

ANFRAGE

des Abgeordneten Michael Gmeindl
an den Bundesminister für Inneres
betreffend **Cyberkriminalität, Krypto-Betrug, internationale Scam-Netzwerke und der Schutz der österreichischen Bevölkerung vor organisierter Internet-kriminalität**

Cyberkriminalität, organisierter Internetbetrug, Krypto-Betrug, Social Engineering sowie internationale Scam-Netzwerke stellen eine stetig wachsende Bedrohung für die Sicherheit der österreichischen Bevölkerung dar. Immer häufiger werden Bürger durch professionell organisierte Tätergruppierungen mittels täuschend echter Identitäten, manipulierter Dokumente, Phishing-Angriffen oder Kryptowährungstransaktionen um erhebliche Vermögenswerte gebracht.

Besonders problematisch erscheint dabei, dass sich zahlreiche Täter außerhalb Europas befinden und moderne Kommunikations- sowie Blockchain-Technologien nutzen, um ihre Identität zu verschleiern und Geldströme international zu verlagern. Für viele Geschädigte entsteht dadurch der Eindruck, dass Ermittlungen bei grenzüberschreitenden Cyberdelikten oftmals nur eingeschränkt oder gar nicht erfolgreich geführt werden können.

Darüber hinaus wächst in der Bevölkerung die Sorge, dass Österreich aufgrund seiner wirtschaftlichen und technischen Infrastruktur zunehmend auch als Drehscheibe für internationale Geldwäsche, Krypto-Betrug oder sonstige Formen organisierter Cyberkriminalität missbraucht werden könnte.

Vor diesem Hintergrund stellt sich die Frage, welche Erkenntnisse den Sicherheitsbehörden über das tatsächliche Ausmaß dieser Kriminalitätsform vorliegen, welche Maßnahmen bereits gesetzt wurden und wie die österreichische Bevölkerung künftig besser vor derartigen Straftaten geschützt werden soll.

In diesem Zusammenhang richtet der unterfertigte Abgeordnete an den Bundesminister für Inneres nachstehende

Anfrage

1. Wie viele Anzeigen wegen Cyberkriminalität wurden seit dem Jahr 2020 registriert? (Bitte um Aufschlüsselung nach Jahren)
 - a. Wie viele davon betrafen Krypto-Betrug?
 - b. Wie viele davon betrafen Social-Engineering-Angriffe?
 - c. Wie viele davon betrafen Phishing-, Smishing- oder ähnliche Betrugsformen?
2. Wie hoch war seit 2020 die Aufklärungsquote bei Cyberkriminalität? (Bitte um Aufschlüsselung nach Jahren)
 - a. Wie hoch war die Aufklärungsquote bei Krypto-Betrugsfällen?
3. Wie hoch war der den Sicherheitsbehörden bekannte finanzielle Gesamtschaden durch Cyberkriminalität seit 2020? (Bitte um Aufschlüsselung nach Jahren)

- a. Wie hoch war davon der Schaden durch Krypto-Betrug?
 - b. Wie hoch war davon der Schaden durch Social Engineering?
4. Welche Herkunftsländer oder Regionen konnten seit 2020 bei abgeschlossenen Ermittlungen als Ursprung entsprechender Cyberdelikte festgestellt werden? (Bitte um Aufschlüsselung nach den häufigsten Herkunftsstaaten)
- b. Welche Formen organisierter Kriminalität konnten dabei festgestellt werden?
5. Welche Erkenntnisse liegen Ihrem Ressort über international organisierte Scam-Netzwerke vor?
 - a. Welche Staaten stellen dabei aus Sicht Ihres Ressorts besondere Brennpunkte dar?
 - b. Welche internationalen Kooperationen bestehen zur Bekämpfung dieser Netzwerke?
6. Welche Erkenntnisse liegen Ihrem Ressort über die Täterstruktur (Alter, Geschlecht, Nationalität, sozialer Hintergrund, Tatmotivation) der an derartigen Straftaten beteiligten Personen vor?
 - a. Wie viele Personen waren seit 2020 unmittelbar an derartigen Straftaten beteiligt? (Bitte um Aufschlüsselung nach Jahren)
 - b. Wie viele Personen waren mittelbar beteiligt, etwa durch Geldwäsche, Bereitstellung technischer Infrastruktur oder Unterstützungshandlungen? (Bitte um Aufschlüsselung nach Jahren)
7. Welche Maßnahmen setzt Ihr Ressort derzeit, um Cyberangriffe, Krypto-Betrug, Social Engineering, Phishing sowie vergleichbare Betrugsformen zum Schutz der österreichischen Bevölkerung zu verhindern?
8. Welche personellen und technischen Ressourcen stehen den österreichischen Sicherheitsbehörden derzeit zur Bekämpfung von Cyberkriminalität zur Verfügung?
 - a. Wurden diese seit 2020 ausgebaut?
 - i. Wenn ja, in welchem Umfang?
 - ii. Wenn nein, warum nicht?
9. Welche Möglichkeiten bestehen für österreichische Ermittlungsbehörden, Kryptowährungstransaktionen im Rahmen strafrechtlicher Ermittlungen nachzuverfolgen?
 - a. Welche spezialisierten technischen Systeme kommen dabei zum Einsatz?
 - b. Besteht eine Zusammenarbeit mit privaten Blockchain-Analyseunternehmen?
10. Wie viele internationale Rechtshilfeersuchen im Zusammenhang mit Cyberkriminalität wurden seit 2020 gestellt? (Bitte um Aufschlüsselung nach Jahren)
 - a. In wie vielen Fällen kam es zu einer erfolgreichen Zusammenarbeit mit ausländischen Behörden?
11. Welche Maßnahmen setzt Ihr Ressort, um Geldwäsche im Zusammenhang mit Kryptowährungen und virtuellen Vermögenswerten zu verhindern?
12. Welche Informations- und Präventionskampagnen wurden seit 2020 durchgeführt, um die österreichische Bevölkerung über Cyberkriminalität, Krypto-Betrug, Phishing und Social Engineering aufzuklären?
 - a. Welche finanziellen Mittel wurden dafür eingesetzt?
 - b. Wie beurteilt Ihr Ressort deren Wirksamkeit?
13. Sieht Ihr Ressort angesichts der steigenden Zahl internationaler Cyberangriffe zusätzlichen legislativen oder organisatorischen Handlungsbedarf?
 - a. Wenn ja, welche konkreten Maßnahmen werden vorbereitet?
 - b. Wenn nein, weshalb nicht?

14. Welche konkreten Schritte werden Sie setzen, um den Schutz der österreichischen Bevölkerung vor organisierter Cyberkriminalität künftig nachhaltig zu verbessern?

Alles kann

(Michael)

[Signature]

[Signature]

[Signature]

	Unterzeichner	Parlamentsdirektion
	Datum/Zeit-UTC	2026-10-13T16:02:48+02:00
Prüfinformation	Dieses Dokument wurde elektronisch besiegelt. Informationen zur Prüfung des elektronischen Siegels und des Ausdrucks finden Sie unter: https://www.parlament.gv.at/siegel	