Prüfung des Schutzes kritischer Infrastrukturen – Umsetzung der Mindeststandards in der Flugsicherung

Skyguide

Das Wesentliche in Kürze

Kritische Infrastrukturen (KI) stellen die Versorgung der Schweiz mit unverzichtbaren Gütern und Dienstleistungen sicher. Um diese KI zu schützen, muss eine möglichst permanente Funktionstüchtigkeit gewährleistet sein. In diesem Zusammenhang kommt der Resilienz der Informations- und Kommunikationstechnik (IKT) bzw. dem Schutz der kritischen Infrastrukturen (SKI) vor Cyberbedrohungen eine hohe Bedeutung zu. Der Bundesrat hat am 8. Dezember 2017 die nationale Strategie zum SKI (2018–2022) verabschiedet. Dazu gehören auch die zivile Luftfahrt und die Flugsicherung. Skyguide besorgt im Auftrag des Bundes die zivile und militärische Flugsicherung in der Schweiz und in angrenzenden Gebieten. Der Bund ist Mehrheitsaktionär der Skyguide.

Die Eidgenössische Finanzkontrolle (EFK) hat die Einhaltung von Minimalanforderungen zum IKT-Schutz gegen Cyberangriffe bei Skyguide geprüft. Dabei kam der vom Bundesamt für wirtschaftliche Landesversorgung (BWL) für Betreiber von KI empfohlene «Minimalstandard zur Verbesserung der IKT-Resilienz» zum Einsatz. Dieser deckt im Wesentlichen die fünf Themenbereiche «Identifizieren», «Schützen», «Detektieren», «Reagieren» und «Wiederherstellen» ab und bietet konkrete Massnahmen zur Umsetzung an.

Skyguide bearbeitet die fünf Themenbereiche systematisch. Das minimale Sicherheitsniveau, wie durch den IKT-Minimalstandard empfohlen, wird aktuell noch nicht vollständig erreicht. Der Grossteil der dazu noch notwendigen Arbeiten ist bereits identifiziert und angestossen. Die Prüfung der EFK hat jedoch zusätzliches Optimierungspotenzial erkannt.

Das Informationssicherheitsmanagement muss bereitstehen

Ein Information Security Management System (ISMS, engl. für «Managementsystem für Informationssicherheit») ist ein grundlegender Baustein der Informationssicherheit. Im ISMS sind Regeln, Verfahren, Massnahmen und Werkzeuge definiert, mit denen sich die Informationssicherheit steuern, kontrollieren, sicherstellen und optimieren lässt.

Bei Skyguide laufen nach Anforderungen des Bundesamts für Zivilluftfahrt zielführende Arbeiten zur Implementierung eines ISMS. Zum Zeitpunkt der Prüfung war dieses noch nicht fertiggestellt und die Umsetzung muss gewährleistet werden.

Zugriffsrechte, das Schwachstellenmanagement und eine konsequente Umsetzung von Vorgaben sind zu verbessern

Um Sicherheitsrisiken zu minimieren, sollte ein Benutzer nur über Berechtigungen verfügen, welche er für die Ausübung seiner Arbeit zwingend benötigt. Skyguide wendet dieses «Prinzip der geringsten Privilegien» an. Jedoch werden die vergebenen Zugriffsrechte nicht regelmässig überprüft. So ist nicht sichergestellt, dass nach Veränderungen der Aufgaben eines Benutzers (z. B. Abteilungs- oder Funktionswechsel) die Berechtigungen angepasst werden.

Administratoren verfügen über umfassende Berechtigungen, mit welchen Sicherheitsmassnahmen der Systeme verändert oder sogar ausgeschaltet werden können. Entsprechend sind Administratoren primäre Ziele für Angreifer. Administratoren müssen zum Thema IT-Sicherheit regelmässig sensibilisiert und geschult werden. Dies findet im Moment nicht systematisch statt.

Skyguide hat zur Erfassung von technischen Verwundbarkeiten ihrer Hard- und Software eine automatisierte Verwundbarkeitsanalyse implementiert. Jedoch müssen die Entwickler sowie Applikationsverantwortlichen noch besser im Umgang mit den Resultaten der Analysen geschult werden. Verwundbarkeiten sind zwingend zentral zu erfassen und zu kategorisieren, um sie anschliessend kontrolliert zu beheben.

Die EFK hat in einer Stichprobe festgestellt, dass nach Änderungen von Vorgaben die betroffenen Parameter auf einem bestehenden System nicht an die neuen Werte angepasst wurden. Skyguide muss im Rahmen des formellen Änderungsprozesses sicherstellen, dass alle Systeme an neue Anforderungen angepasst werden.

Fehlende Georedundanz könnte längere Serviceunterbrüche zur Folge haben

Die Systeme für die Flugsicherung sind redundant vorhanden, jedoch physisch nicht in verschiedenen Lokalitäten aufgebaut. Entsprechend wird beim Ausfall eines gesamten Standorts der Service unterbrochen, wodurch die Flugsicherung in der ganzen Schweiz nicht mehr sichergestellt ist. Zudem bestanden noch keine Business-Continuity- oder Disaster-Recovery-Pläne für ein solches Szenario, sodass Skyguide im Moment schlecht auf einen solchen Vorfall vorbereitet ist.

Eine Optimierung des Lieferantenmanagements ist nötig

Skyguide hat den Betrieb wichtiger Teile ihrer IKT-Infrastruktur an Dienstleister ausgelagert. Dies erhöht die Komplexität bei Änderungen an den Systemen und bedingt eine sehr gute Kommunikation und Zusammenarbeit, um Systemausfällen vorzubeugen. Ebenso müssen die Reaktionen auf Systemausfälle sehr gut vorbereitet werden. Verschiedene Vorfälle haben gezeigt, dass in diesem Bereich noch Optimierungspotenzial besteht.

Skyguide muss bei sämtlichen kritischen Dienstleistern die Risiken aus den Lieferketten adressieren.