Prüfung der Wirksamkeit der Vorfallbewältigung beim Schutz der Bundes-IKT vor Cyberrisiken

Nationales Zentrum für Cybersicherheit

Das Wesentliche in Kürze

Als Fachstelle IKT-Sicherheit des Bundes (IKT steht für Informations- und Kommunikationstechnologie) erlässt das Nationale Zentrum für Cybersicherheit (NCSC) Vorgaben zur Cybersicherheit innerhalb der Bundesverwaltung (BV), überprüft deren Einhaltung und unterstützt die Leistungserbringer bei der Beseitigung von Schwachstellen.

Die vom Bundesrat verabschiedete Verordnung über den Schutz vor Cyberrisiken in der Bundesverwaltung ist seit dem 1. Juli 2020 in Kraft. Sie bildet die rechtliche Grundlage für den Auf- und Ausbau des NCSC und regelt Struktur und Aufgaben sowie Kompetenzen der beteiligten Behörden. Darin wurde das NCSC ermächtigt, bei einem Cybervorfall der das ordnungsgemässe Funktionieren der BV gefährdet, nach Rücksprache mit den betroffenen Dienststellen, die Federführung bei der Bewältigung zu übernehmen.

Im Rahmen dieser Prüfung hat die Eidgenössische Finanzkontrolle (EFK) den entsprechenden Prozess auf seine Wirksamkeit überprüft. Dabei wurden insbesondere die Fragestellungen des zeitnahen Informationsflusses von den Informationsquellen zum NCSC, sowie die Zusammenführung dieser Informationen mit den eigenen Überwachungsergebnissen beurteilt. Des Weiteren wurden das Erkennen eines Cybervorfalls und die zeitgerechte Umsetzung von Massnahmen und der Informationsfluss zu den relevanten Stellen evaluiert.

Der Vorfallbewältigungsprozess ist definiert, publiziert und wird durchgeführt. Die Rollen und Zuständigkeiten sind grundsätzlich zugewiesen, aber die Rolle der Informatiksicherheitsbeauftragten der Organisationseinheiten (ISBO) muss gestärkt werden. Verbesserungsbedarf besteht hinsichtlich der Übersicht über die Akteure, wenn externe Leistungserbringer involviert sind. Die Rahmenbedingungen sind zwar grundsätzlich geeignet, doch die Kommunikationswege und die Aktualität von Meldungen müssen verbessert werden.

Die Meldung eines Cybervorfalls muss schneller erfolgen

Die unverzügliche Meldung eines Cybervorfalls ist wichtig, damit eine übergeordnete Analyse und Einschätzung der Gefahr gemacht werden kann. Dadurch kann die Gefahr einer lateralen Ausbreitung in der gesamten BV eingedämmt oder im besten Fall verhindert werden. Im Rahmen der Prüfung hat die EFK festgestellt, dass die Kommunikation ans NCSC noch ausgebaut werden muss. So ist die horizontale Steuerung, insbesondere der Informationsaustausch zwischen den Leistungserbringern (LE), noch nicht überall sichergestellt. Zudem müssen die Informatiksicherheitsbeauftragten der Departemente schneller informiert werden.

Herausfordernd ist auch die Koordination respektive Harmonisierung der Kategorisierung von Cybervorfällen, wenn ein solcher mehrere LE betrifft. Wenn dies nicht geschieht, be-

steht die Gefahr, dass die verschiedenen LE einen Vorfall mit unterschiedlicher Priorität angehen. Eine solche Konstellation kann auch zu inkonsistenter Kommunikation gegenüber Dritten führen.

Die Rolle des ISBO sollte gestärkt und eine Übersicht externer LE geschaffen werden

Eine wichtige Rolle, um Cybervorfälle zu melden, nehmen die ISBO ein: Als Leistungsbezüger (LB) melden sie Cybervorfälle an ihre LE, die wiederum das NCSC informieren. Da je nach Grösse der LB unterschiedliche Maturitätsniveaus bestehen, ist jedoch nicht immer eine Stellvertretung definiert. Bei Abwesenheit des ISBO kann sich die Meldung eines Cybervorfalls entsprechend verzögern und damit auch die zeitnahe Meldung an das NCSC. Dies sollte umgehend korrigiert werden.

Bei Auftreten eines Cybervorfalls kann nicht innert kurzer Zeit festgestellt werden, welche Applikationen und Services von welchem Lieferanten für welche Verwaltungseinheit (VE) betreut werden. Somit können bei der Meldung eines IT-Sicherheitsvorfalls bei einem externen LE die betroffenen VE nicht umgehend informiert werden, was grundsätzlich die Verwundbarkeit der BV erhöht. Die Erstellung eines übergreifenden Inventars sollte folglich in Betracht gezogen werden.

Werkzeuge sollten effizienter eingesetzt werden

Die Beschaffung von Überwachungswerkzeugen sollte auf Stufe BV harmonisiert werden und zentral erfolgen, um nicht unterschiedliche Werkzeuge mit denselben oder ähnlichen Funktionalitäten einzusetzen. Dadurch werden mögliche Skaleneffekte hinsichtlich der Kosten und des Know-how–Aufbaus genutzt.

Die Mustervertragsklausel muss optimiert werden

Die Beschaffungskonferenz des Bundes hat eine Mustervertragsklausel betreffend Cyberrisiken erstellt. Die vertraglichen Punkte zur Informatiksicherheit gehen in die richtige Richtung. Fristen zur Meldung von Cybervorfällen sind jedoch nicht einheitlich vorgegeben und müssten entsprechend praxistauglich definiert werden. Zudem müsste diese Klausel bei langjährigen Verträgen nachverhandelt werden.