PRÜFBERICHT

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

INTERN

Querschnittsprüfung Teil II Informatik-Sicherheit in der Bundesverwaltung

Bericht zu Handen des Bundesrates

28. November 2012

Das Wesentliche in Kürze

Die EFK überprüfte erstmalig in 2011 im Auftrag des Bundesrates den Umsetzungsstand von Massnahmen zur Erhöhung der Informatiksicherheit in der Bundesverwaltung. In 2012 fand eine Weiterführung des Auftrags statt. Zum einen wurde erhoben, ob die fälligen Empfehlungen aus dem letzten Jahr fristgerecht umgesetzt worden sind. Zum anderen wurden die Themen „Einhaltung der Passwortanforderungen" und „zeitgerechte Schliessung von Sicherheitslücken" bei ausgewählten Fachanwendungen mit hoher Geschäfts- oder Finanzrelevanz geprüft, sowie die Prozesse für die Behandlung von Sicherheitsvorfällen als Teilaspekt der „intensivierten Netzwerküberwachung" beurteilt. Die Themen entsprechen den Sofortmassnahmen gemäss Bundesratsbeschluss (BRB) vom 16. Dezember 2009.

Die wesentlichen Ergebnisse sind wie folgt:

Die Umsetzung der Empfehlungen aus dem Vorjahr benötigt länger Zeit als geplant. Die EFK hat sich bei den acht Leistungserbringern und dem Informatiksteuerungsorgan Bund (ISB) über den Stand der Umsetzung der fälligen Empfehlungen aus dem Vorjahr informiert. Es haben verschiedentlich Verbesserungen stattgefunden, dennoch konnten diverse Massnahmen nicht innerhalb der von den Ämtern angestrebten Frist umgesetzt werden. Insgesamt bietet sich kein zufriedenstellender Fortschritt. In diversen Fällen verhindern die bereits bekannten Schwierigkeiten beim Zusammenspiel von Leistungserbringer und Leistungsbezüger die Behebung von Sicherheitslücken. Desweiteren fehlen noch die verbindlichen Grundlagen des ISB für die Regelung der lokalen Administratorenrechte. Auf bundesweiter Ebene vermisst die EFK nach wie vor ein vollständiges Inventar der informationsschutzkritischen Anwendungen, wie im BRB Punkt 3.3.3 gefordert. Das ISB plant, dieses Thema im Rahmen der Überprüfung des Inventarstandards anzugehen.

Im Rahmen der Umsetzung der neuen Bundesinformatikverordnung (BinfV) sieht die EFK eine grosse Chance für das ISB, seine Rolle in übergeordneten Sicherheitsthemen zu stärken. Die EFK begrüsst hier ausdrücklich eine deutlichere Führungsrolle des ISB. Dies würde beispielsweise auch die Definition einheitlicher Kriterien für die Einstufung und Eskalation von sicherheitskritischen Ereignissen und eine fortlaufende Überprüfung der Wirksamkeit der relevanten Prozesse in den Ämtern und im ISB ermöglichen.

Bei der Umsetzung der Network Security Policy (NSP) in den Kantonen werden zwar Fortschritte gemacht, diese erachtet die EFK allerdings als nicht genügend: Die erzielten Resultate stehen in einem schlechten Verhältnis zu der benötigten Zeitspanne. Ursache dafür ist die fehlende Durchsetzungskraft des BIT gegenüber den Kantonen. Für 2013 und 2014 sind seitens BIT geplant, die Kantone bei der normativen Umsetzung der NSP zu unterstützen und ISO-konforme Audits aufzusetzen und durchzuführen. Es sollte darüber hinaus überlegt werden, ob die Bemühungen nicht durch kompensierende technische Massnahmen (mit evtl. Kosten- und Performancenachteilen) flankiert werden sollten.

Die selektierten Fachanwendungen können die Passwortanforderungen nicht vollständig technisch durchsetzen. Für die Prüfung wurden insgesamt fünf Anwendungen bei der Bundeskanzlei (BK), bei der Eidgenössischen Steuerverwaltung (ESTV) und bei der Eidgenössischen Zollverwaltung (EZV) beurteilt. Die EFK hat festgestellt, dass weder die geprüften Anwendungen der ESTV noch die Anwendungen der EZV die Einhaltung der Passwortanforderungen in allen

Teilen technisch durchsetzen können. Bei der EZV existieren für die internen Anwender kompensierende Massnahmen, die eine Anmeldung an einer vorgelagerten Anwendung erzwingen, bevor man auf die Kernsysteme zugreifen kann. Die vorgelagerte Anmeldeinstanz setzt die Passwortregeln grundsätzlich durch. Bei der ESTV konnten keine kompensierenden technischen Kontrollen festgestellt werden. Die EFK hat empfohlen, die betreffenden Anwendungen anzupassen. Die geprüfte Anwendung bei der BK setzt die Einhaltung der Passwortrichtlinien technisch durch.

