Konferenz den Handlungsbedarf und betonte die Wichtigkeit nationaler Cyber-Strategien und internationaler Kooperationen. „Die Herausforderungen, mit denen wir uns konfrontiert sehen, enden nicht an nationalen Grenzen, sie sind globaler Natur. Cybercrime, Hacker-Angriffe, Cyber-Spionage und Cyber-War sind die vier Themen, die das 21. Jahrhundert in diesem Bereich bestimmen werden“, sagte Clarke. „Wir können uns nur durch differenzierte gesamtstaatliche Cyber-Strategien und internationale Kooperationen wirkungsvoll dagegen wappnen.“