18.44

Präsidentin des Rechnungshofes Dr. Margit Kraker: Sehr geehrte Frau Präsidentin! Sehr geehrte Damen und Herren! Ja, es ist tatsächlich so, dass wir uns vonseiten des Rechnungshofes bemühen, aktuelle und relevante Themen in unsere Prüfarbeit aufzunehmen und Ihnen Berichte zu liefern, in denen wir den Handlungsbedarf aufzeigen.

Wir hatten Mitte März mit dem Herrn Innenminister eine Sitzung im Rechnungshofausschuss. Die ersten beiden Punkte, die jetzt auf der Tagesordnung stehen, betreffen die Bekämpfung und die Prävention von Cyberkriminalität und die Koordination der Cybersicherheit in Österreich. Es sind dies Themen von großer Bedeutung und aktueller Relevanz, denn es geht um die Sicherheit der Netz- und Informationssysteme, und es geht um den Schutz vor kriminellen Handlungen im virtuellen Raum.

Was die Cyberkriminalität betrifft: Wir haben dieses Thema schon vor Covid in unser Prüfprogramm aufgenommen. Dann haben wir miterleben können, wie es gerade während der Covid-Pandemie einen Digitalisierungsschub gab, wie sich auch die Arbeitswelt dort, wo es möglich war, in den virtuellen Raum verlagert hat. Aber nicht nur die Nutzung von IT im positiven Sinne und im guten Sinne nahm zu, sondern es stieg auch die Kriminalität in diesem Bereich an. Im Prüfungszeitraum verdoppelten sich die polizeilichen Anzeigen wegen Internetbetrugs, und die steigenden Delikte waren natürlich eine Herausforderung für die Behörden. Leider lag die Aufklärungsquote 2019 mit über 36 Prozent deutlich unter der Gesamtaufklärungsquote.

Bei der Prüfung haben wir den Fokus auf Prävention und Ausbildung für die Bekämpfung von Cyberkriminalität gelegt. Wir haben schon gehört, es gibt keine einheitliche Definition von Cyberkriminalität. Es gibt die im engeren Sinn, das sind Angriffe auf IT-Systeme wie Hackerangriffe, und die im weiteren Sinn, wenn IT zur Begehung von Straftaten verwendet wird. Die Datengrundlagen zwischen den Ministerien – zwischen dem Innenministerium und dem Justizministerium – passen nicht zusammen. Es kann daher zwischen dem Einlangen einer Anzeige

bei der Polizei und der Erledigung bei der Justiz kein Zusammenhang hergestellt werden.

Ein schwieriges Problem – darauf wurde auch schon eingegangen – ist die Rekrutierung von geeignetem Personal. Wir haben daher dem Innenministerium ein modernes Personalmanagement empfohlen. Es geht da um personelle und qualitative Verbesserungen. Es geht um Rekrutierung, Personalentwicklung, Aus- und Fortbildung, damit wir Personal in ausreichender Anzahl und Qualität zur Verfügung haben.

Wesentlich ist für uns auch, dass eine laufende Anpassung der Organisation auf Ebene der jeweiligen Kommanden – der Bezirks- und Stadtpolizeikommanden –, der Landeskriminalämter und im Bundeskriminalamt stattfindet.

Ein Punkt war die Prävention: Da geht es um die Freiwilligkeit bei den Bediensteten selbst, aber es geht eben auch darum, dass die Präventionsarbeit verstärkt wird. Wir sprechen da die Jugend an, aber es geht auch um Erwachsene, und es geht um die ältere Generation. Darüber hinaus ist es wichtig, dass die Polizei über die notwendigen geeigneten technischen und räumlichen Infrastrukturen verfügt.

Was die Cybersicherheit betrifft, geht es um die Koordination. Wir haben die vier sogenannten Sicherheitsministerien geprüft: Das Bundeskanzleramt, das Innenministerium, das Verteidigungsministerium und das Außenministerium, und ja, wir sind auf den Cyberangriff auf das Außenministerium Anfang 2020 eingegangen und haben uns angeschaut, wie dieser Angriff bewältigt werden konnte. Da gab es erstmals eine Cyberkrise, und da wurden die dafür vorgesehenen Strukturen aktiviert.

Grundsätzlich konnte die Krise erfolgreich bewältigt werden, aber es gab einige Aspekte, auf die wir im Bericht hingewiesen haben. Es gab Ende 2019, Anfang 2020 keine Krisen-, Kontinuitäts- und Einsatzpläne, obwohl die Cybersicherheitssteuerungsgruppe die Ausarbeitung solcher Pläne bereits Jahre zuvor gefordert hatte. Es fehlte an einer Cyberkriseninfrastruktur, daher mussten

Räumlichkeiten und sonstige Ausstattung wie Hardware und Software erst in der Cyberkrise organisiert werden. Es stand kein ständig verfügbares Einsatzteam zur Verfügung, und es gab auch keine staatliche Cybersicherheitsleitstelle mit einer Einsatzzentrale und einsatzbereitem Personal.

Das sind alles Punkte, die wir aufgezeigt haben und von denen wir sagen, dass das ein Anlass ist, damit man das besser macht und auch angesichts der wachsenden Bedrohungen darauf achtet.

Die Prüfung hat hinsichtlich der strategischen und operativen Cyberkoordination Optimierungsbedarf gezeigt. Der äußere Kreis, die OpKoord, hat bisher keine eigenständige Tätigkeit entfaltet, deshalb wären die Aufgaben dieser Koordinierungsstruktur zu evaluieren. Es gibt da einen Verbesserungsbedarf. Was auch fehlte, war ein Meldeanalysesystem sowie ein Frühwarnsystem für die Analyse und die Erkennung von Risken. Beides ist noch nicht umgesetzt. Der Rechnungshof hat darüber hinaus gefordert, dass das für Digitalisierung zuständige Ministerium eingebunden wird – das ist jetzt das Finanzministerium – und dass natürlich auch die Länder in die Koordinierungsstruktur einbezogen werden. – Ich danke für die Aufmerksamkeit. *(Allgemeiner Beifall.)*

18.50

Präsidentin Doris Bures: Nächster Redner: Herr Abgeordneter Reinhold Einwallner. – Bitte.