Bei der zeitgerechten Schliessung von Sicherheitslücken in den selektierten Anwendungen hat die EFK keine weiteren Risiken festgestellt. Die meisten der selektierten Anwendungen sind Host-basierte Systeme. Die Verfahren für die zeitgerechte Schliessung von Sicherheitslücken unterscheiden sich hinsichtlich Häufigkeit und Bedrohungslage von denen bei Windows-Systemen. Sie sind im Grossen und Ganzen etabliert und bewährt. In einigen Fällen werden neue Releases von den Leistungserbringern nur selektiv eingespielt. Die EFK weist darauf hin, dass bei der Entscheidung für oder gegen die Installation eines neuen Release nicht nur funktionale, sondern auch sicherheitsrelevante Aspekte berücksichtigt werden müssen. Dieser Entscheidungsprozess wurde nicht geprüft. Kritisch wertet die EFK ausserdem die Situation, wenn die Wartung der Altsysteme in der ESTV durch den Hersteller ausläuft.

Die Security Incident Management Prozesse bei den acht geprüften Leistungserbringern sind unterschiedlich gestaltet. Übergeordnete Vorgaben für die Ausgestaltung der Prozesse und einheitliche Kriterien für die Identifikation und zeitgerechte Eskalation von sicherheitsrelevanten Vorfällen in den Verwaltungseinheiten gibt es nicht. Die sicherheitsrelevanten Vorfälle werden bei den meisten Leistungserbringern situativ durch den Einsatz von Task Forces bewältigt.

Die beiden grössten Leistungserbringer BIT und FUB verfügen über separate Organisationseinheiten für die Erkennung und die Bewältigung von sicherheitsrelevanten Vorfällen. Im einen Fall ist dies ein Computer Security Incident Response Team (CSIRT) und im anderen Fall ein Computer Emergency Response Team (CERT). Als Querschnittsdienstleister für Netze informiert das BIT die übrigen Leistungserbringer bei potenziellen Bedrohungen. Die Informationswege laufen über die bestehenden Strukturen der Sicherheitsbeauftragten. Die Zusammenarbeit zwischen den beiden Teams sollte verbessert werden.

Ein weiteres Frühwarnsystem für Sicherheitsbedrohungen stellt die Melde- und Analysestelle Informationssicherung (MELANI) des ISB dar. Mit Ausnahme des Leistungserbringers der Arbeitslosenversicherung (TCSB) sind alle geprüften Leistungserbringer Mitglieder der geschlossenen Benutzergruppe von MELANI und werden somit rascher und direkt über Sicherheitsbedrohungen informiert.

Die Informationspolitik bei schwerwiegenden Sicherheitsereignissen wird seitens der Leistungserbringer als Hemmnis wahrgenommen. In Fällen, wo die Bundesanwaltschaft involviert ist, wird eine sehr restriktive Informationspolitik betrieben. Die Leistungserbringer fühlen sich verunsichert, ob sie aufgrund der unkonkreten Informationen ausreichende präventive oder korrigierende Massnahmen ergreifen können. Die EFK ist der Meinung, dass eine Abwägung zwischen der strafrechtlichen von der sicherheitsrelevanten Dimension stattfinden muss mit dem Ziel, den Leistungserbringern eine rasche und umfassende Reaktion auf den Vorfall zu ermöglichen. Dazu ist eine Absprache zwischen der Bundesanwaltschaft und dem ISB nötig.

Die konkrete Empfehlung der EFK zu den aufgezeigten Schwachstellen ist dem Hauptteil des Berichtes zu entnehmen. Empfehlungen, welche die einzelnen Leistungserbringer, bzw. Leistungsbezüger und das ISB betrafen, wurden in Anschluss an die jeweilige Teilprüfung direkt an diese abgegeben.

Inhaltsverzeichnis

1 Auftrag und Vorgehen

1.1 Ausgangslage

Die EFK erhielt am 24. Juni 2010 gemäss BRB vom 4. Juni 2010 vom „Delegierten Informatikstrategie Bund" (heute „Delegierter Informatiksteuerung Bund") die schriftliche Anfrage, den Stand der Umsetzung von Massnahmen zur Erhöhung der Informatiksicherheit zu überprüfen (gemäss BRB vom 16. Dezember 2009). Der BRB sah folgende Sofortmassnahmen vor:

1a) Einhaltung der Passwortanforderungen

1b) Zeitgerechte Korrektur von Sicherheitslücken

1c) Verbessertes Informationsmanagement

1d) Intensivierte Netzwerküberwachung

Der Bundesrat hat zudem noch weiterführende Massnahmen definiert, wie beispielsweise die Einführung einer Zwei-Faktor Authentisierung. Diese waren bisher nicht Gegenstand von Prüfungen durch die EFK.

Die EFK hat auf die Anfrage am 27. August 2010 positiv geantwortet und 2011 den ersten Teil der Querschnittsprüfung durchgeführt. Die Ergebnisse wurden veröffentlicht (www.efk.admin.ch). Die Querschnittsprüfung wurde im Jahr 2012 mit geänderten Prüfungsschwerpunkten in reduziertem Umfang weitergeführt.

