EZ/OZ: n/v

Schriftliche Anfrage an die Landesregierung oder eines ihrer Mitglieder (§ 66 GeoLT)

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

Betreff:
Stand der Maßnahmen gegen „Cyberkriminalität" für die Steiermark

Eine mögliche Definition des Begriffs „Cyberkriminalität" lautet: „ *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.*" (Quelle: http://steiermark.orf.at/news/stories/2848195/)

Die Cyberkriminalität des Typs I umfasst unter anderem Phishing, Diebstahl oder Manipulation von Daten oder Diensten durch Hacker oder Viren, Identitätsdiebstahl sowie Bank- oder E-Commerce-Betrug. Unter Cyberkriminalität des Typs II fallen hauptsächlich Aktivitäten wie Online-Belästigung und Nötigung, Verführung Minderjähriger, Erpressung, Börsenmanipulation, komplexe Industriespionage sowie Planung oder Durchführung von Terroranschlägen.

Laut Steiermark-Ausgabe der Online-Plattform des Österreichischen Rundfunks (ORF) hat die Steiermark bereits erste Schritte zur Bekämpfung von digitalen Angriffen gesetzt: „ *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.

Die FPÖ-Steiermark hat mit dem Betreff „ *Wachsende Gefahr von ‚Cyberkriminalität' für die Steiermark*" bereits einen Selbstständigen Antrag auf Einrichtung eines „Runden Tisches" zur Ausarbeitung einer Abwehrstrategie gegen digitale Angriffe eingebracht. Dieser soll unter Einbeziehung der zuständigen Sicherheitsorgane, Vertreter sämtlicher politischen Parteien und fachkundiger Experten stattfinden.

Um einen Eindruck vom tatsächlichen Gefährdungspotenzial für die Steiermark, die eingesetzten Ressourcen, den derzeitigen Stand der Vorkehrungen uvm. rund um das Thema „Cyberkriminalität" zu erhalten, ist es notwendig, eine Schriftliche Anfrage hinsichtlich dieses Themas einzubringen.

Es wird daher folgende

Schriftliche Anfrage

gestellt:

1. Wie viele Cyberangriffe hat es in den Jahren 2012 bis 2017 gegen Einrichtungen des Landes Steiermark (Politik, Verwaltung, Gesellschaften wie KAGes etc., kritische Infrastruktur) gegeben? (bitte um Aufschlüsselung nach den einzelnen Jahren)

2. Um welche Angriffe handelte es sich im Zeitraum 2012 bis 2017 konkret?

3. Welche Dienststellen des Landes Steiermark bzw. welche landeseigenen Gesellschaften waren in den Jahren 2012 bis 2017 von Angriffen betroffen?

4. Bestand bei diesen Angriffen tatsächlich auch eine Gefahr für Menschen, Daten, Infrastruktur, etc.?

5. Wenn ja, bei welchen Angriffen?

6. Wenn ja, wurden bei diesen Angriffen Daten entwendet? (bitte um Aufzählung der einzelnen Vorkommnisse)

7. Hat die Steiermärkische Landesregierung bereits Maßnahmen gegen Cyberkriminalität gesetzt?

8. Wenn ja, welche?

9. Wurden sämtliche Cyberangriffe zur Anzeige gebracht?

10. Wenn ja, wie viele davon wurden aufgeklärt?

11. In wie vielen Fällen kam es tatsächlich zu der Ausforschung der Täter?

12. In wie vielen Fällen kam es zu einer strafrechtlichen Verurteilung der Täter?

13. In wie vielen Fällen war bei einem digitalen Angriff ein anderer Staat beteiligt? (bitte um Aufschlüsselung nach Zeitpunkt, verdächtigter Staat und Art des Angriffs)

14. Wie hoch waren die finanziellen Schäden aufgrund von digitalen Angriffen gegen das Land Steiermark oder landeseigene Gesellschaften im Zeitraum von 2012 bis 2017? (bitte um Aufschlüsselung nach Jahr, Beschreibung des Angriffs und Schaden des einzelnen Angriffs)

15. In wie vielen Fällen konnte erfolgreich ein Schadenersatzanspruch gegen den Verursacher eines Cyberangriffs gerichtlich durchgesetzt werden?

16. Um welche Fälle handelt es sich hierbei konkret und wie hoch waren die einzelnen Schadenersatzsummen?

17. Sind sowohl Politik als auch landeseigene Gesellschaften (zum Beispiel KAGes, ESTAG) und andere Einrichtungen (zum Beispiel kritische Infrastrukturen) gegen mögliche Cyberangriffe geschützt?

18. Wenn ja, wie?

19. Wenn nein, warum wurde diesbezüglich noch nichts unternommen?

20. Wenn nein, werden sie sich künftig verstärkt für den Schutz gegen Cyberkriminalität einsetzen?

21. Welche Maßnahmen sind in den Jahren 2017, 2018, 2019 und 2020 zum Schutz gegen Cyberkriminalität angedacht?

22. Welchen Zeitplan verfolgen Sie für die Umsetzung der einzelnen Maßnahmen?

23. Wie hoch sind die budgetären Mittel, die für die Umsetzung dieser Maßnahmen in den Jahren 2017, 2018, 2019 und 2020 vorgesehen sind?

24. Sind diesbezüglich bereits landesexterne Unternehmen beauftragt worden?

25. Wenn ja, welche?

26. Wenn ja, wie hoch waren die Kosten für die einzelnen Unternehmen (unter Angabe der Leistungen) in den Jahren 2012 bis 2017?

27. Gibt es in Bezug auf Cyberkriminalität Kooperationen mit Gemeinden?

28. Wenn ja, in welcher Form?

29. Wenn ja, mit welchen Gemeinden?

30. Wenn nein, warum nicht?

31. Wird Software, welche gegen Cyberkriminalität Schutz bietet, landeseigenen Gesellschaften und Gemeinden zur Verfügung gestellt?

32. Entwickelt das Land Steiermark selbst auch Schutzprogramme gegen digitale Angriffe?

33. Wenn ja, welche Abteilung ist hierfür zuständig?

34. Wenn nein, ist dies in Zukunft geplant?

35. Gibt es in den einzelnen Dienststellen des Landes Steiermark und den landeseigenen Gesellschaften Mitarbeiter, die für Cyberangriffe zuständig sind (Erkennen, Melden, Informationen für andere Mitarbeiter, etc.)?

36. Wenn ja, wie viele dieser Personen gibt es insgesamt beim Land Steiermark und den landeseigenen Gesellschaften?

37. Wenn nein, warum nicht?

38. Wenn nein, ist künftig geplant, solche Personen in den einzelnen Dienststellen zu benennen (analog z.B. zum Brandschutz- oder Erste-Hilfe-Beauftragten)?

39. Gibt es bereits ein Schulungsangebot des Landes Steiermark in Bezug auf Erkennen und die weitere Vorgehensweise bei dem Verdacht auf einen digitalen Angriff?

40. Wenn ja, wie gestaltet sich dieses konkret?

41. Wenn nein, warum nicht?

42. Wenn nein, werden Sie sich dafür einsetzen, dass ein solches zeitnah vom Land Steiermark für seine Mitarbeiter und das Personal landeseigener Gesellschaften angeboten wird?

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