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

Nachprüfung der Umsetzung der Netzwerk Security Policy der Schweizerischen Informatik-konferenz durch die Kantone

Bundesamt für Informatik und Telekommunikation

EFK-16603 / inkl. Stellungnahmen / 26. Mai 2016

Impressum

Bestelladresse **Adresse de commande** **Indirizzo di ordinazione** **Order address**	Eidgenössische Finanzkontrolle (EFK) Monbijoustrasse 45, CH - 3003 Bern http://www.efk.admin.ch
Bestellnummer **Numéro de commande** **Numero di ordinazione** **Order number**	1.16603.609.00216.008
Zusätzliche Informationen **Complément d'informations** **Informazioni complementari** **Additional information**	E-Mail: info@efk.admin.ch Tel. +41 58 463 11 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 »)

Nachprüfung der Umsetzung der Netzwerk Security Policy der Schweizerischen Informatikkonferenz durch die Kantone
Bundesamt für Informatik und Telekommunikation

Das Wesentliche in Kürze

Die Eidgenössische Finanzkontrolle (EFK) hatte im Jahr 2009 geprüft, wie weit in den Kantonen die von der Schweizerischen Informatikkonferenz (SIK) vorgegebene Network Security Policy (NSP) umgesetzt worden war[1]. Aufgrund der Resultate wurde dem Bundesamt für Informatik und Telekommunikation (BIT) eine Empfehlung abgegeben, welche nach Ansicht der EFK bisher nicht umgesetzt ist. Die Verträge zwischen dem BIT und den Kantonen sollten mit Sicherheitselementen ergänzt werden. Zudem sollten die Kantone verpflichtet werden, Nachweise über die Umsetzung der vereinbarten Sicherheitsanforderungen in ihren Netzwerken zu erbringen. Wenn sie diesen Vereinbarungen nicht nachkommen, so hätte das BIT oder von ihm beauftragte Dritte entsprechende Sicherheitsaudits durchzuführen.

Das BIT hat diese Empfehlung so weit möglich in den *Service Level Agreement* (SLA) mit den Kantonen umgesetzt. Es sieht sich jedoch weder in der Lage noch in der Pflicht bei den Kantonen Prüfungen in sicherheitsrelevanten Bereichen durchzuführen. Dazu fehlen im föderalistischen System der Schweiz die Rechtsgrundlagen, welche einem Bundesamt das Recht geben würden, in die Hoheit der Kantone einzugreifen oder umgekehrt. Die EFK wird daher die noch offene Empfehlung als erledigt ablegen.

Jede Partei muss ihre Netze selber vor Bedrohungen schützen

Seit dem Bericht der EFK haben sich die Bedrohungslage und das daraus resultierende Risikopotenzial verschärft. Früher herrschte die Tendenz, sich innerhalb von Netzstrukturen gegenseitig zu vertrauen. Heute steht im Vordergrund, dass die sensitiven Daten der Verwaltungseinheiten sehr gezielt geschützt werden müssen. Daher werden nicht nur die Aussengrenzen eines Netzwerkes mit möglichst hohen Barrieren versehen, es wird auch innerhalb desselben der Datenverkehr laufend überwacht.

Das zwischen den Kantonsnetzwerken und dem Bundesnetzwerk liegende Transportnetz (KOMBV-KTV) gilt aus Bundessicht als Fremdnetz. Die Kantone haben über dieses Netz eine hoch verfügbare und leistungsfähige Verbindung, um auf Bundesanwendungen im Rahmen ihrer gesetzlichen Aufgaben zugreifen zu können. Für den Zugriff braucht es als erste Sicherheitshürde eine Zwei-Faktoren-Authentifikation. Aufgrund des damit verbundenen personifizierten Profils werden als zweites Sicherheitselement nur die Zugriffsrechte auf Anwendungen freigeschaltet, die diese Person auch haben darf. Die Vertraulichkeit der übertragenen Daten wird durch Verschlüsselung gewährleistet.

Die Umsetzung von Netzwerksicherheit ist Kantonshoheit

Die Sicherheit der Kantonsnetzwerke müsste aufgrund eigener Interessen zum Schutz ihrer Daten auf ähnlichem Niveau wie beim Bund gehandhabt werden. Nebst der NSP-SIK bestehen weitere

[1] „Prüfung der Umsetzung der Netzwerk Security Policy der Schweiz. Informatikkonferenz (NSP-SIK) durch die Kantone“, 8421, 2009

Grundlagen bzw. Vorgaben, die es jedem Kanton ermöglichen, die minimalen Sicherheitsvorkehrungen treffen zu können. In verschiedenen Gremien der SIK findet zudem eine Zusammenarbeit zwischen Bundes- und Kantonsvertretern statt, immer mit dem Ziel eines einheitlichen Vorgehens. Es fehlt jedoch eine übergeordnete Instanz, welche die Umsetzung von verbindlichen Vorgaben regelmässig kontrolliert bzw. diese auch durchsetzen kann. Diesen Anforderungen soll bei der Überarbeitung der NSP-SIK mehr Beachtung geschenkt werden, was die EFK begrüsst.

