2632/AB
vom 21.03.2019 zu 2656/J (XXVI.GP)

Bundesministerium
Inneres

bmi.gv.at

Herbert Kickl
Bundesminister

Herrn
Präsidenten des Nationalrates
Mag. Wolfgang Sobotka
Parlament
1017 Wien

Geschäftszahl: BMI-LR2220/0105-II/2019

Wien, am 8. März 2019

Sehr geehrter Herr Präsident,

die Nationalrätin Mag. Beate Meinl-Reisinger, MES, Kolleginnen und Kollegen haben am 22. Jänner 2019 unter der Nr. **2656/J** an mich eine schriftliche parlamentarische Anfrage betreffend „Folgeanfrage Maßnahmen gegen Cyberkriminalität" gerichtet.

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

Zu den Fragen 1, 1a und 2:

- *Wie viele Personen sind im „Cyber Security Center" (CSC) des Bundesamtes für Verfassungsschutz und Terrorismusbekämpfung beschäftigt?*
- *Wie viele dieser Personen sind aktiv mit der Aufklärung von Straftaten im Bereich Cyberkriminalität befasst?*
- *Wie viel Budget hat das „Cyber Security Center" (CSC) des Bundesamtes für Verfassungsschutz und Terrorismusbekämpfung zur Verfügung?*

Aus sicherheits- und kriminaltaktischen Überlegungen muss von einer Beantwortung dieser Fragen Abstand genommen werden (vgl. Beantwortung der Fragen 4 und 6 der parlamentarischen Anfrage 1823/J vom 5. Oktober 2018 – 1837/AB XXVI. GP).

Zur Frage 3:

- *Wie viele Personen sind im "Cybercrime Competence Center" (C4) des Bundeskriminalamtes beschäftigt?*

Im C4 sind derzeit tätig:

Stammpersonal	45 Personen
Keine Planstellen, temporäre Dienstzuteilungen	8 Personen
auf Payroll	7 Personen
Keine Planstelle, temporäre Verwaltungspraktikanten	5 Personen
Gesamt	**65 Personen**

Zur Frage 3a:

- *Wie viele dieser Personen sind aktiv mit der Aufklärung von Straftaten im Bereich Cyberkriminalität befasst?*

Von diesen Personen sind aktiv mit der Aufklärung von Straftaten im Bereich Cyberkriminalität befasst:

Ermittelnde Beamte	17
IT Beweissicherung	16

Zur Frage 4:

- *Wie viel Budget hat das "Cybercrime Competence Center" (C4) des Bundeskriminalamtes zur Verfügung?*

Kostenstellen werden jeweils für gesamte Abteilungen und nicht für deren einzelne Teilbereiche ausgewiesen. Das für die Agenden des C4 benötigte Budget ist aus dem Gesamtbudget der Abteilung zu bedecken und kann somit nicht genau beziffert werden (vgl. Beantwortung der Frage 9 der parlamentarischen Anfrage 1823/J vom 5. Oktober 2018 – 1837/AB XXVI. GP).

Zu den Fragen 5, 5a, 5b und 6:

- *Wie sieht das genaue Aufgabenprofil des:*
- *"Cyber Security Center" (CSC) des Bundesamtes für Verfassungsschutz und Terrorismusbekämpfung aus?*
- *"Cybercrime Competence Center" (C4) des Bundeskriminalamtes aus?*
- *Inwiefern unterscheiden sich die beiden Entitäten hinsichtlich des Aufgabenprofils bzw wie sieht die Aufgabenverteilung zwischen den beiden Einrichtungen im Bereich Ermittlung, Aufklärung, Prävention im Bereich der Cyberkriminalität aus?*

Das Cyber Security Center (CSC) wurde mit dem Fokus Schutz kritischer Infrastruktur und Schutz der verfassungsmäßigen Einrichtungen gegründet und legt den Schwerpunkt auf Cyber-Sicherheit und Prävention.

Das CSC übernimmt folgende Aufgaben:

