Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für Verteidigung,
Bevölkerungsschutz und Sport VBS

Verhinderter Datenabfluss im Nachrichtendienst des Bundes

Bericht des VBS

11. April 2013

Inhaltsverzeichnis

1. Zusammenfassung 3
2. Auftrag Chef VBS 4
3. Ausgangslage und Diebstahl 4
3.1 Auftrag des NDB 4
3.2 Vorgeschichte des Datendiebstahls 5
3.3 Die Ereignisse von Ende Mai 2012 6
4. Reaktion des NDB nach dem Diebstahl 9
4.1 Massnahmen des NDB 9
4.2 Personelle Ressourcen im NDB 10
4.3 Risikomanagement 11
4.4 Kommunikation 11
5. Ergebnisse der in Auftrag gegebenen Überprüfungen 13
5.1 Nachrichtendienstliche Aufsicht 13
5.2 Informations- und Objektsicherheit VBS (IOS VBS) 14
5.3 Neues Bundesgesetz über die Informationssicherheit 15
5.4 Externe Überprüfung der ND-Aufsicht 16
6. Fazit und Empfehlungen für das weitere Vorgehen 18

1. Zusammenfassung

Im Mai 2012 hat ein Mitarbeiter des Nachrichtendienstes des Bundes (NDB) trotz bestehender Sicherheits- und Schutzmassnahmen eine beträchtliche Menge an klassifizierten Daten gestohlen und diese ausserhalb der Räumlichkeiten des NDB verbracht. Es handelte sich dabei um einen Systemspezialisten, der seit einiger Zeit mit der Integration in sein berufliches Umfeld Mühe bekundete, Führungsentscheide nur schwierig akzeptierte und längere gesundheitsbedingte Abwesenheiten aufwies. Bereits vor dem Diebstahl hat sich der NDB intensiv um diesen problematischen Mitarbeiter bemüht und alles unternommen, um ihn in seiner schwierigen persönlichen Situation zu unterstützen.

Dank seinem guten Beziehungsnetz mit der Privatwirtschaft erfuhr der NDB umgehend vom Vorfall und konnte mit den beigezogenen Strafverfolgungsbehörden eine allfällige Datenweitergabe verhindern. VBS und NDB haben nach Bekanntwerden des Diebstahls sofort alle zuständigen Behörden informiert (Bundespräsidentin, Bundesanwaltschaft, Geschäftsprüfungsdelegation, Bundesrat).

Es sind keine Daten des NDB in unbefugte Hände gelangt. Ohne rasches und konsequentes Handeln innerhalb und ausserhalb der Verwaltung wäre es jedoch möglich gewesen, dass nachrichtendienstliche Daten an Dritte im In- und Ausland oder an die Öffentlichkeit hätten gelangen können.

Im Anschluss an die Ereignisse haben VBS und NDB ohne Verzug die notwendigen Führungsentscheide getroffen. Mehrere verwaltungsinterne und -externe Dienststellen und Expertengruppen wurden mit der Analyse der Situation und mit dem Aufzeigen des Handlungsbedarfs beauftragt.

In eigener Kompetenz hat der NDB 40 Massnahmen identifiziert und eingeleitet. Es handelt sich dabei um technische und organisatorische Massnahmen sowie um die Einschränkungen von Zugriffen und Zutritten. Das VBS hat auf seiner Ebene beschlossen, gemäss Antrag des NDB und Empfehlung der IOS die personellen Ressourcen im NDB aufzustocken. In den Bereichen Informatik und Sicherheit werden elf neue Stellen geschaffen. Ebenso wird auch die Nachrichtendienstliche Aufsicht im GS VBS personell und methodisch verstärkt. Es kann somit festgehalten werden, dass die für die wirksame Verhinderung der Wiederholung eines solchen Ereignisses notwendigen Massnahmen von den Verantwortlichen im NDB und im VBS ergriffen wurden.

Der Bundesrat hat als Folge des Datendiebstahls dem EFD den Auftrag erteilt, Informations- und Schulungsmassnahmen für das Bundeskader in den Belangen der Informationssicherheit durchzuführen. Weitere Verbesserungen bei der Sicherheit werden sich als Folge eines neuen Informationsschutzgesetzes ergeben, das zurzeit unter Führung des VBS erarbeitet und demnächst in die Vernehmlassung gegeben wird.

Aus Sicht des VBS kann abschliessend festgehalten werden, dass die notwendigen Massnahmen als Folge des Datendiebstahls sehr rasch ergriffen und umgesetzt wurden und weiterhin werden. Da die Weitergabe der Daten verhindert werden konnte, ist für die Schweiz und ihre Sicherheit keinerlei Schaden entstanden.

2. Auftrag Chef VBS

Am 21. Januar 2013 hat der Chef VBS den Chef Stab Chef VBS damit beauftragt, mit dem hier vorliegenden Bericht die Ereignisse und die daraufhin eingeleiteten bzw. noch einzuleitenden Massnahmen darzustellen. Der Bericht legt die Vorgänge vor, während und nach dem Diebstahl wie auch die Ergebnisse der im Nachgang angeordneten Überprüfungen umfassend dar.

3. Ausgangslage und Diebstahl

3.1 Auftrag des NDB

Der Nachrichtendienst des Bundes (NDB) ist eine als Bundesamt organisierte Dienststelle der zentralen Bundesverwaltung, die nachrichtendienstliche Aufgaben im Bereich der inneren und äusseren Sicherheit wahrnimmt. Damit sollen frühzeitig Gefährdungen durch Terrorismus, verbotenem Nachrichtendienst und gewalttätigem Extremismus erkannt und bekämpft werden. Ebenso hat sich der NDB mit Vorbereitungen zu verbotenem Handel mit Waffen und radioaktiven Materialien sowie zu verbotenem Technologietransfer zu befassen. Zur Darstellung der Lage der inneren Sicherheit betreibt der NDB ein elektronisches System (Lagedarstellung). Dieses dient den zuständigen Behörden von Bund und Kantonen als Führungsinstrument und zur Verbreitung von Informationen im Hinblick auf die Steuerung und Umsetzung von sicherheitspolizeilichen Massnahmen. Die Kantone haben dem NDB unaufgefordert Meldung zu erstatten, wenn sie konkrete Gefährdungen der inneren oder äusseren Sicherheit feststellen.

