793/AB
vom 06.04.2020 zu 742/J (XXVII. GP)

Bundesministerium
Inneres

Karl Nehammer, MSc
Bundesminister

Herrn
Präsidenten des Nationalrates
Mag. Wolfgang Sobotka
Parlament
1017 Wien

Geschäftszahl: 2020-0.094.750

Wien, am 6. April 2020

Sehr geehrter Herr Präsident!

Der Abgeordnete zum Nationalrat Laimer, Genossinnen und Genossen haben am 6. Februar 2020 unter der Nr. **742/J** an mich eine schriftliche parlamentarische Anfrage betreffend „Internetbetrug" gerichtet.

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

Die in der Anfrage angeführten Zahlen für das Kalenderjahr 2019 werden in Erfüllung des parlamentarischen Interpellationsrechtes vorgelegt. Es wird ausdrücklich darauf hingewiesen, dass Experten aus der Wissenschaft im Rahmen des Projektes „Kriminalstatistikneu“ festgestellt haben, dass Aussagen über die Sicherheitslage und die Kriminalitätsbelastung aus quartalsmäßigen und halbjährlichen Zahlenwerten nicht möglich sind, weil daraus gezogene Schlüsse einer wissenschaftlichen Überprüfung nicht standhalten. Es wird auch darauf hingewiesen, dass es sich hier um Rohdaten handelt, die noch nicht der Qualitätskontrolle und weiteren Prüfmechanismen unterzogen wurden. Ergo können aus dem Zahlenmaterial weder die gegenwärtige kriminalpolizeiliche Lage noch Trends bzw. Aussagen über die Sicherheitslage und die Kriminalitätsbelastung abgeleitet werden.

Zur Frage 1:

- *Wie definiert das Bundesministerium für Inneres den sogenannten Internetbetrug?*

In der Polizeilichen Kriminalstatistik werden die Delikte mit der Örtlichkeit „Internet“, die in den §§ 146 bis 148 Strafgesetzbuch (StGB) angeführt sind (Betrug, schwerer Betrug und gewerbsmäßiger Betrug), als Internetbetrug bezeichnet.

Zur Frage 2:

- *Auf Grund welcher Systematik werden die einzelnen Delikte dem Kapitel „Internetbetrug" zugeordnet?*

Da es sich bei Internetbetrug um Betrug handelt, wurden der Betrug (§ 146 StGB), der schwere Betrug (§ 147 StGB) und der gewerbsmäßige Betrug (§ 148 StGB) zugeordnet.

Zur Frage 3:

- *Auf Grund welcher Ereignisse kann die hohe Summe an Delikten im Jahre 2009 im Bereich des Internetbetrugs erklärt werden?*

Das Jahr 2009 beinhaltet zwei Internetbetrugsstraftaten mit insgesamt 6.624 Einzeldelikten.

Zur Frage 4:

- *In welchen Bereichen des Internetbetrugs wurden im Jahre 2019 besondere Steigerungen verzeichnet?*

Im Jahr 2019 gab es an absoluten Zahlen folgende Steigerungen im Bereich des Internetbetruges:

Internetbetrug - 2019 - Österreich - Anzahl der Straftaten				
	Jahr 2018	**Jahr 2019**	**Veränder-ung absolut**	**Veränder-ung Prozent**
Bestell-/Warenbetrug	9.379	10.473	1.094	+ 11,7%
Sonstiger Betrug	103	707	604	+ 590,2%
Trickbetrug	442	917	475	+ 107,5%
Betrug mit unbaren Zahlungs-	747	1.140	393	+ 52,6%

mitteln				
Vorauszahlungsbetrug	1.245	1.522	277	+ 22,2%
Kontoeröffnungs/ Überweisungs-betrug	697	927	230	+ 33,0%
Dienstleistungs-/Zechbetrug	0	224	224	
Darlehens-/Kreditbetrug	171	292	121	+ 70,8%
Anlagebetrug	169	285	116	+ 68,6%
Urkunden-/Beweismittelbetrug	11	27	16	+ 145,5%
Versicherungsbetrug	2	3	1	+ 50,0%

Zur Frage 5:

- *Welche Bundesländer sind in welchem Ausmaß davon betroffen (detailliert nach Bundesland und Delikt)?*