1.2 Prüfungsziel und -fragen

Ausgehend von den Erkenntnissen aus der Prüfung in 2011 hat die EFK die Risiken neu bewertet und die folgenden Themenschwerpunkte für 2012 ausgewählt:

- Beurteilung der „Einhaltung der Passwortanforderungen" und der „zeitgerechten Schliessung von Sicherheitslücken" an ausgewählten Fachanwendungen mit hoher finanzieller Relevanz oder grosser Bedeutung für die gesamte Bundesverwaltung.
- Beurteilung der Prozesse für die Behandlung von Sicherheitsvorfällen als Teilaspekt der intensivierten Netzwerküberwachung.
- Überprüfung des Umsetzungsstands der Empfehlungen aus dem vergangenen Jahr.

1.3 Prüfungsumfang und -grundsätze

Die Prüfung wurde von Peter Bürki, Brigitte Schnyder von Morisch, Hans-Jörg Uwer, Stefan Wagner sowie Markus Künzler (Revisionsleiter) im Zeitraum von Mai bis Oktober 2012 durchgeführt. Die Verantwortung lag bei Brigitte Christ. Von der Prüfung waren folgende Organisationseinheiten betroffen:

Leistungerbringer

- SCI-BK, als Leistungserbringer der Bundeskanzlei
- ISCeco, als Leistungserbringer des EVD

- TCSB, als Leistungserbringer der Arbeitslosenversicherung
- IT-EDA, als Leistungserbringer des EDA
- BIT, als Leistungserbringer für EFD, UVEK und EDI sowie für Teile des EJPD
- ISC-EJPD, als Leistungserbringer des EJPD
- PD-DINT, als Leistungserbringer der Parlamentsdienste
- FUB, als Leistungserbringer des VBS
- ISB, als Betreiber der Melde- und Analysestelle Informationssicherung (MELANI)

Leistungsbezüger

- EZV, als Eigner von Anwendungen mit hoher finanzieller Relevanz
- ESTV, als Eigner von Anwendungen mit hoher finanzieller Relevanz
- BK, als Eigner der Geschäftsverwaltungsanwendungen GEVER BK und GEVER ÜDP

1.4 Unterlagen und Auskunftserteilung

Die notwendigen Auskünfte wurden bei den Prüfungen von allen Beteiligten zuvorkommend erteilt.

1.5 Ergebniskommunikation der einzelnen Teilprüfungen

Zu den eingangs genannten Themengebieten fanden insgesamt zwölf Teilprüfungen bei den verschiedenen Verwaltungseinheiten statt. Für jede dieser Prüfungen hat die EFK ein Prüfprotokoll mit den Feststellungen und Beurteilungen erstellt und, wo nötig, Empfehlungen abgegeben. Diese Protokolle wurden im Rahmen einer Schlussbesprechung diskutiert oder durch eine kurze formelle Stellungnahme des Amtes finalisiert. Das Protokoll wurde anschliessend an die Generalsekretärin bzw. den Generalsekretär oder die Direktorin bzw. den Direktor der betreffenden Verwaltungseinheit verschickt. Die geprüften Verwaltungseinheiten wurden auf diesem Weg über die einzelnen Feststellungen, Beurteilungen und eventuelle Empfehlungen der EFK in Kenntnis gesetzt. Die Informatiksicherheitsbeauftragten des betreffenden Departements (ISBD) sowie der Delegierte für die Informatiksteuerung des Bundes haben gleichzeitig eine Kopie des Protokolls erhalten.

2 Die neue Organisation der Informatik in der Bundesverwaltung

Am 1.1.2012 ist die revidierte Bundesinformatikverordnung (BinfV) in Kraft getreten. Die BinfV regelt Aufgaben und Zuständigkeiten bei der Steuerung und Führung des Einsatzes von Informations- und Kommunikationstechnik (IKT) in der Bundesverwaltung.

Die wesentlichen Änderungen sind:

- Der Bundesrat übernimmt neu die strategische Gesamtverantwortung für die Bundesinformatik. Er bestimmt die IKT-Strategie und überwacht deren Umsetzung.

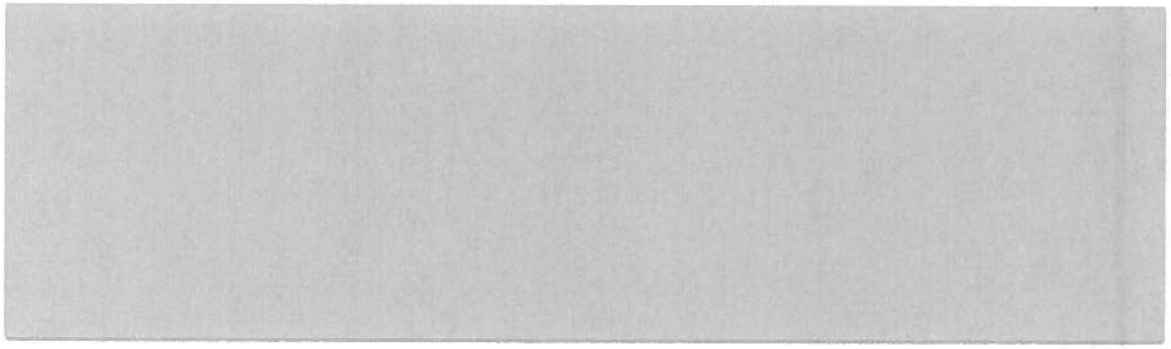
- Das EFD erarbeitet die IKT-Strategie des Bundes und erlässt im Rahmen seiner Aufgaben Verwaltungsverordnungen.
- Mit der revidierten BinfV erhielt das ISB die neue Bezeichnung „Informatiksteuerungsorgan Bund". Es ist zuständig für die Umsetzung der IKT-Strategie, bereitet die IKT-Geschäfte des Bundesrates vor und vollzieht die Aufträge des Bundesrates.
- Unverändert regeln die Departemente / Bundeskanzlei und die Verwaltungseinheiten im Rahmen der gültigen Vorgaben die Steuerung und Führung der IKT in ihrem jeweiligen Bereich. Sie sind verantwortlich für die Einhaltung der IKT-Vorgaben und der Beschlüsse des Bundesrats, des EFD, des ISB und der Departemente/Bundeskanzlei in ihrem Zuständigkeitsbereich.

