

18.17

**Abgeordneter Lukas Brandweiner (ÖVP):** Sehr geehrter Herr Präsident!  
Geschätzte Frau Rechnungshofpräsidentin! Werte Kolleginnen und Kollegen!  
Liebe Zuseherinnen und Zuseher auf der Galerie und zu Hause vor den  
Bildschirmen! Der Rechnungshof hat die Datengrundlagen zur Cyberkriminalität  
und den damit einhergehenden Strategien von Innen- und Justizministerium  
überprüft. Es wurden insbesondere Prävention und Bekämpfung in Bezug auf  
Organisation und Zusammenarbeit von Kriminalpolizei und Justiz beurteilt.  
Beurteilt beziehungsweise geprüft wurden die Jahre 2016 bis 2019. Ich möchte  
mich gleich zu Beginn bei der Frau Präsidentin und ihren Mitarbeiterinnen und  
Mitarbeitern sehr herzlich für diese ausführliche Prüfung bedanken.

Cyberkriminalität ist ein wichtiges Thema, weil sie leider immer mehr zunimmt  
und auch immer mehr Menschen betrifft. Internationale Erhebungen gehen von  
einem Schaden durch Cyberkriminalität von über 700 Milliarden US-Dollar im  
Jahr 2017 aus. In Österreich dürfte der Schaden nach Schätzungen mehrere  
100 Millionen Euro ausmachen. Neben den finanziellen Folgen gibt es aber  
leider auch immaterielle Folgen wie zum Beispiel Cybermobbing oder Verhet-  
zung und Hass im Netz, und leider nehmen auch diese kontinuierlich zu.

Seit dem Frühjahr 2020, mit dem Auftreten der Covid-Pandemie, war die klas-  
sische Kriminalität in Österreich rückläufig, die Cyberkriminalität ist im  
Gegensatz jedoch wirklich stark angestiegen. Allein im Jahr 2019 haben sich die  
Anzeigen verdoppelt. Es gibt sehr viele Beispiele, und ich bin überzeugt, dass  
auch viele Kolleginnen und Kollegen viele kennen. Ich denke da an kleinere und  
mittlere Unternehmen, die gehackt werden, wo ganze Verrechnungssysteme  
lahmgelegt werden und die Unternehmen im Anschluss erpresst werden. Quasi  
eine Betrugerei: Zahlt mich und ich bringe euer Rechnungssystem wieder zum  
Laufen! – Leider Gottes gibt es auch – davon bin ich überzeugt – viele Firmen,  
die solche Dinge nicht zur Anzeige bringen, sondern diesen Forderungen einfach  
nachkommen und dadurch natürlich einen großen Schaden erleiden.

Plötzlich verstorbene Verwandte, die es angeblich gibt, die etwas zu vererben haben: Wer von uns hat nicht schon so ein E-Mail oder eines, in dem es heißt, dass man plötzlich im Lotto gewonnen hat, bekommen? So wird geködert und im schlimmsten Fall gehackt, Daten werden gestohlen, und man ist dann natürlich auch mit finanziellen Folgen gestraft.

Daher bin ich froh und möchte auch unserem Innenminister Gerhard Karner danken, dass bereits Reformen auf den Weg gebracht wurden. Die wesentlichen Säulen sind die Stärkung der Kriminalpolizei in den Regionen draußen, der Fokus eben auf Cybercrime und die Weiterentwicklung der Bekämpfung sowie der Prävention von organisierter Kriminalität.

Ein Problem ist natürlich auch, das geeignete Personal zu finden. Da ist es wie in vielen Bereichen so, dass es aktuell einfach schwierig ist, Personen mit diesen Fähigkeiten zu finden, und daher ist es wichtig, massiv in die Aus- und Weiterbildung der Kolleginnen und Kollegen zu investieren. Ich möchte aber auch diesen Personen für den Einsatz, den sie leisten, wirklich Danke sagen.

Es muss aber auch an den Strafen gedreht werden. Durch eine Gesetzesnovelle soll die Polizei mehr Ermittlungsmöglichkeiten in Fällen von Cyberkriminalität bekommen. Es sollen aber eben auch die Strafen erhöht werden. Im Falle eines gehackten Computers sollen zwei Jahre Freiheitsstrafe drohen, aber auch bei Angriffen auf infrastrukturell kritische Einheiten müssen wir reagieren, und da ist der Vorschlag, die Strafe auf drei Jahre zu erhöhen.

Geschätzte Damen und Herren, keiner von uns würde sein Geldbörsel irgendwo liegen lassen oder das Auto offen in der Tiefgarage stehen lassen. (*Abg. Loacker: Mit einer Waffe drin!*) – Bitte, Herr Kollege? (*Abg. Loacker: Das Auto in der Tiefgarage stehen lassen mit einer Waffe drin!*) – Ah, genau! Herr Kollege Loacker sagt es richtig: Es gibt schon welche, die das Auto offen und sogar mit Waffe drin stehen lassen, aber ich glaube, das ist nicht alltäglich und macht nicht jeder. Also der Großteil von uns würde das nicht machen. Genauso wichtig ist es natürlich auch, dass wir im virtuellen Raum auf Sicherheit schauen, egal ob im privaten Bereich oder auch bei Firmen, denn sonst kann natürlich ein erheblicher

Schaden entstehen, und daher lautet der Tipp, da wirklich vorsichtig zu sein und in die Sicherheit zu investieren.

Eingangs habe ich aber auch erwähnt: Leider wird auch Hass im Netz ein immer größeres Thema, genauso wie Cybermobbing. Zu Hause vor dem Computer fühlen sich leider viele Menschen sehr stark und glauben, sie können sagen und schreiben, was sie wollen. Dem ist natürlich nicht so. Egal ob in der realen oder in der virtuellen Welt – wir müssen in Zukunft verstärkt darauf schauen. Das Internet ist kein rechtsfreier Raum, und ich bin da auch unsererer Jugendstaatssekretärin Claudia Plakolm sehr dankbar, dass sie sich aktuell sehr für ein Dickpicverbot starkmacht, denn eines ist auch klar: Belästigung bleibt Belästigung, egal ob in der realen Welt oder im virtuellen Raum, und daher muss da auch reagiert werden. *(Beifall bei der ÖVP und bei Abgeordneten der Grünen.)*

18.23

**Präsident Mag. Wolfgang Sobotka:** Zu Wort gemeldet ist Abgeordnete Greiner. – Bitte.