EIDGENÖSSISCHE FINANZKONTROLLE
CONTRÔLE FÉDÉRAL DES FINANCES
CONTROLLO FEDERALE DELLE FINANZE
SWISS FEDERAL AUDIT OFFICE

Querschnittsprüfung IT-Sicherheit in der Bundesverwaltung

Bericht zu Handen des Bundesrates

Oktober 2011

Impressum

Bestelladresse **Adresse de commande** **Indirizzo di ordinazione** **Order address**	Eidgenössische Finanzkontrolle (EFK) Monbijoustrasse 45, CH - 3003 Bern http://www.efk.admin.ch/I
Bestellnummer **Numéro de commande** **Numero di ordinazione** **Order number**	1.11387.600.00184.44
Zusätzliche Informationen **Complément d'informations** **Informazioni complementari** **Additional information**	Fachbereich Informatikprüfungen E-Mail: brigitte.christ@efk.admin.ch Tel. 031 323 10 11
Originaltext **Texte original** **Testo originale** **Original text**	Deutsch Allemand Tedesco German
Zusammenfassung **Résumé** **Riassunto** **Summary**	Deutsch (« Das Wesentliche in Kürze ») Français (« L'essentiel en bref ») Italiano (« L'essenziale in breve ») English (« Key facts »)

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.

Audit transversal sur la sécurité TI dans l'administration fédérale
Rapport à l'attention du Conseil fédéral

L'essentiel en bref

Le Contrôle fédéral des finances (CDF) a reçu le 24 juin 2010, par décision du Conseil fédéral du 4 juin 2010, une demande écrite du Délégué à la stratégie informatique de la Confédération, qui le priait de contrôler le degré de mise en œuvre des mesures prises pour renforcer la sécurité informatique. Le CDF y a répondu favorablement le 27 août 2010, en promettant de mener un audit transversal en 2011. Son rapport de révision a été porté à la connaissance des membres du Conseil fédéral le 2 décembre 2011, par une note d'information du Département fédéral des finances (DFF).

Dans son concept des audits de 2011, le CDF a défini pour cette révision tant les mesures à examiner, avec le degré de priorité ou d'approfondissement requis, que les domaines pertinents de l'administration fédérale. Trois thèmes ont été retenus, soit le «respect des exigences en matière de mot de passe», la «réparation dans les délais des lacunes de sécurité» et la «surveillance accrue des réseaux». L'audit portait au total sur sept fournisseurs de prestations informatiques de l'administration fédérale. En outre, le CDF a mené auprès de 71 bénéficiaires de prestations une enquête écrite sur le «respect des exigences en matière de mot de passe», la «réparation dans les délais des lacunes de sécurité» et l'«amélioration de la gestion de l'information». Ces thèmes se recoupaient avec les mesures immédiates de l'arrêté du Conseil fédéral du 16 décembre 2009.

Les principales conclusions de cet audit sont les suivantes:

L'environnement Windows ne présente que des lacunes sans gravité. Les fournisseurs de prestations examinés ont atteint un bon niveau, tant pour le respect des exigences en matière de mot de passe que pour la réparation dans les délais des erreurs des nouveaux systèmes Windows.

La sécurité de l'environnement non-Microsoft laisse sérieusement à désirer. Le CDF constate que les lacunes de sécurité des produits non-Microsoft fonctionnant sur les plates-formes Windows sont loin d'être corrigées dans les délais. Le problème vient des applications spécialisées, qui ne permettent parfois plus d'actualiser les composantes vulnérables. En outre, les compétences pour la mise à jour de tels produits ne sont pas clairement définies. Enfin, les systèmes anciens sont techniquement peu sûrs: d'une part, ils ne satisfont pas aux exigences en matière de mot de passe, d'autre part on ne trouve parfois plus d'actualisation pour corriger les lacunes de sécurité récentes.

Les bénéficiaires de prestations s'accommodent de ces lacunes de sécurité, et les fournisseurs de prestations ne parviennent pas à s'imposer. Bien des utilisateurs n'accordent, exemples à l'appui, qu'un faible degré de priorité aux questions de sécurité:

- Une partie des postes de travail bénéficient de droits d'accès privilégiés (droits d'administrateur local). Ces paramètres ont été installés en réponse aux vœux des utilisateurs.
- Les domaines d'activité continuent d'exploiter des applications et des systèmes désuets, en sachant pertinemment qu'ils laissent à désirer sur le plan de la sécurité ou qu'ils empêchent de mettre à jour des composantes importantes pour la sécurité.

- Les règles concernant les mots de passe avaient été désactivées au niveau de la direction d'un département. Les mécanismes d'escalade en place ont visiblement été impuissants face aux ordres venus d'en haut.
- La responsabilité en matière de sûreté de l'information reste souvent assimilée, de manière réductrice, à la responsabilité technique incombant aux fournisseurs de prestations. La prise de conscience de la répartition des tâches et des responsabilités entre fournisseurs et bénéficiaires de prestations ne s'est pas encore faite.
- Certains fournisseurs de prestations déplorent de ne pas avoir, bien souvent, les moyens de s'imposer face aux utilisateurs, faute de réglementation contraignante ou suffisamment spécifique. D'où la nécessité de préciser sur ce plan les directives de sécurité.

Les synergies entre les fournisseurs de prestations sont plutôt le fruit du hasard. Lors de ses vérifications, le CDF a constaté que de bonnes solutions ont été adoptées à bien des endroits. Or à ses yeux, ce savoir est trop peu diffusé parmi les fournisseurs de prestations, et les synergies sont insuffisamment exploitées. Chaque fournisseur de prestations a tendance à créer ou faire développer isolément ses propres solutions.

De nombreuses activités sont déployées au titre de la surveillance accrue du réseau. Les fournisseurs de prestations concernés ont réalisé de premiers projets et en sont à la phase de collecte des expériences. De nouvelles étapes sont prévues, notamment pour maîtriser et analyser l'afflux de données. Tous les fournisseurs de prestations ne sont pas favorables au délai de conservation de deux ans exigé d'eux pour les fichiers journaux. La volonté de renforcer la sécurité TI a beau être là, il ne faut pas s'attendre à des améliorations à court terme

La sécurité des réseaux cantonaux reste la «grande inconnue». Faute de base contractuelle, l'Office fédéral de l'informatique et de la télécommunication (OFIT) n'est pas habilité à s'assurer jusqu'ici que les cantons connectés ont atteint la qualité requise sur le plan de la sécurité des réseaux, et à prendre le cas échéant les mesures nécessaires. La situation changera d'ici la fin de l'année, avec la signature d'accords de niveau de service (SLA) remaniés avec les cantons. Leur mise en œuvre, soit la garantie de la sécurité des réseaux cantonaux et la fourniture des preuves correspondantes, ne sera possible dans certains cantons qu'à moyen terme.

Les réactions parvenues au CDF suggèrent que les bénéficiaires de prestations n'ont pas encore partout entièrement identifié leurs applications essentielles pour la protection de l'information.

Le CDF a adressé des recommandations ciblées au Conseil de l'informatique de la Confédération (CI) et à l'Unité de stratégie informatique de la Confédération (USIC), ainsi qu'aux divers fournisseurs de prestations. Les recommandations destinées à l'USIC ou au CI visaient notamment à préciser les exigences, à intensifier la collaboration entre les fournisseurs de prestations ainsi que la formation en matière de sécurité. Les réponses écrites reçues montrent que les recommandations du CDF ont été bien acceptées.

