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

Verschiebung von IT-Arbeitsplätzen erhöhte Cyber-Sicherheitsrisiko in Ministerien

In der öffentlichen Verwaltung ist ein hohes Maß an IT-Sicherheit unverzichtbar. Ändern sich, etwa nach Wahlen oder Regierungsumbildungen, Kompetenzen zwischen Ministerien, werden oft auch Arbeitsplätze verschoben. Das birgt IT-Sicherheitsrisiken. Das stellt der Rechnungshof in seinem heute veröffentlichten Bericht „Management der IT-Sicherheit im Finanzministerium, Klimaschutzministerium und Landwirtschaftsministerium“ fest. Diese kritische Phase dauerte bei den überprüften Ministerien bis zu einem Jahr. Die Prüferinnen und Prüfer empfehlen eine Überarbeitung der IT-Sicherheitsstrategien, klare Zuständigkeiten in den IT-Abteilungen, mehr Awareness-Schulungen für das Personal und teils umfangreichere IT-Sicherheitsprüfungen. Der überprüfte Zeitraum umfasste vor allem die Jahre 2018 bis 2022.

IT-Sicherheitsvorfälle in Österreich

Die öffentliche Verwaltung war in den vergangenen Jahren vermehrt von IT-Sicherheitsvorfällen betroffen. Allein im ersten Quartal 2023 kam es zu mehr als 50 Sicherheitsvorfällen im Cyber-Bereich, fünf davon waren schwerwiegend. Auch die drei Ministerien waren im überprüften Zeitraum von IT-Sicherheitsvorfällen betroffen.

Verschiebung von IT-Arbeitsplätzen aufgrund geänderter Ressortkompetenzen

Im überprüften Zeitraum verschoben sich mehrmals die Kompetenzen zwischen den Bundesministerien. Nach der Nationalratswahl im Jahr 2019 wanderte etwa die Kompetenz „Digitalisierung“ vom Bundesministerium für Digitalisierung und Wirtschaftsstandort zunächst zum Bundesministerium für Finanzen. Ab Mai 2024 übernahm das Bundeskanzleramt diese Agenden. Mit Verschiebungen von Ressortkompetenzen gingen auch Übertragungen von den jeweils zuständigen Organisationseinheiten und Bediensteten sowie deren IT-Arbeitsplätzen einher. Diese Migrationsprozesse dauerten bei den drei überprüften Stellen bis zu

einem Jahr. Dieser Zeitraum ist kritisch für die durchgängige Gewährleistung der IT-Sicherheit. Der Rechnungshof stellt in diesem Zusammenhang fest, dass das Bundesministeriengesetz zwar die Kompetenz für die Koordination der IT festlegte, es aber die Aspekte der Koordination der IT-Sicherheit nicht ausdrücklich erwähnte. Er empfiehlt dem seit Mai 2024 auch für Digitalisierungsangelegenheiten zuständigen Bundeskanzleramt, eine Regierungsvorlage zu erarbeiten, mit der im Bundesministeriengesetz eine Kompetenz zur Koordination der IT-Sicherheit klar und ausdrücklich festgelegt wird.

Der Rechnungshof weist auch darauf hin, dass die Integration der neu einzugliedernden und das Herauslösen der abzugebenden Organisationseinheiten mit hohem Arbeits- und Zeitaufwand verbunden waren.

NIS-2-Richtlinie in Vorbereitungsprozess

Ende 2022 erließen das Europäische Parlament und der Rat die NIS-2-Richtlinie (Netz- und Informationssystemsicherheit). Durch die Richtlinie soll ein hohes gemeinsames Cybersicherheitsniveau in der EU erreicht werden. Die EU-Mitgliedstaaten sind verpflichtet, sie bis Oktober 2024 in nationales Recht umzusetzen. Die Vorbereitung zur Umsetzung in Österreich obliegt dem Bundeskanzleramt. Die Begutachtung zum nationalen Gesetzesentwurf endete mit 1. Mai 2024.