Der NDB hat auch den Auftrag, sicherheitspolitisch bedeutsame Informationen über das Ausland zu beschaffen, zu dokumentieren und auszuwerten. Der Dienst sorgt für eine umfassende Beurteilung der Bedrohungslage und pflegt weltweit Kontakte zu über 100 Nachrichten-, Polizei- und Sicherheitsdiensten. Diese Kontakte sind alle vom Bundesrat genehmigt.

In Erfüllung dieser Aufgaben ist der NDB von Gesetzes wegen befugt, Personendaten einschliesslich besonders schützenswerter Personendaten und Persönlichkeitsprofile zu bearbeiten, auch ohne Wissen der betroffenen Personen.

NDB 2010 entstanden

Der NDB existiert in seiner heutigen Form seit dem 1. Januar 2010. Vorher waren die Aufgaben auf den Dienst für Analyse und Prävention (DAP, bis Ende 08 im EJPD) und den Strategischen Nachrichtendienst (SND, VBS) aufgeteilt. Seine gesetzlichen Grundlagen findet der NDB insbesondere im Bundesgesetz vom 3. Oktober 2008 über die Zuständigkeiten im Bereich des zivilen Nachrichtendienstes (ZNDG, SR 121) und im Bundesgesetz vom 21. März 1997 über Massnahmen zur Wahrung der inneren Sicherheit (BWIS, SR 120). Diese Rechtsgrundlagen sollen abgelöst werden durch ein neues Nachrichtendienstgesetz, welches sich bis am 30. Juni 2013 in der Vernehmlassung befindet.

Die parlamentarische Oberaufsicht über den NDB wird durch die Geschäftsprüfungsdelegation wahrgenommen. Als verwaltungsinterne Instanz überprüft die Nachrichtendienstliche Aufsicht im Auftrag des Chefs VBS die Tätigkeit des NDB auf Rechtmässigkeit, Zweckmässigkeit und Wirksamkeit.

3.2 Vorgeschichte des Datendiebstahls

Zur Erfüllung der diversen Aufgaben betreibt der NDB eine Vielzahl von zum Teil komplexen Datenbanken und Informationssystemen, aus Sicherheitsgründen zu einem grossen Teil in einem abgeschotteten Netzwerk. Dafür unterhält er einen internen Informatikdienst.

Der Mitarbeiter X, der in der Informatik des NDB eine zentrale Funktion inne hatte, missbrauchte im Frühjahr 2012 den ihm durch seine Arbeit zustehenden Zugriff auf Daten des NDB zum Herunterladen umfangreicher Datensätze. X war seit dem 1. April 2007 als Datenbankspezialist im SND und anschliessend im NDB tätig. Nach seinem Eintritt erfolgte ordnungsgemäss eine Personensicherheitsprüfung gemäss Art. 11 der Verordnung vom 4. März 2011 über die Personensicherheitsprüfungen (PSPV, SR 120.4), welche mit einer positiven Risikoverfügung abgeschlossen wurde. Seit 2008 traten bei X zunehmend krankheitsbedingte Absenzen auf, welche auf den Informatikbetrieb nicht ohne Auswirkungen blieben. Im Jahr 2009 bewarb sich X auf eine Kaderstelle im Informatikbereich des NDB. Ihm wurde aber ein anderer Mitarbeiter des NDB vorgezogen. Die Einbindung von X in das IKT-Team gestaltete sich in der Folge als zunehmend schwierig. Der hoch spezialisierte und sehr kompetente Individualist grenzte sich gegenüber Kollegen und Vorgesetzten zunehmend ab.

Die Häufung der gesundheitlich bedingten Absenzen veranlassten die Vorgesetzten von X, im Jahr 2011 eine vertrauensärztliche Abklärung in die Wege zu leiten. Die Abklärungen ergaben, dass in Zukunft Arbeitsfähigkeit und Berufstauglichkeit nicht beeinträchtigt sein würden. Arbeits- oder Berufsprobleme hätten keine Auswirkungen auf die Gesundheit von X. Der NDB hatte somit keinerlei Anlass, von einer grundsätzlichen gesundheitlichen Beeinträchtigung von X auszugehen. Dennoch hielten die gesundheitlichen Probleme trotz einer vorübergehenden Besserung an. Zudem zeichneten sich zunehmend Spannungen zwischen X und seinem direkten Vorgesetzten ab. Klärende Gespräche ermöglichten nur kurzzeitig eine Normalisierung des Verhältnisses. Die Abwesenheiten häuften sich ebenso wie sich die Bedenken der Vorgesetzten akzentuierten.

Angespannte persönliche Situation

In dieser angespannten persönlichen Situation wurde am 10. Februar 2012 die nach fünf Jahren fällige Erneuerung der Personensicherheitsprüfung im Einklang mit den Grundsätzen des NDB auf einer höheren Stufe eingeleitet. Gemäss Art. 12 der PSPV sollte eine erweiterte Sicherheitsprüfung mit Befragung durchgeführt werden.

Am 16. April 2012 wurde X von seinem Arzt zu 100 % krankgeschrieben. Daraufhin erging der Auftrag des Chefs Führungs- und Einsatzunterstützung (NDBU) an die Informatik NDB abzuklären, inwieweit das Verhalten von X ein Risiko für den Betrieb und die Sicherheit des

NDB darstelle und mit welchen Massnahmen man diesen begegnen könne. Diese Abklärung, die am 27. April vorlag und am 7. Mai aktualisiert wurde, hielt fest, dass X immer stärkere Abgrenzungstendenzen gegenüber seinen Kollegen und Vorgesetzten zeigte. Weiter wurde festgehalten, dass X durch seine Fachkompetenz als einziger Mitarbeiter des NDB über sehr spezifische Kenntnisse über den Betrieb wichtiger Datenbanken des NDB verfügte. Sollte X weiter unter Druck kommen, seien seine Zugänge zu den Datenbanken zu sperren. Dies zum Schutz des Datenbankbetriebs sowie des Mitarbeiters vor Affekthandlungen.

