EZ/OZ: n/v

Selbstständiger Antrag von Abgeordneten (§ 21 GeoLT)

Landtagsabgeordnete(r): LTAbg. Erich Hafner (FPÖ), LTAbg. Helga Kügerl (FPÖ)
Fraktion(en): FPÖ
Zuständiger Ausschuss: Infrastruktur
Regierungsmitglied(er): Landeshauptmann Hermann Schützenhöfer

Betreff:
Wachsende Gefahr von „Cyberkriminalität" für die Steiermark

Cyberkriminalität kann in verschiedenen Formen auftreten. So wird dieser Begriff für viele Formen der Kriminalität in Zusammenhang mit Computern und Internet verwendet.

Auf der Homepage des Softwareunternehmens „Symantec", welches das Antivirenprogramm „Norton AntiVirus" betreibt, wird auf die Problematik der Definition des Begriffes „Cyberkriminalität" eingegangen: „ *In der Cybercrime Convention des Europarats wird der Begriff ‚Cyberkriminalität' in Zusammenhang mit Verbrechen wie Datenmissbrauch bis hin zu Urheberrechtsverletzungen verwendet [Krone, 2005]. Andere [Zeviar-Geese, 1997-98] hingegen wählen eine umfassendere Definition, die Aktivitäten wie Betrug, unerlaubten Zugriff, Kinderpornographie und Online-Belästigung einschließt. Die Vereinten Nationen schließen in ihrem Handbuch zur Vorbeugung und Kontrolle von Computerverbrechen (Manual on the Prevention and Control of Computer Related Crime) Betrug, Fälschungen und unerlaubten Zugriff in ihre Definition von Cyberkriminalität mit ein.*" (Quelle: https://at.norton.com/cybercrime-definition)

Aus diesen verschiedenen Definitionen dieses Begriffs lässt sich ableiten, dass eine Vielzahl an Straftaten inzwischen darunter subsumiert werden kann.

„Symantec" fasst die Vielfalt an Auslegung des Wortes „Cyberkriminalität" zusammen und gibt so eine gute Erklärung dieses Begriffes: „ *Jedes Verbrechen, das mit Hilfe eines Computers, Netzwerks oder Hardware-Geräts begangen wird. Der Computer oder das Gerät ist möglicherweise der Agent, der Vermittler oder das Ziel des Verbrechens. Das Verbrechen kann auf einem Computer, oder an mehreren Orten gleichzeitig begangen werden. Das Verständnis der breitgefächerten Bedeutung von Cyberkriminalität wird durch die Aufteilung in zwei Kategorien erleichtert. Diese werden im Rahmen dieser Studie als Typ I und Typ II bezeichnet.*

Cyberkriminalität Typ I hat die folgenden Eigenschaften:

- *Kommt aus der Sicht des Opfers nur einmal vor. Zum Beispiel: Das Opfer lädt ohne es zu wissen einen Trojaner herunter, der auf dem Computer einen Tastenaufzeichner (Keystroke Logger) installiert. Das Opfer könnte auch eine E-Mail mit einem Link zu einem scheinbar bekannten Ziel empfangen, das sich dann aber als böswillige Website herausstellt.*

- *Diese Websites enthalten häufig Crimeware-Programme wie Tastenaufzeichner, Viren, Rootkits oder Trojaner.*

- *Softwarefehler oder Sicherheitslücken bieten häufig den Ansatzpunkt für den Angreifer. Verbrecher, die hinter einer Website stecken, können beispielsweise eine Sicherheitslücke in einem Internet-Browser ausnutzen, um einen Trojaner auf dem Computer des Opfers einzuschleusen.*

Diese Art der Cyberkriminalität umfasst unter anderem Phishing, Diebstahl oder Manipulation von Daten oder Diensten durch Hacker oder Viren, Identitätsdiebstahl sowie Bank- oder E-Commerce-Betrug.

