Querschnittsprüfung IT-Sicherheit des Bundes
Informatiksteuerungsorgan des Bundes

Das Wichtigste in Kürze

In der vierten Querschnittsprüfung der IT-Sicherheit des Bundes seit 2011 hat die Eidgenössische Finanzkontrolle (EFK) die Massnahmenumsetzung des IKT-Grundschutzes geprüft. Die Massnahmen sind in einem 17 Kapitel umfassenden Katalog enthalten, das vom Informatiksteuerungsorgan des Bundes (ISB) herausgegeben wird. Ihre Umsetzung obliegt sowohl den Leistungserbringern (LE) als den Leistungsbezügern (LB) und muss dokumentiert werden. Unter die Lupe genommen wurden die Praktiken der sieben Departemente, der Bundeskanzlei, von fünf LE und des ISB. Ausserdem wurden zwölf als kritisch beurteilte Anwendungen untersucht. Schliesslich hat die EFK die Umsetzung des Risikomanagementprozesses im Zusammenhang mit der nachrichtendienstlichen Ausspähung sowie die Umsetzung der Empfehlungen aus früheren Querschnittsprüfungen evaluiert.

Die Prüfung der Praktiken der Leistungsbezüger zeigt ein kontrastreiches Bild

Die überwiegende Mehrheit der untersuchten Verwaltungseinheiten (VE) führt ein aktuelles Inventar der bestehenden Anwendungen. Vom Standpunkt der Sicherheit aus betrachtet empfiehlt die EFK jedoch, möglichst auf die Zusammenlegung von kleineren Anwendungen zu verzichten. Die Sicherheitsdokumente werden nicht für alle Anwendungen herausgegeben und aktualisiert. Im Zuge der RUAG-Affäre sind Korrektivmassnahmen im Gang. Die EFK begrüsst die laufenden Verbesserungen der Tools, mit denen die Sicherheitsdokumente kontrolliert werden können. Ihres Erachtens sind die Kontrollen der Massnahmenumsetzung allerdings noch ungenügend.

Die periodische Kontrolle der Nutzerrechte wird oft vernachlässigt. Die EFK hat zuhanden der betroffenen Departemente Empfehlungen abgegeben. Sie hat zudem festgestellt, dass im Zulassungsprozess der Informatikbeschaffungen der Sicherheitsaspekt bisweilen vernachlässigt werden kann. Sie hat dem ISB empfohlen, seine Rolle in diesen Prozessen zu überprüfen.

Für die meisten der untersuchten kritischen Anwendungen sind aktuelle Sicherheitsdokumente verfügbar. Auf materieller Ebene ist die EFK der Auffassung, dass die Mehrheit der Sicherheitskonzepte dem Schutzbedürfnis inhaltlich angemessen Rechnung trägt. In einem Fall werden die Vertraulichkeitsanforderungen aber unterschätzt. Die Umsetzung einer Lösung ist bereits in Gang. Bei den drei Anwendungen mit Fernwartung werden die Vorschriften eingehalten: Es werden spezielle Anwenderkonten definiert, deren Zugang und Aktivitäten gespeichert und kontrolliert werden. Es ist keinerlei sofortige Verbesserungsmassnahme notwendig.

Die Praktiken der Leistungserbringer sind insgesamt zufriedenstellend

Die untersuchten LE arbeiten aktiv bei der Erarbeitung und der Kontrolle der projektbezogenen Sicherheitsdokumente mit. In den meisten Fällen kontrollieren sie auch die Umsetzung der Sicherheitsmassnahmen, die ihnen obliegen. Ausserdem führen sie regelmässig verschiedene Tätigkeiten durch, die der ständigen Verbesserung der Sicherheit dienen. Die EFK erachtet die Situation als insgesamt zufriedenstellend.