Am 10. Mai 2012 kamen die Vorgesetzten von X unter der Führung des Chefs NDBU zum Schluss, dass er zu einem Gespräch vorzuladen sei und die von ihm erstellten Datenbankscripts analysiert werden sollen. Am 16. Mai sowie am 18. Mai 2012 erschien X nicht zu den vorgeschlagenen Gesprächsterminen.

Vor dem Datendiebstahl war es schwierig, die spätere Eskalation und die Reaktion von X zu erkennen. Dies insbesondere, weil die verschiedenen Abklärungen zu unterschiedlichen Aussagen führten (vertrauensärztliches Gutachten vs. Erfahrungen am Arbeitsplatz). Die persönliche Situation und die Absichten von X waren schwierig zu beurteilen, auch wenn der NDB sich sehr darum bemüht hat, das Gespräch mit dem Betroffenen zu suchen. Die Handlungsoptionen waren durch das Personalrecht des Bundes begrenzt.

3.3 Die Ereignisse von Ende Mai 2012

Am 18. Mai 2012 wurde ein Mitarbeiter des NDB über einen bestehenden Informationskanal von Seiten einer Grossbank telefonisch darüber orientiert, dass ein Herr X bei einer Filiale dieser Bank ein Nummernkonto eröffnen wolle. Als Grund für die Kontoeröffnung gab er an, eine grössere Summe aus Verkäufen von Bundesdaten zu erwarten. Als X vom Bankmitarbeiter darauf hingewiesen wurde, dass Gelder aus kriminellen Aktivitäten von der Bank nicht akzeptiert würden und X seinen Vorgesetzten informieren müsse, antwortete dieser, dass sein Vorgesetzter nicht im Bild sei. Von Seiten der Bank wurde klar festgehalten, dass die Eröffnung eines Nummernkontos nur dann möglich sei, wenn die einbezahlten Beträge deklariert seien und nicht aus illegalen Aktivitäten stammten.

Umgehend wurden von der Führung des NDB die notwendigen Schritte eingeleitet, um die Person, welche auf der Bank vorgesprochen und sich als X ausgegeben hatte, als ebendiese Person und somit als Mitarbeiter des NDB zu identifizieren. Dies nahm einige Tage in Anspruch, da eine Identifizierung aufgrund eines übermittelten Fotos zunächst nicht möglich war. Aufgrund der Bilder der Videoüberwachung der Bank konnte X am 23. Mai schliesslich eindeutig von einem seiner Vorgesetzten identifiziert werden.

Umgehende Reaktion

Am Abend des 23. Mai beauftragte der Direktor des NDB den Chef NDBU, bis am darauffolgenden Tag um 12.00 Uhr eine Auslegeordnung zu erstellen und Antrag zum weiteren Vorgehen zu stellen. Oberstes Ziel sei die Sicherung der Daten des NDB und damit das Ab-

wenden von möglichem Schaden für die Schweiz. Es seien Sofortmassnahmen einzuleiten und eine Besprechung mit der Bundesanwaltschaft anzusetzen. Die schriftliche Dokumentation des Falls und der in der Folge ergriffenen Massnahmen sei lückenlos sicherzustellen.

Am Vormittag des 24. Mai zeigte die Überprüfung der Datenbankscripts, dass womöglich mehrere Tausend Dateien auf externe Datenträger exportiert wurden.

Sofortige Information

Gleichentags um 12.30 Uhr informierte der Direktor des NDB zusammen mit seinem Stellvertreter und dem Chef NDBU den Chef VBS und die Generalsekretärin VBS über die Lage und die Ereignisse. Der Chef VBS informierte noch gleichentags die Bundespräsidentin und bei nächster Gelegenheit, anlässlich seiner Sitzung vom 1. Juni, den Bundesrat. Die Informationen wurden zur Kenntnis genommen, ohne dass ihnen weitere Folge gegeben worden wäre.

Am Abend des 24. Mai stand schliesslich zweifelsfrei fest, dass eine beträchtliche Datenmenge exportiert wurde, die einem sehr tiefen einstelligen Prozentsatz des gesamten Datenbestandes des NDB entspricht. X konnte eindeutig als zugreifende Person identifiziert werden. Dabei hatte er verhindert, dass sein Datenexport für die anderen Mitarbeiter der Informatikabteilung erkennbar wurde. Mit seinem Vorgehen verschaffte sich X unerlaubterweise eine grosse Menge an Daten des NDB. Er nützte sein umfassendes Wissen, das in ihn gesetzte Vertrauen sowie die ihm zugeteilten Zugriffsrechte aus, um widerrechtlich Daten zu kopieren und zu exportieren.

Anzeige bei Bundesanwaltschaft

Am späten Abend des 24. Mai wurde der Fall durch den Direktor NDB dem Bundesanwalt dargelegt. Am 25. Mai reichte der NDB bei der Bundesanwaltschaft eine Strafanzeige ein, in der auch festgehalten wurde dass die Sicherstellung der Daten und die Abwendung von Schaden für die Schweiz absoluten Vorrang haben. Am Abend des 25. Mai wurde X verhaftet. Dabei konnten die Datenträger vollständig sichergestellt werden. Noch am selben Wochenende wurden sie überprüft. Dabei stellte sich heraus, dass die kopierten Daten vollständig vorhanden waren. Am 27. September 2012 wurde von der Bundesanwaltschaft öffentlich bekannt gegeben, dass X bereits konkrete Vorbereitungen für einen Datenverkauf getroffen hatte. Ebenso wurde von den Strafverfolgungsbehörden bekannt gegeben, dass es keine Hinweise gebe, dass die entwendeten Daten kopiert oder weitergegeben worden seien. Dem NDB wurde von der Bundesanwaltschaft aber keine Einsicht in die sichergestellten Daten gewährt. Das von der Bundesanwaltschaft eröffnete Verfahren gegen X läuft nach wie vor.

Am 30. Mai 2012 informierte der Direktor NDB den Präsidenten der Geschäftsprüfungsdelegation sowie den Chef der Nachrichtendienstlichen Aufsicht im GS VBS über den Vorfall. Im Verlauf des Juni kam es zu mehreren Kontakten des Direktors NDB mit dem Präsidenten der Geschäftsprüfungsdelegation.