Cyberkriminalität Typ II, am anderen Ende des Spektrums, umfasst unter anderem Aktivitäten wie Online-Belästigung und Nötigung, Verführung Minderjähriger, Erpressung, Börsenmanipulation, komplexe Industriespionage sowie Planung oder Durchführung von Terroranschlägen. Cyberkriminalität Typ II hat die folgenden Eigenschaften:

- *Kommt häufig vor, wobei eine wiederholte Kommunikation mit dem Opfer stattfindet. Zum Beispiel: Das Opfer wird in einem Chat-Room von einer Person kontaktiert, die versucht, im Lauf der Zeit eine Beziehung aufzubauen. Früher oder später nutzt der Verbrecher diese Beziehung für illegale Machenschaften aus. Mitglieder einer Terrorzelle bzw. einer kriminellen Organisation benutzen möglicherweise auch versteckte Botschaften in einem öffentlichen Forum, um beispielsweise Aktivitäten zu planen oder Geldwäscheangelegenheiten zu besprechen.*

- *Dies wird häufig mit Hilfe von Programmen durchgeführt, die nicht in die Kategorie der Crimeware-Programme fallen. Die Kommunikation kann beispielsweise über ein Instant-Messenger-Programm erfolgen und Dateien können mit FTP übertragen werden.*“

(Quelle: https://at.norton.com/cybercrime-definition)

In diesem Zusammenhang hat die Steiermark bereits die ersten Schritte zur Bekämpfung von digitalen Angriffen gesetzt. So berichtete der Österreichische Rundfunk (ORF) auf der Steiermark-Ausgabe seiner Homepage unter dem Titel „ *Kostenlose Hotline bei Cyber-Kriminalität*“ wie folgt: „ *Hacker greifen über das Internet immer öfter steirische Unternehmen an, das hat die Wirtschaftskammer am Freitag aufgezeigt. Ab sofort können sich betroffene Unternehmen an eine neue Hotline für Cyber-Crime wenden. […] Wie die Wirtschaftskammer am Freitag bekanntgab, steigt die Zahl der Cyber-Angriffe auch in der Steiermark stetig an. Im Vorjahr sind mehr als 1.400 Fälle angezeigt worden, das ist ein Plus von 31 Prozent gegenüber 2015, sagt WK-Präsident Josef Herk: ‚Es sind etwa 1,6 Milliarden Euro, die der österreichischen Wirtschaft jährlich durch Cyber-Kriminalität und Betriebsspionage abhanden kommen. Diese Angriffe betreffen alle Bereiche der Wirtschaft.‘*“ (Quelle: http://steiermark.orf.at/news/stories/2848195/)

In der Landtagssitzung vom 20. Juni 2017 wies Landeshauptmann Hermann Schützenhöfer im Zuge einer „Aktuellen Stunde“ der FPÖ zum Thema „Sicherheitslage in der Steiermark“ darauf hin, dass laut Information von Innenminister Wolfgang Sobotka die „Internetkriminalität“ die am stärksten steigende Form von Straftaten hierzulande darstellt.

Cyberkriminalität ist ein weltweites Problem und kann überall stattfinden, wo Menschen Computer, Smartphones und ähnliche elektronische Geräte benutzen. Betroffen von dieser Form der Kriminalität sind neben Privatpersonen und Firmen natürlich öffentliche Einrichtungen wie Universitäten, Behörden, Gemeinden, Länder und ganze Staaten. In der Vergangenheit wurde medial mehrmals von Seiten der Politik betont, dass man diesbezüglich Hotlines und andere Formen der Hilfestellung für Private und Unternehmen anbieten würde. Wie es hingegen um die Schutzvorkehrungen des Landes Steiermark gegen die Cyberkriminalität bestellt ist und welche Ansätze zur zukünftigen Abwehr gegen derartige „digitale“ Angriffe verfolgt werden, ist nicht bekannt. Aus diesem Grund scheint es vernünftig, einen „Runden Tisch“ unter Einbeziehung der zuständigen Sicherheitsorgane, Vertreter sämtlicher politischen Parteien und fachkundiger Experten zu installieren.

Es wird daher der

Antrag

gestellt:

Der Landtag wolle beschließen:

Die Landesregierung wird beauftragt, einen „Runden Tisch“ zum Thema „Cyberkriminalität“ einzurichten, welchem Vertreter der zuständigen Sicherheitsbehörden und sämtliche Landtagsparteien angehören. Dieses Gremium soll unter Einbindung externer Experten Maßnahmen zur Bekämpfung von Cyberkriminalität erarbeiten und dem Landtag diesbezügliche Anträge zur Beschlussfassung vorlegen.

Unterschrift(en):
LTAbg. Erich Hafner (FPÖ), LTAbg. Helga Kügerl (FPÖ)