Internetbetrug - 2019 - Anzahl der Straftaten				
	Jahr 2018	**Jahr 2019**	**Veränder-ung absolut**	**Veränder-ung Prozent**
Burgenland	**288**	**380**	**92**	**31,9%**
§ 146 StGB (Betrug)	255	336	81	31,8%
§ 147 StGB (Schwerer Betrug)	17	34	17	100,0%
§ 148 StGB (Gewerbsmäßiger Betrug)	16	10	-6	-37,5%
Kärnten	**681**	**801**	**120**	**17,6%**
§ 146 StGB (Betrug)	613	704	91	14,8%
§ 147 StGB (Schwerer Betrug)	43	68	25	58,1%
§ 148 StGB (Gewerbsmäßiger Betrug)	25	29	4	16,0%
Niederösterreich	**2.036**	**2.628**	**592**	**29,1%**
§ 146 StGB (Betrug)	1.678	2.241	563	33,6%
§ 147 StGB (Schwerer Betrug)	211	267	56	26,5%
§ 148 StGB (Gewerbsmäßiger Betrug)	147	120	-27	-18,4%

Oberösterreich	**1.849**	**2.600**	**751**	**40,6%**
§ 146 StGB (Betrug)	1.588	2.211	623	39,2%
§ 147 StGB (Schwerer Betrug)	157	260	103	65,6%
§ 148 StGB (Gewerbsmäßiger Betrug)	104	129	25	24,0%
Salzburg	**680**	**959**	**279**	**41,0%**
§ 146 StGB (Betrug)	618	807	189	30,6%
§ 147 StGB (Schwerer Betrug)	46	121	75	163,0%
§ 148 StGB (Gewerbsmäßiger Betrug)	16	31	15	93,8%
Steiermark	**1.577**	**2.071**	**494**	**31,3%**
§ 146 StGB (Betrug)	1.346	1.740	394	29,3%
§ 147 StGB (Schwerer Betrug)	151	182	31	20,5%
§ 148 StGB (Gewerbsmäßiger Betrug)	80	149	69	86,3%
Tirol	**965**	**1.284**	**319**	**33,1%**
§ 146 StGB (Betrug)	802	1.132	330	41,1%
§ 147 StGB (Schwerer Betrug)	95	126	31	32,6%
§ 148 StGB (Gewerbsmäßiger Betrug)	68	26	-42	-61,8%
Vorarlberg	**460**	**692**	**232**	**50,4%**
§ 146 StGB (Betrug)	391	584	193	49,4%
§ 147 StGB (Schwerer Betrug)	50	84	34	68,0%
§ 148 StGB (Gewerbsmäßiger Betrug)	19	24	5	26,3%
Wien	**4.792**	**5.416**	**624**	**13,0%**
§ 146 StGB (Betrug)	4.126	4.739	613	14,9%
§ 147 StGB (Schwerer Betrug)	478	418	-60	-12,6%
§ 148 StGB (Gewerbsmäßiger Betrug)	188	259	71	37,8%

Zur Frage 6:

- *Welche Maßnahmen wurden von Ihnen im Bereich der Cyberkriminalität insgesamt gesetzt? (detaillierte Darstellung)?*

Wie bereits in der Beantwortung der gleichlautenden Frage 1 der parlamentarischen Anfrage 2294/J XXVI. GP vom 16. November 2018 (2279/AB XXVI. GP) ausgeführt wurde, werden im „Cybercrime Competence Center“ (C4) des Bundesministeriums für Inneres laufend Maßnahmen gesetzt, um den europäischen und internationalen Austausch im Bereich der Bekämpfung von Cybercrime zu verstärken. Dies betrifft vornehmlich die Zusammenarbeit mit dem European Cybercrime Centre (EC3) von Europol, die Leitung von und Mitarbeit bei Operational Actions (OAs) aus den Operational Action Plans (OAPs) im Rahmen der European Cybercrime Task Force (EUCTF), die Beteiligung an multinationalen Joint Investigation Teams (JITs), die Mitarbeit in der European Cybercrime Training and Education Group (ECTEG), die Beteiligung an der European multidisciplinary platform against criminal threats (EMPACT), die Mitveranstaltung des Symposiums „Neue Technologien“, die Mitarbeit beim European malware analysis system (EMAS) – einem Tool von Europol zur Klassifizierung von Schadsoftware, die Mitveranstaltung des jährlichen DACH-Symposiums „Neue Technologien“, sowie die Beteiligung am G7 24/7 Netzwerk.

Die oben angeführten Maßnahmen stärken die europäische und internationale Zusammenarbeit in vielen Bereichen wie z.B. internationale Ermittlungen, Spezialisierungen im Bereich Darknet, Kryptowährungen, Ransomware, KFZ-Forensik oder Ausbildung.