Fristlose Kündigung

Am 4. September 2012 wurde dem fehlbaren Mitarbeiter X die geplante fristlose Kündigung angezeigt, wobei die Möglichkeit einer gegenseitigen Vereinbarung offen gelassen wurde. X lehnte eine solche Vereinbarung ab. Einen Tag nachdem die Bundesanwaltschaft öffentlich erklärte, dass X bereits konkrete Vorbereitungen für einen Datenverkauf getroffen hatte, wurde ihm am 28. September erneut die fristlose Kündigung angezeigt, allerdings ohne Möglichkeit zu einer Vereinbarung. X bestand jedoch darauf, dass das Arbeitsverhältnis weiterzuführen sei, weil kein Kündigungsgrund vorliege. Schliesslich wurde am 10. Oktober 2012 die fristlose Kündigung ausgesprochen. X hat gegen diese Kündigung eine Beschwerde eingereicht.

Es kann festgehalten werden, dass das Hauptziel erreicht wurde, die gestohlenen Daten sicherzustellen, deren Abfluss zu verhindern und so das Auftreten eines Schadens für die Schweiz abzuwenden. Dank dem guten Beziehungsnetz und dem entschlossenen Handeln des NDB wurden in der Krise die richtigen Massnahmen ergriffen. Die zuständigen Behörden wurden umgehend informiert.

4. Reaktion des NDB nach dem Diebstahl

4.1 Massnahmen des NDB

Bereits am 1. Juni 2012 stellte der Chef NDBU dem Direktor NDB Anträge zum weiteren Vorgehen und für Sofortmassnahmen. Es ging dabei insbesondere um die Verbesserung der Kontrolle über Importe und Exporte in die Datensysteme des NDB. Eine externe Stelle solle beauftragt werden, die Sicherheitsprozesse innerhalb der Informatik NDB zu überprüfen und Massnahmen vorzuschlagen. Die Anträge wurden genehmigt und durch einen weiteren Auftrag ergänzt.

Am 12. Juli 2012 wurden dem Direktor NDB vom Chef NDBU 17 kurz-, mittel- und langfristige Massnahmen zur Erhöhung der IKT-Sicherheit unterbreitet. Dabei ging es insbesondere um die Risikoreduktion für unerlaubtes Entfernen bzw. die Mitnahme grosser Datenmengen. In einem zweiten Schritt wurden die Massnahmen anfangs Oktober auf 27 erhöht. Per 5. November legte der NDB schliesslich insgesamt 40 Massnahmen als Reaktion auf den Datendiebstahl vor.

Die 40 vom NDB eingeleiteten und teilweise bereits umgesetzten Massnahmen können hier aus Gründen der Geheimhaltung nicht detailliert aufgeführt werden. Es handelt sich um Massnahmen in den Bereichen Organisation, Zugriffe/Zutritte, Technik und Führung.

Bildung einer Task Force

Innerhalb des NDB wurde im Nachgang zum Datendiebstahl nach verschiedenen internen Abklärungen vom Direktor NDB am 28. September 2012 eine Task Force eingesetzt. Dies bedingte eine breitere interne Information und wurde möglich, nachdem der Fall durch die Medien bekannt gemacht worden war. Die Task Force löste die bestehende Arbeitsgruppe ab. Der Chef VBS wurde vom NDB regelmässig über die Aufarbeitung des Falls informiert.

Zur besseren Aufarbeitung des Vorfalles hat der NDB am 30. Oktober bei der Bundesanwaltschaft einen Antrag auf forensische Spiegelung, also auf die Zurverfügungstellung einer Kopie der entwendeten Daten gestellt. Ebenso hat die NDA ein Gesuch auf Akteneinsicht gestellt. Beide Begehren wurden von der Bundesanwaltschaft aus strafprozessualen Gründen abgelehnt.

Neue Weisungen über Sicherheits- und Kontrollmassnahmen

Schliesslich hat der Direktor des NDB am 13. Dezember 2012 neue „Weisungen über Sicherheits- und Kontrollmassnahmen im NDB“ erlassen. Damit wurden im Sinne einer Übergangsregelung bis zum Inkrafttreten des sich zurzeit in der Vernehmlassung befindenden neuen Nachrichtendienstgesetzes wichtige Anordnungen zur Gewährleistung der Sicherheit von Informationen und Einrichtungen des NDB erteilt. Festgelegt wird dort, dass der Leistungserbringer des NDB beim Gebrauch der Informatikmittel die Nutz- und Randdaten (Datenfluss, Datentransfers, Datensicherung, Zugriff auf Daten, erfolgte Ausdrucke) automatisch aufzeichnet. Damit wird die Rückverfolgbarkeit der Nutzung der Informatikmittel sichergestellt.

Die Weisungen beinhalten auch die Möglichkeit von namentlichen personenbezogenen Auswertungen für allfällige Abklärungen eines konkreten Verdachts auf Missbrauch der elektronischen Infrastruktur bzw. zur Abwehr konkreter Gefährdungen der Informatik-Infrastruktur. Im Rahmen von Personen- und Taschenkontrollen kann der NDB neu bei seinen Mitarbeiterinnen und Mitarbeitern Datenträger wie Computer, CD, DVD, Memory Sticks, Aufnahmegeräte, Kameras, Mobiltelefone oder Papierdokumente auf klassifizierte Inhalte überprüfen. Im Eingangsbereich der ständigen Standorte des NDB wurden abschliessbare Behältnisse für die Lagerung von privaten Gegenständen (z.B. Mobiltelefone) während des Aufenthalts an diesen sensiblen Standorten zur Verfügung gestellt. Vor dem Verlassen der Standorte können Taschen und andere mitgeführte Gegenstände durchsucht werden. Ebenso sind Personenkontrollen bis hin zum Abtasten des Körpers möglich.