Obwohl diverse Auswirkungen durch die Umsetzung der neuen BinfV zu erwarten sind, hatten diese keine wesentliche Relevanz auf die Durchführung der aktuellen Prüfung. Allerdings war bei der Erhebung des Umsetzungsstandes der Empfehlungen aus dem letzten Jahr die Tendenz feststellbar, diverse Massnahmen im Rahmen der Umsetzung der neuen BinfV anzugehen. Dies bringt zwar durchaus Synergien, allerdings auch zeitliche Verzögerungen mit sich.

3 Einhaltung der Passwortanforderungen ist in den selektierten Anwendungen technisch nicht vollständig umsetzbar

Für die Prüfung in diesem Jahr hat die EFK am Beispiel von fünf Anwendungen die technische Durchsetzung der Passwortrichtlinien geprüft. Als Stichprobe hat die EFK zwei Anwendungen der EZV, zwei Anwendungen der ESTV und eine Anwendung der BK gewählt. Diese Anwendungen wurden durch die EFK aufgrund ihrer finanziellen und geschäftlichen Relevanz und dem damit verbundenen Schadenspotenzial ausgewählt.

ESTV



EZV

Die EFK hat bei der EZV für die Passwortanforderungen der beiden Anwendungen e-dec und Minöst geprüft. Dabei stellte die EFK fest, dass die Anforderungen an die Passwörter nicht in allen Teilen technisch umgesetzt werden können.

Allerdings sind kompensierende Mechanismen vorhanden: Der Zugriff auf die Anwendungen erfolgt über die Anmeldung an einem vorgelagerten System (Citrix Lösung), ohne die kein Zugriff der internen Anwender auf die beiden Zollapplikationen möglich ist. Diese Vorstufe wird über das Windows Active Directory (AD) gesteuert und unterstützt somit ein WIsB-konformes Passwort. Die EFK beurteilt diesen Passwortschutz für Minöst als ausreichend, zumal nur ein überschaubarer Benutzerkreis Zugriff hat und die mittelfristige Ablösung von Minöst geplant ist.

BK

Bei der BK hat die EFK die Passwortanforderungen der Anwendungen GEVER BK und GEVER ÜDP geprüft. Die EFK stellte fest, dass die Anforderungen an die Passwörter auf technischer Ebene umgesetzt werden konnten. Da beide Anwendungen auf der Basis von Microsoft Windows arbeiten, stützt sich die EFK bei dieser Aussage auf die Prüfung der Windows-basierten Systeme beim ISCeco des vergangenen Jahres.

GEVER BK nutzt Benutzername und Passwort, während GEVER ÜDP bereits heute über eine sicherere Anmeldung mittels Smartcard (PIN und Token) verfügt.

4 Keine neuen Risiken bei der zeitgerechten Schliessung von Sicherheitslücken in den selektierten finanz- und geschäftsrelevanten Anwendungen

Als Stichprobe für die Prüfung der Umsetzung der „zeitgerechten Schliessung von Sicherheitslücken" dienten die gleichen Anwendungen bei der EZV, ESTV und der BK. Die EFK gelangte zu den folgenden Beurteilungen:

ESTV

Die Anwendungen MOLIS und STOLIS basieren auf einer älteren Host Infrastruktur. Die Verfahren für die zeitgerechte Schliessung von Sicherheitslücken unterscheiden sich von denjenigen von Windows-Systemen. Korrekturen finden nicht in der gleichen Häufigkeit statt wie beispielsweise auf Windows Systemen. Die Tatsache, dass solche Host Systeme ausgesprochen komplex und weniger bekannt sind, macht sie als Angriffsziele weniger attraktiv. Die vom Hersteller angebotenen Aktualisierungen des Betriebssystems werden selektiv eingespielt. Eine aktuelle Version wird im Rahmen der Hardwaremigration im 2012 eingespielt. Die EFK verlässt sich darauf, dass bei der Selektion der Releases die Schliessung der Sicherheitslücken als wichtiges Kriterium berücksichtigt wird. Dieser Bereich wurde jedoch nicht geprüft. Kritisch wertet die EFK die Situation, wenn die Wartung der beiden Kernsysteme durch den Hersteller ausläuft.