Texte original en allemand

Verifica trasversale della sicurezza IT nell'Amministrazione federale
Rapporto all'attenzione del Consiglio federale

L'essenziale in breve

Conformemente alla decisione del 4 giugno 2010 del Consiglio federale, il 24 giugno 2010 il Controllo federale delle finanze (CDF) ha ricevuto dal «delegato per la strategia informatica della Confederazione» una richiesta scritta di verifica dello stato di attuazione delle misure volte a potenziare la sicurezza informatica. Il 27 agosto 2010 il CDF ha accettato la richiesta dichiarandosi disposto a effettuare una verifica trasversale per il 2011. Mediante la nota d'informazione del 2 dicembre 2011, il Dipartimento federale delle finanze (DFF) ha trasmesso il rapporto di revisione per conoscenza ai membri del Consiglio federale.

Nel programma di verifica per l'anno 2011 il CDF ha stabilito le misure da sottoporre a esame, il loro ordine di priorità e il loro grado di approfondimento in relazione a tale esame, nonché i settori dell'Amministrazione federale interessati. I temi scelti riguardavano il rispetto dei requisiti delle password, l'eliminazione tempestiva delle lacune di sicurezza e il rafforzamento della sorveglianza della rete. La verifica è stata effettuata presso sette fornitori di prestazioni informatiche dell'Amministrazione federale. Il CDF ha inoltre condotto un sondaggio scritto tra 71 beneficiari di prestazioni riguardo al rispetto dei requisiti delle password, all'eliminazione tempestiva delle lacune di sicurezza e al miglioramento della gestione dell'informazione. Questi temi costituiscono l'oggetto delle misure immediate decise dal Consiglio federale il 16 dicembre 2009.

Le verifiche hanno permesso di trarre le seguenti principali conclusioni.

In ambiente Windows non sono stati rilevati punti deboli significativi. Dalla verifica è emerso che i fornitori di prestazioni esaminati hanno raggiunto un buon grado di rispetto sia dei requisiti delle password sia dei termini che garantiscono una tempestiva eliminazione delle lacune di sicurezza dei nuovi sistemi Windows.

In ambiente non Microsoft sussistono importanti lacune di sicurezza. Il CDF individua notevoli punti deboli nell'eliminazione tempestiva delle lacune di sicurezza presenti in prodotti non Microsoft che operano su sistemi operativi Windows. Il problema risiede in parte nelle dipendenze da applicazioni specifiche che non consentono più l'aggiornamento di componenti fondamentali del sistema. Sono state constatate inoltre lacune nella definizione delle competenze relative alla manutenzione dei prodotti. Anche i vecchi sistemi sono a rischio in termini di sicurezza, poiché non soddisfano i requisiti delle password e per alcuni di essi non si dispone più degli aggiornamenti necessari per colmare le attuali lacune di sicurezza.

I beneficiari di prestazioni gestiscono sistemi e applicazioni nella consapevolezza delle lacune di sicurezza e i fornitori di prestazioni non riescono ad imporsi. Sulla base di esempi è emerso che spesso gli utenti attribuiscono un basso grado di priorità alle questioni di sicurezza:

- vi sono sistemi di postazioni di lavoro con diritti di accesso privilegiati (diritti di amministratore locali) che sono stati impostati su richiesta degli utenti registrati;
- i settori di attività continuano a gestire applicazioni e sistemi obsoleti pur sapendo che questi presentano lacune di sicurezza o impediscono l'aggiornamento di componenti critici dal punto di vista della sicurezza;

- le regole concernenti le password sono state disattivate a livello di direzione di un dipartimento. I meccanismi esistenti dell'escalation non hanno evidentemente funzionato in presenza di un siffatto ordine;
- tutt'ora la responsabilità per i temi in materia di sicurezza è spesso equiparata alla responsabilità meramente tecnica dei fornitori di prestazioni. Non c'è una sufficiente consapevolezza della ripartizione dei compiti e delle responsabilità tra fornitori e beneficiari di prestazioni;
- alcuni fornitori di prestazioni affermano che molte volte non hanno la possibilità di imporsi sui beneficiari di prestazioni, dato che non esistono regolamentazioni vincolanti o sufficientemente specifiche. A questo proposito sarebbe necessario precisare le direttive di sicurezza.

Le sinergie tra i fornitori di prestazioni sono considerate frutto del caso. Nel quadro delle verifiche il CDF ha constatato che in diversi settori sono state trovate buone soluzioni. Secondo il CDF queste conoscenze non vengono sufficientemente condivise tra i fornitori di prestazioni e le sinergie non vengono sfruttate abbastanza. Ne consegue che ogni singolo fornitore tende a sviluppare (o a far sviluppare) soluzioni proprie.

Sono in corso numerose attività per la sorveglianza intensificata della rete. I fornitori di prestazioni interessati hanno attuato i primi progetti e stanno raccogliendo le relative esperienze. Sono previste ulteriori tappe, segnatamente per la gestione e l'analisi del flusso di dati. Non tutti i fornitori di prestazioni sono d'accordo sul termine di conservazione di due anni richiesto per i file di registro. Benché esista la volontà di ottimizzare la sicurezza, non bisogna attendersi miglioramenti a breve termine.

La sicurezza delle reti cantonali rimane la «grande incognita». In assenza di una base contrattuale l'Ufficio federale dell'informatica e della telecomunicazione (UFIT) non può accertare la qualità della sicurezza delle reti dei Cantoni collegati né adottare le necessarie contromisure. Con la prevista firma del Service Level Agreement (SLA), rielaborato insieme ai Cantoni, la situazione dovrebbe cambiare entro la fine dell'anno. In diversi Cantoni l'attuazione del SLA, ovvero la garanzia e la prova della sicurezza delle reti cantonali, sarà possibile soltanto a medio termine.

I riscontri pervenuti al CDF lasciano supporre che le applicazioni critiche per la protezione dell'informazione non siano state ovunque completamente identificate dai beneficiari di prestazioni.

Il CDF ha trasmesso, in considerazione del livello gerarchico, diverse raccomandazioni al Consiglio informatico della Confederazione (CIC) e all'Organo direzione informatica della Confederazione (ODIC), come pure ai vari fornitori di prestazioni. Le raccomandazioni indirizzate all'ODIC e al CIC riguardavano la precisazione di direttive, l'intensificazione della collaborazione tra i fornitori di prestazioni nonché la formazione in materia di sicurezza. Dai pareri espressi in forma scritta risulta che le raccomandazioni del CDF sono state accettate.

Testo originale in tedesco

Horizontal audit of IT security in the Federal Administration
Report for the attention of the Federal Council

Key facts

As per the Federal Council's decision of 4 June 2010, the Swiss Federal Audit Office (SFAO) received a written request from the "Delegate for Federal IT Strategy" on 24 June 2010 to audit the implementation status of measures to improve IT security. The SFAO accepted the request on 27 August 2010 and agreed to perform a horizontal audit for the year 2011. The audit report was brought to the attention of the Federal Council members on 2 December 2011 in an information memo from the Federal Department of Finance (FDF).

In its audit schedule for 2011, the SFAO set out which measures were to be audited, with which priority and to what extent, and which areas of the Federal Administration were to be covered in the audit. The topics thus selected were "Adherence to password rules", "Timely resolution of security deficiencies" and "Intensified network monitoring". The audit was performed on a total of seven IT service providers within the Federal Administration. In addition, the SFAO conducted a written survey among 71 service users on the areas "Adherence to password rules", "Timely resolution of security deficiencies" and "Improved information management". These areas correspond to the immediate measures set out in the Federal Council's decision of 16 December 2009.

The main findings from the individual audits are as follows:

Only minor deficiencies were revealed in the Windows environment. The audit found a good level of conformity among the audited service providers with regard to the adherence to password rules and the timely resolution of security deficiencies on new Windows systems.

