Informatiksicherheit im Nachrichtendienst des Bundes
Bericht der Geschäftsprüfungsdelegation (Zusammenfassung)

vom 30. August 2013

Bericht

1 Einleitung

Am 30. Mai 2012 wurde der Präsident der Geschäftsprüfungsdelegation (GPDel) vom Direktor des Nachrichtendienstes des Bundes (NDB) darüber informiert, dass ein Mitarbeiter des Dienstes in grossem Umfang klassifizierte Daten entwendet hatte und später verhaftet wurde.

Nach diversen Abklärungen zu diesem Vorfall beschloss die GPDel am 15. Oktober 2012, zur Informatiksicherheit im NDB eine formelle Inspektion durchzuführen. Darüber informierte die GPDel am 16. Oktober 2012 die Öffentlichkeit (Medienmitteilung[1] und Pressekonferenz), nachdem sie zuvor mit dem Vorsteher des Departements für Verteidigung, Bevölkerungsschutz und Sport (VBS) eine Aussprache geführt hatte.

In den Monaten November 2012 bis Februar 2013 führte die GPDel für ihre Inspektion verschiedene Anhörungen durch. Zusätzlich stattete die Delegation im Dezember 2012 der Informatik des NDB einen Besuch ab. Anlässlich ihrer Sitzung von Ende April 2013 hielt sie mit dem Vorsteher des VBS ihre letzte Aussprache in dieser Angelegenheit.

Anfang Juni 2013 bat die GPDel die betroffenen Departemente um eine Stellungnahme zum Entwurf ihres Inspektionsberichts. Am 2. Juli 2013 besprach die GPDel mit einer Vertretung des Bundesrates die Schlussfolgerungen, welche sie aus ihrer Inspektion gezogen hatte. Am folgenden Tag übermittelte sie den Inspektionsbericht mit ihren 11 Empfehlungen an den Bundesrat.[2]

Weil die GPDel verhindern wollte, dass mit der Publikation von Informationen über den Nachrichtendienst höherrangige Interessen des Staates verletzt werden, verzichtete sie auf eine Publikation ihres umfassenden Inspektionsberichts. Für die Information der Öffentlichkeit verfasste sie diesen Kurzbericht mit ihren Empfehlungen und einer Zusammenfassung der wesentlichen Erkenntnisse aus der Inspektion.

2 Schaffung der Informatik des NDB

Um die Vorgaben des Bundesgesetzes über die Zuständigkeiten im Bereich des zivilen Nachrichtendienstes (ZNDG)[3] umzusetzen, beschloss der Bundesrat im März 2009, den DAP (Dienst für Analyse und Prävention) und den SND (Strategischer Nachrichtendienst) zu einem einzigen Bundesamt zusammenzufassen. Auf Antrag des VBS sollte dies auf Anfang 2010 und «ohne zusätzliche Ressourcen» realisiert werden. Dies bedeutete, dass der zukünftige NDB mit den Informatikressourcen des bisherigen SND auskommen musste, weil das VBS zuvor vom Eidgenössischen Justiz- und Polizeidepartement (EJPD) den DAP ohne das Personal, das dessen

1 Informatiksicherheit im Nachrichtendienst des Bundes, Medienmitteilung der GPDel vom 16. Okt. 2012.
2 Inspektion der GPDel: Informatiksicherheit im NDB, Medienmitteilung der GPDel vom 3. Juli 2013.
3 Bundesgesetz vom 3. Okt. 2008 über die Zuständigkeiten im Bereich des zivilen Nachrichtendienstes (ZNDG; SR **121**).

Informatikbedürfnisse abdeckte, übernommen hatte. Da dieser Mangel weder bei der Konzeption des NDB noch danach korrigiert wurde, musste der NDB eine komplexe und immer stärker wachsende Systemlandschaft mit sehr knappen Ressourcen betreuen.

Für die Datenbanken des NDB bedeutete dies, dass beim Ausfall des einzigen internen Datenbankadministrators ihre Betriebssicherheit nur gewährleistet werden konnte, solange keine gravierenden Probleme auftauchten. Als Folge der Fusion mussten verschiedene Systeme, die der NDB übernommen hatte, ersetzt oder angepasst werden. Der Mangel an verfügbaren Informatikern beschränkte jedoch die Zahl der Projekte, welche der NDB an die Hand nehmen konnte.

Laut dem Bericht vom 11. April 2013, den das VBS zum Datendiebstahl veröffentlichte, «stand der NDB somit vor der Situation, eine massiv erhöhte Anzahl von Systemen und Anwendungen sowie rund doppelt so viele Benutzer mit den gleichen personellen Kapazitäten betreuen zu müssen»[4]. Für die GPDel war dies das Resultat einer ungenügenden Planung, die mit dem Beschluss des Bundesrats über den Transfer des DAP ins VBS im Mai 2008 ihren Anfang genommen hatte. Auf Antrag des VBS entschied der Bundesrat am 25. März 2009, den NDB ressourcenneutral aus den bestehenden Diensten zu schaffen. Die daraus entstandenen Mängel in der Informatik hätte das VBS, wenn nicht während den Konzeptionsarbeiten für den neuen NDB, dann spätestens nach seiner Schaffung, beheben müssen.

Der NDB wies die GPDel erstmals im Frühjahr 2011 auf die Personalsituation in der Informatik hin, die sich aus der Konzeption des NDB ergeben hatte. Vor dem Datendiebstahl gab es seitens des NDB jedoch keine Aussagen, wonach der Dienst wegen der erwähnten Personalsituation die Informatiksicherheit beeinträchtigt sah. Auch die Finanzdelegation (FinDel) erhielt keine Informationen, aus denen sich ein Handlungsbedarf ergeben hätte.[5]

Die GPDel kommt zum Schluss, dass sowohl der Transfer des DAP in das VBS wie auch die nachfolgende Schaffung des NDB nicht genügend sorgfältig vorbereitet worden waren. Mit Blick auf das neue Nachrichtendienstgesetz erachtet es die Delegation deshalb als zwingend, dass das VBS seine Einschätzungen bezüglich der künftig notwendigen Personalressourcen des Dienstes auf eine einwandfreie Analyse des Ist- und des Soll-Zustandes abstützt.

Empfehlung 1

Die GPDel empfiehlt dem Bundesrat, das VBS mit einer vertieften und detaillierten Analyse der personellen Ressourcen zu beauftragen, die für die Erfüllung der zusätzlichen Aufgaben, welche mit dem neuen ND-Gesetz vorgeschlagen werden, notwendig sind.

