Presseinformation

Rechnungshof Österreich
Unabhängig und objektiv für Sie.

Mag. Christian Neuwirth
Sprecher des Rechnungshofes
1030 Wien, Dampfschiffstraße 2
Tel.: +43 (1) 711 71 – 8435

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

Permanentes und national verfügbares Cyber-Einsatzteam erforderlich

Ereignisse, wie die Cyber-Angriffe auf Websites von Parteien und öffentlichen Einrichtungen im Umfeld der Nationalratswahl 2024, zeigen, wie bedeutend Cyber-Sicherheit und deren Koordination sind. Diesem Thema widmete sich der Rechnungshof bereits 2022 in seinem Bericht „Koordination der Cyber-Sicherheit". Die Umsetzung damaliger Empfehlungen wurde nun auch in einer Follow-up-Überprüfung und im Hinblick auf die neue EU-Cyber-Sicherheits-Richtlinie NIS-2 (Netz- und Informationssystemsicherheit) beurteilt. Seither wurde etwa ein permanentes Cyber-Lagezentrum, das das Cyber-Lagebild erstellt und erörtert, eingerichtet. Andere Empfehlungen waren jedoch erst teilweise oder noch nicht umgesetzt: Koordinierungsstrukturen wurden nur teilweise weiterentwickelt. Sowohl dem Bundeskanzleramt als auch dem Innenministerium empfahl der Rechnungshof, ein permanent verfügbares nationales Cyber-Einsatzteam zu schaffen. Zudem wären Lösungsansätze für die Rekrutierung von Cyber-Sicherheits-Expertinnen und -Experten gemeinsam mit dem dafür zuständigen Bundesministerium für öffentlichen Dienst zu erarbeiten. Weiters empfahl der Rechnungshof, eine staatliche Cyber-Sicherheitsleitstelle mit Einsatzzentrale einzurichten. Der überprüfte Zeitraum der Follow-up-Überprüfung umfasst die Jahre 2021 bis 2023. Zu dieser Thematik hat der Rechnungshof heute einen weiteren Bericht veröffentlicht: „Management der IT-Sicherheit im Land Kärnten".

EU-Cyber-Sicherheits-Richtlinie NIS-2

NIS-2 trat 2023 als eine neue Richtlinie zur Netz- und Informationssystemsicherheit in Kraft. Sie ersetzt ab 18. Oktober 2024 die bisher geltende NIS-Richtlinie und ist bis dahin in nationales Recht umzusetzen. Die neue Richtlinie enthält wesentliche Änderungen, wie etwa im Hinblick auf die Einbeziehung der öffentlichen Verwaltung. Daher ist mit mehr koordinativen Aufgaben zu rechnen. So erweitert NIS-2 den Kreis der Unternehmen und öffentlichen Einrichtungen, die zu Sicherheitsmaßnahmen und Meldungen bei Sicherheitsvorfällen verpflichtet sind. Einrichtungen der öffentlichen

Verwaltung auf Bundesebene waren bisher schon zu Sicherheitsmaßnahmen und Meldungen bei Sicherheitsvorfällen verpflichtet.

Länder stärker einbeziehen

Bei Einrichtungen auf Landesebene waren solche Maßnahmen und verpflichtende Meldungen hingegen abhängig von einer risikobasierten Bewertung. Der Rechnungshof hatte dazu empfohlen, die Länder zu den Sitzungen der Cyber Sicherheit Steuerungsgruppe einzuladen. Das Bundeskanzleramt setzte die Empfehlung nur teilweise um: Es informierte einerseits die Länder über die Vorarbeiten zur rechtlichen Umsetzung der NIS-2-Richtlinie. Andererseits lud das Bundeskanzleramt die Länder jedoch nicht zu den Sitzungen der Cyber Sicherheit Steuerungsgruppe ein.

Weiterhin kein permanent verfügbares nationales Cyber-Einsatzteam

Das Innenministerium richtete ein permanentes Cyber-Lagezentrum ein. Zusätzlich empfahl der Rechnungshof ein permanent verfügbares Cyber-Einsatzteam (Rapid Response Team) in Abstimmung mit dem in der Landesverteidigung geplanten Cyber-Einsatzteam zu schaffen, um Cyber-Sicherheitsvorfälle effizient zu bewältigen. Das Bundeskanzleramt und das Innenministerium setzten diese Empfehlung jedoch nicht um. Laut Bundeskanzleramt könne kein Cyber-Einsatzteam geschaffen werden, da das Bundesministerium für öffentlichen Dienst die dafür vorgesehenen Planstellen abgelehnt habe. Laut Innenministerium sei die Umsetzung dieser Empfehlung gesamtstaatlich in Arbeit und mit dem Schwerpunkt im Verteidigungsministerium eingeleitet worden.

Der Rechnungshof erkennt an, dass das Verteidigungsministerium organisatorische Grundlagen für ein Cyber-Einsatzteam geschaffen hatte und dass im Innenministerium anlassbezogen bei Cyber-Sicherheitsvorfällen Einheiten gebildet werden, die Aufgaben eines solchen Teams wahrnehmen können. Er erachtet jedoch ein permanent eingerichtetes Cyber-Einsatzteam als erforderlich.

Einrichtung einer Cyber-Sicherheitsleitstelle weiter offen

Neben dem fehlenden Cyber-Einsatzteam vermisste der Rechnungshof weiterhin auch die Einrichtung einer Cyber-Sicherheitsleitstelle. Das Bundeskanzleramt verwies diesbezüglich auf die Zuständigkeit des Innenministeriums. Laut

Innenministerium könnten sich die Aufgaben einer Cyber-Sicherheitsleitstelle nur aus der Koordinierung der Tätigkeit von Cyber-Einsatzteams und des Frühwarnsystems ergeben. Da sich beides aber noch in der Konzeptionsphase befindet, wäre eine Cyber-Sicherheitsleitstelle noch nicht erforderlich.

Eine staatliche Cyber-Sicherheitsleitstelle mit Einsatzzentrale ist einzurichten, so die Empfehlung des Rechnungshofes. Auch vor dem Hintergrund der laufenden Umsetzung der NIS-2-Richtlinie, in deren Rahmen die Einrichtung eines Cyber-Sicherheitszentrums geplant ist, sollte die Integration einer Cyber-Sicherheitsleitstelle berücksichtigt werden.

Beschränkte Ressourcen und Planstellen im Computer-Notfallteam der öffentlichen Verwaltung

Wiederholt empfahl der Rechnungshof dem Bundeskanzleramt, in Zusammenarbeit mit dem Bundesministerium für öffentlichen Dienst Lösungsansätze für eine Rekrutierung von Cyber-Sicherheits-Expertinnen und Experten zu erarbeiten. Das entsprechende Fachpersonal sei laut Bundeskanzleramt schwer rekrutierbar, da für Fachkräfte auf dem Gebiet der Cyber-Sicherheit im privatwirtschaftlichen Sektor ein höheres Gehaltsniveau üblich sei.

Insgesamt setzte das Bundeskanzleramt von acht überprüften Empfehlungen zwei ganz, zwei teilweise und vier nicht um. Und das Innenministerium setzte von neun überprüften Empfehlungen drei vollständig, drei zum Teil und drei nicht um.