Contrôle subséquent de la mise en œuvre dans les cantons de la politique de sécurité du réseau de la Conférence suisse sur l'informatique
Office fédéral de l'informatique et de la télécommunication

L'essentiel en bref

En 2009, le Contrôle fédéral des finances (CDF) a examiné dans quelle mesure les cantons avaient mis en œuvre la politique de sécurité du réseau (*Network Security Policy, NSP*) dictée par la Conférence suisse sur l'informatique (CSI)[1]. Sur la base des résultats de cet audit, une recommandation a été adressée à l'Office fédéral de l'informatique et de la télécommunication (OFIT) qui, selon le CDF, n'a pas été mise en œuvre jusqu'ici. Les contrats entre l'OFIT et les cantons devaient être complétés par des dispositions de sécurité. De plus, les cantons devraient fournir la preuve que leurs réseaux répondent aux exigences convenues en la matière. S'ils ne respectent pas ces accords, l'OFIT ou les organisations tierces mandatées doivent mener de tels audits de sécurité.

L'OFIT a appliqué cette recommandation autant que possible dans les accords de niveau de service (*Service Level Agreement, SLA*) conclus avec les cantons. Toutefois, il ne se considère pas en mesure ni obligé de mener des audits dans des domaines relatifs à la sécurité auprès des cantons. Les bases juridiques manquent dans le système fédéraliste suisse pour qu'un office fédéral ait le droit d'empiéter sur la souveraineté des cantons, ou inversement. C'est pourquoi le CDF va classer la recommandation en suspens comme liquidée.

Chaque partie doit protéger elle-même ses réseaux des menaces

Depuis le rapport du CDF, les menaces et le potentiel de risques qui en résulte ont augmenté. Auparavant, la tendance voulait que la confiance réciproque règne au sein des structures de réseaux. Aujourd'hui, la protection très ciblée des données sensibles des unités administratives se trouve au premier plan. C'est pourquoi non seulement les limites extérieures d'un réseau sont pourvues de barrières aussi élevées que possible, mais en plus son trafic interne de données est surveillé en permanence.

Du point de vue de la Confédération, le réseau de transmission de données entre les réseaux cantonaux et son pendant fédéral (KOMBV-KTV) est considéré comme un réseau tiers. Par son biais, les cantons disposent d'une liaison hautement disponible et performante pour accéder aux applications de la Confédération dans le cadre de leurs tâches légales. Dans ce but, ils doivent suivre une procédure d'authentification à deux facteurs (première barrière de sécurité). Les profils ainsi personnalisés permettent de libérer uniquement l'accès aux applications auxquelles la personne connectée a réellement droit (deuxième élément de sécurité). Le cryptage assure la confidentialité des données transmises.

La sécurité des réseaux relève de la souveraineté cantonale

Dans leur propre intérêt, les cantons devraient appliquer le même niveau de sécurité que la Confédération pour protéger leurs réseaux et données. Hormis la NSP de la CSI, il existe d'autres bases et directives permettant à chaque canton de mettre en place les mesures de sécurité minimales

[1] « Audit de la mise en œuvre dans les cantons de la politique de sécurité du réseau (*Network Security Policy*) de la Conférence suisse sur l'informatique », 8421, 2009

requises. De plus, la collaboration entre les représentants de la Confédération et des cantons se concrétise au sein de différents organes de la CSI, toujours dans le but d'uniformiser les procédures. Cependant, il manque une instance supérieure contrôlant régulièrement le respect des directives contraignantes et qui puisse aussi les faire appliquer. Une plus grande attention devrait être portée à ces exigences lors du remaniement de la NSP de la CSI, ce que le CDF salue.

Texte original en allemand

Verifica successiva dell'attuazione della politica di sicurezza delle reti della Conferenza svizzera sull'informatica
Ufficio federale dell'informatica e della telecomunicazione

L'essenziale in breve

Nel 2009 il Controllo federale delle finanze (CDF) aveva esaminato il grado di attuazione nei Cantoni della politica di sicurezza delle reti (Network Policy Security, NSP) prescritta dalla Conferenza svizzera sull'informatica (CSI)[1]. Sulla base dei risultati l'Ufficio federale dell'informatica e della telecomunicazione (UFIT) ha ricevuto una raccomandazione che, secondo l'avviso del CDF, non è ancora stata attuata. I contratti tra l'UFIT e i Cantoni dovrebbero essere completati con elementi di sicurezza. I Cantoni dovrebbero inoltre essere obbligati a fornire una prova sull'attuazione dei requisiti in materia di sicurezza convenuti per le loro reti. Se non rispettano questi accordi, l'UFIT o un terzo da esso incaricato dovrebbe effettuare i corrispondenti audit di sicurezza.

Per quanto possibile, l'UFIT ha attuato questa raccomandazione nei *Service Level Agreement* (SLA) con i Cantoni. Non ritiene tuttavia né di essere in grado, né di essere tenuto a svolgere verifiche nei settori rilevanti sotto il profilo della sicurezza dei Cantoni. Nel sistema federalistico della Svizzera mancano le relative basi giuridiche che conferirebbero a un Ufficio federale il diritto di intervenire sulla sovranità dei Cantoni o viceversa. Pertanto il CDF archivia la raccomandazione ancora in sospeso come evasa.