EZV

Das Patch Management betrifft die Betriebssysteme, die Datenbanken und die Netzwerkkommunikation, jedoch weniger die Anwendungen Minöst und e-dec. Unter der Führung des Betriebszentrums BIT hat sich ein monatlicher Aktualisierungs-Rhythmus etabliert und bewährt. Die EFK hat keine weiteren Anmerkungen zu diesem Vorgehen.

BK

Das BIT betreibt die Hardware und das ISCeco betreut die Betriebssysteme der Server und die Anwendung GEVER von Fabasoft. Es gibt von Fabasoft keine separaten Sicherheitspatches, sondern sogenannt funktionale Hotfixes. Die Verantwortlichkeiten der Leistungserbringer und der BK sind klar. Im Regelfall koordiniert die BK die Tätigkeiten (z. B. Wartungsfenster). Die EFK stellt fest, dass das Patch Management der beiden Anwendungen in der BK ein etablierter Prozess ist.

5 Die Prozesse für die Behandlung von Sicherheitsvorfällen

5.1 Die Erwartung der EFK

Mit einem funktionierenden Security Incident Management soll sichergestellt werden, dass auf Sicherheitsvorfälle rasch und wirkungsvoll reagiert werden kann. Zu diesem Zweck müssen klare Meldewege geschaffen werden. Die Behandlung soll wo möglich in standardisierten Prozessen erfolgen, welche dafür sorgen, dass bei und nach einem Sicherheitsvorfall die Sicherheit von Daten und Systemen gewährleistet und wo nötig Beweismittel gesichert werden können. Nach jedem Sicherheitsvorfall sollen die nötigen Lehren gezogen werden. Zur Vorbeugung von Schäden bei anderen Leistungserbringern muss gewährleistet sein, dass Informationen über Bedrohungen zwischen verschiedenen Leistungserbringern rasch und stufengerecht ausgetauscht werden.

Ein Prozess für die Behandlung von sicherheitsrelevanten Vorfällen sollte im Minimum die folgenden Elemente enthalten:

- Erkennung von Sicherheitsvorfällen,
- Kategorisierung von Sicherheitsvorfällen und Alarmierung betroffener Partner,
- Bewältigung von Sicherheitsvorfällen,
- Nachbearbeitung und Dokumentation von Sicherheitsvorfällen und

- falls nötig Umsetzung von Verbesserungsmassnahmen zur Verhinderung gleichartiger Vorfälle in der Zukunft.

5.2 Die Security Incident Management Prozesse bei den Leistungserbringern sind sehr unterschiedlich ausgestaltet

Die EFK hat bei den acht Leistungserbringern die Existenz des Security Incident Management Prozesses beurteilt und machte hierzu folgende Feststellungen:

Die zwei grossen IKT-Leistungserbringer der Bundesverwaltung BIT und FUB verfügen beide über Teams für die Erkennung und Bewältigung von sicherheitsrelevanten Vorfällen:

- Im BIT ist dies ein gut organisiertes Computer Security Incident Response Team (CSIRT). Die Prozesse sind dokumentiert und Arbeitsanleitungen für den „Incident Handler" liegen vor. Die Eskalationswege sind festgelegt und erfolgen primär über den Informationssicherheitsbeauftragten des BIT (ISBO). Die Stelle des ISBO-BIT war zum Zeitpunkt der Prüfung nur ad interim besetzt.
- Bei der FUB werden vergleichbare Aufgaben durch ein Computer Emergency Response Team (Mil CERT) wahrgenommen. Ein informeller Informationsaustausch zwischen dem CSIRT-BIT und dem Mil CERT findet statt. Die EFK hat empfohlen, die Zusammenarbeit der beiden Response Teams auf eine verbindliche Basis zu stellen und dies z. B. in einer Schnittstellenvereinbarung zu formalisieren. Hiermit soll sichergestellt werden, dass wichtige Informationen über sicherheitsrelevante Vorfälle fliessen.

Bei der Informatik EDA ist ein allgemeiner Incident Management Prozess vorhanden, welcher mit spezifischen Prozeduren für die Behandlung von Sicherheitsvorfällen ergänzt wurde. Frühere Sicherheitsvorfälle haben zu überarbeiteten Prozessen geführt.

Im Allgemeinen wird bei den Leistungserbringern in den Prozessen nicht zwischen Incident und Security Incident[1] unterschieden:

- Bei den übrigen Leistungserbringern werden die sicherheitsrelevanten Vorfälle über die normalen Incident Management Prozesse des Informatik Betriebs abgewickelt. Spezifische Prozeduren für die Behandlung von Sicherheitsvorfällen liegen dort kaum vor. Stattdessen werden diese situativ durch die Bildung von „Task Forces" bewältigt.

MELANI und CSIRT-BIT spielen zentrale Rollen bei der Erkennung von Sicherheitsvorfällen:

- Zur Erkennung von Sicherheitsvorfällen stehen verschiedene Mittel zur Verfügung (Virenscanner, Logfiles, Meldungen von Benutzern usw.). Eine zentrale Rolle nimmt hier das CSIRT-BIT wahr. Als Querschnittsdienstleister für die Netze verfügt das BIT über eine Infrastruktur zur Überwachung des Internet Übergangs und erkennt dort potenzielle Bedrohungen. Die betroffenen Leistungsbezüger bzw. deren Leistungserbringer werden über die bestehende Sicherheitsorganisation des Bundes (ISBD, ISBO) alarmiert.

