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

# Prüfung der Wirtschaftlichkeit und der Sicherheit der Informatik nach der Auslagerung

Parlamentsdienste

EFK-16591 | inkl. Stellungnahmen | 24. November 2017 | FinDel D1/2018

| | |
|---|---|
| Bestelladresse<br>Adresse de commande<br>Indirizzo di ordinazione<br>Ordering address | Eidgenössische Finanzkontrolle (EFK)<br>Monbijoustrasse 45<br>3003 Bern<br>Schweiz |
| Bestellnummer<br>Numéro de commande<br>Numero di ordinazione<br>Ordering number | 1.16591.101.00057 |
| Zusätzliche Informationen<br>Complément d'informations<br>Informazioni complementari<br>Additional information | www.efk.admin.ch<br>info@efk.admin.ch<br>twitter: @EFK_CDF_SFAO<br>+ 41 58 463 11 11 |
| Abdruck<br>Reproduction<br>Riproduzione<br>Reprint | Gestattet (mit Quellenvermerk)<br>Autorisée (merci de mentionner la source)<br>Autorizzata (indicare la fonte)<br>Authorized (please mention source) |

# Inhaltsverzeichnis

# Prüfung der Wirtschaftlichkeit und der Sicherheit der Informatik nach der Auslagerung

## Parlamentsdienste

## Das Wesentliche in Kürze

Die Eidgenössische Finanzkontrolle (EFK) hat bei den Parlamentsdiensten (PD) die Wirtschaftlichkeit und Sicherheit der Informatik nach der Auslagerung der Gebiete Netzwerk, Telefonie, WLAN, Mail- und Systemserver und Datenbank der Kollaborationsplattform geprüft. Dabei unterscheidet die EFK bezüglich den Feststellungen und Beurteilungen zwischen dem IKT-Anwendungsbereich der *Ratsmitglieder (IKT-Bereich Parl)* und jenem der *Parlamentsdienste (IKT-Bereich PD)*.

**Der Provider-Wechsel bewirkt eine markante Verbesserung der Wirtschaftlichkeit**

Durch den Provider-Wechsel vom Bundesamt für Informatik (BIT) zur Swisscom, konnten die vom BIT prognostizierten jährlichen Kosten für Netzwerk und Telefonie insgesamt von 3 Millionen Franken auf 700 000 Franken gesenkt werden. Sowohl mit dem Transfer der ursprünglichen Leistungen, als auch bei den Erweiterungen, wurden die Erwartungen somit weit übertroffen. Die Entscheidungsgrundlage zu Händen der Bundesversammlung wurde im Antrag «Businesspartner für die IKT-Dienstleistungen der Parlamentsdienste» und in der Projektstudie «Betrieb und Kosten der IKT-Basis-Infrastruktur für die Bundesversammlung» vom 7. Oktober 2010 korrekt erarbeitet und transparent dargestellt. Allerdings existiert für die Umsetzung des Business Case keine Nachkalkulation. Um dessen Wirtschaftlichkeit nachzuweisen mussten die Realisierungs- und Betriebskosten zum Prüfungszeitpunkt durch die EFK zuerst zusammengetragen und den bisherigen Kosten gegenübergestellt werden.

**Eine angemessene IT Governance im IKT-Sicherheitsbereich des Parlaments ist herausfordernd**

Die IT-Governance, als Instrument zur Festlegung der Rahmenbedingungen und Unterstützung des IT-Managements durch die Führungsebene, ist im *IKT-Bereich Parl* strukturgemäss nicht stark ausgeprägt. Es fehlt eine klare Zuweisung der Verantwortlichkeit für die IT Governance. Die Risikoabwägungen und Bestimmung der Sicherheitsanforderungen erfolgen primär durch die Ressorts Informatik (Ressort IT) und den Informatiksicherheitsbeauftragten (Ressort ISBD) der Parlamentsdienste. Die getroffenen Sicherheitsmassnahmen beruhen somit schwergewichtig auf der Einschätzung der Parlamentsdienste. Bei der Entwicklung von neuen Informatikdiensten für die Räte erfolgte dies in Absprache mit der Verwaltungsdelegation (VD). Es besteht auch eine tiefe Akzeptanz der Benutzer (Räte) für notwendige Sicherheitsvorkehrungen, welche sie in der Nutzung der IKT Dienste direkt betrifft. Diese Situation führt dazu, dass es sowohl für die Verwaltungsdelegation (VD) als auch die Ressorts IT und ISBD schwierig ist, einige wichtige technische und organisatorische Sicherheitsmassnahmen, die heutzutage verbreitet als gute Praxis anerkannt sind, im *IKT-Bereich Parl* einzufordern und umzusetzen.

Im Entwurf zum neuen Informationssicherheitsgesetz (ISG Entwurf) werden die Parlamentsdienste explizit aufgeführt. Es bleibt abzuwarten, inwiefern sich aus dem neuen Gesetz entsprechende Kompetenzen ableiten lassen, welche die Umsetzung der IT-Governance erleichtern.

**Die technische IKT-Sicherheit sollte punktuell verbessert werden**

Die Ressorts ISBD und IT der PD verfügen über ein gutes Sicherheitsbewusstsein. Das Ressort IT lässt sich in sensiblen Bereichen punktuell immer wieder durch externe Spezialisten beurteilen. Auch wenn sie dazu nicht verpflichtet sind (ausgenommen die Anbindung des Parlamentsnetzes an das Netz der BV (VPN-BV), orientieren sich die PD, bzw. die Ressorts ISBD und IT am Bundesstandard. Der *IKT-Bereich PD* bewegt sich grundsätzlich auf einem angemessenen Niveau. Während der Prüfung wurden bei Server Konfigurationen vereinzelt noch Abweichungen von den technischen Vorgaben identifiziert. In diesem Bereich sollten die Kontrollen systematischer durchgeführt und das Monitoring verbessert werden.

# Audit de la rentabilité et de la sécurité de l'informatique après l'externalisation

## Services du Parlement

## L'essentiel en bref


Le Contrôle fédéral des finances (CDF) a vérifié la rentabilité et la sécurité de l'informatique au sein des Services du Parlement après l'externalisation des secteurs suivants: réseau, téléphonie, WIFI, serveurs des messageries et des systèmes et base de données de la plateforme de collaboration. Dans le cadre de ses évaluations et de ses constatations, le CDF fait la distinction entre le secteur informatique des *parlementaires* et celui des *Services du Parlement*.

**Le changement de fournisseur a considérablement amélioré la rentabilité**

En passant de l'Office fédéral de l'informatique et de la télécommunication (OFIT) à Swisscom, le changement de fournisseur a permis de baisser les frais annuels de réseau et de téléphonie prévus par l'OFIT de 3 millions à 700 000 francs au total. Les attentes ont été largement dépassées, aussi bien au niveau du transfert des prestations initiales que de leur extension. Les bases décisionnelles destinées à l'Assemblée fédérale ont été élaborées correctement et présentées avec transparence dans la proposition concernant «le partenaire commercial pour les prestations informatiques des Services du Parlement» et dans l'étude de projet sur «l'exploitation et les frais de l'infrastructure informatique de base pour l'Assemblée fédérale» du 7 octobre 2010. Cependant, il n'existe aucun calcul rétrospectif pour la mise en œuvre du modèle d'affaire. Pour prouver sa rentabilité, le CDF a dû, au moment de l'audit, regrouper tout d'abord les frais de réalisation et d'exploitation et les comparer avec les anciens coûts.