Significant security issues exist in the non-Microsoft environment. The SFAO identified substantial weaknesses in the timely resolution of security deficiencies in non-Microsoft products running on Windows platforms. In some cases, dependencies exist on specialised applications, no longer allowing the relevant components to be updated. Deficiencies were also found in defining responsibilities for maintenance of these products. Other security vulnerabilities were found in legacy systems that cannot conform to the password rules and for which updates are no longer available to resolve the current security shortfalls.

Security deficiencies are accepted by service users; the service providers lack assertiveness. Examples have shown that security matters were often not a priority at the user end:

- Some of the workstation systems give highly privileged user rights (local administrator rights). These were assigned on the basis of user requests submitted.
- The business areas continue to operate legacy applications and systems despite knowing that these present security deficiencies or prevent security-critical components from being updated.
- In one case, password rules were disabled at the department's management level. The escalation mechanisms in place for such an order obviously failed to take effect.

- Responsibility for security-related matters still tends to be regarded by service providers as a purely technical responsibility. There is a lack of understanding of the segregation of tasks and responsibilities between service providers and service users.
- Some service providers maintain that the absence of any binding or sufficiently specific rules often undermines their assertiveness with respect to service users. The security directives need to be more precise in this respect.

Synergies between service providers tend to arise more by coincidence than by design. In the course of its audits, the SFAO found that good solutions had been found in many areas. However, the SFAO believes that this knowledge is not sufficiently shared among service providers and that synergies are not sufficiently exploited. As a result, the individual service providers tend to develop or commission their own solutions.

Numerous activities are underway in the intensification of network monitoring. The service providers concerned have implemented initial projects and are now gathering their experience. Further expansion steps are planned, specifically for the handling and analysis of the data gathered. The required two-year retention period for log files is not supported by all service providers. While measures to improve the security situation are envisaged, no short-term improvements are to be expected.

Security of the cantonal networks remains "the great unknown". The FOITT still does not have the contractual basis to assess the quality of network security in the cantons connected and to take the necessary countermeasures. This should change with the signing of revised service level agreements (SLAs) with the cantons, planned for the end of the year. For several cantons, the implementation of these SLAs, and thus ensuring and evidencing the security of cantonal networks, will only be possible in the medium term.

Based on the SFAO's feedback from service users, it would appear that these have not yet fully identified their critical applications in terms of information protection.

The SFAO has made a number of recommendations at the appropriate level to the Federal IT Council (FITC) or the Federal Strategy Unit for IT (FSUIT) and to the various service providers. The recommendations to the FITC or the FSUIT concerned making guidelines more precise, raising the level of cooperation between service providers, and security-related training. The written feedback shows that the SFAO's recommendations have been accepted.

Original text in German

Inhaltsverzeichnis

1 Auftrag und Prüfungsdurchführung

1.1 Auftrag

Die EFK erhielt am 24. Juni 2010 gemäss BRB vom 4. Juni 2010 vom „Delegierten Informatikstrategie Bund“ die schriftliche Anfrage, den Stand der Umsetzung von Massnahmen zur Erhöhung der Informatiksicherheit zu überprüfen (gemäss BRB vom 16. Dezember 2009). Die EFK hat auf diese Anfrage am 27. August 2010 positiv geantwortet und die Planung sowie Durchführung einer entsprechenden Querschnittsprüfung für das Jahr 2011 zugesagt.

1.1.1 Prüfungsziel

Im Rahmen eines Prüfungskonzepts hat die EFK den möglichen Rahmen der Prüfungen für das Jahr 2011 aufgezeigt. Während der Konzepterstellung wurden erste Gespräche mit Vertretern des Informatikstrategieorgans Bund (ISB) geführt. Im Konzept selber wurde aufgezeigt, welche Massnahmen in welcher Priorität bzw. Tiefe zu prüfen sind und welche Bereiche der Bundesverwaltung mit der Prüfung abgedeckt werden sollen. Die EFK hat nachfolgend die Prüffelder risikoorientiert ausgewählt.

1.1.2 Prüfungsfragen

Im Fokus der Prüfung stand die Frage, wie weit die vom Bundesrat angeordneten Sofortmassnahmen bei den Leistungserbringern umgesetzt wurden. Weitere Details dazu sind im Kapitel 2.3 beschrieben.

1.2 Rechtsgrundlagen und geltende Standards

- Bundesgesetz über die Eidgenössische Finanzkontrolle vom 28. Juni 1967, Stand am 1. Januar 2011 (Finanzkontrollgesetz, FKG, SR *614.0*)
- Verordnung über die Informatik und Telekommunikation in der Bundesverwaltung vom 26. September 2003, Stand am 1. März 2010 (Bundesinformatikverordnung, BinfV, SR *172.010.58*)
- Verordnung über den Schutz von Informationen des Bundes vom 4. Juli 2007, Stand am 1. August 2010 (Informationsschutzverordnung, ISchV, *510.411*)
- Weisungen der IRB über die Informatiksicherheit in der Bundesverwaltung vom 27. September 2004, Stand am 1. November 2007 (WIsB)
- Standard P012 – Betrieb Forest Bund vom 21.5.2007
- Standard P018 – Security Massnahmen Forest Bund vom 9.3.2009
- Standard P022 – Betrieb Mail/Exchange Bund vom 1.12.2003
- Standard A029 – Basissoftwarestandard Arbeitsplatz Bund (BAB) Client Software vom 8.4.2010
- Bundesratsbeschluss vom 16. Dezember 2009
- Bundesratsbeschluss vom 4. Juni 2010

1.3 Prüfungsumfang und -grundsätze

Die Prüfung wurde unter Leitung von Brigitte Christ im Zeitraum von Januar bis September 2011 durchgeführt. Die Prüfung wurde bei folgenden internen IT-Leistungserbringern durchgeführt:

- SCI-BK, Leistungserbringer der Bundeskanzlei
- ISCeco (inkl. TCSB), Leistungserbringer des EVD
- IT-EDA, Leistungserbringer des EDA
- BIT, Leistungserbringer für EFD, UVEK und EDI sowie Teile des EJPD
- ISC-EJPD, Leistungserbringer des EJPD
- PD-DINT, Leistungserbringer der Parlamentsdienste
- FUB, Leistungserbringer des VBS

Im Weiteren hat die EFK bei 71 Leistungsbezügern (Kunden der Leistungserbringer) mit Hilfe eines Fragebogens (Self-Assessment) eine Informationsbeschaffung durchgeführt.

1.4 Unterlagen und Auskunftserteilung

Die notwendigen Auskünfte wurden sowohl bei den Prüfungen vor Ort als auch bei der schriftlichen Umfrage von allen Beteiligten zuvorkommend erteilt.

1.5 Priorisierung der Empfehlungen der EFK

Aus der Sicht des Prüfauftrages beurteilt die EFK die Wesentlichkeit der Empfehlungen und Bemerkungen nach Prioritäten (1 = hoch, 2 = mittel, 3 = klein). Sowohl der Faktor **Risiko** [z. B. Höhe der finanziellen Auswirkung bzw. Bedeutung der Feststellung; Wahrscheinlichkeit eines Schadeneintrittes; Häufigkeit des Mangels (Einzelfall, mehrere Fälle, generell) und Wiederholungen; usw.], als auch der Faktor **Dringlichkeit der Umsetzung** (kurzfristig, mittelfristig, langfristig) werden berücksichtigt.

2 Einleitung und Grundsätzliches zur Prüfung

2.1 Die Organisation der Informatik in der Bundesverwaltung

Mit Nove-IT wurde die Bundesinformatik neu organisiert. Die folgenden Ausführungen geben sinngemäss Informationen aus der Broschüre „Nove-IT, Leistungsbezüger und Leistungserbringer in der Informatik der Bundesverwaltung“ wieder.