[1] Das Incident Management registriert, kategorisiert, priorisiert und verfolgt alle Störungen mit dem Ziel, diese so schnell wie möglich zu beheben. Security Incidents sind eine Spezialform der Incidents und bezeichnen nur die sicherheitsrelevanten Vorfälle. Quelle: Wikipedia

- Ein weiteres Frühwarnsystem stellt die Melde- und Analysestelle Informationssicherung (MELANI) des ISB zur Verfügung. Dieses basiert auf einem Netzwerk von Betreibern kritischer Infrastrukturen und stellt Informationen über potenzielle Bedrohungen zusammen. Diese Informationen werden im Fall von akuten Bedrohungen über MELANI-net zur Verfügung gestellt. Mit Ausnahme von TCSB sind alle der geprüften Leistungserbringer Mitglied der geschlossenen Benutzergruppe von MELANI.

5.3 Die Definition von Kriterien, die systematische Überprüfung der Wirksamkeit der Prozesse und die Kommunikation bei schwerwiegenden Sicherheitsvorfällen müssen verbessert werden

Bundesweit einheitliche Anforderungen für die Ausgestaltung der Security Incident Management Prozesse sind nicht vorhanden. Das führt dazu, dass die Leistungserbringer ihre eigenen Prozesse definieren und auch ihre eigenen Kriterien für die Einstufung und Priorisierung eines Sicherheitsvorfalls vornehmen. Einheitliche Kriterien, wann ein Vorfall als kritisch einzustufen ist bzw. Eskalation erfordert, bestehen nicht. Dadurch ist nicht sichergestellt, dass das ISB in alle relevanten Sicherheitsvorfälle zeitgerecht involviert wird. Daher hat die EFK dem ISB empfohlen, als Teil der Nachbearbeitung von kritischen Sicherheitsvorfällen die Wirksamkeit der Security Incident Prozesse systematisch zu beurteilen und diese gegebenenfalls zu optimieren.

Ausserdem unterstützt die EFK eine starke Führung des ISB in übergeordneten Sicherheitsbelangen (z. B. über die Definition einheitlicher Kriterien), welche bei der aktuellen Ausgestaltung der Aufgaben des ISB berücksichtigt werden sollte. Diese starke Führungsrolle des ISB würde auch eine weitere Schwachstelle adressieren, nämlich den nicht koordinierten horizontalen Informationsaustausch zwischen den Leistungserbringern. Damit wäre eine rasche Reaktion zu erreichen sowie allfällige Synergien bei der Bewältigung von Vorfällen zu nutzen.

Beim Eintreten von schwerwiegenden Sicherheitsereignissen, bei denen die Bundesanwaltschaft eingeschaltet wird, gestaltet sich die Kommunikation gemäss Wahrnehmung verschiedener Leistungserbringer schwierig. Für die nicht direkt betroffenen Leistungserbringer ist eine angemessene und konkrete Reaktion in diesen Fällen unmöglich, weil nur unkonkrete Informationen fliessen. Das führt für die Leistungserbringer zur unbefriedigenden Situation, dass sie zwar von Bedrohungen erfahren, aber nicht wissen, ob und wie sie diesen begegnen sollen. Aus Sicht der EFK ist in solchen Fällen klar abzuwägen zwischen den strafrechtlichen und sicherheitsbezogenen Aspekten mit dem Ziel, der Alarmierung der betroffenen Stellen Priorität einzuräumen. Wo immer möglich, müssen diese Stellen mit ausreichender Information versorgt werden, die es ihnen erlaubt, rasche und umfassende Massnahmen zur Bewältigung oder Verhinderung von Schäden zu ergreifen.

Empfehlung 1, Priorität 1

Die EFK empfiehlt dem Informatiksteuerungsorgan und der Bundesanwaltschaft das genaue Vorgehen bei schwerwiegenden Sicherheitsereignissen abzusprechen. Inhalt dieser Absprachen muss sein, eine bewusste Abwägung zwischen strafrechtlichen und sicherheitsrelevanten Aspekten vorzunehmen und eine rasche und umfassende Alarmierung und Information aller Betroffenen sicherzustellen.

Auf Stufe Verwaltungseinheit hat die EFK Verbesserungspotenzial in folgenden Bereichen ausgemacht:

- Die Zusammenarbeit der beiden Response Teams (CSIRT-BIT, Mil-CERT).
- Die Aufarbeitung der „Lessons Learned", die bei den meisten Leistungserbringern nicht systematisch erfolgt und wodurch die Chance für die stetige Verbesserung ungenutzt bleibt.

6 Überprüfung der Umsetzung der fälligen Empfehlungen aus dem vergangenen Jahr

Die EFK hat sich bei den acht Leistungserbringern und dem ISB über den Stand der Umsetzung der fälligen Empfehlungen aus dem Vorjahr informiert. Die EFK stellte fest, dass Verbesserungen stattgefunden haben. Dennoch sind diverse Lücken nicht innert der von den Ämtern vorgesehenen Frist geschlossen worden. Das Tempo der Umsetzung ist insgesamt unbefriedigend. Die EFK erwartet eine rasche Umsetzung der vereinbarten Massnahmen.