**Une gouvernance appropriée dans le domaine de la sécurité informatique du Parlement est un défi**

La gouvernance informatique, en tant qu'instrument destiné à fixer les conditions-cadres et à soutenir la gestion informatique à l'échelon de la direction, est peu visible dans la structure du secteur informatique des parlementaires. La responsabilité de la gouvernance informatique n'a pas été clairement attribuée. L'évaluation des risques et la détermination des exigences en matière de sécurité incombent avant tout aux domaines de l'informatique (Domaine IT) et des délégués à la sécurité informatique (Domaine DSI) des Services du Parlement. Les mesures de sécurité prises reposent principalement sur l'estimation de ces derniers. Dans le cadre du développement de nouveaux services informatiques pour les Chambres fédérales, les mesures de sécurité ont été prises en accord avec la Délégation administrative (DA). De plus, les utilisateurs – à savoir les parlementaires – acceptent mal les mesures de sécurité qui concernent directement leur utilisation des services informatiques. Dès lors, il est difficile aussi bien pour la DA que pour les Domaines IT et DSI d'imposer et de mettre en œuvre dans le secteur informatique des parlementaires des mesures techniques et organisationnelles importantes visant à renforcer la sécurité, alors qu'elles ont fait leurs preuves et sont largement répandues.

Dans le nouveau projet de loi sur la sécurité de l'information, les Services du Parlement sont explicitement mentionnés. Reste à voir dans quelle mesure cette nouvelle loi débouchera sur des compétences correspondantes, capables de faciliter la mise en œuvre de la gouvernance informatique.

**La sécurité informatique sur le plan technique devrait être améliorée ponctuellement**

Les Domaines IT et DSI des Services du Parlement sont conscients des impératifs de sécurité. Le Domaine IT demande régulièrement à des spécialistes externes de l'évaluer dans des secteurs sensibles. En outre, les Services du Parlement, et donc les Domaines IT et DSI, suivent le standard de la Confédération, même s'ils n'y sont pas tenus (à l'exception de la connexion du réseau du Parlement au réseau VPN de l'administration fédérale). D'une manière générale, le secteur informatique des Services du Parlement se situe à un niveau approprié. Au cours de l'audit, le CDF a encore identifié quelques écarts par rapport aux directives techniques concernant les configurations des serveurs. Dans ce domaine, il faudrait mener des contrôles plus systématiques et améliorer la surveillance.

**Texte original en allemand**

# Verifica della redditività e della sicurezza dell'informatica in seguito all'esternalizzazione

## Servizi del Parlamento

## L'essenziale in breve

Il Controllo federale delle finanze (CDF) ha verificato la redditività e la sicurezza dell'informatica presso i Servizi del Parlamento in seguito all'esternalizzazione dei settori reti, telefonia, WLAN, server di posta elettronica e di sistema e banca dati della piattaforma di collaborazione dell'Amministrazione federale. A tal proposito, il CDF distingue i pareri e le valutazioni tra i settori di applicazione delle TIC dei *membri delle Camere (settore TIC Parl)* e quelli dei *Servizi del Parlamento (settore TIC SP).*

**Il cambiamento di provider ha determinato un netto miglioramento della redditività**

Con il passaggio a Swisscom l'Ufficio federale dell'informatica e della telecomunicazione (UFIT) ha potuto ridurre i costi annui per le reti e la telefonia previsti da un totale di 3 milioni a 700 mila franchi. Le aspettative sono state ampiamente superate per quanto riguarda il trasferimento delle prestazioni iniziali nonché gli ampliamenti delle stesse. Le basi decisionali da presentare all'Assemblea federale sono state elaborate correttamente e presentate chiaramente nell'istanza «Partner commerciali per le prestazioni TIC dei Servizi del Parlamento» e nello studio di fattibilità «Gestione e costi dell'infrastruttura di base delle TIC per l'Amministrazione federale» del 7 ottobre 2010. Tuttavia, non esiste alcun calcolo retrospettivo per la realizzazione del *business case*. Per dimostrarne la redditività, al momento della verifica il CDF ha dovuto dapprima raccogliere i costi di realizzazione e d'esercizio e poi confrontarli con quelli attuali.

**Un'adeguata governance informatica nel settore della sicurezza TIC del Parlamento è difficile da realizzare**

Dal punto di vista strutturale, la governance informatica come strumento per definire le condizioni quadro e supporto per la gestione informatica a livello dirigenziale non è molto incisiva nel *settore TIC del Parlamento*. Manca una chiara attribuzione delle responsabilità per la governance informatica. Le valutazioni dei rischi e la determinazione dei requisiti di sicurezza vengono effettuate in primo luogo dalla sezione informatica (sezione IT) e dagli addetti alla sicurezza informatica (sezione ISID) dei Servizi del Parlamento. In questo modo, le misure di sicurezza adottate si basano soprattutto sulle valutazioni dei Servizi del Parlamento. È stato possibile realizzare nuovi servizi informatici per le Camere d'intesa con la Delegazione amministrativa. Gli utenti (Camere) sono assolutamente favorevoli ad adottare le misure di sicurezza necessarie per l'utilizzo dei servizi TIC che li riguarda. In un tale contesto, per la delegazione amministrativa e per i settori IT e ISID è difficile richiedere e realizzare nel *settore TIC Parl* importanti misure di sicurezza tecniche e organizzative che attualmente siano riconosciute come buona prassi.

Nel progetto della nuova legge sulla sicurezza delle informazioni (progetto LSIn), i Servizi del Parlamento vengono esplicitamente indicati. Resta ancora da determinare come dalla

nuova legge si possano determinare le relative competenze che semplifichino la realizzazione della governance informatica.

**La sicurezza TIC tecnica deve ancora essere migliorata in casi specifici**

Le sezioni ISID e IT dei Servizi del Parlamento sono consapevoli della sicurezza informatica. Le aree sensibili della sezione IT sono costantemente esaminate da specialisti esterni. Anche quando non sono obbligati (ad eccezione della connessione della rete del Parlamento alla rete dell'Amministrazione federale – VPN-AF), i Servizi del Parlamento o le sezioni IT e ISID si basano sugli standard federali. Il *settore TIC SP* in linea di principio ha un livello adeguato. Durante la verifica, in singoli casi sono stati individuati degli scostamenti dalle prescrizioni tecniche nelle configurazioni dei server. In questo ambito si dovrebbero effettuare sistematicamente dei controlli e migliorarne il monitoraggio.

**Testo originale in tedesco**

# Audit of economic efficiency and security of IT after outsourcing

## Parliamentary Services

## Key facts

The Swiss Federal Audit Office (SFAO) audited the economic efficiency and security of IT in Parliamentary Services (PS) after the network, telephony, WLAN, mail and system servers and the collaboration platform database areas were outsourced. In this regard, the SFAO makes a distinction in its findings and assessments between the ICT application area of *Council members* (*ICT Parl area*) and that of *Parliamentary Services* (*ICT PS area*).

