

Vortrag an den Ministerrat

Maßnahmenpaket zur verbesserten Bekämpfung von Cyber-Kriminalität in Österreich

Die globale Vernetzung sowie die zunehmende Digitalisierung hat konkrete Auswirkungen auf die Cyber-Kriminalität, wie die Kriminalitätsstatistiken belegen. Sicherheitsrelevante Schwachstellen von neuentwickelten Soft- und Hardwarelösungen sowie die nicht immer vorhandene Sachkenntnis der AnwenderInnen werden verstärkt von Kriminellen für widerrechtliche Zwecke ausgenutzt.

So werden durch die technischen Entwicklungen sowie der mittlerweile hohen Bandbreite, die nahezu jedermann zur Verfügung steht, die Angriffsszenarien immer komplexer und die Anzahl der Opfer immer höher. Während verschlüsselte Kommunikationsdienste und –services den sicheren Austausch von Meinungen und Information unter Wahrung der Privatsphäre ermöglichen und Schutz von sensiblen Daten bieten, können Verschlüsselungstechniken und versteckte Services wie z.B. im Darknet Tätern die Möglichkeit verschaffen sich unentdeckt zu vernetzen sowie deren Expertise zu vermarkten. Unter dem Motto „Crime as a Service“ werden kriminelle Werkzeuge, technische Fachkenntnisse und Dienstleistungen angeboten, welche auch für nicht IT-affine Personen nahezu professionell anwendbar sind. Daraus ergibt sich, dass klassische Delikte in der realen Umgebung immer mehr in den Hintergrund treten und sich in den virtuellen Cyberraum verlagern.

Die Sicherheitsbehörden müssen sich diesen Entwicklungen immer wieder anpassen, modernen Techniken öffnen und zu Nutze machen.

Auf Grundlage des aktuellen Regierungsprogramms 2020 – 2024, welches die nachhaltige und effiziente Bekämpfung der Cyberkriminalität vorsieht, ist nunmehr beabsichtigt ein Maßnahmenpaket zur verbesserten Bekämpfung der Cyberkriminalität zu schnüren, welches folgende Schwerpunkte umfasst:

- Schaffung eines Ausbildungscampus für IT-SpezialistInnen in polizeilichen und kriminalpolizeilichen Tätigkeitsbereichen.
Damit die entsprechenden Personalressourcen in IT-orientierten Polizeibereichen entsprechend zur Verfügung stehen, ist die Einrichtung eines Ausbildungscampus für IT-SpezialistInnen dringend notwendig. Die Ausbildung soll die Bereiche digitale Ermittlungen und digitale Forensik umfassen und für technisch versierten Nachwuchs in der Zentralstelle als auch in den Bundesländern sorgen.
- Weitere Implementierung von IT-Themen in die polizeiliche Grundaus- und Fortbildung zur Schaffung eines technischen Basisverständnisses in der täglichen Polizeiarbeit inklusive verstärkter Sensibilisierung im Umgang mit Cybercrime betroffenen Opfern sowie Opfern von „Hass im Netz“
- Weiterentwicklung der bestehenden Cyber-Bereiche in den Landeskriminalämtern und Stärkung dieser durch Zuführung von IT-Experten auch im regionalen Bereich.
- Weiterentwicklung des Cybercrime Competence Centers im Bundeskriminalamt.
 - Sukzessive Personalzuführungen von 60 IT-ErmittlerInnen bzw. IT-ExpertInnen in den folgenden Jahren zur Erhöhung der Cyberfähigkeiten der Zentralstelle, insbesondere im Ermittlungs-, Forensik- und Wissenschafts-bereich.
 - Einrichtung einer zentralen Anlaufstelle für Anfragen an Social Media & Online Service Provider für polizeiliche Ermittlungszwecke.
- Schaffung einer Kriminalpolizeilichen IT-Infrastruktur (KIS).
- Stärkung des Bewusstseins, dass das Offizialprinzip (Strafverfolgungspflicht) auch online gilt (Internet ist kein rechtsfreier Raum).

- Erstellung eines Strategiekonzepts zur verbesserten Bekämpfung von Cybercrime in Österreich (z.B. Verbesserung der Bekämpfung von Cybercrime).
- Verbesserung der Aufklärungsquote.
- Reduzierung von Cybercrime durch umfassende Prävention.

Mit dieser Maßnahme allfällig verbundene budgetäre Auswirkungen werden aus dem laufenden Ressortbudget bedeckt.

Ich stelle daher den

Antrag,

die Bundesregierung wolle diesen Maßnahmenkatalog zur Kenntnis nehmen und im o.a. Sinne beschließen.

20. Oktober 2020

Karl Nehammer, MSc
Bundesminister