Die Mitarbeiterinnen und Mitarbeiter müssen auf Verlangen verschlossene Behältnisse oder elektronische Datenträger öffnen, so dass deren Inhalte kontrolliert werden können. Zur Sicherstellung der so genannten Clean Desk Policy, d.h. dem Wegschliessen klassifizierter Informationen am Arbeitsplatz, kann der NDB in seinen Einrichtungen Raumkontrollen durchführen, was allerdings bereits vor dem Vorfall so gehandhabt wurde. Zur Überwachung von Archiv-, Tresor-, Server- und Lagerräumen sowie von einzelnen Tresoren können Videokameras eingesetzt werden.

Ebenso werden neu auch stichprobenweise Fahrzeugkontrollen ermöglicht. Für besonders schützenswerte Räume hat der Chef Führungs- und Einsatzunterstützung NDB ein formelles Verbot für das Mitführen von Mobiltelefonen, Tablets, Fotoapparaten und ähnlichen Geräten erlassen. Mit dieser Vielfalt von Anordnungen wird eine wesentliche Verbesserung des Informationsschutzes im NDB erreicht.

Der NDB hat alle in seiner Kompetenz stehenden Massnahmen rasch ergriffen. Die Massnahmen ermöglichen eine wesentliche Verbesserung der Sicherheit in allen Belangen und reduzieren das Risiko eines weiteren derartigen Datendiebstahls substanziell.

4.2 Personelle Ressourcen im NDB

Der Datendiebstahl hat aufgezeigt, dass die personellen Ressourcen im Bereich Informatik des NDB zu knapp bemessen sind. Ein Grund dafür ist die Tatsache, dass anlässlich der Überführung vom EJPD ins VBS des unterdessen im NDB integrierten ehemaligen Dienstes für Analyse und Prävention DAP auf den Transfer insbesondere von Informatik-, Sicherheits- und Personalmitarbeitenden weit gehend verzichtet wurde. Somit stand der NDB 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. Darauf hat der NDB in der Vergangenheit wiederholt hingewiesen, unter anderem im Schlussbericht vom 27. Mai 2011 zur Massnahme „Erschliessung von Synergiepotenzialen bei den zivilen Nachrichtendiensten“ im Rahmen der Aufgabenüberprüfung des Bundes.

Insgesamt wurde vom NDB per Ende 2012 ein Bedarf von insgesamt zwölf zusätzlichen Stellen in den Bereichen Informatik, Sicherheit und Personal angemeldet. Vom VBS wurden elf Stellen bewilligt, und zwar für die Bereiche Datenbankadministration, Netzwerkbetrieb und -überwachung, Betrieb der Anwendungs- und Kommunikationssysteme, Mail-Infrastruktur, Informatiksicherheit und integrale Sicherheit. Nicht bewilligt wurde eine Stelle im Personalbereich.

Mit den zusätzlichen Stellen können sicherheitskritische Leistungen weitestgehend durch interne Mitarbeitende erbracht werden. Aufgestaute Migrationsprojekte können realisiert werden. In der Informatik- und Betriebssicherheit können fehlende Fähigkeiten aufgebaut und Redundanzen geschaffen werden. Das Vier-Augen-Prinzip kann insbesondere in besonders sicherheitskritischen Aktivitäten während den erweiterten Betriebszeiten permanent gewährleistet werden.

Die personelle Verstärkung im NDB ermöglicht eine erhöhte Qualität und Sicherheit des Informatikeinsatzes.

4.3 Risikomanagement

Bereits seit dem März 2010 verfügt der NDB über ein genehmigtes Dokument zu Schutz und Sicherheit. Dies bildete die Grundlage des Risikomanagements des NDB. In diesem Dokument wurden die Hauptrisiken identifiziert sowie Methoden, Prozesse und Strukturen beschrieben, wie mit diesen Risiken umzugehen ist. Massnahmen zum Zweck der Minderung der verschiedenen Risiken wurden bereits vor dem Datendiebstahl identifiziert und umgesetzt. Nach dem Datendiebstahl wurden die Prozesse und Massnahmen einer detaillierten Analyse unterzogen und Anpassungen vorgenommen. Neben den zusätzlich getroffenen Massnahmen zur Erhöhung der Sicherheit wurde auch die Integration des Risikomanagements in das Amtscontrolling verbessert. In einem neu zu erstellenden Dokument zum Risikomanagement NDB soll die Verknüpfung der einzelnen Ebenen des Risikomanagements festgelegt werden. Daneben wurden auch die Kontrollen inhaltlich und in ihrer Frequenz erhöht.

4.4 Kommunikation

Bereits unmittelbar nach dem Datendiebstahl erhielt die Vorbereitung der internen und externen Kommunikation über die Ereignisse ein hohes Gewicht in der Zusammenarbeit zwischen dem Chef VBS und dem Direktor NDB. Anfänglich wurde bewusst auf eine Kommunikation verzichtet, handelte es sich doch um ein laufendes Verfahren und entstand durch das Verhindern der Datenweitergabe kein Schaden für die Schweiz. In Absprache und auf Empfehlung der Strafverfolgungsbehörden war es stets das Ziel, den Vorfall nicht publik zu machen.

Es wurden stets verschiedene Varianten für die Kommunikation evaluiert. Aus Vertraulichkeitsgründen – man war sich der Gefahr von Indiskretionen bewusst – wurden dazu keinerlei schriftliche Planungen erstellt oder anderweitige Aufzeichnungen gemacht. Massnahmen für den Fall des Bekanntwerdens einer Quelle gehören zu den essenziellen Aufgaben der Quellenführung und mussten nicht gesondert vorbereitet werden. Dass die Daten selber an die Öffentlichkeit gelangen, konnte bis zum heutigen Tag erfolgreich verhindert werden.

Nachdem das VBS Hinweise auf Rechercheaktivitäten der Medien erhielt, wurde der Beschluss gefasst, aktiv zu kommunizieren. Am 26. September 2012 veröffentlichte das VBS eine Medienmitteilung, in der über den Datendiebstahl, die rasche Reaktion des VBS sowie die vollumfängliche Sicherstellung und die Verhinderung des Datenabflusses informiert wurde. Auf Wunsch der Geschäftsprüfungsdelegation wurde ihr die Medienmitteilung vor der Veröffentlichung zur Stellungnahme vorgelegt. In der Folge hat das VBS gemäss der Rückmeldung der Geschäftsprüfungsdelegation die Medienmitteilung abgeändert.