**Provider change resulted in significant improvement in economic efficiency**

By switching provider from the Federal Office of Information Technology, Systems and Telecommunication (FOITT) to Swisscom, the total annual network and telephony costs predicted by the FOITT were reduced from CHF 3 million to CHF 700,000. Expectations were thus considerably exceeded with both the transfer of the original services and expansions. The decision-making basis for the Federal Assembly was correctly and transparently presented in the proposal "Business partner for ICT services for Parliamentary Services" and the project study "Operation and costs of the basic ICT infrastructure for the Federal Assembly" of 7 October 2010. However, there is no post calculation for the implementation of the business case. In order to prove its economic efficiency, the SFAO first had to gather the implementation and operating costs at the time of the audit and compare them with the earlier costs.

**Appropriate IT governance in Parliament's ICT security area is challenging**

IT governance as a tool for defining the framework conditions and as a supporting tool for IT management at managerial level is not strongly developed structurally in the *ICT Parl area*. There is no clear allocation of responsibility for IT governance. Risk assessments and the determination of the security requirements are carried out primarily by the IT Section and the IT security officer (ISBD Section) of PS. The security measures taken are therefore based largely on the assessment of PS. When new IT services were being developed for the Councils, this was done in consultation with the Administration Delegation (ADel). There is also high acceptance by users (Councils) of necessary security precautions that affect them directly in the use of ICT services. As a result of this situation, it is difficult for both the ADel and the IT and ISBD Sections to require and implement some important technical and organisational security measures which are now widely recognised as good practice in the *ICT Parl area*.

The draft of the new Information Security Act (ISA draft) explicitly lists PS. It remains to be seen to what extent corresponding powers which facilitate the implementation of IT governance can be derived from the new law.

**Technical ICT security should be improved selectively**

The PS ISBD and IT Sections have a good level of security awareness. The IT Section repeatedly has selective assessments carried out by external specialists in sensitive areas. Even though they are not obliged to do so (except for the parliamentary network's connection to the Fed. Adm. network – VPN-Fed. Adm.), PS and the ISBD and IT Sections are oriented towards the federal standard. The *ICT PS area* is generally at an appropriate level. During the audit, some deviations from the technical specifications were still identified in the case of server configurations. Controls should be carried out more systematically in this area, and monitoring should be improved.

**Original text in German**

# Generelle Stellungnahme der Parlamentsdienste

Die Parlamentsdienste nehmen mit Befriedigung zur Kenntnis, dass die EFK ihnen ein gutes Sicherheitsbewusstsein attestiert und dass sie sich auf einem angemessenen Niveau bewegen. Die Empfehlungen der EFK nehmen die Parlamentsdienste dankend auf, um sich weiter zu verbessern und das erreichte Niveau zu festigen.

# 1 Auftrag und Vorgehen

## 1.1 Ausgangslage

Gestützt auf Artikel 6 und 8 des Finanzkontrollgesetzes (FKG) hat die Eidgenössische Finanzkontrolle (EFK) im Herbst 2016 im Ressort IT der Parlamentsdienste eine Finanzaufsichtsprüfung durchgeführt. Nach dem Dienstleisterwechsel vom Bundesamt für Informatik und Telekommunikation (BIT) zum Outsourcing-Anbieter Swisscom AG, sowie weiteren Auslagerungen von IT-Dienstleistungen zu den Anbietern Abraxas Informatik AG (Mail) und Fabasoft Schweiz AG (Datenaustauschplattform), standen die Wirtschaftlichkeit und Nachhaltigkeit sowie die Sicherheit der Systeme (Netz, Server, an Ratsmitglieder abgegebene PC) im Vordergrund.

## 1.2 Prüfungsziel und -fragen

Das Prüfungsziel beinhaltet die Beurteilung der Zuverlässigkeit und der Wirtschaftlichkeit nach der Auslagerung an Swisscom sowie die Gewährleistung der IT-Sicherheit im Parlament und den Parlamentsdiensten.

Zusammengefasst ergeben sich daraus folgende zentrale Fragen:

- Kann die Auslagerung an Swisscom als wirtschaftlich betrachtet werden (Kosten-Nutzen-Analyse)
- Ist der Zugang Externer zu den betriebenen Systemen (Server, Netze) der Parlamentsdienste ausreichend abgesichert und überwacht?
- Werden angemessene Massnahmen bestimmt und umgesetzt, um die Sicherheit der Systeme zu gewährleisten?
- Werden die definierten Massnahmen zur Einhaltung des IKT-Grundschutzes umgesetzt?
- Liegen zu den kritischen Anwendungen mit sensitiven Daten gültige und adäquate Schutzbedarfsanalysen (SchuBan) und ISDS-Konzepte vor?

## 1.3 Prüfungsumfang und -grundsätze

Die EFK führte die Prüfungsarbeiten in der Zeit von Ende September 2016 bis Mitte April 2017 mit Unterstützung externer Spezialisten durch. Anders als die Verwaltungseinheiten (VE) der Bundesverwaltung (BV), sind die Bundesversammlung (BVers) und die Parlamentsdienste nicht zwingend einem spezifischen Sicherheitsstandard unterstellt. Ausgenommen ist die Anbindung des Parlamentsnetzes an das VPN-BV, welche den „Bundessicherheitsstandard“ zwingend erfüllen muss. Die PD hat sich im *IKT-Bereich PD* jedoch selbständig dem IKT-Sicherheitsstandard des Bundes verpflichtet. Daher wurden die Überprüfungen und Beurteilungen in diesem Bereich unter Anwendung des „Bundesstandards“ durchgeführt. Im *IKT-Bereich PARL* orientiert sich die BVers am Parlamentsgesetz (ParlG) und an der Parlamentsverwaltungsverordnung (ParlVV). Alle die im Rahmen des Audits verwendeten Grundlagen finden sich in der Übersicht „Grundlagen“ im Anhang 1.

Die Schlussfolgerungen im Bericht stützen sich auf Prüfungen von Unterlagen, ergänzenden Erhebungen und Interviews mit Fachvertretern der involvierten Bereiche, sowie stichprobenweise technische Überprüfungen.

## 1.4 Schlussbesprechung

Die Schlussbesprechung fand am 10.08.2017 statt. Teilgenommen haben:

PD: Leiter Infrastruktur, Informatiksicherheitsbeauftragter (ISBD), Stv. CIO / Supply Manager Infrastruktur / IT