2.1.1 Die Bundesinformatikverordnung regelt das Zusammenspiel

Die Spielregeln für den Informatikeinsatz in der Bundesverwaltung sind in der Bundesinformatikverordnung (BinfV) definiert. Diese regelt insbesondere die Grundsätze für das Management der Informations- und Kommunikationstechnik (IKT) und beschreibt die Aufgaben und Kompetenzen des Informatikrats Bund (IRB), des Informatikstrategieorgans des Bundes (ISB), der Departemente und der Bundeskanzlei (BK), der Leistungsbezüger (LB) und Leistungserbringer (LE). Die Informatikprozesse der Bundesverwaltung binden Leistungsbezüger, interne Leistungserbringer und externe Lieferanten in gemeinsame Abläufe ein.

2.1.2 Die wesentlichen Akteure und ihre wichtigsten Aufgaben in Kürze

Der **Informatikrat des Bundes** (IRB) trägt die strategische Gesamtverantwortung für die IKT in der Bundesverwaltung.

Die **Departemente und die Bundeskanzlei** erstellen die strategische Informatikplanung (SIP), welche die Schwerpunkte des Informatikeinsatzes, die Informatikarchitekturen und die departementale Aufbau- und Ablauforganisation umschreibt.

Die **Leistungsbezüger** (d.h. die Verwaltungseinheiten) führen den Einsatz der Informatik. Die Anwendungsverantwortlichen der Leistungsbezüger stellen die optimale Unterstützung des Geschäftsprozesses durch die Informatik-Anwendungen sicher und sind insbesondere verantwortlich für die Aufrechterhaltung von Nutzen und Wirtschaftlichkeit, sowie für die Einhaltung der Sicherheitsanforderungen.

Die **Leistungserbringer** betreiben die Infrastruktur und Anwendungen für die Leistungsbezüger. Ausgewählte Leistungen, beispielsweise der Betrieb des Netzwerks, wurden vom IRB als sog. Querschnittsleistungen definiert. Der Bezug dieser Leistung ist für alle Leistungsbezüger obligatorisch. Die internen Leistungserbringer sind Mitglied der Informatikbetreiberkonferenz (IBK, Koordinationsorgan der internen Leistungserbringer). Die IBK stellt die für die Leistungserbringung notwendigen technischen Abstimmungen sicher und koordiniert die Betriebsschnittstellen, das Konfigurations- und Release-Management. Den Vorsitz in der IBK hat das Bundesamt für Informatik und Telekommunikation (BIT). Mitglieder mit Stimmrecht sind die BK, das EDA, EJPD, EVD, VBS und BIT als Vertreter des EFD/UVEK/EDI.

Informatiksicherheitsbeauftragte sind sowohl bei den Leistungsbezügern als auch bei den Leistungserbringern benannt. Sie zeigen Sicherheitsrisiken auf, bewerten diese gemäss den Vorgaben des ISB und überwachen die Umsetzung, Einhaltung sowie die Wirksamkeit von Sicherheitsmassnahmen. Jedes Departement verfügt über einen Informatiksicherheitsbeauftragten (ISBD), der dieses im Ausschuss Informatiksicherheit (A-IS) vertritt.

2.2 Was hat die EFK zur Durchführung dieser Prüfung veranlasst?

Die EFK hat am 24. Juni 2010 vom „Delegierten Informatikstrategie Bund“ die schriftliche Anfrage erhalten, den Stand der Umsetzung von Massnahmen zur Erhöhung der Informatiksicherheit zu überprüfen. Ein Sicherheitsvorfall in der Bundesverwaltung im 2009 veranlasste den Bundesrat zu dem Beschluss, zu den Punkten

a) Einhaltung der Passwortanforderungen

b) Zeitgerechte Korrektur von Sicherheitslücken

c) Verbessertes Informationsmanagement

d) Intensivierte Netzwerküberwachung

eine Überprüfung der aktuellen Situation bei allen Departementen anzuordnen.

2.3 Welchen Prüfungsansatz hat die EFK verfolgt?

Bei der Auswahl der Leistungserbringer, Plattformen und Prüfthemen (Anforderungen) erfolgte eine risikoorientierte Selektion der Elemente, die im Rahmen dieses Auftrags abgedeckt wurden.

Die Prüfungshandlungen wurden schwergewichtig auf die zwei Themen „Einhaltung der Passwortanforderungen“ sowie „zeitgerechte Korrektur von Sicherheitslücken“ gelegt. Aufgrund ihrer grossen Verbreitung in der Bundesverwaltung und der bekannten Verletzbarkeiten fokussierten sich die Prüfungen auf die Windows-basierten Systeme. Für weitere Plattformen (UNIX, LINUX) erfolgte zudem eine erste Informationsbeschaffung. Die Prüfung der Systeme hat bei sieben Leistungserbringern stattgefunden.

Zu den beiden Themen „verbessertes Informationsmanagement“ und „intensivierte Netzwerküberwachung“ hat eine Informationsbeschaffung stattgefunden.

Bei 71 Leistungsbezügern hat die EFK eine schriftliche Selbstbeurteilung darüber durchführen lassen, wie weit die Leistungsbezüger ihre Verantwortung bezüglich Informatiksicherheit kennen und vor allem auch wahrnehmen.

3 Wie interpretiert die EFK die gestellten Anforderungen?

Bei diversen Anforderungen besteht Raum für Interpretationen. Für die Prüfung wurden die definierten Sicherheitsvorgaben daher präzisiert, um klare Aussagen über den aktuellen Status treffen zu können.

3.1 Einhaltung der Passwortanforderungen

Die Weisungen des IRB über die Informatiksicherheit in der Bundesverwaltung legen im Anhang 1 die minimalen Sicherheitsvorgaben bezüglich Passwortanforderungen fest und zwar für persönliche, unpersönliche und technische bzw. funktionsbezogene Accounts. Da keine anderslautenden Angaben gemacht werden, gelten diese Vorgaben nach Auslegung der EFK sowohl für Benutzeridentifikationen zur Anmeldung an den Arbeitsplatzstationen (APS) als auch für Fachapplikationen.

3.2 Zeitgerechte Korrektur von Sicherheitslücken

Im Auftrag an die Departemente wurde die „zeitgerechte Korrektur von Sicherheitslücken“ gefordert. Da Computerprogramme nie absolut fehlerfrei sind, können Fehler in der Software für die Durchführung von Angriffen genutzt werden. Die Zeitspanne zwischen dem Bekanntwerden eines Fehlers und der tatsächlichen Ausnutzung der Schwachstelle wird immer kürzer. Viele Softwarehersteller liefern deshalb sog. Security Patches, welche der sofortigen Behebung von erkannten Schwachstellen dienen. Die Betreiber von IT-Systemen müssen sich daher laufend über verfügbare Patches informieren und diese über definierte Prozesse möglichst zeitgerecht und flächendeckend verteilen. Der Begriff „zeitgerecht“ war im ursprünglichen BRB nicht näher spezifiziert, die EFK hat sich deshalb auf die gängige Praxis der Hersteller bezogen.

3.3 Intensivierte Netzwerküberwachung

Die Departemente haben den Auftrag erhalten, die Netzwerküberwachung zu intensivieren. Ziel dieser Intensivierung ist, Unregelmässigkeiten im Datenverkehr frühzeitig zu erkennen und einen unerkannten Abfluss von Daten zu verhindern. Ohne weitere Spezifizierung der Anforderungen an den Umfang einer Protokollierung ist eine klare Aussage seitens der EFK über den Umsetzungsgrad nicht möglich.