Unabhängig von dieser Teilnahme an zahlreichen internationalen operativen Einsätzen wurden als Maßnahmen entsprechende Veranstaltungen und Projekte organisiert bzw. es wurde daran teilgenommen:

- Gemeinsame Veranstaltungen und Vorträge zur Bewusstseinsbildung mit der Wirtschaftskammer Österreich (WKO) und dem Kuratorium Sicheres Österreich (KSÖ) mit dem Schwerpunkt Schutz von Klein- und Mittelbetrieben (KMU) vor Cybercrime;
- Kooperationsvereinbarungen mit der WKO im Rahmen der Initiative Geminsam.Sicher z.B. zur Schaffung von Standards – „Certified Data & IT Security Expert“ oder zum Betrieb einer Cyber-Security-Hotline für Wirtschaftstreibende bei der WKO.
- Symposium „Neue Technologien“, veranstaltet vom Bundeskriminalamt gemeinsam mit dem Landeskriminalamt (LKA) Bayern, dem LKA Baden Württemberg, dem Bundesamt für Polizei Schweiz (FEDPOL) und unter Beteiligung von Universitäten, Hochschulen und Unternehmen;
- Zusammenarbeit mit Europol z.B. im Rahmen des European Expert Forum;
- United Nations Office on Drugs and Crime (UNODC) – Zusammenarbeit des Bundeskriminalamtes zum Thema Onlinemissbrauch von Kindern;

— Zahlreiche nationale und internationale Projekte z.B. Social Media Crime; BitCrime und Internet of Threats im Rahmen von KIRAS; Fortsetzung des ISF Projekts CyberKids in der Linienorganisation; Fahrzeugforensik im Rahmen von ISF (Fonds für die innere Sicherheit);

Über diese Beantwortung hinausgehend darf ich überdies auf die mit 1. Dezember 2018 im Bundeskriminalamt eingerichtete „Kompetenzstelle virtuelle Währungen und Kryptowährungen“ hinweisen. Diese Kompetenzstelle verfolgt den Zweck, dem Phänomen der virtuellen Währungen und Kryptowährungen aus kriminalpolizeilicher Sicht zu begegnen. Ergebnisse der Kompetenzstelle sind unter anderem die Teilnahme am Horizon 2020 Projekt „Titanium“ sowie den Kiras Projekten „Bitcrime“ und „Virtcrime“, deren Erkenntnisse in die Ermittlungsarbeit einfließen.

Seit dem Jahr 2018 wird ein starker Anstieg massenhaft ausgesandter E-Mails verzeichnet, deren Inhalt versuchte und vollendete Delikte nach § 144 und 145 StGB (Erpressung und schwere Erpressung) sind. Zur Bekämpfung dieser Deliktsform wurde am 1. Februar 2019 im Bundeskriminalamt die „ARGE Erpressungsmail“ eingerichtet und erlassgemäß eine einheitliche und strukturierte Regelung der Vorgehensweise bei der Anzeigenaufnahme, Protokollierung, Analyse und Ermittlung verfügt.

Zur Frage 7:

- *Welche Maßnahmen wurden im Bereich Internetbetrug von ihrem Ministerium gesetzt und welche Maßnahmen planen Sie?*

Wie bereits in der Beantwortung der gleichlautenden Frage 2 der parlamentarischen Anfrage 2294/J XXVI. GP vom 16. November 2018 (2279/AB XXVI. GP) ausgeführt wurde, wird - neben der Einbindung in der Gesamtstrategie des Bundesministeriums für Inneres - im Bereich Bekämpfung des Internetbetrugs unter anderem auf die internen IT-Schulungen gesetzt.

Bei diesen Schulungen werden auch neue Themenfelder wie das Darknet und der Umgang mit Kryptowährungen abgebildet. Zusätzlich wird auf eine intensive Zusammenarbeit mit dem Privatsektor im Rahmen eines Private-Public-Partnership gesetzt. In diesem Zusammenhang wurde die E-Commerce Action Week (im Juni 2018; Lead Österreich im Rahmen von EUROPOL-EMPACT) durchgeführt. Private-Public Partnerschaften wie zum Beispiel „GEMEINSAM.SICHER“ oder „Unternehmen Sicherheit“ mit der WKO bieten regelmäßig die Gelegenheit, die Bevölkerung und Unternehmen zu informieren. In der Vorweihnachtszeit wird schwerpunktmäßig die Bevölkerung vom Fachbereich

Internetbetrug medial über das Thema Betrug beim Kauf von Waren im Internet aufgeklärt.

Darüber hinaus wird die internationale Zusammenarbeit im Zuge des EU Projektes P3 (Privat Public Partnership) proaktiv gefördert. Es handelt sich um ein Projekt, welches die Kooperation zwischen Ermittler und Experten sowohl der Sicherheitsbehörden als auch der Privatwirtschaft zur Bekämpfung von Internetbetrug durch gemeinsame Trainings und Webinars stärkt. Das Bundeskriminalamt ist Mitkoordinator des Projektes.