Ogni parte deve proteggere autonomamente le proprie reti dalle minacce

Dall'allestimento del rapporto del CDF la situazione di minaccia e il relativo potenziale di rischio si sono inaspriti. Inizialmente all'interno delle strutture di rete predominava la tendenza a fidarsi l'uno dell'altro. Attualmente, l'accento è posto sulle necessità di proteggere in maniera mirata i dati sensibili delle unità amministrative. Pertanto, non solo i confini esterni di una rete vengono dotati di barriere per quanto possibili elevate, ma anche entro i confini della stessa il flusso di dati viene sorvegliato costantemente.

Dal punto di vista della Confederazione, la rete di trasporto (KOMBV-KTV) tra le reti dei Cantoni e quello della Confederazione è una rete esterna. Grazie a questa rete i Cantoni hanno un collegamento altamente disponibile e performante per accedere ad applicazioni della Confederazione nel quadro dei loro compiti legali. Per garantire la sicurezza, una prima barriera all'accesso consiste nell'autenticazione a due fattori. A causa del relativo profilo personalizzato, quale secondo elemento di sicurezza viene fornito il diritto d'accesso soltanto alle applicazioni cui questa persona può effettivamente accedere. La confidenzialità dei dati trasmessi è garantita dalla cifratura.

L'attuazione della sicurezza delle reti rientra nella sovranità dei Cantoni

A causa del proprio interesse a proteggere i loro dati, la sicurezza delle reti dei Cantoni dovrebbe essere trattata come al livello della Confederazione. Oltre alla NSP-CSI esistono altre basi, o prescrizioni, che permettono a ogni Cantone di adottare misure di sicurezza minime. Nei vari organi della CSI esiste inoltre una collaborazione tra rappresentanti della Confederazione e dei Cantoni che

[1] «Verifica dell'attuazione della rete Security Policy svizzera della conferenza informatica nei Cantoni», 8421, 2009

mira sempre a procedere in modo uniforme. Manca tuttavia un'istanza superiore che controlli regolarmente l'applicazione delle prescrizioni vincolanti e che possa anche esigerne l'attuazione. In occasione dell'elaborazione della NSP-CSI occorrerà prestare maggior attenzione a questi requisiti, come auspicato dal CDF.

Testo originale in tedesco

Follow-up audit of the cantons' implementation of the network security policy of the Swiss Conference on Informatics
Federal Office of Information Technology, Systems and Telecommunication

Key facts

In 2009, the Swiss Federal Audit Office (SFAO) carried out an audit on the extent to which the cantons had implemented the network security policy (NSP) prescribed by the Swiss Conference on Informatics (SIK/CSI)[1]. Based on the results, the Federal Office of Information Technology, Systems and Telecommunication (FOITT) was given a recommendation, and this has not yet been implemented in the SFAO's view. Security elements were supposed to be added to the contracts between the FOITT and the cantons. The cantons were also to be obliged to provide evidence of the implementation of the agreed security requirements in their networks. If they failed to comply with these agreements, the FOITT or a third party instructed by it was to carry out corresponding security audits.

The FOITT implemented this recommendation insofar as possible in the *Service Level Agreement* (SLA) with the cantons. However, it sees itself neither in a position nor under an obligation to carry out audits in security-related areas in the cantons. There is no legal basis for this in Switzerland's federalist system that would give a federal office the right to interfere with the cantons' authority or vice versa. Consequently, the SFAO will class the still outstanding recommendation as settled.

Each party has to protect its own networks from threats

The threat situation and the ensuing risk potential have deteriorated since the SFAO's report. Earlier, there was a tendency towards mutual trust within network structures. Now, it is paramount for the administrative units' sensitive data to be protected in a very targeted manner. Therefore, not only are the highest possible barriers installed at a network's external borders, data traffic is also monitored constantly within the network.

The transport network between the cantons' networks and the federal one (KOMBV-KTV) is an external network from the Confederation's viewpoint. It gives the cantons a highly available and fast connection in order to access federal applications within the framework of their statutory tasks. The first security barrier for access is two-factor authentication. Because of the associated personalised profile, the second security component consists of access rights to applications being activated only for people who are entitled to them. Encryption ensures the confidentiality of the data transferred.

The cantons are responsible for the implementation of network security

Because of their own interests in protecting their data at a similar level, the security of the cantons' networks was to be handled in the same way as in the case of the Confederation. Aside from the NSP of the Swiss Conference on Informatics, there are further basic principles and specifications that enable each canton to take the minimum security precautions. There is also cooperation be-

[1] "Audit of the cantons' implementation of the network security policy of the Swiss Conference on Informatics", 8421, 2009

tween federal and cantonal representatives in various SIK/CSI bodies with the invariable aim of ensuring a uniform approach. However, there is no superior body that can regularly check the implementation of binding specifications and also implement them. Greater attention should be paid to these requirements when preparing the NSP of the Swiss Conference on Informatics, which is welcomed by the SFAO.