4 Verhinderter Datenabfluss im NDB, Bericht des VBS vom 11. April 2013, S. 10.
5 Brief der FinDel an die GPDel vom 5. Juni 2013, S. 2.

3 Risikomanagement im NDB

Die Informatiksicherheit war im NDB nicht in ein Risikomanagement eingebettet, das die Konsequenzen der ungenügenden Personalressourcen in der Informatik aufgezeigt und eine gezielte Risikoverminderung ausgelöst hätte. Der NDB brachte sich zwar in den letzten Jahren vermehrt in das Risikoreporting[6] des Departements ein, aber im Rahmen des internen Risikomanagements – auch für die Informatik – wurden die Risiken weder definiert und bewertet, noch einem Risikoeigner zugewiesen. Die Inspektion der GPDel ergab auch keine Hinweise darauf, dass sich die Leitung des NDB vor dem Datendiebstahl aktiv um ein systematisches Risikomanagement im Dienst gekümmert hätte.

Das im Bericht des VBS vom 11. April 2013 erwähnte «genehmigte Dokument zu Schutz und Sicherheit»[7] regelte die Verantwortlichkeiten für das Risikomanagement mangelhaft und war ausserdem allein NDB-intern gutgeheissen worden. Notwendig wäre es, dass der NDB sein Risikomanagement in erster Linie an den übergeordneten Vorgaben des Bundes ausrichten und lediglich dienstspezifische Abweichungen und Ergänzungen in einem eigenen Dokument festhalten würde.

Ausgehend von seiner Risikopolitik aus dem Jahr 2004 hat der Bundesrat im Jahr 2010 die Weisungen[8] über die Risikopolitik des Bundes erlassen, zu denen im Herbst 2011 die Richtlinien der Eidg. Finanzverwaltung (EFV) über das Risikomanagement in Kraft traten. Ergänzt wurden diese Richtlinien durch ein Handbuch zum Risikomanagement Bund.[9]

Empfehlung 2

Die GPDel ersucht den Bundesrat sicherzustellen, dass das VBS ihm bis Juni 2014 über den Stand des Risikomanagements im NDB Bericht erstattet und darlegt, wie der NDB die einschlägigen Vorgaben des Bundes zum Risikomanagement adäquat umsetzt.

4 Vorkehrungen für die Informatiksicherheit im NDB vor dem Datendiebstahl

Die Bundesinformatikverordnung[10] und die Weisungen[11] des Informatikrats des Bundes (IRB) enthalten verschiedene Vorgaben zur Informatiksicherheit. Das VBS hat zudem eine eigene Weisung erlassen und der Fachbereich Informatiksicherheit der IOS (Informations- und Objektsicherheit) gibt als Vorgabe- und Kontrollstelle

6 Risikoreporting zuhanden des Bundesrats, Bericht der GPK-N/S vom 28. Mai 2010 (BBl **2010** 5683–5690).
7 Bericht des VBS vom 11. Apr. 2013, S. 11.
8 Weisungen vom 24. Sept. 2010 über die Risikopolitik des Bundes (BBl **2010** 6549).
9 Zu finden auf der Webseite der EFV unter www.efv.admin.ch /d/dokumentation/finanzpolitik_grundlagen/risiko_versicherungspolitik.php
10 Verordnung vom 9. Dez. 2011 über die Informatik und Telekommunikation in der Bundesverwaltung (Bundesinformatikverordnung, BInfV; SR **172.010.58**).
11 Weisungen des IRB vom 27. Sept. 2004 über die Informatiksicherheit in der Bundesverwaltung (WIsB), zu finden auf der Webseite des ISB: www.isb.admin.ch/themen/sicherheit/00150/00836/index.html?lang=de

ein Handbuch zur Informatiksicherheit heraus, welches allerdings verglichen mit dem angestrebten Standard unvollständig geblieben ist.

Die GPDel kommt zum Schluss, dass der NDB vor dem Datendiebstahl verschiedene technische und organisatorische Massnahmen nicht getroffen hatte, die zum Grundschutz seiner Informatik gehört hätten und teilweise auch vom Bund oder vom VBS vorgeschrieben waren.

Für die Wahrnehmung der Aufgabe des Informatiksicherheitsbeauftragen (ISBO) stand, wenn überhaupt, nur in ungenügendem Ausmass Personal zur Verfügung, was ein adäquates Risikomanagement in der Informatik verunmöglichte. Die vorgeschriebenen Sicherheitskonzepte für die Anwendungen und Systeme waren mehrheitlich ungenügend oder fehlten gar.

Die Passwörter zu den unpersönlichen Administratorenkonten wurden in der Informatik intern verwaltet und ihre Verwendung wurde nicht kontrolliert. Diese Praxis erleichterte angesichts der Personalknappheit die Aufrechterhaltung des Informatikbetriebs, gab aber den betreffenden Informatikern auch uneingeschränkte Zugriffsrechte, deren Verwendung nachträglich nicht mehr persönlich zugeordnet werden konnte.

Während gewisse Systemaktivitäten zu Sicherheitszwecken aufgezeichnet wurden, konnte die GPDel keinen Beleg dafür finden, dass die erstellten Ereignisprotokolle (Logdateien) systematisch ausgewertet worden wären. So fanden in den fünf Monaten des Jahres 2012, welche dem externen Hinweis auf einen möglichen Datendiebstahl vorangingen, keine Auswertungen statt. Es gab auch keine Notfallplanung für den Fall eines Verdachts auf eine Gefährdung der Systeme oder ihrer Daten. Letztlich fehlte dem NDB das zusätzliche Personal, das für den Betrieb eines funktionierenden Überwachungssystems notwendig gewesen wäre.

Nach dem Datendiebstahl sorgte die Leitung des NDB mit der notwendigen Dringlichkeit dafür, dass der Dienst einen vollamtlichen ISBO einstellte (November 2012) und damit die Vorgaben des Bundes erfüllte. Allerdings wurde die Bedeutung der Sicherheitskonzepte für das Management der Risiken, welche mit den Informatiksystemen verbunden sind, erst später erkannt. Das führte dazu, dass der NDB erst Ende 2012 mit Hilfe der IOS zu überprüfen begann, welche Konzepte benötigt werden und wie sie verbessert werden können.