5. Ergebnisse der in Auftrag gegebenen Überprüfungen

5.1 Nachrichtendienstliche Aufsicht

Die Nachrichtendienstliche Aufsicht (NDA) ist eine verwaltungsinterne Dienststelle, welche das Handeln des NDB auf die Einhaltung der verfassungsrechtlichen und gesetzlichen Vorgaben (Rechtmässigkeit), auf die Eignung und Angemessenheit der nachrichtendienstlichen Tätigkeit (Zweckmässigkeit) und auf ihre Zielerreichung (Wirksamkeit) überprüft. Die NDA arbeitet direkt im Auftrag des Chefs VBS und gehört zum Generalsekretariat VBS.

Nach Kenntnisnahme eines Berichts des NDB zum Datendiebstahl hat der Chef VBS bei der NDA am 24. August 2012 einen Bericht zu folgenden Punkten in Auftrag gegeben: Einhaltung der relevanten Vorschriften und Weisungen, Würdigung des Handelns des NDB vor, während und nach den Vorkommnissen um den Datendiebstahl, Beurteilung der getroffenen und geplanten Massnahmen sowie Risikomanagement des NDB. Schliesslich sollte die NDA allfällige weitere Massnahmen empfehlen, die zur Minimierung der Risiken zu ergreifen sind.

Nicht primär Sicherheitsvorfall

Die NDA hat den Chef VBS in der Folge mehrere Male mündlich über ihre Zwischenergebnisse orientiert. In ihrem Schlussbericht vom 30. November 2012 stellt die NDA fest, dass es sich beim Vorfall nicht primär um einen informationstechnischen Sicherheitsvorfall handelt, sondern um eine zögerliche Reaktion in der Personalführung. Die Absichten von X seien aber schwierig zu beurteilen und die personalrechtlichen Handlungsoptionen begrenzt gewesen. Die NDA ortet Mängel beim Risikomanagement des NDB. Es fehle eine bereichsübergreifende Verknüpfung von strategischen und operativen Risiken und die formelle Bezeichnung der für die Risiken und Kontrollen verantwortlichen Personen stehe aus. Die koordinierte Führung eines bereichsübergreifenden Risikomanagement-Prozesses sei wichtig für die Identifikation und Pflege von Risiken. Physische Kontrollen wie die Inspizierung von Büroräumlichkeiten auf der Basis von Stichproben seien bis anhin nur punktuell vorgenommen worden. Zur Behebung dieser Mängel seien die Bereiche Sicherheit und IKT im NDB personell zu verstärken.

Die NDA hat dem Chef VBS fünf Empfehlungen zu Handen des NDB unterbreitet:

- Ausbau des Dispositivs im Bereich Risikomanagement (konsequente Analyse und Bewertung relevanter Risiken, Verknüpfung über die verschiedenen Risikoebenen sowie Formulierung entsprechender Gegenmassnahmen; Ausbau der Sicherheit NDB und von IKT NDB).
- Überprüfung der Positionierung der Sicherheit NDB in der Hierarchie des Dienstes. Die Sicherheit NDB muss ihre wichtige Funktion im ganzen Dienst unabhängig und wirksam wahrnehmen können.
- Frühzeitiges und konsequentes Handeln bei schwierigen Personalfällen, verstärkter Einbezug von Personal- und Rechtsdienst.
- Erhöhung der physischen Sicherheit.
- Einführung eines formellen Änderungswesens für Anpassung bestehender und Einführung neuer Software-Applikationen.

Der Chef VBS hat diese Empfehlungen dem NDB zur Implementierung weitergeleitet. Sie befinden sich in der Umsetzung.

5.2 Informations- und Objektsicherheit VBS (IOS VBS)

Bei der IOS handelt es sich um eine Dienststelle des VBS, die mit der umfassenden Gewährleistung der Sicherheit (Personen-, Informations-, Sachwert- und Umweltsicherheit) betraut ist. Entsprechend werden auch die IKT-Sicherheitsvorgaben durch das VBS hauptsächlich durch die IOS erlassen.

Am 23. Oktober 2012 beauftragte der Chef VBS die IOS mit der Erarbeitung konkreter Vorschläge für die personelle Verstärkung des NDB im IKT-Sicherheitsbereich, für die Verbesserung der Reaktionsfähigkeit des NDB und für zusätzliche technische Lösungen zur Erhöhung der Sicherheit im NDB.

Gegenüber dem VBS hielt die IOS fest, dass die Umsetzung der departementalen Weisungen über die Informatiksicherheit im NDB nicht lückenlos erfolgte. Die aus dem EJPD übernommenen DAP-Systeme seien sicherheitsmässig unzureichend ins VBS überführt worden. Im Bereich IKT verfüge der NDB nicht über genügend Ressourcen, was ein effizienteres Sicherheitshandling verhindere. Bereits per 1. November 2012 wurde zur Verbesserung dieser Situation vom NDB ein IKT-Sicherheitsbeauftragter (100 %) eingesetzt. Weiter monierte die IOS, der Umsetzungsstand der Rechtsgrundlagen Bund vom NDB sei umgehend zu verbessern. Die IOS stellt fest, dass der NDB dazu bereits Sofortmassnahmen eingeleitet habe.

IOS ortet personellen Mehrbedarf

Den gesamten personellen Mehrbedarf in den Bereichen Sicherheit und IKT des NDB beziffert die IOS auf 7-12 Vollzeitstellen. Damit solle bei kritischen Funktionen eine Redundanz aufgebaut werden, was die sofortige Reaktion auf Unregelmässigkeiten und die Umsetzung des Vier-Augen-Prinzips ermögliche. Weiter brauche es arbeitsrechtliche Möglichkeiten um gefährdete Personen bei Bedarf sofort von sicherheitskritischen Arbeiten zu entbinden. Schliesslich brauche es konkurrenzfähige Arbeitsbedingungen, Verbesserungen bei den Führungsstrukturen und der Kultur sowie eine periodische Sensibilisierung und Ausbildung. Das Potenzial an technischen Lösungen sei nicht ausgeschöpft, allerdings sei eine vollständige Ausschöpfung fast nicht finanzierbar.