Original text in German

Generelle Stellungnahme des BIT zur Prüfung:

Das BIT schliesst sich den Erkenntnissen der EFK an und hat keine weiteren Bemerkungen.

Inhaltsverzeichnis

1 Auftrag und Vorgehen

1.1 Ausgangslage

Im Jahresbericht 2014* hat die EFK festgehalten, dass aus ihrer Sicht eine Empfehlung zur Umsetzung der Network Security Policy der Schweizerischen Informatikkonferenz (NSP-SIK) aus dem Jahr 2009 noch nicht abschliessend umgesetzt ist. Das BIT sollte bei seinen kantonalen Partnern dafür sorgen, dass die Qualität der Sicherheit durch periodische Kontrollen sichergestellt ist. Die Finanzdelegation der Eidgenössischen Räte ist nach Rückfrage im August 2015 mittels Aktennotiz über die damaligen Fakten informiert worden. Im September 2015 nahm das BIT Stellung zur offenen Empfehlung der EFK hinsichtlich der NSP-SIK. Es erachtete diese als umgesetzt bzw. für das BIT als erledigt, da es sich nicht in der Verantwortung sieht.

Entsprechend ihrer Strategie zur Behandlung wichtiger als erledigt gemeldeter Empfehlungen hat die EFK eine Nachprüfung der Umsetzung ins Jahresprogramm 2016 aufgenommen.

1.2 Prüfungsziel und -fragen

Grundsätzliches Ziel der Prüfung war, die aktuelle Situation zur Umsetzung der genannten Empfehlung zu beurteilen. Dabei waren die grundlegenden Fragen:

- Kann das BIT nachweisen, dass alle Kantone die gemäss SLA vereinbarten Prüfungen machen bzw. machen lassen und die vereinbarten Auditberichte liefern?
- Wird kontrolliert, ob die vereinbarten Sicherheitsmassnahmen in den Kantonen tatsächlich umgesetzt werden?
- Unternimmt das BIT etwas, wenn die vertraglichen Vereinbarungen durch die Kantone nicht eingehalten werden?
- Sind die Reaktionen bei einer vermuteten oder erfolgten Sicherheitsverletzung durch einen Kanton geeignet?
- Bringen die Gremien der SIK in diesem Umfeld einen Mehrwert?

1.3 Prüfungsumfang und -grundsätze

Die Prüfung wurde von Cornelia Simmen (Revisionsleitung) und André Stauffer, IT-Prüfungsexperte durchgeführt. Zur Erfüllung des Auftrages wurden Interviews mit Schlüsselpersonen geführt und Dokumente beurteilt.

1.4 Unterlagen und Auskunftserteilung

Die Prüfung fand in der Zeit vom 7. bis 31. März 2016 statt. Die EFK hat von allen Beteiligten in offener und konstruktiver Art Auskunft erhalten. Die notwendigen Dokumente standen termingerecht zur Verfügung.

---

* Publiziert auf www.efk.admin.ch

2 Rückblick

2.1 Die Beurteilung der EFK zur Netzwerksicherheit in den Kantonen

Die EFK hatte im Februar 2009 einen Bericht erstellt, welcher sich mit der Umsetzung der NSP-SIK befasste. Als Basis dienten drei Prüfberichte von kantonalen Finanzkontrollen. Das Interesse für Netzwerksicherheit lag seitens EFK darin, dass Kantone und Gemeinden im Rahmen von delegierten Aufgaben Zugriff auf verschiedene Bundesanwendungen haben. Die Integrität und Vertraulichkeit der Daten muss aus Sicht des Bundes über die gesamte Verarbeitungskette hinweg gewährleistet sein. Unter derselben Prämisse hatte die SIK per 2005 die NSP-SIK erstellen lassen. Diese sollte „eine gemeinsame, kooperative Netzwerksicherheit beim Datenaustausch zwischen Bund, den Kantonen und Gemeinden ermöglichen“. Die definierten Sicherheitsvorgaben werden zwar als verbindlich erklärt. Es ist jedoch nicht geregelt, wer die Umsetzung in den Kantonen kontrolliert. Die wichtigste Erkenntnis der EFK war daher per 2009, dass noch keine durchgängige Umsetzung der NSP-SIK in den Kantonen festzustellen war. Entsprechend gab sie zwei Empfehlungen ab. Die erste erging an die SIK, welche die Umsetzung der NSP in den Kantonen verlangen und dafür die Rückendeckung der Finanzdirektorenkonferenz einfordern sollte. Die zweite war an das BIT gerichtet zur Anpassung der Service Level Agreement (SLA) mit den Kantonen in folgenden Punkten:

- Die wichtigsten Sicherheitselemente sollten verbindlich festgehalten werden.
- Die Kantone seien zu verpflichten, a) entweder dem BIT oder einem von diesem bezeichneten Dritten ein auf die vereinbarten Sicherheitselemente beschränktes Auditierungsrecht zu gewähren oder b) die kantonalen Netzwerke regelmässig selber auf Sicherheitsmängel zu auditieren und dem BIT die Auditberichte zuzustellen.
- Regelungen bezüglich Feststellung von Mängeln bei Sicherheitsvorfällen und das Treffen von notwendigen Schutzmassnahmen bei Nichtbehebung durch die Kantone.