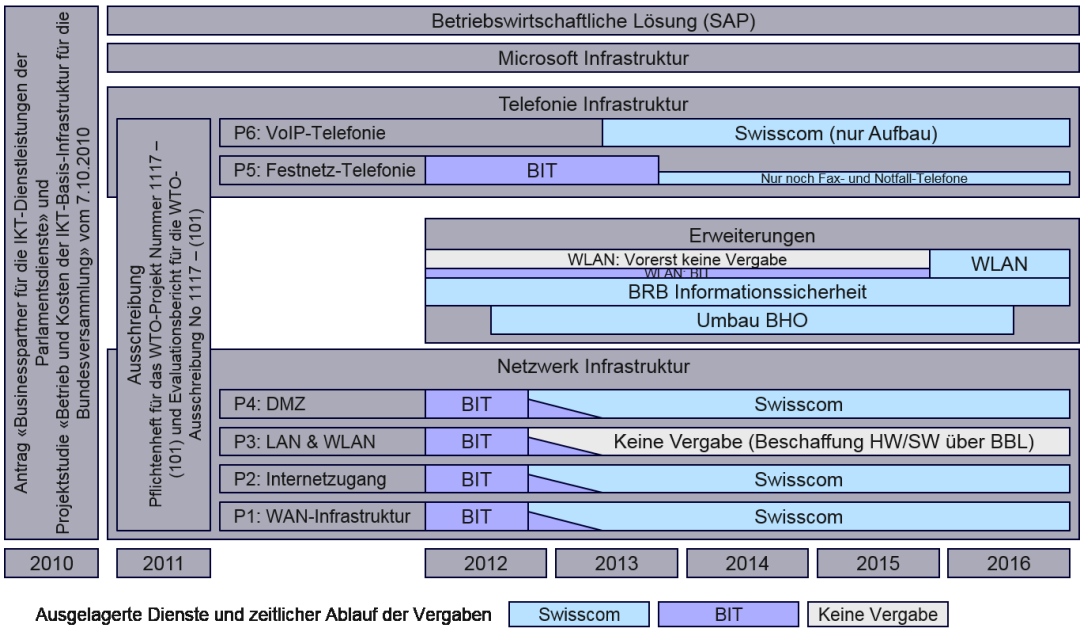
EFK: Federführender, Revisionsleiter

Die EFK dankt für die gewährte Unterstützung und erinnert daran, dass die Überwachung der Empfehlungsumsetzung den Amtsleitungen bzw. den Generalsekretariaten obliegt.

EIDGENÖSSISCHE FINANZKONTROLLE

# 2 Gesteigerte Wirtschaftlichkeit nach Neuausschreibungen und Auslagerungen

Aus Kostengründen und infolge von Inkonsistenzen bei der Leistungserbringung, hat die Verwaltungsdelegation auf Antrag der Parlamentsdienste entschieden, die BIT-Leistungen durch verschiedene Dienstleister neu anbieten zu lassen. Hierzu erfolgte im Kalenderjahr 2011 eine WTO-Ausschreibung (WTO Projekt-Nr. 1117) mit dem Evaluationsentscheid, die bis anhin vom BIT bezogenen Leistungen an Swisscom zu transferieren (Leistungen P1, P2, P4-P6 gemäss Graphik unten). Die Soft- und Hardware für das interne Fest- (LAN) und Funknetz (WLAN) wurde über das BBL beschafft. Nicht von der Ausschreibung betroffen sind die Microsoft Infrastruktur (Büroautomation) sowie die Betriebswirtschaftliche Lösung SAP, welche weiterhin durch das BIT betrieben werden.




Nach der WTO-Ausschreibung 2011 sind Ereignisse eingetreten, welche Anpassungen und Ergänzungen am Business Case (WTO-Projekt Nummer 1117) verlangten:

- Umsetzung des Bundesratsbeschlusses (BRB) zur Informationssicherheit (2012)
- Umbau des Bundeshaus Ost (BHO, Ende 2012 bis Mitte 2016)
- Flächendeckendes WLAN durch Swisscom (2016)

## 2.1 Projektstudie und Beschaffungsantrag bilden eine transparente und nachvollziehbare Entscheidungsgrundlage

Die Ausgangslage, Handlungsoptionen sowie Empfehlungen wurden im Beschaffungsantrag «Businesspartner für die IKT-Dienstleistungen der Parlamentsdienste» übersichtlich und transparent dargestellt.

Das Dokument «Projektstudie: Betrieb und Kosten der IKT-Basis-Infrastruktur für die Bundesversammlung» enthält die Berechnungen zu den alternativen Szenarien «neues Angebot BIT», «Dienstleistungsbezug Extern» und «interne Erbringung durch die Parlamentsdienste». Die im Jahr 2010 durchgeführte Projektstudie ist nachvollziehbar und zeigt das damalige Kostenniveau sowie die prospektiven Einsparungen der untersuchten Alternativen verständlich auf.

Eine Auflistung, welche Leistungen nun wirklich zu diesem Zeitpunkt festgelegt oder aber erst später hinzugekommen sind, fehlt. Zudem war in den zur Verfügung gestandenen Dokumenten auch nirgends ersichtlich, dass die ausgeschriebenen Leistungen nicht ausgeschöpft wurden. Eine vollständige Vergabe erfolgte für die WAN-Infrastruktur (P1), Internet-Zugang (P2) und DMZ (P4). Die Ergänzung LAN&WLAN (P3) wird mit durch das BBL beschaffter Hardware umgesetzt. Die Festnetztelefonie (P5) wird nicht vergeben. Bei VoIP-Telefonie (P6) wird nur der Aufbau, nicht aber der Betrieb extern in Auftrag gegeben.

Die Übersicht der vergebenen Leistungen sowie die Darstellung des zeitlichen Ablaufs mussten durch die EFK im Rahmen der Prüfung zuerst erarbeitet werden (vergl. Graphik oben: Ausgelagerte Dienste und zeitlicher Ablauf der Vergaben). Alle zur Erstellung der Übersicht notwendigen Unterlagen waren vorhanden und im SharePoint abgelegt. Die verschiedenen Dienstleistungen werden jedoch immer wieder anders bezeichnet. Dies erschwerte es zu erkennen, welche Services einander jeweils entsprachen.

Aus Sicht der EFK sollten in künftigen Projekten die chronologische Abwicklung laufend dokumentiert und Veränderungen besser nachgewiesen werden. Nur so ist es möglich Nutzen und Mehrwert solcher Projekte nachzuweisen.

## 2.2 Der Business Case „Auslagerung“ hat die Erwartungen weit übertroffen

Die durch die EFK erstellte Nachkalkulation belegt den bei Projektbeginn erwarteten Erfolg. Sie zeigt auf, dass mit dem Wechsel und den weiteren Auslagerungen eine signifikante Senkung der vom BIT prognostizierten jährlichen Betriebskosten ab 2011 von ca. 3 Millionen Franken auf 700 Tausend Franken erreicht werden konnte. Dieser Betrag liegt auch tiefer als die vom BIT verrechneten historischen Kosten von 1,87 Millionen Franken für 2010.

Die effektiven Kosten sind in einem Excel Sheet erfasst und basieren auf den eingegangenen Rechnungen des Service Providers Swisscom. Soweit überprüfbar decken sich diese auch mit den bei der Ausschreibung vereinbarten Preisen. Mit der Summierung der aufgelisteten Rechnungen sind die Gesamtkosten nachgewiesen.

Was aus Sicht der EFK fehlte, um die prognostizierten Einsparungen zu verifizieren, ist eine Aufzeichnung der Kostenentwicklung der einzelnen Leistungspakete über die Zeit (Leistungserbringung durch BIT, prognostizierte Kosten, effektive Kosten nach Auslagerung). Die notwendige Nachkalkulation wurde durch die EFK im Rahmen der Revisionsarbeiten erstellt. Bedingt durch die zwischenzeitlich vorgenommenen Änderungen an den ursprünglichen Leistungspaketen, waren die Rechnungen vorgängig aufwändig zu separieren und den neu definierten Services entsprechend, wieder zuzuweisen.

## 2.3 Die Leistungserweiterungen erfolgten organisatorisch korrekt, waren kostenmässig jedoch schwierig abzugrenzen

Die Umsetzung des Bundesratsbeschlusses zur Informationssicherheit (BRB vom 16. Dezember 2009) erhöhte die Anforderungen an die bezogenen Swisscom-Leistungen. Die damit verbundenen Änderungen wurden vertraglich und kostenmässig korrekt umgesetzt.