Es ist geradezu der Zweck eines Informationssicherheits- und Datenschutzkonzepts (ISDS-Konzept), die Risiken für die Sicherheit eines Systems zu bewerten und gestützt darauf zu entscheiden, mit welchen technischen, organisatorischen und anderen Massnahmen diese Risiken reduziert werden sollen. Mit dem risikobasierten Ansatz wird verhindert, dass einzelne Massnahmen forciert werden, die im Kontext der verschiedenen Risiken und der verfügbaren Ressourcen keine zweckmässige Risikoreduktion bewirken würden.

Empfehlung 3

Die GPDel ersucht das VBS, dafür zu sorgen, dass der Informatiksicherheitsbeauftragte des Departements (ISBD VBS) auf Ende 2014 alle Anwendungen und Systeme des NDB darauf hin überprüft, ob sie durch ein gültiges Sicherheitskonzept mit einer fundierten und umfassenden Risikobeurteilung abgedeckt sind. Die Behebung allfälliger Mängel ist mittels eines verbindlichen Massnahmenplans auszuweisen.

Die Inspektion hat gezeigt, dass es der Führung des NDB an einem ausreichenden Verständnis für die Frage mangelte, welche Vorschriften der Dienst im Bereich der Informatiksicherheit einzuhalten hatte. Nur so lässt sich erklären, dass die massgebliche Bestimmung von Art. 7 Abs. 1 ISV-NDB[12] zur Chiffrierung des NDB-internen Kommunikationssystems (SiLAN) nie umgesetzt wurde, obwohl sich die spätere Leitung des NDB bei der Schaffung des neuen Dienstes im Jahr 2009 für ein solches Erfordernis entschieden und dem Bundesrat eine entsprechenden Norm auf Verordnungsstufe vorgeschlagen hatte.

Empfehlung 4

Die GPDel ersucht den Bundesrat, beim VBS bis Ende 2013 überprüfen zu lassen, ob die Bestimmung von Art. 7 Abs. 1 ISV-NDB über die Chiffrierung des SiLAN so angewendet werden kann, dass Aufwand und Nutzen für die Informatiksicherheit des NDB in einem vertretbaren Verhältnis stehen. Je nach Ergebnis der Überprüfung ist die Bestimmung entweder innert nützlicher Frist anzuwenden oder umgehend zu streichen.

5 Personensicherheitsprüfungen

Für die beiden Vorgängerorganisationen des NDB galten unterschiedliche Vorschriften für die Personensicherheitsprüfungen (PSP). Während im DAP beispielsweise Personen in rein administrativen Funktionen davon ausgenommen waren, wurden alle Angestellten des SND einer PSP unterzogen. Die höchste Stufe der PSP mit Befragung, d.h. nach Art. 12 PSPV[13], wurde aber nicht für alle SND-Mitarbeitenden, beispielsweise der Informatik, verlangt.

Nach der Fusion wurde im NDB beschlossen, die PSP bei Neueintritten und bei der nach fünf Jahren fälligen Wiederholung nur noch nach Art. 12 PSPV durchführen zu lassen. Es wurde aber darauf verzichtet, die Prüfungen, deren Wiederholung noch nicht anstand, vorzuziehen. Dies erfolgte vor dem Hintergrund der Kapazitätsengpässe bei der Fachstelle PSP und in Absprache mit der IOS.

12 Verordnung vom 4. Dez. 2009 über die Informationssysteme des Nachrichtendienstes des Bundes (ISV-NDB; SR **121.2**).
13 AS **2002** 377

Nach einer Totalrevision der PSPV[14] im Jahr 2011 schrieb das VBS am 1. April 2012 mit der departementalen PSPV-VBS[15] vor, sämtliche Angehörige des NDB nach Art. 12 PSPV zu prüfen. Laut den Übergangsbestimmungen musste die neuerliche Prüfung aller Personen, für die nunmehr eine höhere Prüfstufe vorgeschrieben war, innerhalb eines Monats an die Hand genommen werden. Wie die Inspektion der GPDel ergab, erfüllte der NDB diese Vorgaben nicht, war doch im Februar 2013 ein Drittel der Mitarbeitenden des NDB noch nicht nach Art. 12 PSPV geprüft worden. Bei den Informatikern lag der Anteil weiterhin bei einem Viertel.

Wegen der wachsenden Zahl an Informatikprojekten, die auch eine Folge der Zusammenlegung der Vorgängerorganisationen des NDB waren, ist die Abhängigkeit des NDB von externen Informatikern gestiegen. Diese werden jedoch nicht der höchsten Stufe der Personensicherheitsprüfung unterzogen, die für alle Mitarbeitenden des NDB vorgeschrieben ist. Die Inspektion der GPDel hat zudem keine abschliessende Antwort auf die Frage ergeben, durch welche Stelle auf welcher Stufe die PSP für externe Mitarbeitende einzuleiten ist.

Nach Ansicht der GPDel sollten diejenigen Bundesstellen, für welche Dienstleistungen Dritter letztlich erbracht werden, auch sicherstellen, dass nur externe Mitarbeitende und Firmen für sie tätig sind, die ausreichend sicherheitsüberprüft wurden. Die betroffenen Ämter müssten deshalb auch den vollständigen Überblick über alle für sie tätigen externen Mitarbeitenden haben, was nach den Abklärungen der GPDel zurzeit jedoch nicht gewährleistet ist.

Empfehlung 5

Die GPDel empfiehlt dem Bundesrat, mit einer Revision der PSPV dafür zu sorgen, dass für externe Mitarbeitende die gleichen Anforderungen an die Stufe der PSP gestellt werden wie für Angestellte des Bundes, welche die gleichen Aufgaben wahrnehmen. Die Verantwortung für die Einhaltung der Vorschriften durch externe Firmen und ihre Mitarbeitenden ist derjenigen Bundesstelle zu übertragen, für welche die Externen letztlich ihre Leistung erbringen.

Das Problem einer adäquaten Durchführung der Sicherheitsprüfungen im NDB oder anderswo kann nicht losgelöst von den Kapazitätsengpässen, die bei der Fachstelle PSP der IOS seit Jahren bestehen, betrachtet werden. Laut einem Bericht des Inspektorats VBS vom 21. Dezember 2012 ist die Zahl der pendenten PSP bis Ende 2012 auf rund 1500 Fälle angewachsen. Obwohl der Vorsteher des VBS im November 2012 das Personal der Fachstelle PSP temporär aufgestockt hatte, schätzte das Inspektorat VBS, dass der aktuelle Überhang an ausstehenden PSP erst in fünf Jahren abgebaut sein werde. Dies ist umso problematischer, als es sich bei einem grossen Teil der Pendenzen um Fälle handelt, die potentiell mit einem höheren Risiko behaftet und deshalb auch arbeitsintensiver sind.