Der Rechnungshof empfiehlt, sich auf die Anforderungen durch die Umsetzung der NIS-2-Richtlinie vorzubereiten und den nationalen Umsetzungsprozess zu begleiten. So können wesentliche Aufgaben wie Risikomanagement, Notfallvorsorge, Krisenmanagement oder Verantwortung der Ressortleitung ressortintern zeitgerecht berücksichtigt werden.

Unvollständige und veraltete IT-Sicherheitsstrategien

Verbesserungsbedarf sieht der Rechnungshof jeweils bei den IT-Sicherheits-strategien. So war in der Strategie des Finanzministeriums die Verantwortung der Ressortleitung für die IT-Sicherheit nicht ausdrücklich festgeschrieben. Die Strategie des Klimaschutzministeriums stammte aus dem Jahr 2002 und entsprach damit nicht mehr den aktuellen Gegebenheiten. Das Landwirtschaftsministerium hatte keine intern kundgemachte, ressortweite Strategie erlassen.

Fehlende und vermischte Funktionsrollen in den IT-Sicherheitsorganisationen

Für eine effiziente IT-Sicherheit bedarf es klarer Rollen. Für Fragen der Informations- und IT-Sicherheit ist etwa ein Chief Information Security Officer (CISO) verantwortlich. Die Leiterin/der Leiter der für die gesamte Infrastruktur und den Betrieb verantwortlichen IT-Abteilung wird als Chief Information Officer (CIO) bezeichnet.

Der Rechnungshof hält kritisch fest, dass das Klimaschutzministerium im überprüften Zeitraum über keinen CISO verfügte. Im Landwirtschaftsministerium war die Rolle des CISO mit der Rolle des IT-Abteilungsleiters CIO ident.

Höhere IT-Sicherheit beim Personal durch mehr Awareness-Schulungen

Um die IT-Sicherheit zu erhöhen, muss das Personal auch entsprechend geschult sein und auf potenzielle Gefahren aufmerksam gemacht werden. Auch hier sieht der Rechnungshof Verbesserungsbedarf. Im Finanzministerium hatten erst 60 Prozent der Bediensteten IT-Awareness-Schulungen besucht. Bei den Awareness-Schulungen im Klimaschutzministerium war das Thema IT-Sicherheit noch nicht im Arbeitsalltag integriert. Und im Landwirtschaftsministerium war die Teilnahme an solchen Schulungen nur freiwillig vorgesehen.

Der Rechnungshof empfiehlt, Awareness-Schulungen regelmäßig, in erhöhtem Ausmaß und verbindlich in den Arbeitsalltag zu integrieren. Unabhängig davon empfiehlt er den drei überprüften Stellen, in Bezug auf Telearbeit konkret festzulegen, ob bestimmte dienstliche Aufgaben aus Sicherheitsgründen an der Dienststelle zu verrichten sind.

IT-Infrastruktur flächendeckenden und externen Sicherheitsüberprüfungen unterziehen

Der Rechnungshof erkennt an, dass das Finanzministerium durch die Zertifizierungen und die zahlreichen IT-Sicherheitsüberprüfungen die Sicherheitsrisiken in einem hohen Ausmaß aufdecken, analysieren und durch geeignete Maßnahmen reduzieren konnte. Er kritisiert, dass die von Landwirtschaftsministerium und Klimaschutzministerium durchgeführten IT-Sicherheitsüberprüfungen nicht alle wesentlichen Bereiche im überprüften Zeitraum abdeckten. Außerdem waren externe Expertinnen und Experten zur unabhängigen Überprüfung der IT-Sicherheit nicht eingebunden.

Der Rechnungshof empfiehlt den beiden Bundesministerien daher, den Bedarf an IT-Sicherheitsüberprüfungen mittels umfassender Risikoanalyse zu erheben sowie die notwendigen IT-Sicherheitsüberprüfungen durchzuführen. Die daraus gewonnenen Erkenntnisse sind schließlich zeitnah und unter Einbindung von externem Fachwissen zu evaluieren. Außerdem sollen die zwei Ministerien ihre jeweiligen Authentifizierungsmethoden für die IT-Arbeitsplätze einer Risikoanalyse unterziehen sowie die Möglichkeit einer Zwei-Faktor-Authentifizierung in Erwägung ziehen.