7086/AB
vom 27.08.2021 zu 7158/J (XXVII. GP)

Bundesministerium
Inneres

Karl Nehammer, MSc
Bundesminister

Herrn
Präsidenten des Nationalrates
Mag. Wolfgang Sobotka
Parlament
1017 Wien

Geschäftszahl: 2021-0.511.285

Wien, am 24. August 2021

Sehr geehrter Herr Präsident!

Der Abgeordnete zum Nationalrat Hannes Amesbauer, Kolleginnen und Kollegen haben am 28. Juni 2021 unter der Nr. **7158/J** an mich eine schriftliche parlamentarische Anfrage betreffend „Lösegeldzahlung nach Hacker-Angriff auf Gemeinde Gössendorf“ gerichtet.

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

Zu den Fragen 1 bis 17:

- *Konnten bereits Tatverdächtige ermittelt werden?*
- *Wenn ja, welche Informationen über Tatverdächtige können Sie im Rahmen der Beantwortung mitteilen?*
- *Konnte bereits ermittelt werden, aus welchem Land der Hacker-Angriff wurde?*
- *Wenn ja, welche Informationen über das Land aus dem der Angriff getätigt wurde, können Sie im Rahmen der Beantwortung mitteilen?*
- *In welcher Form wurde das genannte Erpresserschreiben übermittelt?*
- *Konnte der Ursprung des Erpresserschreibens rückverfolgt werden?*
- *Wenn ja, welche Informationen über den Ursprung des Erpresserschreibens können Sie im Rahmen der Beantwortung mittteilen?*
- *In welcher Form und in welcher Höhe wurde das Lösegeld überwiesen?*
- *Konnte die Überweisung der Lösegeldzahlungen nachverfolgt werden?*

- *Wenn ja, welche Informationen können Sie über die Nachverfolgung der Lösegeldüberweisungen im Rahmen der Beantwortung mitteilen?*
- *Gab es seitens des Landeskriminalamtes eine Empfehlung an die Marktgemeinde Gössendorf der Geldforderung nachzukommen?*
- *Wenn ja, wie begründet sich diese Empfehlung?*
- *Wenn ja, ist das in derartigen Fällen eine übliche Vorgehensweise?*
- *Wenn nein, wurde ausdrücklich davon abgeraten, der Geldforderung nachzukommen oder gab es gar keine Empfehlung dazu seitens des Landeskriminalamtes?*
- *Kann laut aktuellem Ermittlungsstand ausgeschlossen werden, dass durch den Hacker-Angriff auch Daten der Marktgemeinde Gössendorf entwendet oder kopiert wurden?*
- *Wenn ja, weshalb kann dies ausgeschlossen werden?*
- *Wenn nein, besteht durch die Entwendung oder das Kopieren von möglicherweise sensiblen Daten für die Einwohner der Marktgemeinde Gössendorf eine Gefahr und wie stellt sich diese Gefahr gegebenenfalls dar?*

Auf Grund der Verpflichtung zur Amtsverschwiegenheit (Art. 20 Abs. 3 B-VG) bzw. auf Grund eines laufenden Ermittlungsverfahrens (§ 12 Abs. 1 StPO) muss von einer Beantwortung dieser Fragen Abstand genommen werden.

Zu den Fragen 18 bis 21:

- *Gab es in den Jahren 2020 und 2021 Anzeigen von anderen Gemeinden aufgrund von Hackerangriffen auf die Server von Kommunen?*
- *Wenn ja, wie viele derartige Fälle gab es österreichweit?*
- *Wenn ja, wie gliedern sich diese Fälle auf die jeweiligen Bundesländer auf?*
- *Wenn ja, welche Gemeinden waren davon konkret betroffen?*

In der Polizeilichen Kriminalstatistik Österreich werden als kleinste Region die politischen Bezirke als Tatort statistisch erfasst.

