# Presseinformation

Rechnungshof Österreich
Unabhängig und objektiv für Sie.

Mag. Christian Neuwirth
Sprecher des Rechnungshofes
1031 Wien, Dampfschiffstraße 2
Tel.: +43 (1) 711 71 – 8435

Twitter: @RHSprecher
Facebook/RechnungshofAT
neuwirth@rechnungshof.gv.at

## Rechnungshof weist auf IT-Sicherheitslücken in Ministerien hin

Um den Dienstbetrieb während der Lockdowns im Zuge der COVID-19-Pandemie aufrechtzuhalten, nutzten Mitarbeiterinnen und Mitarbeiter in Ministerien mitunter ihre private IT-Ausstattung. Dies birgt erhebliche Sicherheitsrisiken. Darauf, sowie auf Mängel bei der Vorbereitung auf mögliche IT-Notfälle und IT-Sicherheitsrisiken bei Kompetenzverschiebungen der Ministerien weist der Rechnungshof in seinem heute veröffentlichten Bericht „Management der IT-Sicherheit in der Verwaltung ausgewählter Bundesministerien“ hin.

Geprüft wurden das Bundeskanzleramt (BKA), das Bundesministerium für Digitalisierung und Wirtschaftsstandort (BMDW), das Bundesministerium für Kunst, Kultur, öffentlichen Dienst und Sport (BMKÖS), sowie das Bundesministerium für Soziales, Gesundheit, Pflege und Konsumentenschutz (BMSGPK). Prüfzeitraum war 2018 bis 2020.

### Herausforderung für die IT bei Änderung der Ressortzuständigkeiten

Ändern sich die Kompetenzen der Ressorts – etwa im Zuge einer Regierungsum- oder -neubildung – ist dies für die betreffenden IT-Abteilungen aufwändig und mit Sicherheitsrisiken verbunden. Wegen organisatorischer, personeller und räumlicher Verschiebungen müssen IT-Ausstattung und Fachanwendungen in das aufnehmende Ministerium integriert werden. Dazu gehört auch die Implementierung der jeweiligen IT-Sicherheitsstrategie. Vor allem die Phase der Überleitung kann IT-Sicherheitsrisiken beinhalten. So war etwa im September 2020 – neun Monate nach Verschiebung von Ressortkompetenzen in den Ministerien BKA, BMKÖS und BMSGPK – noch keine ressorteinheitliche IT-Zuständigkeit gegeben.

Der Rechnungshof empfiehlt im Sinne der kontinuierlichen IT-Sicherheit, eine Regierungsvorlage zu erarbeiten, mit der im Bundesministeriengesetz eine Kompetenz zur Koordination der IT-Sicherheit klar und ausdrücklich festgelegt wird. Eine Vereinheitlichung der IT-Arbeitsplätze des Bundes würde die Kosten

für Beschaffung und Lizenzen reduzieren, die Wartung vereinfachen und die IT-Sicherheit erhöhen. Eine entsprechende Verordnung zum IKT-Konsolidierungsgesetz von 2012 fehlt nach wie vor.

## Nutzung privater IT-Ausstattung als Sicherheitsrisiko

Der Rechnungshof beleuchtete auch Sicherheitsaspekte des Homeoffice im Zuge der COVID-19-Pandemie. Es zeigt sich: Bedienstete des BKA, des BMDW und des BMSGPK nutzten mitunter ihre private IT-Ausstattung, um den Dienstbetrieb aufrechtzuhalten.

Abgesehen davon, dass für den regulären Dienstbetrieb die Nutzung privater IT-Ausstattung für Telearbeit gesetzlich nicht vorgesehen war, weist der Rechnungshof auf die damit verbundenen Risiken hin. Die Nutzung eigener Geräte birgt das Risiko, dass dienstliche Daten auf privaten Geräten gespeichert bleiben. Auch sind auf den privaten Geräten die IT-Sicherheitsvorkehrungen gegenüber Schadsoftware im Vergleich zu den IT-Sicherheitsmaßnahmen auf Dienstgeräten typischerweise geringer. Zudem fehlten für die Nutzung privater IT-Ausstattung während des Homeoffice ausdrückliche Vorgaben zur IT-Sicherheit. Für den regulären Dienstbetrieb sollte der Einsatz privater IT-Ausstattung für Telearbeit daher nicht standardmäßig vorgesehen werden.

## Dienstliche Ausstattung für Homeoffice

Der Rechnungshof empfiehlt: Im Hinblick auf mögliche weitere Phasen von krisenbedingtem Homeoffice wäre die IT-Ausstattung der Arbeitsplätze so einzurichten, dass die Aufrechterhaltung des Betriebs mit dienstlichen Geräten außerhalb der Arbeitsstelle möglich ist. Außerdem soll festgelegt werden, ob bestimmte Tätigkeiten jedenfalls aus Sicherheitsgründen an der Dienststelle zu verrichten sind.

## Externes Personal im EU-Ausland: unmittelbare Aufsicht nicht möglich

Der Rechnungshof stellte fest, dass das BMDW im Wege seines externen Dienstleisters auch Personal – mit Zugriff auf die IT-Systeme des Ministeriums – einsetzte, das seinen Arbeitsort im EU-Ausland hatte. Die notwendigen Sicherheitsüberprüfungen des Personals erfolgten mit Hilfe der lokalen Behörden. Da das externe IT-Personal auch Zugriff auf wichtige Dienste des Ministeriums hatte, lag darin ein Risiko

hinsichtlich der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit der vom Ministerium verarbeiteten Daten. Durch den Arbeitsort im EU-Ausland war eine unmittelbare Aufsicht beziehungsweise Kontrolle des externen Personals weder für den externen Dienstleister noch für das Ministerium direkt möglich.

## Vorbereitung auf IT-Notfälle mangelhaft

Verbesserungsbedarf sieht der Rechnungshof bei der Vorbereitung auf IT-Notfälle. Das Bundeskanzleramt hatte Notfallszenarien für intern betriebene IT-Systeme nicht ausreichend festgelegt. Es existierte etwa kein IT-Notfallhandbuch, und Kriterien für den Eintritt eines IT-Notfalls waren nicht klar definiert. Im Wirtschaftsministerium waren Notfallkonzepte, etwa IT-Notfallhandbücher, IT-Notfallszenarien oder IT-Notfallpläne, für die intern betriebenen IT-Systeme nicht vorhanden.

Der Rechnungshof empfiehlt, für die intern betriebenen IT-Systeme und IT-Dienste ein IT-Notfallhandbuch mit allen wichtigen IT-Notfallszenarien zu erstellen und darin klare Kriterien für den Eintritt von IT-Notfällen und eine eigene IT-Notfallorganisation festzulegen.