Querschnittsprüfung der Massnahmen bei Systemausfällen von Fachapplikationen

Bundesamt für Zoll und Grenzsicherheit, Eidgenössische Steuerverwaltung, Bundesamt für Informatik und Telekommunikation

Das Wesentliche in Kürze

Ein Business Continuity Management (BCM) dient der Aufrechterhaltung des Geschäftsbetriebs einer Organisation beim Eintreten eines Schadensereignisses. Darunter fällt die Vorbereitung, die Bewältigung und die Nachbereitung eines Ereignisses. Im Frühjahr 2017 wurde ein bundesweites BCM-Regelwerk verabschiedet und von den Departementen und der Bundeskanzlei in Kraft gesetzt.

Die Eidgenössische Finanzkontrolle (EFK) prüfte beim Bundesamt für Zoll und Grenzsicherheit (BAZG) und bei der Eidgenössische Steuerverwaltung (ESTV) den Stand der Umsetzung des BCM anhand eines Frameworks zur Ermittlung des Reifegrades.

Da die Datensicherung und die Wiederherstellung nach einem Ereignis eine wichtige Komponente eines BCM darstellt, wurde in einem parallellaufenden Audit die Sicherungsanwendung «NetBackup» beim Bundesamt für Informatik und Telekommunikation (BIT) geprüft. Dabei wurde der sichere Betrieb und die Zuverlässigkeit der Sicherungs- und Wiederherstellungsprozesse untersucht.

Das BCM-System des BAZG verfügt über einen hohen Reifegrad

Die Dokumentationen und Konzepte für das BCM weisen beim BAZG einen hohen Detaillierungsgrad aus. Die kritischen Geschäftsprozesse sind identifiziert und das Vorgehen im Schadenfall ist ausführlich beschrieben. Die geplanten Massnahmen sind nachvollziehbar und für das BAZG angemessen. Die Informatikmittel, die diese Prozesse unterstützen, sind redundant und hochverfügbar aufgebaut.

Das Testen und Üben der BCM-Massnahmen wurden in den vergangenen Jahren aufgrund verschiedener Einflüsse vernachlässigt. Eine detaillierte Aufstellung der geplanten Übungen liegt vor und diese sollen sich in den kommenden Jahren über sämtliche Bereiche des BCM erstrecken.

Die ESTV hat wesentliche Fortschritte erzielt, weitere Arbeiten sind noch zu leisten

Das BCM der ESTV hat, verglichen mit der letzten Beurteilung im Jahr 2016, grosse Fortschritte erzielt. Die erforderlichen Dokumente sind vorhanden, sind jedoch teilweise zu generisch gehalten. So werden die in der Business-Impact-Analyse festgehaltenen kritischen Geschäftsprozesse in der Planung nicht konsequent weiterbehandelt.

Ein übergeordnetes Testkonzept, welches die Testarten und Anspruchsgruppen definiert, ist nicht vorhanden. Zu einzelnen Übungen wurden jedoch gesonderte Konzepte erarbeitet. Eine Evakuierungsübung konnte im letzten Jahr erfolgreich durchgeführt werden.

Schutz vor Verschlüsselungstrojanern hat höchste Priorität

Die Systeme zur Erbringung der Marktleistung «Backup und Recovery» des BIT sind redundant aufgebaut und werden hochverfügbar betrieben. Die implementierten Sicherheitsmassnahmen entsprechen den heutigen Anforderungen.

Die vertraglich vereinbarten Wiederherstellungszeiten können jedoch bei grossen Datenbanken aufgrund ihrer Volumen nicht vollumfänglich sichergestellt werden.

Eines der grössten Risiken hinsichtlich der Verfügbarkeit von Systemen und Datenbanken sind heute Verschlüsselungstrojaner, sogenannte Ransomware. Ein expliziter Schutz dagegen ist auf den Backup-Systemen noch nicht implementiert. Das BIT hat dies adressiert, ausserdem ist ein externes Assessment zum Schutz der Datensicherungen gegen Ransomware geplant. Dieser Sachverhalt gilt es zu priorisieren, allfällige Massnahmen sind zeitnah umzusetzen.