- Operative Koordinierungsstelle für Meldungen über jede Form von Angriffen auf Computersysteme von verfassungsmäßigen Einrichtungen und kritischen Infrastrukturen (§ 4 Polizeiliches Staatsschutzgesetz-PStSG) und
- Beratung von Betreibern kritischer Infrastruktur und verfassungsmäßigen Einrichtungen (§ 7 PStSG). Auf dieser Basis werden z.B. Frühwarnungen und Information verteilt sowie bewusstseinsbildende Vorträge (Awareness-Veranstaltungen) angeboten.
- Leitung der Operativen Koordinierungsstrukturen und deren inneren Kreises (§ 7 Netz- und Informationssystemsicherheitsgesetz – NISG).
- Wahrnehmung der Aufgaben der staatlichen Meldesammelstelle für Pflichtmeldung (3. Abschnitt NISG).
- Zentrale Anlaufstelle („Single Point of Contact" bzw. „SPoC") für andere europäische NIS-Behörden (§ 6 NISG).
- Sicherstellung der Einhaltung der verordneten Mindestsicherungsstandards durch die Betreiber wesentlicher Dienste und digitale Diensteanbieter (§ 17 Abs. 4 NISG).
- Vorbereitung der Verordnung der Kriterien für die Feststellung von qualifizieren Stellen (§§ 17 und 21 NISG) sowie bescheidmäßiges Feststellen der Eignung als qualifizierte Stelle in diesem Sinne auf Antrag (§ 18 NISG).

Das Cybercrime Competence Center (C4) wurde im Jahr 2011 zur Bekämpfung von Computerkriminalität als eigene Einheit innerhalb der Abteilung Kriminalpolizeiliche Assistenzdienste im Bundeskriminalamt etabliert.

- Es ist nationale und internationale Koordinierungs- und Meldestelle für Ermittlungen im Zusammenhang mit Cybercrime.
- Weiters ist das C4 für die elektronische Beweismittelsicherung und deren Auswertung zuständig. Zusätzlich werden im Rahmen von Entwicklung, Innovation und Forschung im Bereich Cybercrime vom C4 Assistenzleistungen im Bundeskriminalamt geleistet.
- Darüber hinaus ist im C4 die Meldestelle als Ansprechstelle für die Bevölkerung und zu den Unternehmen etabliert, wodurch im Schadensfall eine rasche Unterstützung erfolgen kann und neue Phänomene frühzeitig erkannt werden.
- Das C4 fungiert aber auch intern für alle heimischen und globalen Polizeidienststellen als wichtige Drehscheibe sowie Koordinationspunkt und gliedert sich mit seinen Schnittstellen zum Cyber Security Center (CSC) des Bundesamtes für Verfassungsschutz und Terrorismusbekämpfung als wesentlicher Bestandteil in die

österreichische Strategie für Cyber-Sicherheit ein. Im Krisenfall erfolgt so die Unterstützung des Inneren Kreises der Operativen Koordinierungsstrukturen (IKDOK).

Das definierte Wirkungsziel der Kernaufgaben ist die konsequente und zielgerichtete Kriminalitätsbekämpfung, die enorme materielle Schäden abwenden und das Vertrauen der Bevölkerung stärken soll. Diese Zielerreichung sollte mit der Stärkung der Cybercrime-Ermittlungen und durch die Bekämpfung der Internetkriminalität erfolgen.

Zur Frage 7:

- *Welche Maßnahmen werden getroffen um die Aufklärungsquote im Bereich der Cyberkriminalität zu verbessern?*

Die Anzahl der verfassungsgefährdenden Angriffe im Cyberraum ist zu gering, um von einer statistisch relevanten Aufklärungsquote sprechen zu können.

Im „Cybercrime Competence Center" (C4) des Bundesministeriums für Inneres werden laufend Maßnahmen gesetzt, um den europäischen und internationalen Austausch im Bereich der Bekämpfung von Cybercrime und somit die Aufklärungsquote 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 – sowie die Beteiligung am G7 24/7 Netzwerk.

Die oben angeführten Maßnahmen stärken die europäische und internationale Zusammenarbeit in vielen Bereichen wie z.B.

- SOKO Clavis – Bekämpfung von Ransomware,
- internationale Ermittlungen,
- Spezialisierungen im Bereich Darknet und Kryptowährungen,
- 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 GEMEINSAM.SICHER z.B.
  - zur Schaffung von Standards – „Certified Data & IT Security Expert",
  - zur Installation einer Cyber-Security-Hotline für Wirtschaftstreibende,
  - zur Abhaltung von Cyber-Planspielen für KMU;
- 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,
  - CyberKids und Fahrzeugforensik im Rahmen von ISF (Fonds für die innere Sicherheit)

(vgl. Beantwortung der Frage 1 der parlamentarischen Anfrage 2294/J vom 16. November 2018 – 2279/AB XXVI. GP).

Zur Frage 8:

- *Welche Maßnahmen werden getroffen um die österreichischen Wirtschaftstreibenden aktiv vor Cyberkriminalität zu schützen?*

Die präventiven Maßnahmen des CSC zielen vorwiegend auf die Steigerung der Resilienz der Betreiber kritischer Infrastruktur und der verfassungsmäßigen Einrichtungen ab.