Der Bericht der EFK wurde an der Frühjahrstagung der SIK im Mai 2009 präsentiert. Die Arbeitsgruppe Netzwerksicherheit SIK legte an dieser Tagung ihren Standpunkt ebenfalls dar. Sie stellte u. a. die Frage, wie repräsentativ die drei Kantone seien, welche beurteilt worden waren. Dem Plenum wurde aufgezeigt, dass Bund und Kantone gleichwertige Partner seien. Daher könne man sich untereinander nur über Empfehlungen einigen. Es sei an den Kantonen die Verbindlichkeit der NSP-SIK durch Regierungsratsbeschlüsse zu regeln. Das BIT könne höchstens bis zur Verantwortlichkeitsgrenze der involvierten Netze prüfen. Klar zum Ausdruck gebracht wurde, dass man die Empfehlungen der EFK betreffend Umsetzung der NSP bis Ende 2010 begrüsse. Es solle dazu eine neue Arbeitsgruppe der SIK gegründet werden, die sich vermehrt um die IT-Sicherheit in den Kantonen kümmere.

2.2 Aus den Erkenntnissen abgeleitete Aktivitäten

Die Arbeitsgruppe Informatiksicherheit (AGIS-SIK) wurde ins Leben gerufen und begann ihre Arbeit Ende 2009. Nebst Sicherheitsspezialisten aus den Kantonen sitzen sowohl Vertreter des BIT wie auch des Informatiksteuerungsorgans Bund (ISB) in diesem Gremium. Mit Beobachterstatus sind zudem IT-Revisoren der Kantone und die EFK zugelassen. Gemäss Pflichtenheft kümmert sich die AGIS um alle Aspekte der IKT-Sicherheit. Sie hat in den vergangenen Jahren einige Vorlagen bzw. Regelwerke erarbeitet, die den Kantonen als Grundlage für ihre Tätigkeit nützlich sind. Nicht zuständig ist sie dagegen für die Umsetzung von Informatiksicherheit in den Kantonen und Gemeinden.

Das BIT hat ebenfalls Aktivitäten gezeigt, um die Empfehlung der EFK umzusetzen. So sind in Zusammenarbeit mit der AGIS Themenblätter erstellt worden, welche einer breit ausgelegten Umfrage in den Kantonen dienten. Im Mai 2012 wurde über die Resultate dieser Umfrage informiert. Diese zeigten auf, dass mehr als die Hälfte der Kantone im Bereich Netzwerksicherheit ungenügend waren. Es wurde seitens BIT nochmals an die Kantone appelliert, dass sie für eine genügende Umsetzung der geforderten Sicherheitsmassnahmen zu sorgen haben. Die SLA waren zwischenzeitlich mit einem Kapitel „IT Sicherheit“ ergänzt worden. Unterzeichnet hatten damals diese neuen Vereinbarungen mit dem BIT noch nicht alle Kantone.

Der Lenkende Ausschuss Telekommunikation (LA TK) der SIK ist das wichtigste Gremium. In diesem sitzen Personen, welche für die Netzwerke in den Kantonen und beim Bund verantwortlich sind. Sie legen die gemeinsamen Strategien fest und sind federführend beim Vorhaben „Durchgängige Netzwerkinfrastruktur für alle Verwaltungsebenen“. Die Strategie KOMBV-KTV 2016–2020 (Datenkommunikation Bund – Kantone) ist im November 2015 vom LA TK und dem ISB publiziert worden. Wenn auf operativer Ebene zwischen Bund und Kanton ein Problem auftauchen sollte, so sind es in der Regel die Vertreter des LA TK, welche miteinander Lösungen suchen.

Im Weiteren besteht der Sicherheitsverbund Schweiz (SVS), welcher sich ebenfalls mit IKT-Sicherheitsthemen beschäftigt. Ende 2014 wurde durch diesen in Zusammenarbeit mit der AGIS-SIK eine Umfrage bei den Kantonen im Rahmen der Umsetzung der nationalen Cyber Strategie (NCS) gestartet. Diese beinhaltete Fragen im Bereich „Sicherheit der eigenen Netzwerke“, da hier das höchste Risikopotenzial erkannt worden war. Die Resultate wurden im Mai 2015 in anonymisierter Form der Landsgemeinde KOMBV-KTV vorgestellt. Die Kantone haben gemäss Selbstdeklaration diesen Bereich grossmehrheitlich gut im Griff. Der SVS hat jeden Kanton über dessen eigenen Resultate informiert und wo notwendig den Handlungsbedarf aufgezeigt. Gleichzeitig wurden geeignete Massnahmen vorgeschlagen, um allfällige Schwachstellen zu beseitigen. Es ist vorgesehen anfangs 2017 eine weitere gleichartige Umfrage bei den Kantonen durchzuführen. Für den SVS ist das Thema Netzsicherheit allerdings nur eines von vielen in einem wesentlich komplexeren schweizweiten Umfeld. Er nimmt dadurch wenig Einfluss auf Detailthemen wie die Netzwerksicherheit.