3.4 Verbessertes Informationsmanagement

In der Informationsschutzverordnung (IschV) ist geregelt, was unter klassifizierten Daten zu verstehen ist, wann solche durch wen zu klassifizieren sind und wie bei einer Klassifizierung mit diesen Daten umzugehen ist. Die Departemente sind verpflichtet, einen Informationsschutzverantwortlichen zu benennen, welcher die korrekte Umsetzung der IschV überwacht. Da Daten in aller Regel bei den Leistungsbezügern entstehen, sind diese auch in erster Linie für die Einhaltung der vorgegebenen Regeln verantwortlich. Eine Ablage und Übertragung von klassifizierten Daten ab der Stufe „vertraulich“ ist nur in verschlüsselter Form erlaubt. Entsprechend müssen solche Möglichkeiten sowohl bei der Datenablage wie auch für die Übertragung (z. B. per E-Mail) vorhanden sein.

4 Die wesentlichen Ergebnisse und Erkenntnisse der Prüfung

Zu den einzelnen Themen wurden den Leistungserbringern Empfehlungen abgegeben, die an dieser Stelle nicht mehr wiederholt werden.

4.1 Wichtige Aspekte der Informatiksicherheit sind in den Informatiksicherheitsweisungen des Bundes nicht genügend präzisiert

Die EFK hat festgestellt, dass diverse Benutzende über lokale Administratorenrechte (d. h. unbeschränkte, hochprivilegierte Rechte) auf Arbeitsplatzsystemen verfügen. In den meisten Fällen wird dies damit begründet, dass die Benutzenden (z. B. ausserhalb der Leistungserbringer) selber Installationen von Software und Treibern etc. vornehmen wollen. Die EFK vertritt den Standpunkt, dass die Leistungsbezüger nicht über Administratorenrechte verfügen sollen, vielmehr müsste die Dienstleistungsqualität der Leistungserbringer so gestaltet sein, dass dieses Bedürfnis gar nicht erst auftritt. Konkret heisst dies, dass einerseits ein Leistungserbringer in angemessener Zeit in der Lage sein sollte, die Bedürfnisse zu befriedigen und andererseits Prozesse aufgesetzt sind, damit lokale Administratorenrechte nicht mehr benötigt werden.

Einige Leistungserbringer halten fest, dass ihnen in diesem Zusammenhang oftmals die Durchsetzungskraft gegenüber Leistungsbezügern fehlt. Die bestehenden Verordnungen bzw. Weisungen regeln nirgends verbindlich, dass lokale Administratorenrechte für die Arbeitsplatzsysteme nicht in den Händen des einzelnen Benutzenden sein dürfen. Aus Sicherheitsüberlegungen lässt sich jedoch ein Verbot sehr wohl ableiten. Aus Sicht der EFK sollte dies in der WIsB (Weisungen des IRB über die Informatiksicherheit in der Bundesverwaltung) verbindlich geregelt werden. Abweichungen sollten nur in absolut betriebsverhindernden Ausnahmefällen - unter Einhaltung von strengen Regeln und der Genehmigung durch ein zuständiges Gremium - möglich sein.

In einem Fall stiess die EFK bei einem LE auf eine Eigenentwicklung für die Zuweisung von Administratorenrechten. Damit wird einerseits ein falsches Signal an die Benutzenden gesandt und andererseits stellt dieses Werkzeug selber ein Sicherheitsrisiko dar. Dem betroffenen Leistungserbringer hat die EFK empfohlen, diese Eigenentwicklung einzustellen und durch verfügbare Standardsoftware zu ersetzen. Der Leistungserbringer hat der Empfehlung zugestimmt, in Zusammenarbeit mit den Leistungsbezügern mittelfristig eine Lösung zu suchen.

Die WIsB legt fest, für welche Art von Benutzer-Identifikationen (persönliche, unpersönliche oder technische) welche Passwortregeln gelten. Mit diesen Definitionen sind grundsätzlich alle Möglichkeiten abgedeckt, also auch die Zugriffe auf Fach-Anwendungen. Im Rahmen der Prüfung hat sich jedoch gezeigt, dass verschiedene Anwendungen im Einsatz sind, für welche die vorhandenen Regeln in Frage gestellt werden. Bei einer Überarbeitung der Weisung sollte daher auch thematisiert werden, in klar definierten Fällen Unterschreitungen der Mindestanforderungen zuzulassen (z. B. Zugangsbeschränkung zu Newslettern), um Effizienzpotenziale auszuschöpfen.

Empfehlung 5.1 (Priorität 1)

Das Verbot von lokalen Administratorenrechten für die Benutzer von Arbeitsplätzen sollte durch den IRB in den bestehenden Weisungen verbindlich geregelt und anschliessend durch die Leistungserbringer flächendeckend umgesetzt werden. Bei der Überarbeitung der Weisungen sind diese so zu präzisieren, dass kein Interpretationsspielraum mehr besteht (zum Beispiel bezüglich Zugriffe in Fachanwendungen).

4.2 Einhaltung der Passwortanforderungen

4.2.1 Nicht alle der heute eingesetzten Betriebssystemversionen erlauben eine vollständige Umsetzung der Passwortanforderungen

Bei der Beurteilung der Umsetzung ging die EFK davon aus, dass die Einhaltung der Passwort-anforderungen technisch durchgesetzt wird (siehe hierzu auch Kapitel 3.1). Gemäss den Anforderungen der WIsB beträgt die minimale Passwortlänge 8 Zeichen für persönliche Accounts und 12 Zeichen für Administratoren- sowie technische Accounts. Eine Unterscheidung zwischen persönlichen oder technischen Accounts und solchen von Administratoren kann mit älteren, zum Teil in der Bundesverwaltung noch verwendeten Betriebssystemversionen technisch nicht durchgesetzt werden. Bis zur endgültigen Ablösung der älteren Systeme kann die Durchsetzung

der Passwortlänge für technische und Administratoren-Accounts nur durch organisatorische Massnahmen erfolgen.

4.2.2 Die Passwortanforderungen für die Anmeldung im Active Directory (AD) werden durchgesetzt, Mängel bestehen bei der regelmässigen Kontrolle

Bei den Benutzer-Accounts, welche für die Anmeldung an einer Domäne (eine Domäne ist ein lokaler Sicherheitsbereich mit zentraler Verwaltung der Ressourcen und stellt die administrative Grenze dar) verwendet werden, sind die Passwortanforderungen grundsätzlich überall technisch durchgesetzt. Je nach Konfiguration können jedoch auf einzelnen Accounts verschiedene Parameter (z. B. Passwort läuft nie ab, kein Passwort notwendig) abgeändert werden. In einzelnen Fällen kann ein solches Vorgehen berechtigt sein, dies müsste allerdings schriftlich genehmigt und dokumentiert werden zuhanden der AD-Verantwortlichen. Die Prüfung hat hier zum Teil Unregelmässigkeiten festgestellt, die auf unvollständige Prozesse hinweisen. Vor allem im Bereich der regelmässigen Kontrolle von bestehenden Accounts sieht die EFK noch Verbesserungspotential. Die betroffenen Leistungserbringer haben in ihrer Stellungnahme zugesichert, die Prozesse anzupassen.

4.2.3 Ausnahmen bestätigen die Regel

Passwortregeln wurden in einem Fall auf Stufe Departementsleitung deaktiviert. Bestehende Mechanismen zur Eskalation bei einer solchen Anordnung haben nicht gegriffen oder sind nicht vorhanden. In diesem Zusammenhang soll erneut die Wichtigkeit der Vorbildfunktion des Managements herausgestrichen werden.