Risiken, die bereits hätten adressiert werden sollen, bestehen weiter:

Ein bundesweites Inventar der sicherheitskritischen Anwendungen liegt noch nicht vor

Als Folge der revidierten BinfV wird das ISB im Rahmen seines Change-Programms „UBIS" (Umsetzung BinfV und IKT Strategie Bund) definieren können, wie ein zukünftiges Inventarsystem zu konzipieren ist, um die Anforderungen des BRB zu erfüllen. Das Thema wird vom ISB im Rahmen der Überprüfung des Inventarstandards aufgegriffen.

Die Defizite im Bereich der Passwortanforderungen und Benutzerverwaltung bestehen weitgehend weiter

Das Werkzeug zur Vergabe von lokalen Administratorenrechten konnte bis zum Zeitpunkt der Prüfung nicht ausser Betrieb gesetzt werden. Zwar wurden Konzepte zur Entschärfung der Situation erstellt, aber die Inbetriebsetzung ist noch nicht erfolgt. Zudem sieht das Konzept nach wie vor den selektiven Einsatz des betreffenden Werkzeugs vor.

Eine verbindliche Regelung betreffend Verbot von lokalen Administratorenrechten (z. B. lokale Standard-Administratorenaccounts für Supportzwecke) ist in die Weisungen über die Informatiksicherheit noch nicht eingeflossen. Eine entsprechende Ergänzung soll mit der geplanten Überarbeitung der WIsB stattfinden. Die Fertigstellung der Weisung wurde für Mitte 2013 in Aussicht gestellt; die Herausforderung wird die Umsetzung der Weisung sein.

Die Umsetzung der Passwortrichtlinien konnte aus technischen Gründen nach wie vor nicht überall umgesetzt werden. Die EFK nahm zur Kenntnis, dass die Ausnahmen zwar mittlerweile bekannt und dokumentiert sind, aber dass die Ausnahmen immer noch toleriert werden.

Die Überprüfung der Accounts findet noch nicht überall regelmässig statt.

Die zeitgerechte Schliessung von Sicherheitslücken ist aufgrund niedriger Priorität seitens Leistungsbezüger nicht überall möglich

Im Bereich der „zeitgerechten Schliessung von Sicherheitslücken" hat die EFK im vergangenen Jahr bemängelt, dass nicht mehr unterstützte Softwareversionen aufgrund von Abhängigkeiten mit

den Anwendungen der Leistungsbezüger nicht abgelöst werden können. Die EFK konnte feststellen, dass die grossen Leistungserbringer heute teilweise über Release-Pläne verfügen. Diese zeigen die Abhängigkeiten zwischen verschiedenen Produkten und sollen eine geordnete und planbare Ablösung ermöglichen. Die Umsetzung dieser Pläne gestaltet sich aber nach wie vor schwierig, da nicht alle Leistungsbezüger von der Notwendigkeit einer Ablösung überzeugt sind. Die entstehenden Aufwände für die Durchführung eines entsprechenden Projekts, die mit der Ablösung verbundenen Risiken und die entstehenden Kosten ohne zusätzlichen Gewinn an Funktionalität wirken hier verhindernd. In der Folge müssen Leistungserbringer auch heute noch Systeme mit nicht mehr unterstützten Betriebssystem-Versionen im Auftrag des Kunden betrieben. Den Leistungserbringern fehlt in diesen Fällen die nötige Weisungsbefugnis. Als Fortschritt wertet die EFK die Tatsache, dass diese Systeme mittlerweile in Form von Ausnahmelisten dokumentiert werden.

Die Umsetzung der Network Security Policy bei den Kantonen macht langsame Fortschritte, kann aber nicht befriedigen

Bei der Umsetzung der Network Security Policy (NSP) in den Kantonen sind mittlerweile alle Service Level Agreements (SLA) zwischen dem BIT und den Kantonen unterzeichnet. Die erste Runde der „Self-Assessments" über den Umsetzungsstand der NSP ist abgeschlossen. Erwartungsgemäss zeigt sich ein breites Spektrum zwischen Kantonen, die den Umsetzungsgrad als hoch, und den Kantonen, die den Umsetzungsgrad als sehr niedrig einschätzen. Je nach Ergebnis wird das BIT nächstes Jahr unterschiedliche Massnahmen in Zusammenarbeit mit den Kantonen ergreifen, um die weitere Umsetzung der NSP Vorgaben zu unterstützen und zu validieren. Dieses Thema beschäftigt die Beteiligten bereits seit Jahren, die erzielten Ergebnisse stehen in einem schlechten Verhältnis zu der benötigten Zeitspanne: Ursache dafür ist die fehlende Durchsetzungskraft des BIT gegenüber den Kantonen. Für 2013 und 2014 sind seitens des BIT geplant, die Kantone bei der normativen Umsetzung der NSP zu unterstützen und ISO-konforme Audits aufzusetzen und durchzuführen. Es sollte darüber hinaus überlegt werden, ob die Bemühungen nicht durch kompensierende technische Massnahmen (mit evtl. Kosten- und Performancenachteilen) flankiert werden sollten.