Da die PSP regelmässig wiederholt werden muss, kann mit einem temporären Zusatzaufwand das Kapazitätsproblem nicht nachhaltig behoben werden. Ausserdem

14 Verordnung vom 4. März 2011 über die Personensicherheitsprüfungen (PSPV; SR **120.4**).
15 Verordnung des VBS vom 12. März 2012 über die Personensicherheitsprüfungen (PSPV-VBS; SR **120.423**).

hat die Zahl der Prüfaufträge aus den Departementen in den letzten Jahren laufend zugenommen. Es stellt sich somit die Frage, ob der Bund grundsätzlich zu wenig Personal für die Durchführung der PSP besitzt oder ob die Departemente für zu viele Funktionen die höchste Prüfstufe vorgeschrieben haben, dies beispielsweise deshalb, weil Vorgesetzte damit ihre Verantwortung delegieren, anstatt ihre Führungsaufgabe effektiv wahrzunehmen.

Während die GPDel ohne Vorbehalte von der Notwendigkeit der PSP als eine Art Grundschutz im Bereich der Informationssicherheit überzeugt ist, unterstreichen die Erkenntnisse aus ihrer Inspektion die Notwendigkeit einer effektiven Personalführung, die im Fall des Datendiebstahls im NDB trotz rechtzeitigen Warnzeichen während Wochen nicht wahrgenommen wurde.

Die Tendenz, für die Gewährleistung der Sicherheit den Akzent auf die PSP anstatt auf die Führungsverantwortung zu legen, kommt auch in der offiziellen Reaktion des VBS auf den Datendiebstahl zum Ausdruck. Das VBS geht in seinem Bericht vom 11. April 2013 davon aus, dass eine erweiterte PSP mit Befragung keine Vorbehalte gegen eine weitere Beschäftigung des Datenbankadministrators an den Tag gebracht hätte.[16] Trotzdem und ohne die Ressourcenfrage zu berücksichtigen hält es das VBS für erstrebenswert, zur weiteren Minimierung der Risiken in der gesamten Bundesverwaltung die Prüfstufe und der Prüfungsrhythmus bei den PSP zu erhöhen.

Je stärker und undifferenzierter die PSP auf alle möglichen Funktionen innerhalb der Bundesverwaltung ausgeweitet wird, umso mehr besteht die Gefahr, dass Führungspersonen auf andere Ansätze im Risikomanagement oder auf bereits existierende Instrumente des Personalrechts verzichten.

Empfehlung 6

Die GPDel empfiehlt dem Bundesrat, in seiner Botschaft zum Informationssicherheitsgesetz (ISG) die Rollen, welche die Personensicherheitsprüfung und die Personalführung im Bereich der Informationssicherheit spielen, ausführlich darzulegen und klar voneinander abzugrenzen. Gleichzeitig soll in einem separaten Bericht erläutert werden, wie viele personelle Ressourcen der Bund für die Durchführung der PSP einsetzen soll und welchen Beitrag an den Informationsschutz er damit leisten will.

6 Datendiebstahl im Mai 2012

Die GPDel stellt fest, dass der NDB aufgrund der knappen Personalsituation in der Informatik und des unzulänglichen Risikomanagements zu wenig darauf ausgerichtet war, die Verfügbarkeit, die Integrität und die Vertraulichkeit der Daten als zentrale Zielsetzung der Informatiksicherheit zu gewährleisten.

Im April 2012 gefährdete die erneute krankheitsbedingte Abwesenheit des einzigen Datenbankadministrators aus Sicht seiner Vorgesetzten zunehmend die Betriebssicherheit der Datenbanken des NDB. Überdies wurde die Zusammenarbeit mit ihm wieder verstärkt als problematisch erlebt. Die Leitung der Informatik ortete deshalb

16 Bericht des VBS vom 11. Apr. 2013, S. 18.

einen Handlungsbedarf auf ihrer vorgesetzten Stufe und machte diese am 26. April 2012 darauf aufmerksam, dass unter Umständen der Datenbankadministrator auch die Integrität der Datenbankprogramme beeinträchtigen könnte. Konkret wurde auch vorgeschlagen, dem Datenbankadministrator die Zugriffsberechtigungen für die von ihm betreuten Systeme zu entziehen.

In der Folge stand die Leitung der Abteilung, zu welcher die Informatik, die Sicherheitszelle sowie der Rechts- und Personaldienst gehörten, vor dem Dilemma, entweder mit der Freistellung des Datenbankadministrators die Verfügbarkeit der Systeme zu gefährden oder bei seinem weiteren Einsatz ein Risiko für die Integrität – und wie es sich nachträglich zeigte, auch für die Vertraulichkeit der Daten – in Kauf zu nehmen.

Obwohl ihm eine klare Risikobeurteilung unterbreitet wurde, liess der zuständige Abteilungsleiter eine Woche verstreichen, bis er am 7. Mai 2012 mit seinen Direktunterstellten mögliche Handlungsoptionen besprach. Auch dann ergriff er keine Massnahme gegenüber dem Datenbankadministrator, sondern wartete drei weitere Tage bis zum Entscheid, ein Gespräch mit diesem vereinbaren zu lassen.

In dieser kritischen Zeit fehlte eine enge Führung und Betreuung des Datenbankadministrators. So konnte der Datenbankadministrator nur eine Stunde nach dem nicht eingehaltenen Gesprächstermin vom 16. Mai 2012 längere Zeit am Arbeitsplatz verweilen, ohne dass dies eine Reaktion der Abteilungsleitung zur Folge gehabt hätte.

Die ungenügende Reaktion der zuständigen Abteilung in Sachen Personalführung und Risikomanagement erlaubte es dann letztlich, dass der Datendiebstahl im Mai 2012 stattfinden konnte. Der Direktor NDB erfuhr erst von den im April 2012 erkannten Risiken, als der externe Hinweis auf ein verdächtiges Verhalten des Datenbankadministrator am 18. Mai 2012 eingegangen war.

