1333/J
vom 01.04.2020 (XXVII. GP)

Anfrage

der Abgeordneten Douglas Hoyos-Trauttmansdorff, Kolleginnen und Kollegen

an den Bundesminister für Inneres

betreffend Erhöhte Cyberkriminalität im Zuge der Corona Krise

Dass einer der Krimal-Hotspots die Cyberkriminalität ist, ist längst kein Geheimnis mehr. Mittlerweile ist amtlich, dass sich Kriminalität zunehmend ins Internet verlagert.

Dort sind die Zahlen alarmierend. Bei einem Deliktsanstieg von fast 17% im letzten Jahr und ca 20.000 angezeigten Fällen, entstand ein Schaden von über 60 € Mio Euro. Das ist ein erheblicher volkswirtschaftlicher Schaden. (Quelle: Sicherheitsbericht 2018, Innenministerium, abrufbar unter: https://www.bmi.gv.at/508/files/SIB_2018/1_SIB_2018_Hauptteil_web.pdf)

Seit dem Ausbruch der Corona Krise wird nun auch vermehrt darüber berichtet, dass sich Online-Kriminelle die aktuelle Situation zu Nutze machen.

"Mit Millionen Menschen, die weltweit von zuhause aus arbeiten, und Kindern, die für ihre Hausaufgaben online sind, potenziert sich die Gefahr, Opfer eines Angriffs zu werden. Einmal falsch geklickt und schon ist es passiert.

IT-Security-Unternehmen verzeichnen parallel zur Ausbreitung des Coronavirus weltweit einen Anstieg von Cyberattacken. Die Protagonisten sind dem Security-Spezialisten FireEye zufolge einzelne Kriminelle. Aber auch staatlich geförderte Spionagekampagnen nehmen das Covid-19-Thema zum Anlass für gezielte Angriffe.

Das wohl bekannteste Beispiel derzeit dürfte die interaktive Karte sein, die vorgibt, von der Johns Hopkins Universität zu sein. Entdeckt hat diese Form von Angriff der Securityspezialist Shai Alfasi von Reason Labs. Der Anhang, der sich auf Messenger-Plattformen und per Mail verbreitete, zeigte diese Karte zwar, aber im Hintergrund installierte sich Schadsoftware. Meist lautet die Datei auf den Namen "Coronavirus-Map.com.exe" oder als "CoronaMap.exe" und ist knapp 3,26 Megabyte groß.

Mit ähnlichem Inhalt, aber einer Android-App als Basis versuchten Kriminelle, die Smartphones der Nutzer zu kapern. Kaum war nämlich die Anwendung installiert, wurde das Gerät gesperrt und sollte erst gegen Bezahlung von 100 Dollar wieder freigegeben werden. Die Sicherheitsforscher fanden aber schnell eine Schwachstelle in der schlecht programmierten App und konnten einen Entschlüsselungscode veröffentlichen.

„Seit mehr als fünf Wochen hat unser Threat Research Team zahlreiche gefährliche E-Mail-Kampagnen mit Bezug zu Covid-19 beobachtet. Viele der Kampagnen setzen dabei auf den Faktor 'Angst', um potenzielle Opfer zum Klicken zu bewegen", erklärt Sherrod DeGrippo, Senior Director of Threat Research and Detection bei Proofpoint. Die E-Mail-Wellen reichen von einem Dutzend Empfänger bis hin zu 200.000 Adressaten. Und während früher meist nur eine Kampagne pro Tag zu beobachten war, sind es mittlerweile drei bis vier.

In den USA wurden zahlreiche Domain-Neuanmeldungen verzeichnet, nahezu alle mit Coronavirus-Bezug. Täglich mehrere Hundert, berichtet zum Beispiel Recorded Future. Das National Cyber Security Center (NCSC) berichtet, dass es Versuche

gibt, die offizielle Webseite der Centers for Desease Control (CDC) nachzuahmen, um "Passwörter und Bitcoin-Spenden zur Finanzierung eines gefälschten Impfstoffs" abzugreifen.