Gemeinsam mit der Wirtschaftskammer werden Maßnahmen zur Awarenessbildung und Prävention bei Unternehmen gesetzt sowie Veranstaltungen, insbesondere für den Onlinehandel, durchgeführt.

Zur Frage 8:

- *In welchem Ausmaß wird die Prävention und Information der Bürger und Bürgerinnen verbessert?*

Mit Hinweis auf die Beantwortung der gleichlautenden Frage 3 der parlamentarischen Anfrage 2294/J XXVI. GP vom 16. November 2018 (2279/AB XXVI. GP), in der die geplante bundesweite Ausbildung theamtisiert wurde, darf ich berichten, dass seit 2019 Exekutivbedienstete in ganz Österreich speziell im Bereich „Kriminalprävention im Bereich Computer- und Internetkriminalität“ ausgebildet werden. Diese führen kostenlose Beratungen und Vorträge durch und können über die Landeskriminalämter und die Kooperation mit dem Bundesministerium für Digitalisierung und Wirtschaftsstandort/Verein fit4internet angefordert werden.

In der Ausbildung der Präventionsbediensteten wird ein spezielles Augenmerk auf Internetbetrug gelegt, die Exekutivbediensteten werden von Fachexperten des Vereins Watchlist Internet und Internet Ombudsmann geschult.

Eine enge Kooperation mit Watchlist Internet, Internet Ombudsmann, Wirtschaftskammer Österreich, Bundesministerium für Digitalisierung und Wirtschaftsstandort und Gemeinsam.Sicher ermöglicht, dass aktuelle Informationen ausgetauscht und rasch verbreitet werden. Unterstützt werden diese Schritte durch die jeweiligen Pressestellen, Social-Media-Kanäle und interne strukturelle Maßnahmen.

Zur Frage 9:

- *Planen Sie eine zusätzliche Hilfestellung für Bürger und Bürgerinnen, die bei einem Internetbetrug unschuldig zu Verdächtigen werden?*

Wie bereits in der Beantwortung der gleichlautenden Frage 4 der parlamentarischen Anfrage 2294/J XXVI. GP vom 16. November 2018 (2279/AB XXVI. GP) ausgeführt wurde, finden sich auf der Internetseite des Bundeskriminalamtes zu diesem Themenkomplex zahlreiche Präventionstipps. Unter anderem sind dort ausführliche Informationen zu derartigen Sachverhalten abrufbar. Wie zum Beispiel die Informationsblätter zum „SCHUTZ VOR BESTELL-, WAREN- UND DIENSTLEISTUNGSBETRUG“, „SCHUTZ VOR DATEN-DIEBSTAHL“, „SCHUTZ VOR PHISING“ sowie „SCHUTZ VOR RECHNUNGSLEGUNGS-BETRUG“.

Zur Frage 10:

- *Wird der Bereich zur Bekämpfung von Cyberkriminalität personell und finanziell aufgestockt werden:*
  a. *Wenn ja: In welchem Ausmaß (detaillierte Darstellung)*
  b. *Wenn nein: Warum nicht?*

Im Regierungsprogramm ist unter anderem auch die Erstellung eines Strategiekonzeptes zur verbesserten Bekämpfung von Cyberkriminalität festgelegt.

Im Hinblick auf das noch nicht beschlossene Bundesfinanzgesetz 2020 ersuche ich um Verständnis, dass ich dazu keine weiteren detaillierten Angaben machen kann.

Karl Nehammer, MSc

	Datum/Zeit	2020-04-06T16:44:09+02:00
	Aussteller-Zertifikat	CN=a-sign-corporate-light-02,OU=a-sign-corporate-light-02,O=A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH,C=AT
	Serien-Nr.	1710479
Prüfinformation	Informationen zur Prüfung des elektronischen Siegels bzw. der elektronischen Signatur finden Sie unter: https://www.signaturpruefung.gv.at. Eine Verifizierung des Ausdruckes kann bei der ausstellenden Behörde/Dienststelle erfolgen.	
Hinweis	Dieses Dokument wurde amtssigniert.	

REPUBLIK ÖSTERREICH Parlamentsdirektion SIEGEL	**Unterzeichner**	Parlamentsdirektion
	Datum/Zeit-UTC	2020-04-06T16:50:08+02:00
	Prüfinformation	Informationen zur Prüfung des elektronischen Siegels und des Ausdrucks finden Sie unter: https://www.parlament.gv.at/siegel
Hinweis	Dieses Dokument wurde elektronisch besiegelt.	