- Im Jahr 2018 wurden vom CSC 48 zielgerichtete Awareness- und Präventionsveranstaltungen bei Betreibern kritischer Infrastruktur und verfassungsmäßigen Einrichtungen abgehalten.
- Durchführung/Teilnahme an Planspielen gemeinsam mit Cyber-Betreiber wesentlicher Dienste.
- Durch die Einführung des NISG wird eine Steigerung der Resilienz der Betreibern wesentlicher Dienste erwartet.

Die Erkenntnisse der Kriminalprävention richten sich vor allem an Einzelunternehmer sowie an kleine und mittelgroße Unternehmen, die den Großteil der Unternehmerinnen und Unternehmer ausmachen.
Vom Bundeskriminalamt, Büro 1.6 – Kriminalprävention und Opferhilfe, wird der regelmäße Kontakt zur WKO aufgrund der fortlaufenden Kooperation mit dem Bundesministerium für Inneres zwecks Informationsaustausch und Informationsweitergabe proaktiv aufrecht erhalten.
Beispielhaft darf ein in der aktuellen 9. Auflage des IT-Sicherheitshandbuches für kleine und mittelgroße Unternehmen befindlicher Beitrag der Polizei zum Thema erwähnt werden.
Vom C4 werden laufend präventive Vorträge, wie z.B. im Rahmen der Initiative GEMEINSAM.SICHER in Kooperation mit der WKO, abgehalten, wobei die Experten des C4 für die Beantwortung von Fragen zur Verfügung stehen.

Zu den Fragen 9 und 10:

- *Ist es angedacht das Prinzips der Tatortzuständigkeit und der grundsätzlichen Zuständigkeit aller Exekutivbediensteten für die Aufklärung von CybercrimeDelikte abzuändern?*
- *Macht es aus Sicht des Ministers Sinn, eine spezialisierte und zentrale Sonderermittlungseinheit (Soko) zu schaffen, die für die Aufklärung von CybercrimeDelikten im engeren Sinn betraut ist und somit Know-How innerhalb der Kriminalpolizei auf dem Gebiet der Cyberkriminalität zu bündeln?*

Eine derartige Abänderung des Prinzips der Tatortzuständigkeit ist zurzeit nicht angedacht. In der Regel ist eine erstinstanzliche sicherheitsbehördliche Zuständigkeit gegeben. Wenn eine Zusammenarbeit bzw. Koordinierung der einzelnen Sicherheitsbehörden und Sicherheitsdienststellen notwendig ist, übernimmt das Bundeskriminalamt gemäß dessen Geschäftsordnung die diesbezüglichen Koordinierungsmaßnahmen.

Im Übrigen darf darauf hingewiesen werden, dass dem Fragerecht gemäß Art. 52 Bundes-Verfassungsgesetz und § 90 des Geschäftsordnungsgesetzes 1975 nur Handlungen und Unterlassungen unterliegen (vgl. Morscher, Die parlamentarische Interpellation, 1973, 434 f.; Nödl, Parlamentarische Kontrolle, 1995, 104 f.; Atzwanger/Zögernitz, Nationalrat-Geschäftsordnung, 1999, 366).
Da die Frage keinen Gegenstand der Vollziehung des Bundesministeriums für Inneres betrifft, sondern Meinungen und Einschätzungen einfordert, ist sie daher im Sinne der zitierten Bestimmungen keiner Beantwortung durch das Bundesministerium für Inneres zugänglich.

Sollte eine derartige Sonderermittlungsbehörde gegründet werden, ist jedenfalls darauf Bedacht zu nehmen, dass sie in die staatlichen Strukturen zur Koordinierung von

Cybersicherheit (IKDOK, OpKoord - Operative Koordinierungsstrukturen) eingebunden sind, da nur so ein holistischer Überblick über die aktuelle Lage möglich ist.

Zu den Fragen 11 und 11a bis 11c:

- *ln Ergänzung zur Beantwortung der Fragen 16-18 in der Anfragebeantwortung 1837/AB vom 04.12.2018 zu 1823/J des Herrn BM:*
- *Wie viele angezeigte Fälle gab es im Bereich der Cyberkriminalität im gesamten Jahr 2018? Bitte um Aufschlüsselung nach Delikt?*
- *Wie hoch war die Aufklärungsquote im Bereich der Cyberkriminalität im gesamten Jahr 2018? Bitte um Aufschlüsselung nach Delikt?*
- *Wie hoch war die Schadenssumme der im Bereich der Cyberkriminalität im gesamten Jahr 2018 begangenen Delikte?*

Es wird darauf hingewiesen, dass es sich hier um Rohdaten handelt, die noch nicht der Qualitätskontrolle und weiteren Prüfmechanismen unterzogen wurden.
Somit können aus dem Zahlenmaterial weder die gegenwärtige kriminalpolizeiliche Lage noch Trends bzw. Aussagen über die Sicherheitslage und die Kriminalitätsbelastung abgeleitet werden.