4.3 Zeitgerechte Korrektur von Sicherheitslücken

4.3.1 Die Vorgaben lassen Interpretationsspielraum

Bei den zahlreichen Gesprächen, welche die EFK mit den Vertretern der Leistungserbringer geführt hat, hat sich gezeigt, dass nicht alle Vorgaben eindeutig sind und sie sich daher unterschiedlich interpretieren lassen. Der Begriff „zeitgerecht“ im Zusammenhang mit der Korrektur von Sicherheitslücken liess am Anfang den Leistungserbringern eigenen Interpretationsspielraum. Für die Windows-basierten Systeme wurde der Begriff „zeitgerecht“ jedoch am 28. März 2011 durch den Informatikrat Bund (IRB) eindeutig festgelegt. Für alle nicht-Windows-basierten Systeme wurde eine Definition des Begriffs bisher lediglich in Aussicht gestellt.

4.3.2 Einige Anwendungen verhindern die Aktualisierung der darunter liegenden Komponenten

Die EFK hat verschiedene veraltete Betriebssystemversionen gesehen, welche durch den Hersteller nicht mehr gepflegt werden. Die schnellen Erneuerungszyklen der Betriebssysteme stellen die Hersteller von Fachanwendungen immer wieder vor die Herausforderung, ihr Produkt auf den neusten Betriebssystemversionen lauffähig zu halten, was nicht immer „zeitgerecht“ gelingt. Da immer Abhängigkeiten zwischen verschiedenen Softwareschichten bestehen, sind Prozesse nötig, welche nicht nur die Aktualisierung einer bestimmten Schicht, sondern die Aktualisierung der gesamten Software vorsehen (horizontales Release Management). Die Leistungsbezüger, welche in vielen Fällen die Software für Fachanwendungen beschaffen, sind

noch zu wenig in diese Prozesse eingebunden. Die Beschaffer von Software, typischerweise von Fachanwendungen, sind auch für die laufende Pflege der Software zuständig. Idealerweise werden die Hersteller in den Wartungsverträgen verpflichtet, die Anwendungen auf den als sicher geltenden Versionen von eingebundenen Standardprodukten (z. B. Adobe Acrobat Reader, Java usw.) und benutzten Betriebssystemen lauffähig zu halten. Das BIT plant, diesen horizontalen Release Management Prozess einzuführen. Hierzu wird die Zusammenarbeit mit den Leistungsbezügern gesucht, welche in der Regel für die Fachanwendungen zuständig sind. Die EFK hat die Weiterverfolgung dieses Ansatzes empfohlen.

Empfehlung 5.3.2 (Priorität 1)

Die Zusammenarbeit im Patch Management muss auf übergeordneter Ebene zwischen Leistungserbringer und Leistungsbezüger intensiviert werden. Es muss verhindert werden, dass bekannte Sicherheitslücken auf Systemen nicht geschlossen werden können, weil die Fachanwendungen des Leistungsbezügers mit den neusten Versionen nicht kompatibel sind (horizontales Release Management über sämtliche voneinander abhängigen Produkte nötig). Die EFK empfiehlt, dass durch die Leistungserbringer ein Inventar der Anwendungen erstellt wird, die ein angemessenes Patch Management verhindern. Dieses ist mit dem Leistungsbezüger zu diskutieren im Hinblick auf mögliche Verbesserungsmassnahmen oder eventuell notwendige kompensierende Massnahmen. Dieses Inventar wird dem jährlichen Reporting an das ISB beigelegt.

4.3.3 Die Sensibilität für die zeitgerechte Korrektur von Sicherheitslücken ist im Microsoft-Umfeld stark gewachsen, bei den übrigen Produkten besteht noch deutlicher Handlungsbedarf

Die zeitgerechte Korrektur von Sicherheitslücken für Microsoft Betriebssysteme hat praktisch bei allen Leistungserbringern einen guten Stand erreicht. Nicht zuletzt auch dank der grossen Anstrengungen des Herstellers Microsoft in den vergangenen Jahren sind diese Prozesse weitgehend automatisiert. Der Hersteller informiert laufend über bekannte Sicherheitslücken und bietet automatisch entsprechende „Patches“ zur Korrektur an. Die Verteilung auf die Server und die Arbeitsplätze kann mit den von Microsoft zur Verfügung gestellten Werkzeugen in einem hohen Mass automatisiert werden.

Bei der Aktualisierung von nicht-Microsoft Produkten sind die Verfahren bei den geprüften Leistungserbringern noch weit weniger gut standardisiert was von verschiedenen Leistungserbringern selber als problematisch beurteilt wurde. Dies nicht zuletzt auch aufgrund der Tatsache, dass zahlreiche Fachanwendungen auf einer bestimmten Version von darunterliegenden Produkten aufbauen und eine Aktualisierung verhindern (siehe hierzu auch Kapitel 4.3.2). Ein weiteres Problem in diesem Zusammenhang ist die oftmals unklare Zuständigkeit für die Pflege eines Produkts auf Seite Leistungserbringer.

4.4 Intensivierte Netzwerküberwachung

4.4.1 Erste Projekte für die intensivierte Netzwerküberwachung sind umgesetzt

Das BIT hat vom IRB die Aufgabe erhalten, die Netzwerke der Bundesverwaltung als Querschnittsleistung zu betreiben. Diese Leistung muss grundsätzlich von allen Departementen bezogen werden. Im „blauen“ Netz (geschütztes Bundesnetz) bilden die lokalen Netzwerke für die Auslandvertretungen des EDA und die Netzzonen des EJPD für den Betrieb der Fachanwendungen sowie das SSO-Portal eine Ausnahme. Diese stehen unter entsprechender Verantwortung des jeweiligen departementalen Leistungserbringers. Weitere Netzbereiche werden ebenfalls ausserhalb des BIT betrieben, gehören jedoch zum „roten“ Netz (weniger geschütztes Netz).

Die Prüfung hat ergeben, dass beim Querschnittsleistungserbringer BIT ein erstes Projekt zur Netzwerküberwachung umgesetzt und gleichzeitig ein Computer Security Incident Response Team (CSIRT) etabliert wurde. Weitere Ausbauschritte werden gemäss BIT nötig sein, um die grossen Datenmengen im Zusammenhang der Netzwerküberwachung bewältigen zu können. Weitere Massnahmen sind bereits geplant. Die geforderte Aufbewahrungsfrist von zwei Jahren für Protokolldateien wird nicht bei allen Leistungserbringern unterstützt.

Die Parlamentsdienste werden ihre Netzwerkleistungen in Zukunft nicht mehr vom BIT, sondern von Swisscom beziehen. Der IRB als Eigner des Bundesnetzwerkes wird entscheiden müssen, ob unter diesen Umständen die PD weiterhin am „blauen“ Netz angeschlossen sein können und wie weit dieses Vorgehen mit der geforderten Netzwerksicherheit und -überwachung vereinbar ist.

Empfehlung 5.4.1 (Priorität 2)

Die EFK empfiehlt dem Informatikrat Bund (als Eigner des Bundesnetzes), rasch zu entscheiden, ob die Parlamentsdienste bei einem allfälligen Leistungsbezug ausserhalb des BIT weiterhin im „blauen Netz“ angeschlossen sein können.

4.5 Die Empfehlungen der EFK wurden in allen eingegangenen Stellungnahmen der Leistungserbringer akzeptiert

Aus den bisher eingegangenen Stellungnahmen ist erkennbar, dass die Leistungserbringer bereit sind, die Prozesse weiter zu verbessern. Die in Aussicht gestellten Termine zeigen allerdings auch, dass nicht alle Empfehlungen kurzfristig umgesetzt werden können. Grössere Vorhaben werden bis ins vierte Quartal 2012 dauern. Eine sofortige Verbesserung ist also nicht in allen Bereichen zu erwarten.