Aus Sicht der GPDel trifft es nicht zu, dass das Personalrecht des Bundes dem NDB kein zweckmässiges Handeln gegenüber dem Datenbankadministrator erlaubt hätte. Der NDB hätte die Möglichkeiten von Art. 103 Bundespersonalverordnung (BPV)[17], welcher die Freistellung oder anderweitige Beschäftigung von Angestellten des Bundes regelt, rechtzeitig ins Auge fassen müssen. Da der NDB die seit längerer Zeit auftauchenden Probleme nicht dokumentiert hatte, konnte er sich in der kritischen Phase nicht darauf abstützen, um beispielsweise eine Freistellung wegen erwiesenen und wiederholten Unregelmässigkeiten gemäss Art. 103 Abs. 1 Bst. b BPV anzuordnen.

Die GPDel teilt die Einschätzung des NDB nicht, wonach dieser aufgrund der im April 2012 erkannten Probleme bereits ausreichend reagiert hatte, um dem Diebstahl auch ohne externen Hinweis innert nützlicher Frist selber auf die Spur zu kommen. Als sich die Identifikation des Datenbankadministrators mit Hilfe der schweizerischen Grossbank, die sein verdächtiges Verhalten gemeldet hatte, verzögerte, zog es der NDB beispielsweise nicht in Betracht, die Logdateien zu den externen Schnittstellen, über welche der Datenbankadministrator hätte Daten kopieren können, zu überprüfen. In diesem Zeitraum wurde auch der Verdacht, dass der Datenbankadministrator die Datenbankprogramme kompromittiert haben könnte, nicht überprüft. Beides wurde erst überprüft, nachdem der NDB den Hinweis der Grossbank endgültig verifiziert hatte.

17 Bundespersonalverordnung vom 3. Juli 2001 (BPV; SR **172.220.111.3**).

Die GPDel hat keinen Grund zur Annahme, dass das bestenfalls ansatzweise vorhandene Überwachungs- und Kontrolldispositiv in der Informatik des NDB von sich aus einen Hinweis auf den Datendiebstahl generiert hätte.

7 Massnahmen des NDB nach dem Diebstahl

Aus Sicht der GPDel hat der Direktor NDB seine Aufsicht nach dem Datendiebstahl zu wenig konsequent wahrgenommen und die internen Untersuchungen nicht den richtigen Stellen im Dienst anvertraut. Insbesondere war der Entscheid problematisch, die interne Aufarbeitung des Falles dem Abteilungschef, der direkt für alle Bereiche verantwortlich war, welche die Handlungsweise des NDB im Vorfeld des Datendiebstahls bestimmt hatten, zu übertragen.

Dieser fokussierte dann auch seine Analyse auf die Person des Datenbankadministrators, ohne anderweitigen Ursachen für den Datendiebstahl im Bereich der Organisation und Verfahren im NDB nachzugehen. Es erfolgte auch keine Beurteilung, ob der NDB im Bereich Informatik die vorgeschriebenen Sicherheitsvorkehrungen getroffen hatte. Damit wurde später der Chef Sicherheit beauftragt. Zur Klärung der Frage, ob die Führungsverantwortung gegenüber dem Datenbankadministrator korrekt wahrgenommen worden war, war der Chef Sicherheit jedenfalls nicht die geeignete Person, um das Verhalten seines Abteilungschefs zu beurteilen.

Ebenso wie die ND-Aufsicht erachtet auch die GPDel die organisatorische Einbettung der Sicherheitszelle in einer operativen Abteilung als problematisch. Der Fall des Datendiebstahls hat gezeigt, wie die divergierenden Interessen der Bereiche Sicherheit, Informatikbetrieb und Personalwesen ein entschiedenes Vorgehen im Interesse der Sicherheit verunmöglicht hatten. Unter diesen Umständen hätten die notwendigen Entscheide auf einer übergeordneten Stufe getroffen werden müssen.

Empfehlung 7

Die GPDel empfiehlt dem Vorsteher VBS, dafür zu sorgen, dass der NDB eine neue Unterstellung der Sicherheitszelle ausserhalb der Abteilung NDBU vornimmt. Zugleich ist die Aufgabenverteilung für das Risikomanagement im gesamten Dienst zu überdenken.

Aus Sicht der GPDel war es zweckmässig, dass der NDB mit einzelnen Sofortmassnahmen relativ schnell auf den Vorfall reagierte, beispielsweise beim Passwort-Management. Im Verlauf der Zeit erhielt die GPDel aber den Eindruck, dass die steigende Zahl der Massnahmen der Leitung des NDB vor allem dazu diente, ihre aktive Bewältigung der Folgen des Datendiebstahls unter Beweis zu stellen. Die Betonung der laufenden und geplanten Massnahmen drängte die Frage nach den Ursachen für den Vorfall in den Hintergrund.

Die Massnahmen zur Erhöhung der Sicherheit wurden zudem ohne Abstützung auf einen nachvollziehbaren Risikomanagementprozess beschlossen. Der Direktor NDB setzte seine Unterschrift auch unter Massnahmen, welche danach gar nie an die Hand genommen wurden oder sich technisch als unrealistisch herausstellten. Aus

Sicht der GPDel ist ein funktionierendes Risikomanagement die Voraussetzung für die richtige Wahl und Priorisierung der Sicherheitsmassnahmen im Dienst.

Da der NDB die Analyse von systemischen Ursachen für den Datendiebstahl vernachlässigt hatte, erhielt das Problem der Personalressourcen zu lange nicht die gebührende Priorität. Erst nach Mitte Oktober 2012 liess die Leitung des Dienstes die Bereitschaft erkennen, sich für mehr als einen minimalen Personalausbau zugunsten der Informatik einzusetzen.

Der Personalbedarf für die Informatiksicherheit im NDB wird letztlich durch den Entscheid des Bundesrats vom 1. Mai 2013 bestätigt (11 zusätzliche Stellen). Die GPDel begrüsst diesen Entscheid, auch wenn er erst ein Jahr nach dem Datendiebstahl erfolgte. Die Delegation bedauert aber, dass die beschlossene Personalerhöhung teils erst ab 2014 und teils erst ab 2015 wirksam werden soll. Damit hält die kritische Personalsituation in der Informatik des NDB länger an, als es angesichts der Sensitivität der Daten des NDB eigentlich verantwortbar ist.

