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

Bessere Abstimmung im Fall von Cyber-Angriffen auf den Staat notwendig

Cyber-Defence ist die Abwehr von Cyber-Angriffen: etwa auf die Souveränität des österreichischen Staates oder auf die Einrichtungen des Bundesheeres. Ein sogenannter Souveränitätsfall tritt ein, wenn die Informations- und Kommunikationstechnologie (IKT) der obersten Organe der Republik sowie kritische Infrastruktur, beispielsweise Krankenhäuser oder Energieversorger, aus dem Cyber-Raum angegriffen werden – und die Unabhängigkeit und Funktionsfähigkeit dieser Einrichtungen maßgeblich beeinträchtigt sind. Wann aber die damit einhergehende notwendige Überleitung von der Cyber-Krise in den Cyber-Defence-Fall vorgenommen wird und welche Schritte zu setzen sind, darüber herrscht Unklarheit. Das stellt der Rechnungshof in seinem heute veröffentlichten Bericht „Koordination der Cyber-Defence“ fest. Als Entscheidungsgrundlage soll die Leitlinie Cyber-Defence dienen, die die Verantwortlichkeiten und die einzelnen Verfahrensschritte im Detail klarstellt, empfiehlt der Rechnungshof. Diese war zur Zeit der Prüfung jedoch noch nicht fertiggestellt. Was ebenfalls fehlte: Cyber-Übungen für das Szenario einer Souveränitätsgefährdung. Der überprüfte Zeitraum umfasst im Wesentlichen die Jahre 2021 bis November 2022.

Konzepte müssen zügig vorangetrieben werden

Die Verantwortung, die Cyber-Sicherheit zu koordinieren, liegt bei den Sicherheitsressorts: Bundeskanzleramt, Innenministerium, Außenministerium sowie Verteidigungsministerium. Im Cyber-Vorfalls- und Krisenmanagement ist das Innenministerium für operative Maßnahmen zuständig. Das Bundesheer wirkt mit, wenn seine Assistenzleistung eigens angefordert wird. Beim Übergang von einer Cyber-Krise in einen Cyber-Defence-Einsatz im Zuge eines Souveränitätsfalls geht die Zuständigkeit von der Innenministerin beziehungsweise dem Innenminister auf die Verteidigungsministerin beziehungsweise den Verteidigungsminister über.

Zu beurteilen, wann tatsächlich ein Souveränitätsfall eintritt, ist Aufgabe der Verteidigungsministerin oder des Verteidigungsministers. Das Verteidigungsministerium hatte dazu jedoch noch keine konkreten Kriterien und Szenarien ausgearbeitet. Zu klären war, welches Ausmaß die Auswirkungen eines Cyber-Angriffs erreichen müssten, um einen militärischen Einsatz zu rechtfertigen. Zudem hat das Bundesheer die Souveränität des Staates im Cyber-Raum erst zu schützen, wenn bei einem Angriff der Verdacht auf ausländische staatliche Akteure vorliegt. Die Leitlinie zur Cyber-Defence war zur Zeit der Rechnungshof-Prüfung erst in Ausarbeitung; der Rechnungshof empfahl, diese mit konkreten Kriterien und Szenarien zur Beurteilung eines Souveränitätsfalls zu ergänzen.

Rund 390.000 Sicherheitsereignisse im Monat abgewehrt

Beispielsweise allein in der Zeitspanne von einem Monat, Ende Oktober bis Ende November 2022, wurden im Verteidigungsministerium rund 390.000 Sicherheitsereignisse abgewehrt. Die Direktion 6 der Generaldirektion für Landesverteidigung ist für die gesamten IKT-Agenden des Verteidigungsministeriums und Bundesheeres zuständig. Darunter fällt auch die operative Umsetzung der Cyber-Defence.

Vor dem Hintergrund der steigenden Bedeutung von Cyber-Defence und um die Sicherheit im Cyber-Raum aufrechtzuerhalten, sollten die Entwicklung der Cyber-Fähigkeiten und die Stärkung der Cyber-Kräfte des Bundesheeres zügig vorangetrieben werden, empfiehlt der Rechnungshof. Koordiniertes, strategisch geleitetes und rasches Eingreifen soll sichergestellt werden. Neben den fehlenden Konzepten kritisieren die Prüferinnen und Prüfer, dass das Verteidigungsministerium beziehungsweise das Bundesheer noch keine spezifischen Übungen zu einem Cyber-Defence-Fall aufgrund einer Souveränitätsgefährdung durchgeführt hatte.

Geplante Einsatz-Teams fehlen, Cyber-Grundwehrdiener verstärkt bewerben

Um auf Cyber-Angriffe rasch reagieren zu können, plante das Verteidigungsministerium die Einrichtung von bis zu acht ständig verfügbaren Einsatzteams – bis Ende 2022 sollten zwei dieser Teams einsatzbereit sein. Aber: Im November 2022 lagen dazu lediglich Planungsunterlagen vor. Das Verteidigungsministerium machte dafür fehlende Personalressourcen verantwortlich. Der Rechnungshof empfiehlt, diese Personallücken rasch zu füllen. Und: Etwa bereits bei der Stellungskommission könnten Personen mit IKT-Ausbildung für den Einsatz als Cyber-Grundwehrdiener verstärkt motiviert werden.