5 Die Schlüsse der EFK aus der Selbstbeurteilung der Leistungsbezüger

Anhand eines Fragebogens wurden die Leistungsbezüger gebeten, zu den Punkten

- Einhaltung der Passwortanforderungen,
- Zeitgerechte Korrektur von Sicherheitslücken,

- Verbesserung des Informationsmanagement

Stellung zu nehmen. In den folgenden Kapiteln stellt die EFK die wesentlichen Ergebnisse dar.

5.1 Die Einhaltung der Passwortanforderungen wurde sehr selbstkritisch beurteilt

Nur rund die Hälfte der befragten Leistungsbezüger gibt an, dass in ihrem Bereich die Passwortanforderungen überall umgesetzt wurden. Da die gleiche Prüfung bei den Leistungserbringern gezeigt hat, dass die Umsetzung auf den Windows-basierten Betriebssystemen einen guten Stand erreicht hat, muss die EFK annehmen, dass es sich bei den kommentierten Fällen um spezifische Fachanwendungen der Leistungsbezüger handelt. Die damit verbundenen Risiken scheinen nicht allen Anwendungsverantwortlichen bewusst zu sein.

5.2 Die zeitgerechte Schliessung von Sicherheitslücken kann nicht in allen Anwendungen garantiert werden

Mehr als 80% der befragten Leistungsbezüger geben an, einen funktionierenden Prozess für die Schliessung von Sicherheitslücken zu haben. Fast zwei Drittel geben an, dass ihre Leistungserbringer diese Aufgabe übernehmen. Die Korrektur von Sicherheitslücken ist in allen Bereichen der Informatik notwendig. Auf den Betriebssystemen (Arbeitsplatzsystemen, Server, Host usw.) aber auch auf der eingesetzten Anwendungssoftware (z. B. Fachanwendungen, Adobe Acrobat Reader, Adobe Flashplayer, Java u. v. m.) müssen bekannte Sicherheitslücken geschlossen werden. Fast ein Drittel der Leistungsbezüger gibt allerdings an, Anwendungen zu haben, die sich am Ende des Lebenszyklus befinden und nicht mehr gepflegt werden. Solche Anwendungen können Sicherheitslücken darstellen oder verhindern, dass Betriebssysteme auf die neusten Versionen aktualisiert werden können. Da die Fachanwendungen aber essentiellen Einfluss auf die Aktualisierbarkeit der darunter liegenden Software nehmen können, hat der Leistungsbezüger eine aktive Aufgabe in der Rolle des Anwendungsverantwortlichen. Im Bereich des Release Management muss die Zusammenarbeit zwischen Leistungserbringer und Leistungsbezüger intensiviert werden (siehe auch Kapitel 4.3.2).

5.3 Die Klassifizierung von Informationen wird nicht durchgängig umgesetzt

Etwas mehr als zwei Drittel geben an, dass in ihrem Bereich die Daten entsprechend der Informationsschutzverordnung klassifiziert werden. Rund 40% sind allerdings der Ansicht, dass die technischen Mittel den Anforderungen nicht genügen. Eine korrekte Auslegung der Verordnung würde beispielsweise bedeuten, dass „Vertraulich“ klassifizierte Informationen auch innerhalb der Bundesverwaltung nur verschlüsselt verschickt oder gespeichert werden dürften. Gemäss den Umfrageergebnissen wurden die technischen Voraussetzungen noch nicht durchgängig umgesetzt (verschlüsseltes E-Mail, Verschlüsselung in Dokumenten-Management- oder GEVER-Systemen, Verschlüsselung auf Ablagen).

5.4 Allgemeine Feststellung zu der Umfrage bei den Leistungsbezügern

Aus den eingegangenen Antworten der Leistungsbezüger leitet die EFK ab, dass betreffend Umsetzung der Anforderungen noch weiterer Schulungsbedarf besteht. Insbesondere das genaue Verständnis für die Aufgaben- und Verantwortungsteilung zwischen Leistungserbringern und Leistungsbezügern muss weiter geschärft werden.

Die EFK hat die Leistungsbezüger im Vorfeld gebeten, ihre kritischen Anwendungen zu melden (in Anlehnung an BRB Ziffer 3.3.3)[1]. Die Rückmeldungen, welche die EFK erhalten hat, lassen vermuten, dass noch nicht alle Leistungsbezüger ihre informationsschutzkritischen Anwendungen vollständig identifiziert haben.

Empfehlung 6.4 (Priorität 2)

Die EFK empfiehlt dem Informatikstrategieorgan Bund (ISB), weitere stufengerechte Schulungsmassnahmen betreffend Verantwortlichkeiten und Umsetzung von Sicherheitsmassnahmen bei den Leistungsbezügern durchzuführen. Diese Schulung sollte als obligatorisch erklärt werden. Aufgrund der wichtigen Vorbildfunktion sollte sich das Training in erster Priorität (aber nicht ausschliesslich) an das Management richten.

6 Die Ergebnisse des Follow-up betreffend NSP-SIK

Im Zuge der vorliegenden Querschnittsprüfung sollte auch das Follow-up zum EFK-Bericht „Netzwerksicherheit, Prüfung durch die Kantone der Umsetzung der Network Security Policy der Schweizerischen Informatikkonferenz (NSP-SIK)“ durchgeführt werden.

6.1 Welche Empfehlungen hat die EFK damals abgegeben?

In diesem Bericht ging es um die generelle Netzwerksicherheit in den Kantonen und die Umsetzung der Network Security Policy der Schweizerischen Informatikkonferenz (NSP-SIK). Diese wurde beispielhaft dargestellt anhand von Prüfungen in drei Kantonen, sowie einer flächendeckenden Erhebung, welche im Laufe des Jahres 2008 durchgeführt wurden.

Im ihrem Bericht vom Februar 2009 hat die EFK die nachfolgend aufgeführten Empfehlungen abgegeben (*Originaltext).*

(a) Die EFK empfiehlt dem BIT, die SLA mit den Kantonen in folgender Reihenfolge anzupassen:

- *Die wichtigsten Sicherheitselemente sind verbindlich festzuhalten*
- *Die Kantone sind zu verpflichten,*
  a) entweder dem BIT beziehungsweise einem von diesem bezeichneten Dritten ein auf die vereinbarten Sicherheitselemente beschränktes Auditierungsrecht zu gewähren oder
  b) die kantonale Netzwerke regelmässig selber auf Sicherheitsmängel zu auditieren und dem BIT die entsprechenden Auditberichte zuzustellen.
- *Bei Feststellung von Mängeln im Zusammenhang mit Sicherheitsvorfällen kann das BIT eine der Bedrohung und dem Umfang der Massnahmen angemessene Frist zur Behebung festsetzen. Wird dieser Aufforderung nicht termingerecht nachgekommen, so kann das BIT die notwendigen Schutzmassnahmen treffen.*

[1] Originaltext gem. BRB: 3.3 Umsetzung der Informations- und Datenschutzanforderungen, 3.3.3. Die Departemente identifizieren die bereits bestehenden informationsschutzkritischen Anwendungen bis Ende 2010 und sichern diese bis Ende 2013

(b) Die EFK empfiehlt der SIK, die Umsetzung der NSP in den Kantonen bis Ende 2010 zu verlangen und dazu die Rückendeckung der Finanzdirektorenkonferenz einzufordern.

Die Beurteilung durch die EFK ist im Folgenden zusammengefasst.