Empfehlung 8

Die GPDel empfiehlt dem VBS, dem NDB die Besetzung der Informatikerstellen aus der Personalreserve des Departements bereits im Jahr 2013 zu ermöglichen, obwohl der Bundesrat diese Stellen erst ab 2014 bewilligt hat.

8 Abklärungen zur Informationssicherheit im Auftrag des Bundesrats

Am 24. Oktober 2012 beschloss der Bundesrat auf Antrag des VBS, als Folge des Datendiebstahls im NDB eine Analyse der Gefahren für die Informationssicherheit auf Stufe Bund durchführen zu lassen. Eine Arbeitsgruppe, die bereits unter der Leitung von Prof. Markus Müller (Universität Bern) das zukünftige ISG erarbeitete, sollte bis Ende Februar 2013 Lücken in der Informationssicherheit aufzeigen und Sofortmassnahmen für ihre Behebung vorschlagen. Als sich dieser Termin als zu knapp erwies, wurde der Untersuchungsgegenstand auf den Datendiebstahl durch Innentäter begrenzt.

Das VBS unterbreitete den Bericht am 1. März 2013 dem Bundesrat mit dem formellen Antrag auf Kenntnisnahme. Der Bundesrat nahm den Bericht am 15. März 2013 zur Kenntnis. Gleichzeitig schloss er sich der Empfehlung des Berichts an, wonach der Innentäter-Problematik mit einer Ausbildung und Sensibilisierung des Kaders in der Bundesverwaltung zu begegnen sei und ordnete deren Umsetzung ab Herbst 2013 an.

Die Arbeitsgruppe hat auch auf die Notwendigkeit hingewiesen, die geltenden Vorgaben des Bundes zur Informatik- und Informationssicherheit uneingeschränkt anzuwenden. Weiter sollten die Massnahmen zur Verbesserung der Informatiksicherheit, die der Bundesrat im Nachgang zu den Angriffen auf die Informatik des Eidg. Departements für auswärtige Angelegenheiten (EDA) im Dezember 2009 und im Juni 2010 für die gesamte Bundesverwaltung beschlossen hatte, konsequent umgesetzt werden. Einzelne dieser Massnahmen waren von der Eidgenössischen

Finanzkontrolle (EFK) in den Jahren 2011 und 2012 im Auftrag des Bundesrats überprüft worden.

In diesem Zusammenhang ist auch zu erwähnen, dass das Informatiksteuerungsorgan des Bundes (ISB)[18] jährlich zuhanden des Bundesrats den Informatiksicherheitsbericht Bund über den Umsetzungstand der Informatiksicherheitsmassnahmen erstellt (vgl. Art. 11 Abs. 2 und 3 BinfV). Bis anhin verfasste die IOS ausserdem einen «Jahresbericht Informationsschutz Bund» zuhanden des Sicherheitsausschusses des Bundesrats (SiA). Als Folge der letzten Revision der Informationsschutzverordnung (ISchV) vom 1. Mai 2013 soll dieser Bericht zukünftig nur noch alle zwei Jahre an die Generalsekretärenkonferenz gehen.

In beiden Fällen stützen sich die Berichte auf die Angaben, die von den Departementen geliefert werden, ab. Um den Stand der Informatiksicherheit und des Informationsschutzes effektiv erfassen zu können, müssten die betreffenden Meldungen auch überprüft werden, wie es bei den vom Bundesrat in den Jahren 2009 und 2010 beschlossenen Massnahmen zur Informatiksicherheit teilweise geschieht.

Angesichts der bereits institutionalisierten Verfahren erscheint der GPDel der Auftrag an die Arbeitsgruppe von Prof. Müller als eine isolierte Massnahme, die vom VBS ohne Berücksichtigung der bereits auf Stufe Bund verfügbaren Instrumente beantragt worden war.

Aus Sicht der GPDel bieten der jährliche Informatiksicherheitsbericht Bund des ISB und die Massnahmen zur Erhöhung der Informatiksicherheit, die der Bundesrat auf Antrag des EFD in den Jahren 2009 und 2010 beschlossen hat, eine geeignete Ausgangslage, um einen nachhaltigen Prozess für die Verbesserung der Informatiksicherheit auf Stufe Bund in Gang zu bringen. Die Berichterstattung des ISB, welche heute hauptsächlich auf einer Selbstdeklaration der Departemente beruht, könnte in Richtung eines Controllings ausgebaut werden. Weiter könnte die Überprüfung der vom Bundesrat beschlossenen Sicherheitsmassnahmen, die heute ad hoc von der EFK vorgenommen wird, in geeigneter Form institutionalisiert werden.

Die GPDel ist auch der Ansicht, dass die Erkenntnisse aus der Überprüfung der Informatiksicherheit auf geeignete Art und Weise in die Vorgaben und Anforderungen für die Informatiksicherheit auf Stufe Bund einfliessen sollten. Weiter sollte die Informatiksteuerung auf Stufe Bund so ausgelegt sein, dass die Vorgaben und Erkenntnisse zur Informatiksicherheit möglichst frühzeitig bei der Planung und Beschaffung der Informatikmittel berücksichtigt werden können.

Empfehlung 9

Die GPDel empfiehlt dem Bundesrat, Vorschläge zu erarbeiten, um das Verfahren zur Überprüfung des Standes der Informatiksicherheit im Bund zu verbessern. Die Massnahmen sollen den Bundesrat befähigen, im Rahmen eines institutionalisierten Verfahrens Risiken in der Informatiksicherheit rechtzeitig zu erkennen, die notwendigen risikomindernden Massnahmen zu beschliessen und ihre Umsetzung zu verfolgen.

18 Vor 2012 hiess das ISB Informatikstrategieorgan des Bundes.

9 Aufsicht durch den Vorsteher VBS

Während der ersten drei Monate nach der Aufdeckung des Datendiebstahls stützte sich der Vorsteher VBS auf die Einschätzung des Vorfalls, welche er vom NDB erhalten hatte. Die Beurteilung des NDB fokussierte jedoch auf die Person des Datenbankadministrators und liess andere Ursachen, die zum Vorfall beigetragen haben könnten, völlig ausser Acht.

Erst gegen Ende August 2012 veranlasste der Vorsteher VBS Abklärungen zur Vorgeschichte des Datendiebstahls und zur Reaktion des Dienstes durch eine NDB-externen Stelle. Entsprechende Aufträge ergingen am 24. August 2012 an die departementsinterne ND-Aufsicht und im Oktober 2012 auch an die IOS.