Im Zusammenhang mit dem Umbau des Bundeshauses Ost (BHO), erfolgte auch der Beschluss 2015, das WLAN flächendeckend einzuführen. Dies erforderte Leistungserweiterungen bezüglich Erneuerung und Ausbau der Netzwerke. Auch dafür bestehen korrekte Anträge und Ausschreibungen. Im Endeffekt wurden die ursprünglich durch die VD bewilligten Leistungen für das lokale Netzwerk (LAN), das drahtlose, lokale Netz (WLAN) und die Telefonie nicht vollständig ausgeschöpft.

Die zusätzlichen oder angepassten Leistungen sind durch die Rechnungen prinzipiell ausgewiesen. Auch hier erfolgte die Führung der Kosten nicht in der Struktur der Ausschreibung. Die Leistungserweiterungen waren durch die EFK daher kostenmässig jedoch nur mit entsprechendem Aufwand vom ursprünglichen Business Case abzugrenzen, resp. vergabebezogen zusammenzufassen. Die so erstellten Nachkalkulationen sowie Kostengegenüberstellungen (BIT versus Swisscom) zeigen, dass sich mit dem Providerwechsel auch für die Leistungserweiterungen bedeutende Einsparungen ergeben.

# 3 Die IT-Governance im IKT-Bereich des Parlaments hat Verbesserungspotenzial

Die IT-Governance, als Instrument zur Festlegung der Rahmenbedingungen und Unterstützung für das IT-Management, stellt die geforderte Leistung und Konformität in den IKT-Prozessen sicher. Im *IKT-Bereich Parl* existiert kein übergeordneter Managementbereich, welcher die IT-Governance konsequent adressiert. Die angewandten IKT Sicherheitsvorgaben sind primär vom Bundesgesetz über die Bundesversammlung (ParlG) und der Verordnung der Bundesversammlung zum Parlamentsgesetz und über die Parlamentsverwaltung (ParlVV) abgeleitet.

Die Risikoabwägungen sowie die Bestimmung der IKT-Sicherheitsanforderungen und der notwendigen Massnahmen erfolgen grundsätzlich systematisch, primär aber durch das Ressort IT der PD selbst. Zusätzlich bestehen weder für die VD noch für die PD Weisungsbefugnisse in diesem Gebiet an die Räte. Die Frage der Verantwortlichkeiten muss in jedem einzelnen Fall jeweils wieder neu geprüft werden.
Vorgaben hinsichtlich Sicherheit, Vertraulichkeit und Qualität der Dienstleistungen, sind für den *IKT-Bereich PARL* zu wenig konsequent festgelegt und lassen sich kaum kurzfristig an neue Gegebenheiten anpassen. Beispiele dazu sind die nicht durchgängige Verwendung gehärteter Laptops, unvollständige Vorgaben und Anweisungen zum Mail-Verkehr oder der ungenügend definierte Schutzbedarf von Netzwerk- und Datenservern der Ratsmitglieder. Zudem besteht auch eine tiefe Akzeptanz sicherheitsrelevanter Richtlinien und Anweisungen durch die Anwender.

Aus Sicht der EFK liegen die Abwägung der Risiken und die Bestimmung der Massnahmen in der Verantwortung des Anwenders, bzw. des Daten-Eigentümers. Sie sind ein wesentlicher Bestandteil der Geschäftsführung und deren Organisation. Durch die zu wenig ausgeprägte und zu wenig konsequent wahrgenommene Governance *im IKT-Bereich Parl*, sind wichtige, technische und organisatorische Massnahmen, die heute in zahlreichen Organisationen als gute Praxis angewandt werden, heute nicht oder nur ungenügend definiert und umgesetzt.

Im Entwurf zum neuen Informationssicherheitsgesetz (ISG Entwurf) werden die Parlamentsdienste explizit aufgeführt. Es bleibt abzuwarten, inwiefern sich aus dem neuen Gesetz entsprechende Verfahren, Weisungen und Vorgaben ableiten lassen, welche die Kompetenz der VD im Bereich IT Governance erhöhen.

# 4 Die technische IKT-Sicherheit sollte punktuell verbessert werden

Die IKT des Parlaments und der PD ist bundesseitig keinen Sicherheitsvorgaben unterstellt, mit Ausnahme der Anbindung des Parlamentsnetzes an das Netz der BV (VPN-BV). Die PD orientieren sich jedoch aus eigenem Antrieb am IKT-Sicherheitsstandard der BV und richten sich damit grundsätzlich an einem angemessenen Niveau aus. Das Ressort IT der PD als IKT Betreiber für die Mitglieder der BVers, verfügt über ein gutes Sicherheitsbewusstsein und wird in sensiblen Bereichen (Härtung Laptop, Netzwerk) mittels externer Audits von Zeit zu Zeit durch Spezialisten überprüft.

## 4.1 Härtung der Laptops für die Ratsmitglieder ist auf einem angemessenen Stand, aber schwierig aufrecht zu erhalten

Die Ratsmitglieder können von den PD einen persönlichen, standardisierten Laptop beziehen. Damit sollen ihre Arbeiten unterstützt und eine gewisse Basis-Sicherheit gewährleistet werden.

Die Installation der Laptops erfolgt unterstützt durch ein zentrales Management-Tool, basierend auf zentral definierten Konfigurationen. Für das Fertigstellen eines Laptops für ein Ratsmitglied wird von dem Mitarbeitenden der PD (IT Support) eine Checkliste verwendet. Hinsichtlich der Aktualisierung von Software und Anti-Viren-Programmen vor und nach der Übergabe an das Ratsmitglied, wird ebenfalls das zentrale Management-Tool eingesetzt. Die Lösung erlaubt es, regelmässige Aktualisierungen durchzuführen. Dies erfolgt, nicht nur über das Netzwerk der Ratsmitglieder, sondern auch über eine beliebige Internetverbindung.

Zusätzlich stellt das Ressort IT, bzw. ISBD den Räten einen Leitfaden zum Umgang mit sensiblen Informationen zur Verfügung. Diese Wegleitung enthält generelle Tipps zu verschiedenen Themen wie Festplattverschlüsselung, Passwörter, Viren und Datensicherung.

Nach der Installation der ersten Laptops wurden diese durch einen externen Dienstleister im November 2015 auf ihre Sicherheit überprüft. Zur Behebung der festgestellten Schwachstellen wurden Massnahmen definiert und der Stand der Umsetzung in einer Übersicht nachgeführt. Die Massnahmen zu den Feststellungen aus dieser Sicherheitsprüfung sind zum Zeitpunkt der EFK-Prüfung mehrheitlich umgesetzt.

Im Rahmen des vorliegenden Audits hat die EFK festgestellt, dass die Härtung der Laptops bei der Abgabe an die Ratsmitglieder grundsätzlich ein angemessenes Niveau aufweist, dass es aber schwierig ist, diese über die Zeit aufrecht zu erhalten.

Eine Weisung der Verwaltungsdelegation über die IKT-Dienstleistungen für die Ratsmitglieder beschreibt die Modalitäten und Rahmenbedingungen für das Bereitstellen und die Nutzung der IT-Dienstleistungen, inkl. der persönlichen Informatikausrüstung der Ratsmitglieder. Darin ist festgehalten, dass alternativ zum Bezug eines standardisierten Laptops von den Parlamentsdiensten auch der Bezug eines zweckgebundenen Betrags für die individuelle Beschaffung eines Laptops oder ähnlicher Geräte möglich ist. Auf die Konfiguration dieser Geräte hat das Ressort IT heute keinen Einfluss.

