Querschnittsprüfung IT-Sicherheit in der Bundesverwaltung
Bericht zu Handen des Bundesrates

Das Wesentliche in Kürze

Die Eidgenössische Finanzkontrolle (EFK) erhielt am 24. Juni 2010 gemäss Bundesratsbeschluss vom 4. Juni 2010 vom „Delegierten Informatikstrategie Bund“ die schriftliche Anfrage, den Stand der Umsetzung von Massnahmen zur Erhöhung der Informatiksicherheit zu überprüfen. Die EFK hat auf diese Anfrage am 27. August 2010 positiv geantwortet und die Durchführung einer Querschnittsprüfung für das Jahr 2011 zugesagt. Der Revisionsbericht wurde den Mitgliedern des Bundesrates vom Eidgenössischen Finanzdepartement mittels Informationsnotiz vom 2. Dezember 2011 zur Kenntnis gebracht.

Die EFK definierte im Prüfungskonzept für 2011, welche Massnahmen in welcher Priorität bzw. Tiefe zu prüfen sind und welche Bereiche der Bundesverwaltung mit der Prüfung abgedeckt werden sollen. Dabei wurden die Themen „Einhaltung der Passwortanforderungen“, „zeitgerechte Schliessung von Sicherheitslücken“ und „intensivierte Netzwerküberwachung“ ausgewählt. Die Prüfung wurde bei insgesamt sieben Informatik Leistungserbringern der Bundesverwaltung durchgeführt. Zusätzlich hat die EFK zu den Themen „Einhaltung der Passwortanforderungen“, „Zeitgerechte Schliessung von Sicherheitslücken“ und „Verbessertes Informationsmanagement“ eine schriftliche Umfrage bei 71 Leistungsbezügern durchgeführt. Diese Themen entsprechen den Sofortmassnahmen gemäss Bundesratsbeschluss vom 16. Dezember 2009.

Die wesentlichen Schlussfolgerungen aus den Prüfungen sind wie folgt:

Im Windows Umfeld wurden nur kleinere Schwachstellen entdeckt. Die Prüfung hat gezeigt, dass sowohl die Einhaltung der Passwortanforderungen als auch die zeitgerechte Schliessung von Sicherheitslücken auf neuen Windows-Systemen bei den geprüften Leistungserbringern einen guten Stand erreicht haben.

Signifikante Sicherheitsdefizite bestehen im nicht-Microsoft Umfeld. Erhebliche Schwachstellen ortet die EFK bei der zeitgerechten Schliessung von Sicherheitslücken in nicht-Microsoft Produkten welche auf Windows-Plattformen laufen. Hier bestehen teilweise Abhängigkeiten zu Fachanwendungen, die eine Aktualisierung der betroffenen Komponenten nicht mehr zulassen. Ausserdem wurden Defizite bei der Definition von Zuständigkeiten für die Pflege dieser Produkte festgestellt. Ebenfalls sicherheitstechnisch anfällig sind ältere Systemen, die einerseits die Passwortanforderungen nicht erfüllen können und für die es teilweise keine Aktualisierungen zum Schliessen von aktuellen Sicherheitslücken mehr gibt.

Sicherheitslücken werden von Leistungsbezügern in Kauf genommen, den Leistungserbringern fehlt es an Durchsetzungskraft. An Beispielen wurde ersichtlich, dass die Anwenderseite den Sicherheitsbelangen oft nur geringe Priorität einräumt:

- Unter den Arbeitsplatzsystemen finden sich solche mit hochprivilegierten Rechten (lokale Administratorenrechte). Diese wurden aufgrund angemeldeter Anwenderwünsche eingerichtet.

- Alte Anwendungen und Systeme werden von den Geschäftsbereichen in dem Bewusstsein weiter betrieben, dass sie Sicherheitsdefizite aufweisen bzw. eine Aktualisierung von sicherheitskritischen Komponenten verhindern.
- Passwortregeln wurden in einem Fall auf Stufe Departementsleitung deaktiviert. Bestehende Mechanismen zur Eskalation bei einer solchen Anordnung haben offensichtlich nicht gegriffen.
- Die Verantwortung für sicherheitsbezogene Themen wird noch oft als rein technische Verantwortung bei den Leistungserbringern gesehen. Das Verständnis für die Aufgaben- und Verantwortungsteilung zwischen Leistungserbringern und Leistungsbezügern ist nicht ausreichend.
- Einige Leistungserbringer halten fest, dass ihnen in diesem Zusammenhang oftmals die Durchsetzungskraft gegenüber den Leistungsbezügern fehlt, da keine verbindlichen oder genügend spezifizierten Regelungen bestehen. Die Sicherheitsweisungen müssten diesbezüglich präzisiert werden.

Synergien zwischen den Leistungserbringern sind eher ein Zufallsprodukt. Im Rahmen der Prüfungen konnte die EFK feststellen, dass vielerorts gute Lösungen entstanden sind. Aus Sicht der EFK wird dieses Wissen unter den Leistungserbringern zu wenig geteilt, Synergien werden zu wenig genutzt. Dadurch besteht die Tendenz, dass jeder Leistungserbringer isoliert eigene Lösungen entwickelt oder entwickeln lässt.

Bei der intensivierten Netzwerküberwachung bestehen viele Aktivitäten. Die betroffenen Leistungserbringer haben erste Projekte umgesetzt und sind am Sammeln von Erfahrungen. Weitere Ausbauschritte sind geplant, namentlich zur Bewältigung und Analyse der anfallenden Datenmengen. Die geforderte Aufbewahrungsfrist von zwei Jahren für Protokolldateien wird nicht bei allen Leistungserbringern unterstützt. Der Wille zur Verbesserung der Sicherheitssituation ist gegeben, allerdings sind keine kurzfristigen Verbesserungen zu erwarten.

Die Sicherheit der Kantonsnetze ist noch immer die „grosse Unbekannte". Dem BIT fehlt noch immer die vertragliche Grundlage, sich über die Qualität der Netzwerksicherheit in den angeschlossenen Kantonen Gewissheit verschaffen und wo nötig Gegenmassnahmen ergreifen zu können. Dies soll sich mit der geplanten Unterzeichnung überarbeiteter Leistungsvereinbarungen (SLA) mit den Kantonen zum Jahresende ändern. Die Umsetzung dieser SLA, sprich die Sicherstellung und der Nachweis von sicheren Kantonsnetzen, wird in diversen Kantonen nur mittelfristig möglich sein.

Die Rückmeldungen der Leistungsbezüger, welche die EFK erhalten hat, lassen vermuten, dass diese ihre informationsschutzkritischen Anwendungen noch nicht überall vollständig identifiziert haben.

Die EFK hat stufengerecht verschiedene Empfehlungen an den Informatikrat des Bundes (IRB) bzw. das Informatikstrategieorgan Bund (ISB) und an die diversen Leistungserbringer adressiert. Die Empfehlungen an das ISB bzw. den IRB betrafen namentlich die Präzisierung von Vorgaben, die Intensivierung der Zusammenarbeit zwischen den Leistungserbringern sowie die Schulung betreffend Sicherheit. Die schriftlichen Stellungnahmen zeigen, dass die EFK-Empfehlungen akzeptiert wurden.