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

Verbesserungsbedarf bei IT-Sicherheit des Landes Kärnten nach schwerwiegendem Cyber-Angriff im Jahr 2022

Das Land Kärnten war im Jahr 2022 einem Cyber-Angriff mit Datendiebstahl und Erpressung ausgesetzt. Dabei wurde die IT-Infrastruktur des Landes lahmgelegt, was erhebliche Auswirkungen auf die Landesverwaltung hatte. Die Angreifer kamen in den Besitz personenbezogener Daten und forderten Lösegeld in Höhe von fünf Millionen Euro in Bitcoins. Das Land Kärnten hatte zwar bereits vor dem Cyber-Angriff Maßnahmen im Bereich der IT-Sicherheit umgesetzt, die Maßnahmen konnten den Angriff jedoch weder erkennen noch verhindern. Das IT-Sicherheitsmanagement insgesamt war lückenhaft, stellt der Rechnungshof in seinem heute veröffentlichten Bericht „Management der IT-Sicherheit im Land Kärnten“ fest. Nach dem Cyber-Angriff setzte das Land Kärnten weitere Schritte zur Erhöhung der IT-Sicherheit. Es fehlten aber Ende 2023 weiterhin: die Zwei-Faktor-Authentifizierung für alle IT-Arbeitsplätze, die vollständige Dokumentation der umgesetzten IT-Sicherheitsmaßnahmen oder etwa ein umfassendes IT-Notfallhandbuch sowie verstärkte IT-Sicherheitsüberprüfungen. Das Land Kärnten leistete keine Lösegeldzahlungen im Zusammenhang mit dem Cyber-Angriff. Auch vor dem Hintergrund der DDoS-Angriffe (DDoS: eine Vielzahl von Anfragen führt zur Blockierung eines Dienstes) auf die Websites österreichischer Parteien und öffentlicher Einrichtungen, die im Umfeld der Nationalratswahl 2024 stattfanden, hält der Rechnungshof fest: Neben der Erhöhung der IT-Sicherheit ist auch die Zusammenarbeit mit Bundesbehörden und Cyber-Gremien wesentlich, um die Auswirkungen von Cyber-Angriffen zu verhindern oder möglichst gering zu halten. Der überprüfte Zeitraum umfasste die Jahre 2020 bis 2023. Zu dieser Thematik hat der Rechnungshof heute einen weiteren Bericht veröffentlicht: „Koordination der Cyber-Sicherheit; Follow-up-Überprüfung“.

Cyber-Angriff blieb zunächst unbemerkt

Gemäß einer forensischen Analyse gelangten die Angreifer am 21. April 2022 über einen Arbeitsplatzrechner in die IT-Systeme des Landes Kärnten. Das Land Kärnten

erkannte den Ransomware-Angriff am 24. Mai 2022 aufgrund von Unregelmäßigkeiten im Netzwerk. Das waren beispielsweise Anmeldeschwierigkeiten sowie verschlüsselte Arbeitsplatzrechner und verschlüsselte Server-Systeme. Als Ransomware werden Schadprogramme bezeichnet, die den Zugriff auf Daten und Systeme einschränken oder verhindern und diese Ressourcen nur gegen Zahlung eines Lösegelds (Englisch: ransom) wieder freigeben. Die Angreifer hinterließen eine Erpressernachricht im Darknet, die eine Lösegeldforderung beinhaltete. Am 3. Juni 2022 wurden auf einer öffentlich zugänglichen File-Sharing-Plattform Daten des Landes Kärnten im Umfang von 5,6 Gigabyte (GB) online gestellt. Tatsächlich flossen Daten im Umfang von vermutlich etwa 250 GB ab. Betroffen waren dabei Daten der Landesverwaltung, so eine forensische Untersuchung eines externen Dienstleisters. Darunter waren auch Daten von etwa 80.000 Personen im Zusammenhang mit Niederlassungs- und Aufenthaltsbewilligungen, persönliche Dateien von Regierungsmitgliedern und Landesbediensteten sowie personenbezogene Daten, etwa zu Reisepässen. Das Datensicherungssystem (Backup) konnten die Angreifer nicht kompromittieren.

5,75 Millionen Euro für Sofort- und Wiederherstellungsmaßnahmen

Nach Bekanntwerden des Cyber-Angriffs am 24. Mai 2022 traf das Land Kärnten umgehend technische Vorkehrungen und stellte für Sofort- und Wiederherstellungsmaßnahmen 5,75 Millionen Euro zur Verfügung. Es richtete ein Rapid Response Team ein, baute eine neue Firewall auf und errichtete einen DDoS-Schutz. Zur Zeit der Rechnungshof-Prüfung waren auch weitere technische Maßnahmen abgeschlossen, etwa die Absicherung des Netzwerks oder die Sicherung der notwendigen IT-Dienste. Was noch fehlte, war etwa eine flächendeckende Zwei-Faktor-Authentifizierung, bei der der Identitätsnachweis von Bediensteten mittels einer Kombination aus zwei unterschiedlichen, voneinander unabhängigen Komponenten erfolgt, sowie eine USB-Port-Deaktivierung beziehungsweise -Kontrolle, die das Risiko reduzieren, Schadsoftware zu laden.

IT-Sicherheit an NIS-2-Richtlinie anpassen

In Hinblick auf die NIS-2-Richtlinie (Netz- und Informationssystemsicherheit) der EU ist es für das Land Kärnten zweckmäßig, die empfohlenen Maßnahmen umzusetzen. Die NIS-2-Richtlinie, die bis Mitte Oktober 2024 umgesetzt werden soll, erfordert eine Erhöhung der IT-Sicherheitsmaßnahmen in öffentlichen Einrichtungen auf Bundes- und Landesebene, insbesondere im Bereich Risiko- und Notfallmanagement. Das Land Kärnten sollte auch seine IT-Sicherheitsstrategie aktualisieren und

diese zukünftig regelmäßig überprüfen. Der Rechnungshof empfiehlt zudem, ein umfassendes IT-Notfallhandbuch (inklusive überarbeiteter Anforderungen an das Notfallrechenzentrum) zu erstellen; dieses sollte alle jene Prozesse abbilden, die den Betrieb auch in Ausnahmesituationen aufrecht halten können. Dabei sollten insbesondere die Notfallvorsorge und -bewältigung sowie Tests und Übungen berücksichtigt werden.

Nationale Zusammenarbeit bei Cyber-Angriffen erforderlich

Grundsätzlich hält der Rechnungshof fest: Schwerwiegende Cyber-Angriffe erfordern eine Zusammenarbeit auf Bundes- und Landesebene. Anlaufstellen für die Bewältigung von Cyber-Angriffen können Unterstützung leisten. Darunter sind beispielsweise die NIS-Behörde im Innenministerium, bei der die Einrichtungen der Länder Risiken, Vorfälle und Cyber-Angriffe melden können, oder das Cybercrime Competence Center im Bundeskriminalamt, das als nationale Koordinierungs- und Meldestelle im Bereich Cyberkriminalität zuständig ist. Im Zusammenhang mit der Bewältigung der Cyber-Krise im Außenministerium im Dezember 2019 erstellte das Bundeskanzleramt einen „Lessons Learned"-Bericht. Laut diesem Bericht hätte der Einsatz eines ständig verfügbaren Cyber-Einsatzteams (Rapid Response Team) und eines Security Operations Centers (SOC) bereits zu Beginn des Angriffs zu einer rascheren Behebung der Cyber-Krise beigetragen. Beides war – im Sinne einer staatlichen Cyber-Sicherheitsleitstelle – im Dezember 2023 noch nicht eingerichtet.