Die IOS hält auch fest, dass ein solcher Diebstahl auch in Zukunft nicht absolut zu vermeiden sei. Mit einem vernünftigen Mehraufwand könne aber die Eintretenswahrscheinlichkeit reduziert werden. Es sei allerdings zu vermeiden, dass als Folge einer Überdimensionierung der Sicherheitskontrollen im NDB eine Misstrauenskultur aufgebaut werde. Die Sicherheitsmassnahmen sollen bedrohungsbasiert, nachvollziehbar und transparent bleiben und müssten von der Geschäftsleitung mitgetragen und permanent durch das Management geprüft werden.

5.3 Neues Bundesgesetz über die Informationssicherheit

Am 12. Mai 2010 beauftragte der Bundesrat das VBS, im Rahmen einer interdepartementalen Arbeitsgruppe unter Mitwirkung insbesondere des EJPD, des EDA, des EFD und der BK ein Normkonzept und gestützt darauf formell-gesetzliche Grundlagen für den Informationsschutz des Bundes auszuarbeiten. Damit soll der Geltungsbereich der Informationsschutzregelungen auf alle Personen erstreckt werden, die vom Bund mit der Bearbeitung geschützter Informationen betraut werden. Weiteres Ziel des Gesetzgebungsprojekts ist die Schaffung einheitlicher formell-gesetzlicher Grundlagen für die Durchführung von Geheimschutzverfahren im militärischen und zivilen Bereich. Der Auftrag erging, weil der Bundesrat zum Schluss gekommen war, dass für die Durchsetzung eines koordinierten Informationsschutzes die mangelnde Kohärenz der bestehenden Rechtsgrundlagen ein wesentliches Problem darstellt.

Zur Umsetzung dieses Auftrags des Bundesrates bzw. zur Ausarbeitung eines entsprechenden Entwurfs für ein Bundesgesetz über die Informationssicherheit hat das VBS unter Leitung von Prof. Dr. iur. Markus Müller (Ordinarius für Staats- und Verwaltungsrecht, Universität Bern) eine Expertengruppe eingesetzt. Infolge des Datendiebstahls hat der Bundesrat am 24. Oktober 2012 den Auftrag an das VBS abgeändert. Neben einer Erweiterung der bestehenden Expertengruppe auf alle Departemente und der Bundeskanzlei wurde der Auftrag erteilt, die Gefahren im Bereich der Informationssicherheit im Bund zu analysieren und Lücken aufzuzeigen sowie Vorschläge für Sofortmassnahmen und für formell-gesetzliche Grundlagen zur Verbesserung der Informationssicherheit im Bund zu formulieren.

Zwischenbericht der Expertengruppe

Am 27. Februar 2013 hat das VBS dem Bundesrat einen entsprechenden Zwischenbericht dieser Expertengruppe zur Kenntnis gebracht. Dieser äussert sich nicht spezifisch zum NDB, sondern bezieht sich auf die gesamte Bundesverwaltung. Demnach besteht Handlungsbedarf in den Bereichen Führung, Organisation, Personal und Technik. Sofortigen Handlungsbedarf erkennen die Experten bei der Ausbildung und Sensibilisierung des Kaders der Bundesverwaltung (inkl. Top-Kader) in den Belangen der Informationssicherheit. Gut ausgebildete und sensibilisierte Führungskräfte sowie loyale und zufriedene Mitarbeitende seien die wirksamste Massnahme gegen die Gefahren durch Innentäter.

Entsprechend folgte der Bundesrat am 15. März 2013 dem Antrag des VBS, nahm Kenntnis vom Bericht und beauftragte das EFD in seiner Funktion als Dienststelle für Personalfragen, ab Oktober 2013 Informations- und Schulungsmassnahmen zur stufengerechten Ausbildung und Sensibilisierung des Bundeskaders in den Belangen der Informationssicherheit durchzuführen.

Weitere Verbesserungen bei der Sicherheit werden sich mit Inkrafttreten des neuen Bundesgesetzes über die Informationssicherheit ergeben.

5.4 Externe Überprüfung der ND-Aufsicht

Um im Anschluss an den Datendiebstahl eine möglichst umfassende Überprüfung aller relevanten Akteure im VBS sicherzustellen, hat der Chef VBS eine Aufgaben-, Organisations- und Leistungsüberprüfung der Nachrichtendienstlichen Aufsicht (NDA) in Auftrag gegeben. Auftragnehmer war Prof. Dr. iur. Heinrich Koller, ehemaliger Direktor des Bundesamtes für Justiz. Die Untersuchung hatte zum Inhalt, die Aufgaben der NDA nach geltendem Recht und den Vorgaben des Chefs VBS aufzuzeigen, die in der Praxis effektiv erfüllten Aufgaben darzulegen und die Leistungsfähigkeit der NDA zu beurteilen. Weiter war die Frage zu klären, ob in Bezug auf die Aufgaben, Zuständigkeiten und Organisation der NDA sowie auf Personalbestand, Anforderungsprofil und Pflichtenhefte der Mitarbeiter Änderungen nötig seien. Schliesslich sollte sich Prof. Koller auch zur Notwendigkeit einer Anpassung von Rechtsgrundlagen äussern.

Anfang April 2013 legte Prof. Koller sein Gutachten dem Chef VBS vor. Er kam darin zum Schluss, dass die NDA alle ihre Aufgaben bezüglich NDB pflichtbewusst und sorgsam erfüllt. Die drei Mitarbeiter der NDA seien in ihren jeweiligen Fachbereichen ausgewiesen. Personelle Veränderungen drängen sich nicht auf. Die bisherigen Rechtsgrundlagen reichten grundsätzlich aus und würden im neuen Nachrichtendienstgesetz sinnvoll ergänzt und präzisiert. Bezüglich der rechtlichen Verankerung der Unabhängigkeit der NDA sei eine Ergänzung erwünscht. Einschränkend stellt Prof. Koller fest, dass das Vorgehen der NDA nicht immer zielgerichtet und wegen der beschränkten Ressourcen nicht immer von der erforderlichen Tiefe war.