7 Voraussichtliche Themen für die Prüfung 2013

Die EFK wird sich darauf konzentrieren, was mit den weitergehenden Massnahmen gemäss BRB bisher geschehen ist. Deren Umsetzung (z. B. Zwei-Faktor Authentisierung) ist teilweise für das Jahr 2013 terminiert. Es soll durch die Prüfung von selektierten Anwendungen Antwort gegeben werden, ob die Absicherung der Fernzugänge zum Bundesnetz tatsächlich gemäss den Vorgaben erfolgt und ob das Thema Informations- und Datenschutz ausreichend abgedeckt ist.

8 Schlussbesprechung

Die Schlussbesprechung mit dem Delegierten des Informatikstrategieorgans fand am 21. November 2012 statt. Teilgenommen haben der Delegierte des Informatikstrategieorgans, Peter Fischer und der Leiter ISB-SEC, Marcel Frauenknecht.

Sie ergab Übereinstimmung in den aufgeführten Punkten.

Im Anschluss an die Schlussbesprechung mit dem Delegierten des Informatikstrategieorgans Bund hat am 23. November eine zusätzliche Informationsveranstaltung für die Ansprechpartner der Geprüften und der Informatiksicherheitsbeauftragten der Departemente stattgefunden. Bei dieser Gelegenheit hat die EFK die wesentlichen Prüfergebnisse vorgestellt und die Teilnehmenden erhielten die Gelegenheit sich zum Bericht und den Erläuterungen der EFK zu äussern.

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

EIDGENÖSSISCHE FINANZKONTROLLE

Brigitte Christ
Fachbereichsleiterin

Markus Künzler
Revisionsleiter

Anhang 1: Rechtsgrundlagen

Finanzkontrollgesetz (FKG, SR 614.0)

Finanzhaushaltgesetz (FHG, SR 611.0)

Finanzhaushaltverordnung (FHV, SR 611.01)

Bundesinformatikverordnung (BinfV, SR 172.010.58)

Informationsschutzverordnung (ISchV, 510.411)

Weisungen der IRB über die Informatiksicherheit in der Bundesverwaltung (WIsB)

Standard P012 – Betrieb Forest Bund

Standard P018 – Security Massnahmen Forest Bund

Standard P022 – Betrieb Mail/Exchange Bund

Standard A029 – Basissoftwarestandard Arbeitsplatz Bund (BAB)

Bundesratsbeschluss vom 16. Dezember 2009

Bundesratsbeschluss vom 4. Juni 2010

Anhang 2: Abkürzungen, Glossar, Priorisierung der Empfehlungen der EFK

Abkürzungen:

AD	Aktive Directory, Verzeichnisdienst für Windows
BinfV	Bundesinformatikverordnung
BIT	Bundesamt für Informatik und Telekommunikation
BK	Schweizerische Bundeskanzlei
BRB	Bundesratsbeschluss
CERT	Computer Emergency Response Team
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
FUB	Führungsunterstützungsbasis, IT-Leistungserbringer der VBS
IKT	Informations- und Kommunikationstechnologie
ISB	Informatiksteuerungsorgan 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
IT-EDA	IT-Leistungserbringer des EDA
LB	Leistungsbezüger
LE	Leistungserbringer
MELANI	Melde- und Analysestelle Informationssicherung
NSP	Network Security Policy
PD	Parlamentsdienste

PD-DINT	Dienst für Informatik und neue Technologie, IT-Leistungserbringer der Parlamentsdienste
PIN	Persönliche Identifikationsnummer
SCI-BK	Service Center Informatik BK, IT-Leistungserbinger der Bundeskanzlei
SLA	Service Level Agreement
SSO	Single Sign On (einmalige Anmeldung für die Nutzung mehrerer Anwendungen)
TCSB	IT-Leistungserbringer im SECO
UBIS	Umsetzung BinfV und IKT Strategie Bund
VBS	Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport
WIsB	Weisungen des IRB über die Informatiksicherheit des Bundes

Glossar:

Zwei-Faktor Authentisierung	Ein Anmeldeverfahren, welches auf zwei Faktoren, beispielsweise der Kenntnis eines Passworts und dem Besitz eines Hardware Tokens beruht.
e-dec	Fachanwendung der Eidgenössischen Zollverwaltung
GEVER ÜDP	Geschäftsverwaltungssystem für überdepartementale Prozesse
Minöst	Fachanwendung der Eidgenössischen Zollverwaltung
MOLIS	Fachanwendung der Eidgenössischen Steuerverwaltung
Patch Management	Verfahren für die zeitgerechte Schliessung von bekannten Sicherheitslücken
Security Incident Management	Verfahren für die Bewältigung von sicherheitsrelevanten Vorfällen
Security Patch	Vorübergehende Behebung einer Sicherheitslücke oder eines Fehlers in einer Software bis zum Vorliegen einer neuen, vermeintlich fehlerfreien Version
STOLIS	Fachanwendung der Eidgenössischen Steuerverwaltung

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.