Zu den Fragen 22 bis 25:

- *Gab es in den Jahren 2020 und 2021 Anzeigen von anderen öffentlichen Einrichtungen aufgrund von Hackerangriffen auf die Server der jeweiligen Einrichtungen?*
- *Wenn ja, wie viele derartige Fälle gab es österreichweit?*
- *Wenn ja, wie gliedern sich diese Fälle auf die jeweiligen Bundesländer auf?*
- *Wenn ja, welche öffentlichen Einrichtungen waren davon konkret betroffen?*

In der Polizeilichen Kriminalstatistik Österreich wird das Merkmal „öffentliche Einrichtung“ bei den Paragrafen § 118a StGB (Widerrechtlicher Zugriff auf ein Computersystem),

§ 126a StGB (Datenbeschädigung) und § 126b StGB (Störung der Funktionsfähigkeit eines Computersystems) nicht erfasst.

Zur Frage 26:

- *Wie viele Anzeigen aufgrund von Hacker-Angriffen gab es insgesamt jeweils in den Jahren 2020 und 2021, gegliedert nach Bundesländern?*

Österreich – § 118a StGB (Widerrechtlicher Zugriff auf ein Computersystem), § 126a StGB (Datenbeschädigung), § 126b StGB (Störung der Funktionsfähigkeit eines Computersystems) – Anzahl der Straftaten	
Bundesland	Jahr 2020
Burgenland	29
Kärnten	86
Niederösterreich	246
Oberösterreich	210
Salzburg	88
Steiermark	191
Tirol	75
Vorarlberg	57
Wien	266
Österreich	1.248

Österreich - § 118a StGB (Widerrechtlicher Zugriff auf ein Computersystem), § 126a StGB (Datenbeschädigung), § 126b StGB (Störung der Funktionsfähigkeit eines Computersystems) - Vorläufige Anzahl der Straftaten	
Bundesland	Jan - Jun 2021 (vorläufig)
Burgenland	16
Kärnten	36
Niederösterreich	122
Oberösterreich	100
Salzburg	66
Steiermark	99
Tirol	44
Vorarlberg	35
Wien	144
Österreich	662

Zu den Fragen 27 bis 32:

- *Welche personellen und materiellen Ressourcen hat das Landeskriminalamt Steiermark speziell für den Bereich Cyber-Abwehr?*
- *Ist hier eine Aufstockung der Ressourcen vorgesehen?*
- *Wenn ja, in wie fern?*
- *Wenn ja, bis wann?*
- *Wenn nein, warum nicht?*
- *Welche Unterstützung oder Hilfe bietet das Bundesministerium für Inneres bzw. bietet die Polizei Gemeinden und anderen öffentlichen Einrichtungen präventiv in Zusammenhang mit Cyber-Abwehr an?*

Das Landeskriminalamt Steiermark weist speziell für „Cyber-Abwehr"-Angelegenheiten keine spezielle Organisationseinheit aus. Im Zuge von sicherheitspolizeilichen Aufgaben im Zusammenhang mit Prävention sind jedoch Exekutivbedienstete speziell für den Bereich „Kriminalprävention im Bereich Computer- und Internetkriminalität" ausgebildet. Themenbereiche, die durch die Kriminalprävention thematisiert werden, sind: Basisschutz für internetfähige Geräte, Gefahren im Internet, täglicher Gebrauch, Trend im Netz, Soziale Netzwerke und Kindersicherheit. Die Polizei führt kostenlose Beratungen und Vorträge durch und diese können über die Landeskriminalämter und die Kooperation mit dem Digitalisierungsministerium/Verein fit4internet angefordert werden.

Zusätzlich bietet das BVT/5.1-Prävention im Rahmen seiner gesetzlichen Aufgaben für kritische Infrastrukturen gemäß (L)APCIP, verfassungsmäßige Einrichtungen gemäß SPG und Betreiber wesentlicher Dienste, sowie Einrichtungen der Öffentlichen Verwaltung gemäß NISG auf Anfrage Präventionsveranstaltungen zur Bewusstseinsbildung (Cyber-Awareness) an. Ziel diesbezüglicher Veranstaltungen ist die Schaffung von Awareness in Bezug auf Cyber-Gefahren (Bewusstseinsbildung).

Karl Nehammer, MSc

	Datum/Zeit	2021-08-27T11:40:06+02:00
	Aussteller-Zertifikat	CN=a-sign-corporate-07,OU=a-sign-corporate-07,O=A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH,C=AT
	Serien-Nr.	148769640
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	2021-08-27T11:43:19+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.	