Die LE haben die vom ISB definierten Kontrollmassnahmen in Bezug auf die Systemintegrität umgesetzt. Die EFK stellt jedoch bei den umgesetzten Techniken der einzelnen LE beträchtliche Unterschiede fest. Sie ermutigt das ISB, die Integritätsbegriffe genauer zu definieren und die einschlägigen

Vorschriften zusammenzufassen. Zudem sind die Lösungen, mit denen die Integrität der laufenden Systeme überwacht wird, mit den LE zu koordinieren.

Zunehmende Komplexität der Informatiksicherheit

Die Anforderungen an den Grundschutz werden zunehmend komplexer, was sich in den periodischen Aktualisierungen des Massnahmenkatalogs durch das ISB niederschlägt. Die Umsetzung der Massnahmen kann zu Problemen führen. Es gibt immer mehr technische Plattformen und Anwendungen. Nicht alle Sicherheitsbeauftragten verfügen über genug Zeit, um ihre Aufgaben zu erfüllen. Die EFK erachtet dies als Risiko und empfiehlt dem ISB, die Grundschutzmassnahmen wo immer möglich zu vereinfachen und zu optimieren.

Lückenhafte Kontrolle der Umsetzung und der Wirksamkeit der Massnahmen

Die Kontrolle und die Dokumentation der Umsetzung und Wirksamkeit der Massnahmen sind qualitativ sehr unterschiedlich. Sie werden von den LB nicht systematisch dokumentiert, Letztere fordern die Kontrollberichte von den LE nicht immer an.

Die EFK erachtet dies als Mangel. Sie beurteilt ausserdem das aktuelle Dokumentationssystem als unwirksam. Gemäss aktuellem Verfahren liefern die LE oft redundante Antworten auf gleichbleibende Fragen. Die EFK hat dem ISB empfohlen, Wege zu finden, um die Dokumentation und die periodische Bestätigung der Kontrolle der Umsetzung der Schutzmassnahmen durch die LE zu vereinfachen.

Ausserdem definieren die LB selten ausdrücklich die Verantwortlichkeiten und die Kontrollprozesse für die Umsetzung und Wirksamkeit der Schutzmassnahmen. Nach Meinung der EFK besteht ein echtes Risiko, dass diese Massnahmen mangels Kontrolle schlicht und einfach nicht angewendet werden. Sie hat dem ISB empfohlen, die Weisungen zum Grundschutz dahingehend zu ergänzen, dass den Departementen die Definition von Zuständigkeiten und Kontrollprozessen vorgeschrieben wird.

Das Risikomanagement der nachrichtendienstlichen Ausspähung muss vereinfacht und geklärt werden

Die untersuchten VE wenden die neuen Weisungen über die Risikomanagementmethode zur Reduktion der nachrichtendienstlichen Ausspähung (RINA) an. Sie erachten die Vorgehensweise zwar für nötig, da sie als Reaktion auf ein echtes Risiko erfolgt, halten den dadurch verursachten Aufwand aber für zu gross. Die VE stellen zudem die Relevanz gewisser Analysekriterien und ihre Gewichtung sowie die zu ergreifenden Massnahmen für Objekte mit einem RINA-relevanten Risiko infrage. Die VE konnten diese Einwände in Gesprächen über eine Neuauflage des Prozesses äussern.

Die EFK teilt die Bedenken der Departemente hinsichtlich der Wirksamkeit des RINA-Prozesses in seiner aktuellen Form. [redacted] Die EFK hat dem ISB empfohlen, den Prozess zu vereinfachen und abzuklären, welche Massnahmen zu treffen sind, wenn ein Objekt ein RINA-relevantes Risiko aufweist. Die neue Version der Vorgehensweise könnte sich an den vereinfachten Prozessen orientieren, wie sie in einigen Departementen definiert wurden.

Die Mehrheit der Empfehlungen aus früheren Querschnittsprüfungen wurde umgesetzt

Die EFK stellt fest, dass 12 der 15 in ihrem Monitoringsystem erfassten, noch offenen Empfehlungen aus früheren Querschnittsprüfungen der IT-Sicherheit zwischenzeitlich umgesetzt worden sind. Die Arbeiten für die Umsetzung der drei noch verbleibenden Empfehlungen sind auf Kurs.