Personelle Verstärkung der Nachrichtendienstlichen Aufsicht

Dem VBS empfiehlt das Gutachten Koller, zur personellen Verstärkung der NDA umgehend eine vierte Stelle mit einem IKT-Spezialisten und/oder erfahrenen ND-Fachmann zu besetzen. Die Prüfungsmethodik sei zu verbessern, inkl. der Prüfung entsprechender Zertifizierungen. Nötig seien eine längerfristige Strategieentwicklung, die Identifikation der politischen Risiken, eine Definition der Hauptstossrichtungen sowie die Fokussierung auf die Interessen der Auftraggeber und Kunden. Durch die Sensibilisierung der Betroffenen für die Probleme und Risiken einer nachrichtendienstlichen Tätigkeit, die laufende methodische Weiterbildung und Schulung sei der Stellenwert der NDA zu erhöhen.

Die Kontakte der NDA zum Chef VBS seien regelmässig (minimal alle paar Wochen) zu pflegen und der Beizug zu den regelmässig stattfindenden Führungsgesprächen des Chefs VBS mit dem Direktor NDB zu prüfen. Die Berichterstattung der NDA sei durch regelmässige und laufende Informationen an den Chef VBS zu ergänzen. Die Empfehlungen der NDA seien rechtzeitig mit Zeitvorgaben anzuordnen oder begründet zurückzuweisen. Das gegenseitige Verständnis von Prüfern und Geprüften über die Aufgaben, Rollen, das Vorgehen und den Umgang mit den Ergebnissen sei zu verbessern. Schliesslich solle für die Mitarbeiterinnen und Mitarbeiter des NDB eine Stelle für „whistleblowing“ eingerichtet werden.

Die Empfehlungen aus dem Bericht von Prof. Koller wurden VBS-intern eingehend geprüft und ein Massnahmenplan zu deren Umsetzung dem Chef VBS unterbreitet. Es geht vor allem darum, die Funktion der Aufsicht als Kontroll- und Frühwarnorgan des Chefs VBS zu

verstärken, die Modalitäten der Berichterstattung an den Chef VBS (inhaltlich und zeitlich) zu verbessern und zu intensivieren, die Prüfungsmethodik, insbesondere durch eine gezielte Weiterbildung, zu optimieren, und die Aufsicht personell auszubauen. Der Chef VBS wird den Bericht und die entsprechenden Massnahmen mit der GPDel, auf Wunsch der Delegation, besprechen, bevor definitive Entscheide gefällt werden.

6. Fazit und Empfehlungen für das weitere Vorgehen

Durch rasches und entschlossenes Handeln konnte der NDB die Weitergabe der entwendeten Daten verhindern. Die notwendigen Massnahmen zur Aufarbeitung des Datendiebstahls und zur Erhöhung der integralen Sicherheit wurden verzugslos sowohl auf der Ebene des NDB als auch auf Ebene Departement und Bundesrat eingeleitet.

In Umsetzung befindet sich zurzeit noch ein Teil der 40 Massnahmen, die der NDB in eigener Kompetenz angeordnet hat. Ebenso ist der Prozess für die Besetzung der neuen Stellen beim NDB und bei der NDA noch im Gang. In Umsetzung befinden sich weiter auch die Empfehlungen der NDA sowie die Empfehlungen aus dem Bericht Koller zur NDA. Das neue Bundesgesetz über die Informationssicherheit, welches bereits vor dem Datendiebstahl in Auftrag gegeben wurde, erhält zusätzliche Elemente und wird beschleunigt erarbeitet. Bis Ende April 2013 liegt der Vernehmlassungsentwurf zu diesem Gesetz vor. Die vom Bundesrat in Auftrag gegebenen Informations- und Schulungsmassnahmen für das Bundeskader in den Belangen der Informationssicherheit werden ab Oktober 2013 umgesetzt.

Zu berücksichtigen ist, dass dieser Bericht dem Kenntnisstand des VBS von Anfang April 2013 entspricht. Eine abschliessende Beurteilung und Würdigung wird nach Vorliegen des Berichts der GPDel erfolgen.

Zu prüfen bleibt die verstärkte Ausrichtung des Risikomanagements des Bundes auf die Gefährdungen bei der Verwaltung sensibler Daten. Der NDB ist bei Weitem nicht die einzige Dienststelle der Bundesverwaltung, welche über besonders schützenswerte Daten verfügt und solche verwaltet. Möglicherweise ist der Spektakelwert bei einem Datendiebstahl im NDB höher, doch muss auch im Fall einer Entwendung bei einer anderen Dienststelle von einem beträchtlichen Schadenspotenzial ausgegangen werden. Diese Gefahren systematisch aufzuarbeiten und notwendige Massnahmen zu ergreifen, ist für die gesamte Bundesverwaltung angezeigt. Mit den 40 im Nachgang zum Datendiebstahl ergriffenen Massnahmen hat der NDB Grundlagenarbeit geleistet, die für die gesamte Bundesverwaltung von Nutzen sein könnte. So könnte geprüft werden, inwieweit diese Massnahmen auch ausserhalb des NDB umgesetzt werden sollten.

Auch was die Personensicherheitsprüfungen betrifft, besteht Prüfungsbedarf. Die Frage stellt sich, ob Personen mit Zugang zu besonders schützenswerten Personendaten auf einer höheren Stufe als bisher geprüft werden müssten und ob sich ein rascherer Prüfungsrhythmus aufdrängt. Auch wenn im hier dargelegten Fall des Datendiebstahls keine Hinweise dafür bestehen, dass eine erweiterte Personensicherheitsprüfung mit Befragung Vorbehalte gegen eine weitere Beschäftigung von X an den Tag gebracht hätte, trägt eine Intensivierung der Personensicherheitsprüfungen unzweifelhaft zur Erhöhung der Sicherheit und zur weiteren Minimierung der Risiken bei.

Aus Sicht des VBS kann abschliessend festgehalten werden, dass der NDB rasch, entschlossen und zielgerichtet reagiert hat. Die notwendigen Massnahmen wurden umgehend ergriffen und werden weiterhin umgesetzt. Es ist zu prüfen, inwieweit auch die übrigen Dienststellen der Bundesverwaltung ihr Risikomanagement ausbauen und entsprechende Massnahmen ergreifen sollten.