6.2 Fortschritte bei der Umsetzung der EFK-Empfehlungen sind absehbar

Anlässlich der Landsgemeinde SIK hat das BIT als verantwortlicher Betreiber des „blauen Netzes“ im August 2011 den Kantonen die neuen SLA angekündigt, die die Empfehlungen der EFK aufgreifen. Die Anforderungen an die Überprüfung der Netzwerksicherheit, das Berichtswesen sowie die Verfahren bei sicherheitsrelevanten Vorfällen sind festgehalten.

Ein signifikanter Schritt wurde damit vom BIT gemacht. Gemäss aktueller Planung des BIT sollten diese SLA bis zum Jahresende 2011 unterzeichnet sein. Allerdings ist davon auszugehen, dass die Umsetzung der diversen Vorgaben je nach Vorbereitungsstand der einzelnen Kantone noch deutlich länger benötigen wird. Gleiches gilt für die Etablierung der jährlich vorgesehenen Self-Assessments der Kantone, mit denen die Wirksamkeit der Netzwerk-Sicherheitsrichtlinien validiert werden soll.

7 Grosses Potenzial für Synergien von ausgereiften Lösungen innerhalb der Bundesverwaltung

Die EFK ist im Laufe der Prüfung bei verschiedenen Leistungserbringern auf gute Lösungen gestossen, die auch von Anderen übernommen werden können. Die EFK regt an, dass das Informatikstrategieorgan Bund als übergeordnete Stelle verstärkt darauf hinwirken muss, dass gute Lösungen unter den Leistungserbringern ausgetauscht, standardisiert und damit Synergien genutzt werden. Damit könnte u. a. verhindert werden, dass die gleichen Probleme bei den verschiedenen Leistungserbringern parallel gelöst werden. Beispiele für solche Synergien sind:

- Der Leistungserbringer des VBS (die FUB) hat bereits heute eine Zwei-Faktor-Authentifikation mit Smartcards eingeführt. Die Anmeldung an den Arbeitsplatzsystemen erfolgt nicht mehr mittels Benutzernamen und Passwort, sondern mit der persönlichen Smartcard und der dazugehörenden persönlichen Identifikationsnummer (PIN). Die FUB hat damit bereits heute eine der zusätzlichen Massnahmen gemäss BRB umgesetzt. Aus Sicht der EFK wäre es schade, wenn die übrigen Leistungserbringer mit grossem Aufwand eigene Lösungen entwickeln würden.
- Der Leistungserbringer des EDA (IT-EDA) stellt mit dem Einsatz von Softwareeinschränkungsrichtlinien sicher, dass nur noch erwünschte Programme ausgeführt werden können. Diese Funktion steht bei den neusten Windows Versionen zur Verfügung. Die EFK empfiehlt, dass der Einsatz der technischen Einschränkungsrichtlinien bundesweit geprüft wird.
- Der Leistungserbringer BIT verfügt über eine Infrastruktur, mit welcher Systeme proaktiv nach Verletzbarkeiten untersucht werden können. Diese zusätzlichen Scans unterstützen die Kontrollen, welche im Rahmen des ordentlichen Patch Management gemacht werden

müssen. Ein weiterer Mehrwert solcher Scans ist, dass auch Sicherheitslücken von nicht-Microsoft Produkten erkannt werden.

- Das BIT hat mit dem Aufbau seines CSIRT Erfahrung im Bereich der intensivierten Netzwerküberwachung und der Alarmierung sammeln können. Auch diese Erfahrungen müssten mit anderen Leistungserbringern geteilt werden.

Empfehlung 8 (Priorität 2)

Die EFK empfiehlt der Informatikbetreiberkonferenz (IBK), den Erfahrungsaustausch zwischen den Leistungserbringern zu strukturieren und zu intensivieren mit dem Ziel, gute Lösungen für alle Leistungserbringer zugänglich zu machen. Grundsätzlich sollte vor Beginn einer Neuentwicklung geklärt werden, ob andere Leistungserbringer der Bundesverwaltung bereits über entsprechende Lösungen verfügen.

8 Schlussbesprechung

Die Gesamtschlussbesprechung fand am 3. Oktober 2011 bei der EFK statt. Teilgenommen haben die von den Departementen gemeldeten Vertreter. Die Departemente haben fast ausnahmslos die Sicherheitsbeauftragten ihres Departements (ISBD) zur Teilnahme gemeldet. Die Schlussbesprechung hat keine Widersprüche ergeben.

Im Anschluss zur Gesamtschlussbesprechung hat am 19. Oktober eine persönliche Schlussbesprechung mit dem Delegierten des ISB stattgefunden.

Die EFK dankt allen Beteiligten für die gewährte Unterstützung während der gesamten Prüfung.

Der Revisionsbericht wurde den Mitgliedern des Bundesrates vom Eidgenössischen Finanzdepartement mittels Informationsnotiz vom 2. Dezember 2011 zur Kenntnis gebracht.

EIDGENÖSSISCHE FINANZKONTROLLE

Begriffe und Abkürzungen

AD	Active Directory, Verzeichnisdienst für Windows
A-IS	Ausschuss Informatiksicherheit
APS	Arbeitsplatzsysteme
BinfV	Bundesinformatikverordnung
BIT	Bundesamt für Informatik und Telekommunikation
BK	Schweizerische Bundeskanzlei
BRB	Bundesratsbeschluss
BVerw	Bundesverwaltung
CSIRT	Computer Security Incident Response Team
EDA	Eidgenössisches Departement für auswärtige Angelegenheiten
EDI	Eidgenössisches Departement des Innern
EFD	Eidgenössisches Finanzdepartement
EJPD	Eidgenössisches Justiz- und Polizeidepartement
EVD	Eidgenössisches Volkswirtschaftsdepartement
FFB	Führung Forest Bund
FUB	Führungsunterstützungsbasis, IT-Leistungserbringer der VBS
IBK	Informatikbetreiberkonferenz, Koordinationsorgan der internen Leistungserbringer, Vorsitz BIT
IKT	Informations- und Kommunikationstechnologie
IRB	Informatikrat Bund
ISB	Informatikstrategieorgan Bund
ISBD	Informatiksicherheitsbeauftragte der Departemente
ISBO	Informatiksicherheitsbeauftragte der Organisationen
ISCeco	Informatik Service Center EVD, IT-Leistungserbringer des EVD
ISC-EJPD	Informatik Service Center EJPD, IT-Leistungserbringer des EJPD
ISchV	Informationsschutzverordnung
IT-EDA	IT-Leistungserbringer des EDA
LB	Leistungsbezüger
LBK	Leistungsbezügerkonferenz
LE	Leistungserbringer

NSP	Network Security Policy
Patch	Vorübergehende Behebung einer Sicherheitslücke oder eines Fehlers bis zum Vorliegen einer neuen, vermeintlich fehlerfreien Version
PD	Parlamentsdienste
PD-DINT	Dienst für Informatik und neue Technologie, IT-Leistungserbringer der Parlamentsdienste
PIN	Persönliche Identifikationsnummer
RL	Revisionsleiter/in
SCI-BK	Service Center Informatik BK, IT-Leistungserbinger der Bundeskanzlei
SECO	Staatssekretariat für Wirtschaft
SIK	Schweizerische Informatikkonferenz
SIP	Strategische Informatikplanung
SLA	Service Level Agreement
TCSB	IT-Leistungserbringer im SECO
UVEK	Eidgenössisches Departement für Umwelt, Verkehr, Energie und Kommunikation
VBS	Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport
VE	Verwaltungseinheit
WIsB	Weisungen des IRB über die Informatiksicherheit des Bundes