Am 22. Oktober 2012 erstellte die IOS eine Beurteilung für den Vorsteher VBS zur Informatiksicherheit im NDB. Laut IOS waren die personellen Ressourcen des NDB in den Bereichen Informatik und Sicherheit unzureichend. In einem Zusatzbericht, den die IOS auf Wunsch des Vorstehers VBS verfasste, gelangte sie zum Schluss, zusätzlich zur Stelle des ISBO seien zwei weitere Stellen im Bereich Sicherheit und fünf bis zehn weitere Vollzeitstellen zu schaffen, um besonders sensitive Funktionen in der Informatik doppelt besetzen zu können.

Um die Reaktionsfähigkeit des NDB im Führungs- und Personalbereich zu verbessern, regte die IOS an, die Möglichkeiten zur raschen Freistellung von Personal in sicherheitskritischen Funktionen zu erweitern. Dies sollte aber mit finanziellen und anderen Absicherungen zugunsten dieser Arbeitnehmer kompensiert werden. So schlug die IOS vor, bei einer sofortigen Freistellung eine Lohnfortzahlung für eine längere Dauer zu garantieren oder eine andere gleichwertigen Tätigkeit in einem weniger sicherheitskritischen Bereich anzubieten.

Laut der IOS müsste die Machbarkeit dieser Vorschläge allerdings noch personalrechtlich überprüft werden. Im Hinblick auf seinen Schlussbericht vom 11. April 2013 nutzte das VBS die Gelegenheit jedoch nicht, die rechtlichen Fragen zu klären und Modelle für entsprechende Anstellungsbedingungen zu präsentieren.

Empfehlung 10

Die GPDel empfiehlt dem Bundesrat, unter der Federführung des Eidg. Personalamtes (EPA), eine interdepartementale Arbeitsgruppe einzusetzen, deren Aufgabe es ist, besondere Anstellungsbedingungen zu erarbeiten, welche es erlauben, in der Personalführung die Reaktionsmöglichkeiten gegenüber Innentäterrisiken zu verbessern. Um bei den betroffenen Mitarbeitenden die dafür notwenige Akzeptanz zu schaffen, wären insbesondere auch finanzielle und andere Kompensationsmassnahmen zu prüfen. Der Bundesrat soll bis Ende 2014 zu den Resultaten der Arbeitsgruppe Stellung nehmen.

Die ND-Aufsicht lieferte dem Vorsteher VBS im September 2012 einen ersten und im Hinblick auf das Treffen zwischen der GPDel und dem Vorsteher des VBS von Mitte Oktober 2012 einen zweiten Zwischenbericht ab. Daraufhin wies der Vorsteher VBS die ND-Aufsicht an, die verschiedenen Abklärungen, die er seit August 2012 in Auftrag gegeben hatte, bis Ende November 2012 abzuschliessen.

Wie die GPDel erfuhr, weigerte sich Ende Oktober 2012 der NDB, der ND-Aufsicht eine eigene Analyse zum Schadenspotenzial der entwendeten Daten zur Verfügung zu stellen, bevor der Direktor des Dienstes beim Vorsteher VBS das Einverständnis dazu eingeholt und erhalten hatte. Nach dem Verständnis der GPDel gibt es im geltenden Recht jedoch keine Grundlage für den NDB, einen solchen Vorbehalt anzubringen.

Die GPDel misst diesem Vorfall eine erhöhte Bedeutung zu, weil der NDB in einem anderen Geschäft, das allerdings keinen Bezug zur Inspektion der GPDel hatte, mit dem Einverständnis des Vorstehers VBS der ND-Aufsicht Auskünfte verweigerte. Einen entsprechenden Hinweis erhielt die GPDel von Prof. Koller, als sich die Delegation mit ihm über seine Erkenntnisse zur departementsinternen Aufsicht unterhielt. Aus Sicht der GPDel darf es der Departementsvorsteher nicht zulassen und noch viel weniger unterstützen, dass der NDB entscheidet, welche Informationen die Aufsicht erhalten darf und welche nicht.

Empfehlung 11

Die GPDel fordert den Vorsteher VBS auf, ausnahmslos für die Respektierung der Einsichtsrechte der ND-Aufsicht, die von Gesetz (Art. 8 ZNDG i.V.m. Art. 26 Abs. 1 BWIS) und Verordnung (Art. 33 Abs. 1 V-NDB) garantiert werden, zu sorgen. Der NDB kann diese Informationsrechte weder alleine noch im Einverständnis mit dem Departementsvorsteher beschränken.

In ihren zwei Zwischenberichten an den Vorsteher VBS machte die ND-Aufsicht insgesamt fünf Empfehlungen. Diese fünf Empfehlungen übernahm sie in ihren Schlussbericht von Ende November 2012.

Die GPDel kann nicht nachzuvollziehen, warum der Vorsteher VBS erst im April 2013 über diese Empfehlungen entschieden und sie dem NDB zur Umsetzung überwiesen hat. Dies umso mehr, als diese Empfehlungen bereits mit dem zweiten Zwischenbericht der ND-Aufsicht, d.h. sechs Monate früher, vorlagen.

Insgesamt stellt die GPDel fest, dass der Vorsteher VBS seine Aufsicht auf eine Art und Weise ausübte, welche Unklarheiten bezüglich der Rollen von ND-Aufsicht und NDB zuliess.

Schliesslich beauftragte der Vorsteher VBS am 19. November 2012 den ehemaligen Direktor des Bundesamtes für Justiz (BJ), Prof. Heinrich Koller, mit einer Überprüfung der ND-Aufsicht. Damit wollte er «im Anschluss an den Datendiebstahl eine […] Prüfung aller relevanten Akteure im VBS sicherstellen»[19]. Die Resultate der Untersuchung lagen Ende März 2013 vor. Zur Informatiksicherheit im NDB ergab sie keine zusätzlichen Erkenntnisse.

Angesichts des vom VBS angegebenen Zwecks der Untersuchung von Prof. Koller kann die GPDel allerdings nicht verstehen, warum der Vorsteher VBS diese Überprüfung auf die ND-Aufsicht beschränkt hat. Aus Sicht der GPDel wäre es nicht nur konsequent, sondern auch gerechtfertigt gewesen, im Nachgang zum Datendiebstahl

19 Bericht des VBS vom 11. Apr. 2013, S. 16.

im NDB auch die IOS überprüfen zu lassen, da sie nicht nur eine Aufsichtsrolle hat, sondern auch die ISDS-Konzepte des NDB zu genehmigen hat.