Dadurch entsteht die Situation, dass nur ein Teil der durch die Ratsmitglieder eingesetzten Geräte (aktuell 165) gehärtet ist. Die EFK beurteilt dieses Vorgehen als wenig zielführend und zu wenig konsequent. Es fehlen weiter klar definierte Sicherheitsanforderungen, welche den Bedarf dieser Sicherheitsvorkehrung deutlich erkennen lässt. Wird eine sicherheitsbedingte Härtung gefordert, müssen sämtliche im Parlament eingesetzten Laptops diesen Standard aufweisen. Die Einstellungsmöglichkeiten sind soweit einzuschränken, wie es für die Sicherheit der Informationen des Parlaments notwendig ist. Hierfür gilt es auch die notwendige Akzeptanz zu schaffen (vergleiche dazu auch Kapitel 2, IT-Governance des Parlaments). Aus Sicht der EFK bestehen zum Beispiel durch die Verwendung virtueller Clients, heute diesbezüglich Lösungen auf dem Markt, welche die Sicherheit erhöhten und die private Nutzung der Geräte mit wenig Einschränkung trotzdem zulassen.

## 4.2 Netzwerkarchitektur und -Sicherheit folgen akzeptierter guter Praxis

Der Betrieb der Datennetze für die Parlamentsdienste und die Räte ist an die Swisscom ausgelagert. Dies beinhaltet auch den Betrieb der Netzwerk-Sicherheits-Komponenten. Die Vergabe erfolgte nach einer WTO-Ausschreibung im Jahre 2011. Gemäss der Evaluierung konnte Swisscom belegen, die von den Parlamentsdiensten festgelegten technischen Kriterien hinsichtlich Architektur und Sicherheit zu erfüllen.

Swisscom stellt Berichte zur Einhaltung interner Kontrollen und Sicherheitsstandards nach einem geläufigen Rapportierungsstandard für Dienstleister (ISAE 3402, Type 2) zur Verfügung. Gemäss der vorliegenden Berichte (zu „Managed Connectivity Services“ vom 8. Juni 2016 und zu „Managed Network Security Services“ vom 30. November 2015) wurden von den unabhängigen Prüfern keine für die Parlamentsinfrastruktur bedeutenden Abweichungen festgestellt. Zusätzlich zur Überwachung der Netzwerkkomponenten von Swisscom hat auch das Ressort IT Zugriff auf die Überwachungskonsolen mit Echtzeit-Informationen, welche es zu Kontrollzecken ebenfalls regelmässig nutzt.

Das Netzwerk der Räte, *IKT-Bereich PARL*, dient hauptsächlich der Zurverfügungstellung von Internet-Konnektivität. Weitere Systeme, wie Drucker oder Mediacenter, sind an diesem Netzwerk angeschlossen. Dieses Netzwerk für die Ratsmitglieder ist ein separates Netz. Mit den übrigen Netzen der Parlamentsdienste ist es nur eingeschränkt verbunden. Firewall-Systeme lassen nur restriktiv, die für den Betrieb notwendigen Verbindungen zu. Der Internet-Zugriff vom Netz für die Ratsmitglieder wird automatisch kontrolliert und Internet-Seiten, die für die Sicherheit des internen Netzes und der Systeme eine Gefahr darstellen, werden blockiert. Die Verbindung zwischen den Netzen der Parlamentsdienste (d. h. das Netz für die Ratsmitglieder und die übrigen Netze der Parlamentsdienste) und den Netzen der BV (d. h. den vom BIT betriebenen Netze) sind mittels Firewall-Systeme stark eingeschränkt. Zur Regelung der Sicherheitsanforderungen bei dieser Anbindung besteht ein sogenannter Domänenvertrag, wie von der BV gefordert. Die Sicherheit der Netzwerke und der Netzübergänge wurde nach der Überführung in den jetzigen Betrieb im Jahre 2013 durch die externe Firma scip AG geprüft. Insgesamt wurde im damaligen Bericht ein hohes Sicherheitsniveau attestiert. Weitere Massnahmen zur Erhöhung der Sicherheit wurden ergriffen und die Konfiguration der Firewall-Systeme wurde nochmals verbessert.

Im Rahmen des vorliegenden Audits hat die EFK einzelne, weiterführende Verbesserungsmöglichkeiten festgestellt, die sich teils auf technische Massnahmen, teils auf die Nachvollziehbarkeit durch entsprechende Dokumentation und die interne Berichterstattung

beziehen. Vor allem Im *IKT-Bereich PARL* sind im Bereich der Vorgaben und Regelungen für die Benutzung der Netzwerkinfrastruktur (vergleiche dazu auch Kapitel 2, IT-Governance des Parlaments) Anpassungen und Ergänzungen vorzunehmen.

Um mit der zunehmenden Digitalisierung (eDocuments) den adäquaten Schutz der Integrität, Vertraulichkeit und Authentizität der Daten und Dokumente gewährleisten zu können, sollten zumindest mittelfristig geeignete Maßnahmen festgelegt werden. Aus dem Gesichtspunkt des starken Anstiegs der Cyber-Kriminalität ist dabei besonders auch eine Verbesserung der Fähigkeiten zur frühzeitigen Erkennung von Angriffen und Angriffsversuchen in Erwägung zu ziehen.

## 4.3 Kommunikationswerkzeuge: Die E-Mail-Nutzung der Räte bedarf einer Risiko- und Schutzanalyse

Für die Ratsmitglieder, *IKT-Bereich PARL*, wird von den Parlamentsdiensten ein persönliches E-Mail-Konto betrieben. Auf das E-Mail-Konto können die Ratsmitglieder sowohl via E-Mail-Programm von einem PC, Laptop oder Smartphone als auch über einen Web-Browser zugreifen.

Der Betrieb der Dienstleistung wird von dem externen Unternehmen „Abraxas Informatik AG“ erbracht. Hierzu wurde eine WTO-Ausschreibung im Jahr 2015 durchgeführt. Gemäss Evaluationsbericht werden alle technischen Anforderungen inkl. Sicherheitsanforderungen erfüllt. Die Dienstleistung beinhaltet den Betrieb der eigentlichen E-Mail-Systeme als auch Umsysteme für die Sicherheit: Anti-Virus-Systeme, Systeme zur Netzwerklastverteilung als auch Redundanz-Systeme zur Ausfallsicherheit werden eingesetzt. Der diesbezügliche Vertrag beinhaltet ergänzende Bestimmungen zu den AGB des Bundes. So wird darin u.a. die Ausrichtung von Sicherheitsmassnahmen am internationalen Standard ISO/IEC 27001 als auch am IKT-Grundschutz BV verlangt Anforderungen hinsichtlich Verfügbarkeit der Systeme aber auch für die Betreuung bei Anfragen und Fehlern sind festgehalten.

Die Benutzerverwaltung wird durch das Ressort IT über eine Verwaltungskonsole durchgeführt. Zwischen dem extern betriebenen E-Mail-System für die Räte und den internen E-Mail-Systemen bei den Parlamentsdiensten besteht eine gesicherte Datenverbindung, welche gemäss Weisung der Verwaltungsdelegation den Übertrag von vertraulichen Informationen und Unterlagen gestattet.