Die Angreifer wissen, dass Menschen nach Informationen über Covid-19 suchen und nutzen dies aus. Einerseits geben sie sich als bekannte Quellen wie die Weltgesundheitsbehörde aus, andererseits locken sie mit spezifischen Inhalten für spezielle Zielgruppen. So finden sich auch E-Mails mit dem Betreff "Wichtige Informationen für Eltern und ihre Kinder". "Etwa 70 Prozent der schadhaften E-Mails liefern Malware und weitere 30 Prozent zielen darauf ab, die Zugangsdaten des Opfers zu stehlen", fügt DeGrippe hinzu." (Quelle: https://www.diepresse.com/5788164/cyberkriminelle-nutzen-corona-angst)

Auch das Cybercrime Competence Center im Bundeskriminalamt warnte vor Kriminellen, die aktuell unter dem Deckmantel "Corona" versuchen, die aktuelle Situation auszunützen, und sich auf Kosten anderer zu bereichern. (https://bundeskriminalamt.at/news.aspx?id=7745347A7971512F6968343D)

Dabei stehen sowohl klassische Betrugsszenarien (Internetkriminalität im weiteren Sinne) als auch gezielte Angriffe auf Daten oder Computersysteme unter Ausnutzung der Informations- und Kommunikationstechnik (Internetkriminalität im engeren Sinne) wie etwa im Wege widerrechtlicher Zugriffe auf Computersysteme oder Datenbeschädigungen im Fokus.

Ebenso warnen das österreichische Portal: (https://www.onlinesicherheit.gv.at/service/news/532860.html) sowie das deutsche Bundesamt für Sicherheit in der Informationstechnik (BSI) (https://www.bsi-fuer-buerger.de/BSIFB/DE/Service/Aktuell/Informationen/Artikel/corona-falschmeldungen.html) vor den aktuellen kriminellen Kampagnen.

Die unterfertigten Abgeordneten stellen daher folgende

Anfrage:

1. Wie viele angezeigte Fälle gab es im Bereich der Internetkriminalität im weiteren Sinne im Zeitraum vom 1. März 2020 bis zum Stichtag der Anfragebeantwortung? (Bitte auch um Aufschlüsselung nach einzelnen Delikten)
    a. Wie viele angezeigte Fälle in diesem Deliktsbereich gab es im Vergleichszeitraum 2019?
2. Wie viele angezeigte Fälle gab es im Bereich der Internetkriminalität im engeren Sinne im Zeitraum vom 1. März 2020 bis zum Stichtag der Anfragebeantwortung? (Bitte auch um Aufschlüsselung nach einzelnen Delikten)
    a. Wie viele angezeigte Fälle in diesem Deliktsbereich gab es im Vergleichszeitraum 2019?
3. Wie hoch war die Aufklärungsquote im Bereich der Internetkriminalität im weiteren Sinne in diesem Zeitraum? (Bitte auch um Aufschlüsselung nach einzelnen Delikten)

4. Wie hoch war die Aufklärungsquote im Bereich der Internetkriminalität im engeren Sinne in diesem Zeitraum? (Bitte auch um Aufschlüsselung nach einzelnen Delikten)
5. Wie hoch war die Schadenssumme der im Bereich der Cyberkriminalität (Internetkriminalität im weitern und im engeren Sinne) im Zeitraum vom 1. März 2020 bis zum Stichtag der Anfragebeantwortung? (Bitte auch um Aufschlüsselung nach einzelnen Delikten)
    a. Wie hoch war die Schadenssumme in diesem Deliktsbereich im Vergleichszeitraum 2019?
6. Inwiefern lässt sich die erhöhte kriminelle Aktivität im Zusammenhang mit der Corona-Krise im Bereich der Internetkriminalität im weiteren Sinne statistisch belegen? (Um Erläuterung wird ersucht.)
7. Inwiefern lässt sich die erhöhte kriminelle Aktivität im Zusammenhang mit der Corona-Krise im Bereich der Internetkriminalität im engeren Sinne statistisch belegen? (Um Erläuterung wird ersucht.)
8. Wie viele Personen sind im "Cybercrime Competence Center" (C4) des Bundeskriminalamtes zum Stichtag der Anfragebeantwortung beschäftigt?
    a. Inwiefern hat sich der Personalstand des C4 seit der Anfragebeantwortung (2632/AB) vom 21.03.2019 durch den Bundesminister für Inneres zu der schriftlichen Anfrage (2656/J) verändert?
9. Wie viele dieser Mitarbeiter des C4 sind aktiv mit der Aufklärung von Straftaten im Bereich Cyberkriminalität zum Stichtag der Anfragebeantwortung befasst?
    a. Inwiefern hat sich diese Zahl seit der Anfragebeantwortung (2632/AB) vom 21.03.2019 durch den Bundesminister für Inneres zu der schriftlichen Anfrage (2656/J) verändert?

REPUBLIK ÖSTERREICH Parlamentsdirektion SIEGEL	**Unterzeichner**	Parlamentsdirektion
	Datum/Zeit-UTC	2020-04-01T13:51:17+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.	