Cybercrime gesamt - Österreich 2018 - vorläufig	
Delikt	**Anzahl Straftaten**
§ 107c StGB (Fortgesetzte Belästigung im Wege der Telekommunikation oder eines Computersystems)	308
§ 118a StGB (Widerrechtlicher Zugriff auf ein Computersystem)	404
§ 119 StGB (Verletzung des Telekommunikationsgeheimnisses)	11
§ 119a StGB (Missbräuchliches Abfangen von Daten)	39
§ 126a StGB (Datenbeschädigung)	413
§ 126b StGB (Störung der Funktionsfähigkeit eines Computersystems)	102
§ 126c StGB (Missbrauch von Computerprogrammen oder Zugangsdaten)	204
§ 144 StGB (Erpressung)	1.596
§ 145 StGB (Schwere Erpressung)	92
§ 146 StGB (Betrug)	11.427
§ 147 StGB (Schwerer Betrug)	1.252
§ 148 StGB (Gewerbsmäßiger Betrug)	661
§ 148a StGB (Betrügerischer Datenverarbeitungsmissbrauch)	1.412
§ 207a StGB (Pornographische Darstellungen Minderjähriger)	1.162
§ 207b StGB (Sexueller Missbrauch von Jugendlichen)	1

§ 208a StGB (Anbahnung von Sexualkontakten zu Unmündigen)	108
§ 218 StGB (Sexuelle Belästigung und öffentliche geschlechtliche Handlungen)	10
§ 223 StGB (Urkundenfälschung)	24
§ 224 StGB (Fälschung besonders geschützter Urkunden)	7
§ 225a StGB (Datenfälschung)	170
§ 229 StGB (Urkundenunterdrückung)	1
§ 231 StGB (Gebrauch fremder Ausweise)	15
§ 232 StGB (Geldfälschung)	35
§ 3g VerbotsG	149
Gesamtergebnis	**19.603**

Cybercrime gesamt - Österreich 2018 - vorläufig	
Delikt	**Aufklärungsquote**
§ 107c StGB (Fortgesetzte Belästigung im Wege der Telekommunikation oder eines Computersystems)	72,1%
§ 118a StGB (Widerrechtlicher Zugriff auf ein Computersystem)	23,8%
§ 119 StGB (Verletzung des Telekommunikationsgeheimnisses)	72,7%
§ 119a StGB (Missbräuchliches Abfangen von Daten)	15,4%
§ 126a StGB (Datenbeschädigung)	15,7%
§ 126b StGB (Störung der Funktionsfähigkeit eines Computersystems)	7,8%
§ 126c StGB (Missbrauch von Computerprogrammen oder Zugangsdaten)	25,5%
§ 144 StGB (Erpressung)	3,1%
§ 145 StGB (Schwere Erpressung)	12,0%
§ 146 StGB (Betrug)	33,9%
§ 147 StGB (Schwerer Betrug)	26,0%
§ 148 StGB (Gewerbsmäßiger Betrug)	50,7%
§ 148a StGB (Betrügerischer Datenverarbeitungsmissbrauch)	23,6%
§ 207a StGB (Pornographische Darstellungen Minderjähriger)	89,1%
§ 207b StGB (Sexueller Missbrauch von Jugendlichen)	100,0%
§ 208a StGB (Anbahnung von Sexualkontakten zu Unmündigen)	58,3%
§ 218 StGB (Sexuelle Belästigung und öffentliche geschlechtliche Handlungen)	30,0%
§ 223 StGB (Urkundenfälschung)	54,2%
§ 224 StGB (Fälschung besonders geschützter Urkunden)	71,4%
§ 225a StGB (Datenfälschung)	81,2%
§ 229 StGB (Urkundenunterdrückung)	100,0%
§ 231 StGB (Gebrauch fremder Ausweise)	40,0%

§ 232 StGB (Geldfälschung)	94,3%
§ 3g VerbotsG	91,9%
Gesamtergebnis	**34,8%**

Die Schadensumme beträgt 57.691.818,-- EURO.

Herbert Kickl

REPUBLIK ÖSTERREICH AMTSSIGNATUR	Datum/Zeit	2019-03-21T14:49:14+01:00
	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	2019-03-21T14:53:19+01:00
	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.	