Die Weisung der Verwaltungsdelegation beinhaltet Nutzungsbedingungen für den E-Mail-Dienst. Ein Sicherheitsmerkblatt der Parlamentsdienste zu Händen der Ratsmitglieder sensibilisiert hinsichtlich der grundsätzlichen Unsicherheit von E-Mails, die an andere Empfänger als die offiziellen Adressen der Ratsmitglieder gesendet werden.

Die EFK hat festgestellt, dass keine Schutzbedarfsanalyse, keine Risikobeurteilung und kein gesamtheitliches und detailliertes Informationssicherheits- und Datenschutzkonzept vorliegt. Gewisse Vorgaben für die Informationssicherheit gehen nicht aus den vorliegenden Vereinbarungen mit dem externen Dienstleister hervor. Zudem gibt es Unklarheiten hinsichtlich der Nutzungsbedingungen (vergleiche dazu auch Kapitel 2, IT-Governance des Parlaments). Es sollten adäquate Vorgaben für die Nutzung festgehalten und klar kommuniziert werden. Anzupassende Sicherheitsmassnahmen sind im Konzept zu dokumentieren, in vertraglichen Vereinbarungen mit dem Dienstleister zu adressieren und entsprechend umzusetzen.

Im Zusammenhang mit der steigenden Bedrohung durch Cyber-Attacken sollte das Ressort IT die fehlenden IKT-Sicherheitselemente schnellstmöglich ausarbeiten. Zur Sicherstellung der parlamentsgerechten Umsetzung empfiehlt es sich, das definierte Schutzniveau und die vorgesehenen Massnahmen mit der VD abzustimmen. Über vertragliche Vereinbarungen (SLA) kann die anforderungsgerechte Umsetzung der betriebsbezogenen Anforderungen und Vorgaben auch beim Dienstleister sichergestellt werden.

**Empfehlung 1 (Priorität 1)**

Die EFK empfiehlt dem Ressort Informatik & neue Technologien, eine Schutzbedarfsanalyse, eine Risikobeurteilung und ein Informationssicherheits- und Datenschutzkonzept für die E-Mail-Lösung der Räte auszuarbeiten und die vorhandenen Schutzmassnahmen damit abzugleichen.

**Stellungnahme der Parlamentsdienste**

Die heutige Lösung ist für Dokumente mit der Klassifikation ”vertraulich gemäss ParlG” konzipiert worden, welche ”intern” in der Bundesverwaltung entspricht. Es werden keine Dokumente oder Informationen mit einer höheren Schutzstufe versendet. Ein ISDS-Konzept nachträglich zu erstellen bringt aus Sicht der Parlamentsdienste keinen nennenswerten Mehrwert. Die Parlamentsdienste werden die Zweckmässigkeit eines ISDS-Konzepts bei einer neuen Evaluation oder Konzeption der E-Mail-Lösung frühestens im Hinblick auf den Legislaturwechsel 2019 prüfen.

## 4.4 Die Vorgaben zur Nutzung der Kollaborationsplattform sind noch in die IT-Governance PARL aufzunehmen

Für die Räte, *IKT-Bereich PARL*, wird eine Datenaustausch-Plattform betrieben. Diese Kollaborationsplattform gestattet einen einfachen Datenaustausch via Internet – zugreifbar mit allen gängigen Internet-Browsern. Die Austauschplattform steht den Ratsmitgliedern, den Mitarbeitenden der Parlamentsdienste sowie den Fraktionssekretariaten zur Verfügung. Der Betrieb der Dienstleistung wird von der Firma „Fabasoft Schweiz AG“ erbracht. Hierzu wurde eine WTO-Ausschreibung im Jahr 2015 durchgeführt.

Es liegen ein Sicherheitskonzept und verschiedene Nachweise und Selbstdeklarationen hinsichtlich der Sicherheitsanforderungen und -massnahmen vor. Gemäss Dokumentation erfolgt sowohl der Betrieb der Plattform als auch die Speicherung der Daten in der Schweiz. Ein Teil der Plattform wird durch einen Unterakkordanten in der Schweiz betrieben.

Der diesbezügliche Vertrag beinhaltet ergänzende Bestimmungen zu den AGB des Bundes. Unter Anderem wird die Ausrichtung von Sicherheitsmassnahmen am internationalen Standard ISO/IEC 27001 als auch am IKT-Grundschutz BV verlangt. Die Firma Fabasoft ist gemäss Dokumentation ISO 27001-Zertifiziert und die Kontrollen über den betreffenden Dienst wurden nach dem Prüf- bzw. Berichtsstandard ISAE 3402 geprüft.

Entsprechend Konzept und Selbstdeklaration werden die Daten verschlüsselt auf den Speichermedien abgelegt. Die abgelegten Daten sind somit für den Betreiber nicht lesbar.

Im Februar 2016 fand eine Teilabnahme für die Spezifikationen der Datensicherung statt. Die offenen Pendenzen wurden protokolliert, haben aber weder zur Verhinderung der Abnahme geführt, noch waren diese sicherheitsrelevant. Die Kollaborationsplattform wird zum Prüfungszeitpunkt als Pilot verwendet, ein Produktiveinsatz für alle Ratsmitglieder findet noch nicht statt.

Zugriffsberechtigungen werden durch das Ressort IT initial eingestellt. Danach wird Verwaltung dieser Berechtigungen an die Fraktionssekretariate übergeben. Die Authentifizierung über das Internet erfolgt per starker Authentifizierung, neben dem Passwort muss ein einmalig gültiger PIN eingegeben werden, den der Benutzer per SMS erhält.

Zum Zeitpunkt der Prüfung fehlte noch die Erstellung einer Risikobeurteilung, Schutzbedarfsanalyse sowie ein Informationssicherheits- und Datenschutzkonzept.

Auch im Bereich der Kollaborationsplattform sollte das Ressort IT die fehlenden IKT-Sicherheitselemente schnellstmöglich ausarbeiten. Nur so können Integrität, Vertraulichkeit und Authentizität der Daten und Dokumente bedarfsgerecht sichergestellt werden. Nach Ansicht der EFK empfiehlt es sich aus Governance-Überlegungen, das definierte Schutzniveau und die vorgesehenen Massnahmen mit der VD abzustimmen. Zusätzlich sollten die notwendigen, betriebsbezogenen Anforderungen und Vorgaben über vertragliche Vereinbarungen an den Dienstleister (SLA) adressiert werden. Anwenderseitig lässt sich das Sicherheitsniveau durch entsprechende Weisungen an die Benutzer stärken.

**Empfehlung 2 (Priorität 1)**

Die EFK empfiehlt dem Ressort Informatik & neue Technologien die Sicherheitsanforderungen zur Benutzung und zum Betrieb der Kollaborationsplattform der Räte klar zu definieren, durch die Verwaltungsdelegation bestätigen zu lassen und umzusetzen.

**Stellungnahme der Parlamentsdienste**

Die heutige Lösung ist für Dokumente mit der Klassifikation ”vertraulich gemäss ParlG” konzipiert worden, welche ”intern” in der Bundesverwaltung entspricht. Es werden keine Dokumente oder Informationen mit einer höheren Schutzstufe ausgetauscht. Ein ISDS-Konzept nachträglich zu erstellen bringt aus Sicht der Parlamentsdienste keinen nennenswerten Mehrwert. Die Parlamentsdienste werden die Zweckmässigkeit eines ISDS-Konzepts bei einer neuen Evaluation oder Konzeption der Kollaborationsplattform frühestens im Hinblick auf den Legislaturwechsel 2019 prüfen.

