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

Cyber-Sicherheit: Bund soll Pläne, Personal und Infrastruktur ausbauen

Die Cyber-Sicherheit ist in allen Bereichen der elektronischen Datenverarbeitung maßgeblich. Auf Bundesebene sind das Bundeskanzleramt, das Innenministerium, das Verteidigungsministerium sowie das Außenministerium für die Koordination der Cyber-Sicherheit zuständig. In seinem heute veröffentlichten Bericht zeigt der Rechnungshof Verbesserungsbedarf auf: So fehlte es an Krisen-, Kontinuitäts- und Einsatzplänen für das Cyber-Krisenmanagement. Ein permanent verfügbares Cyber-Einsatzteam wäre ebenso zu schaffen wie ein Cyber-Lagezentrum zur Bearbeitung von Notfällen. Diese Schlüsse ziehen die Prüferinnen und Prüfer des Rechnungshofes unter anderem aus der Cyber-Krise im Außenministerium vom Dezember 2019 bis März 2020. Prüfungszeitraum waren die Jahre 2018 bis 2021.

Cyber-Krise „grundsätzlich erfolgreich“ bewältigt

Im Dezember 2019 erfolgte ein verdeckter Cyber-Angriff auf die Systeme des Außenministeriums. Dieser führte in Österreich erstmals zur Feststellung einer Cyber-Krise und damit auch zur Aktivierung der dafür vorgesehenen Strukturen. Neben dem Inneren Kreis der Operativen Koordinierungsstruktur (IKDOK), der vom Innenministerium geleitet wird und in dem das Bundeskanzleramt sowie das Verteidigungs- und Außenministerium vertreten sind, wurde eine eigene Einsatzstruktur etabliert. Das Innenministerium stellte die Cyber-Krise am 4. Jänner 2020 fest. Am 7. Jänner 2020 konnten die Cyber-Sicherheitskräfte der verantwortlichen Ministerien sowie eines externen Unternehmens ihre operative Tätigkeit aufnehmen. Zuvor mussten noch die Infrastruktur (Räumlichkeiten) sowie die sonstige Ausstattung (Hardware, Software, Büroausstattung) für das Einsatzteam organisiert und beschafft werden.

Die Cyber-Krise wurde „grundsätzlich erfolgreich“ bewältigt. Zu diesem Schluss kommen die Prüferinnen und Prüfer des Rechnunghofes. Dennoch zeigen sie eine Reihe an Verbesserungsmöglichkeiten auf.

Cyber-Einsatzteam und Cyber-Lagezentrum schaffen

Im Hinblick auf das vom Inneren Kreis der Operativen Koordinierungsstruktur (IKDOK) regelmäßig zu erstellende Cyber-Lagebild, vor allem aber, weil ein Zentrum für die Bearbeitung von Cyber-Vorfällen unmittelbar verfügbar sein sollte, wäre ein eigenes, dauerhaft eingerichtetes und jederzeit benutzbares Cyber-Lagezentrum zweckmäßig. Die Koordinationsstruktur des IKDOK selbst, dem wichtigsten interministeriellen Gremium der Cyber-Sicherheit, erachtet der Rechnungshof für geeignet, die ihm übertragenen Aufgaben zu erfüllen.

Außerdem wäre ein permanent verfügbares Cyber-Einsatzteam (Rapid Response Team) zu schaffen. In diesem Zusammenhang macht der Rechnungshof auf den Personalmangel bei Cyber-Sicherheitskräften aufmerksam. So wurden die als notwendig erachteten Personalressourcen, um die Cyber-Sicherheit aufrecht zu halten, im Bundeskanzleramt und im Innenministerium nicht erreicht. Damit mehr geeignetes Personal zur Verfügung steht, wäre ein modernes Personalmanagement einzurichten.

Für ein funktionierendes Cyber-Krisenmanagement sind Krisen-, Kontinuitäts- und Einsatzpläne wesentlich. Solche Pläne lagen jedoch nicht vor, obwohl die Cyber Sicherheit Steuerungsgruppe die Ausarbeitung solcher Pläne bereits 2014 und 2019 beschlossen hatte. Das Bundeskanzleramt und das Innenministerium wären dafür zuständig gewesen.

NIS-Meldeanalysesystem fehlte

Ziel der Cyber-Sicherheit ist, ein hohes Sicherheitsniveau von Netz- und Informationssystemen zu gewährleisten. Anbieter digitaler Dienste, die öffentliche Verwaltung sowie Betreiber wesentlicher Dienste – etwa in den Sektoren Energie, Verkehr, Bankwesen, Finanzmarktinfrastrukturen, Gesundheitswesen, Trinkwasser, digitale Infrastruktur – müssen Sicherheitsvorfälle melden.

Das Innenministerium ist dazu verpflichtet, die weitergeleiteten Meldungen zu Sicherheitsvorfällen zu analysieren und daraus regelmäßig ein Lagebild zu erstellen. Diese Meldungen wurden zwar aktenmäßig erfasst, in einer Meldungsübersicht eingetragen und an das Bundeskanzleramt sowie an das Verteidigungsministerium weitergeleitet. Aber: Der Rechnungshof weist kritisch darauf hin, dass rund zweieinhalb Jahre nach dem Inkrafttreten des Netz- und Informationssystemsicherheitsgesetz (NISG) das gesetzlich geforderte „NIS-Meldeanalysesystem“ noch nicht in Betrieb war. Damit soll die Erstellung des

Lagebildes mittels strategischer und operativer Analyse unterstützt werden. Laut Stellungnahme des Innenministeriums sei ein Meldesammelsystem mittlerweile implementiert und seit dem dritten Quartal 2021 produktiv im Einsatz. Das Meldesammelsystem ist als Vorstufe zum geforderten „NIS-Meldeanalysesystem“ zu betrachten.

Frühwarnsystem war 2021 erst in der Konzeptionsphase

Um etwaigen Sicherheitsvorfällen vorzubeugen, wurde das Innenministerium dazu ermächtigt, ein Frühwarnsystem zu betreiben, das Risiken oder Vorfälle von Netz- und Informationssystemen frühzeitig erkennen kann. Der Rechnungshof stellt kritisch fest, dass das geplante Frühwarnsystem 2021 erst in einer ersten Konzeptionsphase war, obwohl die wirkungsorientierte Folgenabschätzung zum NISG hierzu schon im Jahr 2019 erste Investitionen und bereits im Jahr 2020 Betriebskosten vorsah.

Er empfiehlt dem Innenministerium, das Projekt zur Implementierung des Frühwarnsystems verstärkt zu betreiben und umzusetzen. Im Sinne des gesamtstaatlichen und sektorübergreifenden Ziels, Cyber-Angriffe zu erkennen beziehungsweise deren Auswirkungen so gering wie möglich zu halten sowie Muster und Vorgehensweisen bei Cyber-Angriffen zu analysieren, sollten möglichst viele Organisationen an diesem Frühwarnsystem teilnehmen.