3 Die heutige Situation

3.1 Welche Bedrohungen gehen von den Kantonsnetzen aus?

Die Netzwerkpolitik des Bundes kennt zwei Arten von Netzen:

- Blau werden die Netzwerkteile/-komponenten bezeichnet, welchen vertraut (trusted) wird
- Rot sind alle anderen Netze von und zu Dritten ausserhalb der Bundesverwaltung

Was in der blauen Zone liegt, ist gegenüber roten Netzen durch verschiedene Sicherheitsvorkehrungen geschützt. Das KOMBV-KTV gilt als rotes Netz und liegt zwischen den Netzübergängen des Bundes und jenen der Kantone. Es ist ein reines Transportnetz mit hoher Verfügbarkeit und Leistungsfähigkeit. Den Kantonen dient es zum Zugriff auf Fachanwendungen des Bundes im Rahmen von gesetzlichen Aufgaben und zum interkantonalen Datenaustausch. Das BIT hat die Hoheit über dieses Netz bis zum Router vor den Netzübergängen der Kantone.

Mitarbeitende aus den Kantonen können nur auf Bundesanwendungen zugreifen, wenn sie auch dafür autorisiert sind (siehe Kapitel 3.2). Am Netzübergang selber wird ihnen aufgrund des definierten Profils ausschliesslich der Zugang zu einer oder mehreren Anwendungen innerhalb des blauen Netzes gewährt. Sie können danach nichts anderes als die freigegebenen Bearbeitungsvorgänge innerhalb den Anwendungen ausführen.

Der Netzübergang Bundesnetz – KOMBV-KTV wird bezüglich Gefahren gleich gehandhabt, wie Übergänge ins Internet oder zu anderen Fremdnetzen. Bekannte Risiken wie Cross-Site-Scripting oder SQL-Injections (siehe Glossar) werden erkannt und abgefangen. Wenn ein infiziertes Arbeitsplatzsystem (APS) aus einem Kanton eine Schadsoftware weitergeben will, wird dies mit hoher Wahrscheinlichkeit bereits an der Firewall erkannt. Das Risiko bei infizierten APS liegt hauptsächlich beim potenziellen Verlust der Verfügbarkeit sowie der Vertraulichkeit und Integrität von Informationen, welche auf dem APS in einem Kanton bearbeitet werden. Dabei kann es sich auch um lokal gespeicherte Bundesdaten handeln. Für dieses Risiko tragen die Kantone die Verantwortung.

Sollte trotz aller Sicherheitsvorkehrungen von einem einzelnen APS in einem Kanton oder von einem Kantonsnetz eine Gefahr für das Bundesnetz bestehen, so kann jederzeit die Netzverbindung gekappt werden. Diese Massnahme würde aufgrund der vertraglichen Vereinbarungen zwischen dem BIT und den Kantonen auch jederzeit ergriffen. Bisher musste von dieser Massnahme durch das BIT gegenüber einem Kantonsnetz noch nie Gebrauch gemacht werden. Auch trägt das BIT gelegentlich dazu bei, dass nicht nur bei Kantonsarbeitsplätzen sondern auch bei Drittfirmen bisher unentdeckte Malware eliminiert werden kann.

3.2 Innerhalb eines Netzverbundes hat jede Partei ihre Verantwortung

Durch die flächendeckende Absicherung der Zugriffe aus dem KOMBV-KTV mit einer Zwei-Faktoren-Authentifikation hat die Bundesverwaltung einen relativ hohen Sicherheitsstandard erreicht. Die übertragenen Daten von und zu den Kantonen werden zudem verschlüsselt. Weitere aufgesetzte Sicherheitsmassnahmen seitens BIT an den Fremdnetzübergängen und innerhalb des „blauen“ Netzes sorgen dafür, dass allfällige Angriffe rasch erkannt und blockiert werden. Das BIT verfügt mit dem Computer Security Incident Response Team (CSIRT) über ausgewiesene Fachspezialisten, die sich laufend mit den Risiken und möglichen Gegenmassnahmen befassen. Diese Gruppe arbeitet

sehr eng mit der Melde- und Analysestelle Informationssicherheit (MELANI) zusammen. Die Haltung bezüglich Netzwerksicherheit ist beim BIT dahingehend, dass grundsätzlich niemandem vertraut wird. Dadurch wird der eigenen Sicherheit eine hohe Priorität gegeben.

Die Sicherheit bei den Netzübergängen der Kantone und innerhalb deren eigenen Netzwerken sollte nach denselben Grundsätzen wie beim Bund gehandhabt werden. Es muss im Eigeninteresse der Kantone liegen, ihre heiklen Daten möglichst optimal gegen mögliche Angreifer zu schützen. Die Vorgaben dazu stehen in der NSP-SIK und den SLA mit dem BIT zur Anbindung der Kantonsarbeitsplätze an das KOMBV-KTV. Weitere Regelwerke und Vorlagen der AGIS-SIK sind zudem ausreichend vorhanden, damit jeder Kanton die Mindestanforderungen an Sicherheit erfüllen kann. Kantone, welche ihre Netze, Netzübergänge und Systeme ungenügend absichern, gefährden in erster Linie ihre eigenen Datenbestände.