## 4.5 Die Server-Systeme Parlament und Parlamentsdienste unterliegen grundsätzlich einem sicheren Betrieb

Das Ressort IT betreibt die Server-Systeme sowohl für das Parlament als auch für die Parlamentsdienste. Im separaten Netzwerk der Räte sind einzelne Server für die Ansteuerung der Drucker, für den Betrieb der unpersönlichen Arbeitsplätze als auch für die Softwareverteilung und Verwaltung der Ressourcen im Einsatz. In den Netzen der Parlamentsdienste befinden sich zahlreiche Server für den Betrieb der Infrastruktur und der Anwendungen. Zu diesen Anwendungen zählen insbesondere die Abstimmungssysteme, ein Data Warehouse, die Dokumentenverwaltung (DokV) und ein System zur Protokollierung und Berichterstattung.

Für die Einstellungen und Konfigurationen der Server-Systeme sind die Vorgaben des IKT-Grundschutzes der BV nicht verbindlich. Dennoch wird dieser grundsätzlich als minimales Sicherheitsniveau vom Informatiksicherheitsbeauftragten der Parlamentsdienste eingefordert. Gemäss Informatiksicherheitsbeauftragten der PD kann die Umsetzung im Detail vom IKT-Grundschutz der BV abweichen, das angestrebte Sicherheitsniveau muss aber erhalten bleiben. Verbindliche Vorgaben für den sicheren Betrieb der Systeme sind in der „Richtlinie IKT-Betrieb“ vom Sicherheitsbeauftragten der Bundesversammlung auf Basis der Weisung über die Informatiksicherheit in den Parlamentsdiensten erlassen worden. Diese Richtlinie regelt insbesondere die Inbetriebnahme, die Härtung (Hardening), den Malware-Schutz und die Wartung von Systemen sowie das Schwachstellen- und Zugriffsmanagement. Detaillierte Konfigurations-Dokumente sind von den Parlamentsdiensten in Zusammenarbeit mit dem Software-Lieferanten Microsoft entwickelt worden. Die Basis-Serversysteme werden grundsätzlich automatisiert und gemäss dieser Vorgaben installiert. Die Konfigurationen und Software-Updates werden mit einem zentralen Management-Tool verteilt. Hochprivilegierte Systemzugriffe sind nur sehr restriktiv für einzelne, definierte Personen möglich. Eine automatische Überwachung meldet dem Informationssicherheitsbeauftragten verdächtige Zugriffe und Zugriffsversuche.

Während des Audits wurden einzelne Abweichungen bezüglich Software-Aktualisierung, Passwort-Vorgaben und Malware-Schutz bei internen Server-Systemen festgestellt. Angesichts der steigenden Anzahl von Cyber-Attacken ist es zentral, Abweichungen vom Soll-Zustand systematisch zu erkennen und zu korrigieren. Um bei der laufenden Zunahme der Bedrohungslage den geforderten Schutzbedarf weiterhin zu gewährleisten und richtig reagieren zu können, sollte das Ressort IT die Server-Systeme mittels Prüfplan regelmässig auf ihre Aktualität überprüfen und auf dem neuesten Stand halten.

**Empfehlung 3 (Priorität 2)**

Die EFK empfiehlt dem Ressort Informatik & neue Technologien die Effektivität im Bereich des Konfigurations- und Patch-Management durch verstärkte Kontrollen und ein regelmässiges Monitoring zu verbessern.

**Stellungnahme der Parlamentsdienste**

Dieser Befund wurde bereits adressiert. Das Patchmanagement ist neu konfiguriert. Die Prozesse und Kontrollen müssen noch dokumentiert werden.

# 5 Erledigung der offenen Empfehlungen aus PA 14238

Die offenen Empfehlungen aus PA 14238 (Prüfung der Sicherheit und des Vertragswesens im Informatikbereich) wurden mit der Einführung und dem Betrieb eines SharePoint Portals erledigt. Für die Archivierung von Unterlagen wurde darauf eine systematische und strukturierte Ablage eingerichtet. Die EFK hat die Ablage eingesehen und als Zweckmässig beurteilt.

# Anhang 1: Grundlagen

| **Gesetze, Verordnungen und Standards** |
| --- |
| Finanzkontrollgesetz (FKG, SR 614.0 vom 28. Juni 1967, Stand am 1. Januar 2012) |
| Finanzhaushaltgesetz (FHG, SR 611.0 vom 7. Oktober 2005, Stand am 1. Januar 2016) |
| Finanzhaushaltverordnung (FHV, SR 611.01 vom 5. April 2006 Stand am 1. Januar 2016) |
| Bundesinformatikverordnung (BinfV, SR 172.010.58 vom 9. Dezember 2011, Stand am 1. November 2016) |
| Bundesgesetz über den Datenschutz (DSG, SR 235.1 vom 19. Juni 1992, Stand am 1. Januar 2014) |
| Verordnung zum Bundesgesetz über den Datenschutz (VDSG, SR 235.11 vom 14. Juni 1993, Stand am 16. Oktober 2012 |
| Informationsschutzverordnung (ISchV, SR 510.411 vom 4. Juli 2007, Stand am 1. Juli 2016) |
| Weisungen des Bundesrates über die IKT-Sicherheit in der Bundesverwaltung, (WIsB, W002 vom Juli 2015, Stand am 1. Januar 2016) |
| IKT-Grundschutz Bundesverwaltung (Si001 vom 19. Dezember 2013, Stand am 1. Januar 2016) |
| Zugriffsmatrix Bundesverwaltung (Si002 vom 19. Dezember 2013, Stand am 1. März 2015) |
| Netzwerksicherheit in der Bundesverwaltung (Si003 vom 19. Dezember 2013, Stand am 1. Januar 2014) |
| Parlamentsgesetz, (ParlG, SR 171.10 vom 13. Dezember 2002, Stand am 1. März 2016) |
| Parlamentsverwaltungsverordnung (ParlVV, SR 171.115 vom 3. Oktober 2003, Stand vom 7. September 2015) |
| Informationssicherheitsgesetz (ISG, Entwurf) |

# Anhang 2: Abkürzungen

| | |
|---|---|
| EFK | Eidgenössische Finanzkontrolle |
| BBL | Bundesamt für Bauten und Logistik |
| BR | Bundesrat |
| BVers | Vereinigte Bundesversammlung |
| BRB | Bundesratsbeschluss |
| DMZ | Demilitarized Zone |
| PARL | Parlament |
| PD | Parlamentsdienste |
| VD | Verwaltungsdelegation der BVers |
| VoIP | Voice over IP (IP-basierte Telefonie) |
| LAN | Internes Kabelnetzwerk |
| WAN | Internes Funknetzwerk |

**Priorisierung der Empfehlungen**

Die Eidg. Finanzkontrolle priorisiert die Empfehlungen nach den zugrunde liegenden Risiken (1 = hoch, 2 = mittel, 3 = klein). Als Risiken gelten beispielsweise unwirtschaftliche Vorhaben, Verstösse gegen die Recht- oder Ordnungsmässigkeit, Haftungsfälle oder Reputationsschäden. Dabei werden die Auswirkungen und die Eintrittswahrscheinlichkeit beurteilt. Diese Bewertung bezieht sich auf den konkreten Prüfgegenstand (relativ) und nicht auf die Relevanz für die Bundesverwaltung insgesamt (absolut).