Wie die GPDel im Oktober 2012 erfuhr, plante der Vorsteher VBS, mit den Erkenntnissen aus dem Vorfall einen Schlussbericht mit Lehren für die gesamte Bundesverwaltung zu verfassen. Entgegen seinen Aussagen erging seitens des Bundesrats jedoch nie ein entsprechender Auftrag.

Dieser Bericht wurde vom VBS auf den 11. April 2013 fertig gestellt und dem Bundesrat für die Sitzung des 24. Aprils 2013 als blosse Informationsnotiz vorgelegt. Am 30. April 2013 wurde der Bericht anlässlich einer Pressekonferenz des VBS veröffentlicht.

Das VBS kam zum Schluss, dass der NDB «bei Weitem nicht die einzige Dienststelle der Bundesverwaltung [sei], die über besonders schützenswerte Daten verfüg[e]» und es müsse «auch bei einem Datendiebstahl bei einer anderen Dienststelle von einem beträchtlichen Schadenspotenzial ausgegangen werden».[20] Das VBS zeigte sich überzeugt, dass der NDB mit den 40 im Nachgang zum Datendiebstahl getroffenen Massnahmen Grundlagenarbeit geleistet habe, die für die gesamte Bundesverwaltung von Nutzen sein könnte. Das VBS schlug sogar vor, zu prüfen, inwieweit diese Massnahmen auch ausserhalb des NDB umgesetzt werden sollten.

In den Unterlagen, die dem Schlussbericht des VBS zugrunde liegen, finden sich keine konkreten Angaben zum Schadenspotenzial in der Informatik der Bundesverwaltung. Die GPDel schliesst aber nicht aus, dass einzelne der vom NDB beschlossenen Massnahmen auch der Verbesserung der Informatiksicherheit bei der einen oder anderen Bundesstelle dienen könnten. Die anderen Bundesstellen sollten aber nicht den Fehler des NDB wiederholen und sich primär auf eine Liste von Massnahmen fokussieren, ohne zuvor die relevanten Risiken identifiziert und bewertet zu haben. Erst danach ist zu entscheiden, welche Massnahmen geeignet sind und auch ergriffen werden sollen, um die erkannten Risiken zu verkleinern.

20 Bericht des VBS vom 11. Apr. 2013, S. 18.

10 Weiteres Vorgehen

Die Geschäftsprüfungsdelegation hat bereits am 3. Juli 2013 dem Bundesrat ihren vollständigen Inspektionsbericht zugestellt und ihn gebeten, zu diesem Bericht und den darin enthaltenen Empfehlungen bis Ende Oktober 2013 Stellung zu nehmen. Diese Empfehlungen wurden vollständig in der vorliegende Zusammenfassung des Berichts übernommen.

30. August 2013

Im Namen der Geschäftsprüfungsdelegation

Der Präsident:
Pierre-François Veillon, Nationalrat

Die Sekretärin:
Beatrice Meli Andres

Die Geschäftsprüfungskommissionen des Ständerats und des Nationalrats haben diesen Bericht zur Kenntnis genommen und seiner Veröffentlichung zugestimmt.

4. September 2013

Im Namen der Geschäftsprüfungskommissionen

Der Präsident der Geschäftsprüfungskommission des Ständerats:
Paul Niederberger, Ständerat

Der Präsident der Geschäftsprüfungskommission des Nationalrats:
Ruedi Lustenberger, Nationalrat

Die Sekretärin:
Beatrice Meli Andres

Abkürzungsverzeichnis

BBl	Bundesblatt
BInfV	Verordnung über die Informatik und Telekommunikation in der Bundesverwaltung (Bundesinformatikverordnung; SR *172.010.58*)
BJ	Bundesamts für Justiz
BPV	Bundespersonalverordnung vom 3. Juli 2001 (SR *172.220.111.3*)
BWIS	Bundesgesetz vom 21. März 1997 über die Massnahmen zur Wahrung der inneren Sicherheit (SR *120*)
DAP	Dienst für Analyse und Prävention
EDA	Eidgenössisches Departement für auswärtige Angelegenheiten
EFK	Eidgenössische Finanzkontrolle
EFV	Eidgenössische Finanzverwaltung
EJPD	Eidgenössisches Justiz- und Polizeidepartement
EPA	Eidgenössisches Personalamt
GPDel	Geschäftsprüfungsdelegation
GPK	Geschäftsprüfungskommissionen des National- und des Ständerates
FinDel	Finanzdelegation
IOS	Informations- und Objektsicherheit
IRB	Informatikrat des Bundes
ISB	Informatiksteuerungsorgan des Bundes
ISBD	Informatiksicherheitsbeauftragter des Departements
ISBO	Informatiksicherheitsbeauftragter der Organisation
ISchV	Verordnung vom 4. Juli 2007 über den Schutz von Informationen des Bundes (Informationsschutzverordnung; SR *510.411*)
ISDS-Konzept	Informationssicherheits- und Datenschutzkonzept
ISG	Informationssicherheitsgesetz (Entwurf)
ISV-NDB	Verordnung vom 4. Dezember 2009 über die Informationssysteme des NDB (SR *121.2*)
ND-Aufsicht	Nachrichtendienstliche Aufsicht
NDB	Nachrichtendienst des Bundes
NDBU	Abteilung Führungs- und Einsatzunterstützung des NDB
PSP	Personensicherheitsprüfungen
PSPV	Verordnung vom 19. Dezember 2001 über die Personensicherheitsprüfungen (SR *120.4*)
PSPV-VBS	Verordnung des VBS vom 12. März 2012 über die Personensicherheitsprüfungen (SR *120.423*)
SiA	Sicherheitsausschuss des Bundesrats
SiLAN	Sicherheits-LAN (Local Area Network)
SND	Strategischer Nachrichtendienst
SR	Systematische Rechtssammlung

VBS	Eidg. Departement für Verteidigung, Bevölkerungsschutz und Sport
V-NDB	Verordnung vom 4. Dezember 2009 über den Nachrichtendienst des Bundes
ZNDG	Bundesgesetz vom 3. Oktober 2008 über die Zuständigkeiten im Bereich des zivilen Nachrichtendienstes (SR *121*)