Mit der Revision der Bundesinformatikverordung (BinfV) per 1.1.2012 sind die bis dahin dem BIT zugeordneten Querschnittsdienstleistungen zum ISB übergegangen. In den letzten Jahren sind daraus Standarddienste geworden. Gemäss Marktmodell gehört die Vernetzung der Kantone mit der Bundesverwaltung zum IKT-Standarddienst Datenkommunikation (SD DAKO). Damit hat das ISB die Führungsverantwortung, welche grundsätzlich ein Weisungs- und Kontrollrecht beinhaltet. Es kann dadurch dem BIT Sicherheitsmassnahmen vorgeben und deren Umsetzung nachweisen lassen. Allerdings gehen diese Kompetenzen nur soweit wie das BIT selber die Hoheit im Netzbereich hat. Das ISB sieht sich nicht in der Verantwortung über die Netzwerkgrenzen des Bundes hinaus Rechenschaft über die Umsetzung von Sicherheitsdispositiven einzufordern.

Die AGIS-SIK wird ebenfalls tätig und die mittlerweile in die Jahre gekommene NSP-SIK überarbeiten d. h. vor allem auf die geänderte Risikolage ausrichten. Das Projekt ist von der SIK bewilligt, die Finanzen müssen noch gesprochen werden. Geplant ist, dass im 2. Semester 2016 auf Basis der jahrelangen Erfahrungen und Erkenntnisse eine wesentlich griffigere Policy vorliegen soll. Das neue Regelwerk wird aber nur wirksam sein, wenn es verbindlich ist und die Kantone damit auch in die Pflicht genommen werden. Daher müsste festgelegt werden, wer für die Kontrolle der Umsetzung der NSP-SIK Verantwortung trägt. Die Überlegungen seitens SIK, Fachspezialisten innerhalb der Kantone auszuleihen, um Sicherheitsaudits durchzuführen, können ein Teil der Lösung sein. Insgesamt genügt dies aber nicht.

3.3 Die Rechtsgrundlagen erlauben keine Überwachung der Kantone durch den Bund

Mit ihrer Empfehlung hat die EFK im 2009 gefordert, dass von der Bundesverwaltung her Aufsicht bei den Kantonen ausgeführt wird, wenn diese selber ungenügende Nachweise erbringen. Weder das BIT noch das ISB sehen Möglichkeiten, wie man die konkrete Forderung der EFK umsetzen könnte. Es fehlen die Rechtsgrundlagen, um sicherheitsrelevante Interna eines Kantons einzufordern oder Sicherheitselemente durch das BIT zu prüfen bzw. prüfen zu lassen. Die Hoheit des BIT endet am Router vor den Netzübergängen der Kantone. Alles was dahinter steht kann höchstens in Zusammenarbeit durchleuchtet werden. Genauso verhält es sich auch umgekehrt. Auch die Kantone könnten keine rechtliche Handhabe finden, um beim BIT Nachweise über deren Sicherheitsdispositiv einzufordern.

Daher wiederspiegeln die Regelungen in den SLA des BIT mit den Kantonen zum Thema IT-Sicherheit diese Rechtslage. Die Vereinbarungen sind so festgelegt, dass jede Partei in ihrem Zuständigkeitsbereich die Pflichten wahrnehmen soll. Man setzt dabei auf enge Zusammenarbeit innerhalb der dafür vorhandenen Gremien. Die Kantone können jederzeit ans BIT gelangen, wenn es um Sicherheitsbelange geht, die im gemeinsamen Interesse stehen. Ein vertraglich vereinbartes Auditrecht im Bereich der hoheitlichen Kantonsnetze würde gemäss BIT höchstens dazu führen, dass die SLA nicht mehr unterzeichnet würden. Das BIT könnte auch bei vertraglosem Zustand keinen Kanton ohne Gefährdungslage vom Bundesnetz abkoppeln, da diese gesetzlichen Aufgaben nachzukommen haben.

4 Schlussbetrachtung

Zum Zeitpunkt der Revision der EFK im 2009 und bis vor ein paar Jahren neigte man dazu trusted Netze mit Partnern aufzubauen. Seit damals hat sich aufgrund der stetig ändernden Risikolagen und den massiv gestiegenen Angriffen das Dispositiv im Netzbereich geändert. Heute steht die gezielte Absicherung von sensitiven Daten im Vordergrund. Nebst möglichst hohen Barrikaden an den Netzaussengrenzen werden auch die Tätigkeiten innerhalb des eigenen Netzwerkes permanent überwacht. Ob und welche Sicherheitsmassnahmen in den Kantonen aufgesetzt sind, entzieht sich der Einflussnahme des BIT. Es wird allerdings allgemein davon ausgegangen, dass auch die Kantone ein ureigenes Interesse haben, ihre Netze und Systeme möglichst sicher zu betreiben.

Die von der SIK eingesetzten Gremien, die sich mit Kommunikation und IKT-Sicherheit beschäftigen, haben unterschiedliche Aufgaben. Sie erbringen nach Einschätzung der EFK unterschiedliche Mehrwerte. Die LA TK ist primär eine Plattform von Spezialisten aus allen Kantonen, die im operativen Geschäft tätig sind. Durch regelmässige Treffen kennt man sich untereinander und hat dadurch eine gute Zusammenarbeit über die Grenzen des schweizerischen Föderalismus hinaus. Die AGIS-SIK ist eher eine Instanz, welche versucht den Kantonen mit Regelwerken und Checklisten die Arbeit zu vereinfachen bzw. diese zu vereinheitlichen. Auch hier sind vornehmlich IT-Spezialisten aber auch IT-Revisoren am Werk. In diesem Sicherheitsgremium sind nicht alle Kantone vertreten und es gibt keine kantonsübergreifende Übersicht zum Umsetzungsstand von IT-Sicherheitsvorgaben. Das Engagement variiert von Kanton zur Kanton und hängt stark von den einzelnen Personen ab sowie der Unterstützung von vorgesetzten Linien bzw. letztendlich vom zuständigen Regierungsrat.

Aufgrund des föderalistischen Systems der Schweiz bestehen keine Möglichkeiten, dass eine Bundesstelle im Hoheitsgebiet von Kantonen ohne deren Zustimmung Prüfungen durchführen kann. Auch Nachweise über sicherheitskritische Aspekte im Netzwerkbereich lassen sich nicht einfach einfordern. Daher müssen die ersten drei Fragen gemäss Kapitel 1.2 mit einem „nein“ beantwortet werden. Das BIT verfügt über keine Auditberichte und sieht sich auch nicht in der Lage, deren Lieferung über die SLA mit den Kantonen zu vereinbaren. Aufgrund der vertraglichen Regelungen verfügt das BIT dagegen über ausreichende Möglichkeiten, bei festgestellten Sicherheitsverletzungen durch einen Kanton reagieren zu können.

Aus Sicht der EFK sind die föderalen Strukturen im Hinblick auf eine robuste Informationssicherheit über die staatlichen Ebenen hinweg ein besonderes Hindernis. Die Arbeiten zum neuen Informationssicherheitsgesetz zeigen deutlich, dass sich die verschiedenen Akteure schwer tun, eigene Sicherheits- und Autonomieansprüche abzugeben. In diesem Kontext erscheint der EFK das vom BIT praktizierte Vorgehen sinnvoll, die eigenen Systeme und Zugänge so weit wie möglich zu schützen sowie die Abhängigkeit von anderen Akteuren zu minimieren.

Die EFK wird aufgrund der vorliegenden Resultate die offene Empfehlung 8421.001 an das BIT als erledigt ablegen.

5 Schlussbesprechung

Das BIT ist mit den Resultaten und Feststellungen einverstanden. Es hat auf eine Schlussbesprechung verzichtet.

Die EFK dankt für die gewährte Unterstützung.

EIDGENÖSSISCHE FINANZKONTROLLE

Anhang 1: Rechtsgrundlagen

Finanzkontrollgesetz (FKG, SR 614.0)
Finanzhaushaltgesetz (FHG, SR 611.0)
Finanzhaushaltverordnung (FHV, SR 611.01)
Bundesinformatikverordnung (BinfV, SR 172.010.58)

Anhang 2: Abkürzungen, Glossar, Priorisierung der Empfehlungen

Abkürzungen

AGIS	Arbeitsgruppe Informatiksicherheit
APS	Arbeitsplatzsystem
BIT	Bundesamt für Informatik und Telekommunikation
CSIRT	Computer Security Incident Response Team
EFK	Eidg. Finanzkontrolle
ISB	Informatiksteuerungsorgan Bund
LA TK	Landsgemeinde Telekommunikation
NCS	Nationale Cyber Strategie
NSP	Network Security Policy
MELANI	Melde- und Analysestelle Informationssicherheit
SD DAKO	IKT-Standarddienst Datenkommunikation
SIK	Schweizerische Informatikkonferenz
SLA	Service Level Agreement
SVS	Sicherheitsverbund Schweiz
VPN	Virtual Private Network

Glossar*

Cross-Site-Scripting	Bezeichnet das Ausnutzen einer Computersicherheitslücke in Webanwendungen, indem Informationen aus einem Kontext, in dem sie nicht vertrauenswürdig sind, in einen anderen Kontext eingefügt werden, in dem sie als vertrauenswürdig eingestuft werden. Aus diesem vertrauenswürdigen Kontext kann dann ein Angriff gestartet werden.
SQL-Injection	Bezeichnet das Ausnutzen einer Sicherheitslücke in Zusammenhang mit SQL-Datenbanken. Der Angreifer versucht dabei, über die Anwendung, die den Zugriff auf die Datenbank bereitstellt, eigene Datenbankbefehle einzuschleusen. Sein Ziel ist es, Daten auszuspähen, in seinem Sinne zu verändern, die Kontrolle über den Server zu erhalten oder einfach grösstmöglichen Schaden anzurichten.
KOMBV-KTV	Bezeichnung für das eigens für die Kantone bestimmte Virtual Private Network (VPN) als schnelle und zuverlässige Verbindung zum Bundesnetzwerk.

Priorisierung der Empfehlungen

Die EFK 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).

* Gemäss https://de.wikipedia.org/