4.5 Inspektion zur Informatiksicherheit im NDB

5. Februar 2014

Nach ihren ersten Abklärungen zum Datendiebstahl, der im Mai 2012 im NDB vorgekommen war, beschloss die GPDel im Oktober 2012, diesen Vorfall weiter im Rahmen einer Inspektion über die Informatiksicherheit im NDB zu untersuchen.

Aufgrund ihrer Inspektion stellte die GPDel fest, dass der NDB als Organisation nicht genügend darauf ausgerichtet war, die Verfügbarkeit, die Integrität und die Vertraulichkeit der Daten als zentrale Zielsetzung der Informatiksicherheit zu gewährleisten. Als der NDB Anfang 2010 seine Arbeit aufnahm, waren die Personalressourcen für die Informatik des neuen Dienstes äusserst knapp bemessen. Anfang 2009 hatte das VBS den Inlandnachrichtendienst ohne das Personal, das dessen Informatikbedürfnisse abdeckte, übernommen. Nachdem dieser Mangel bei der Fusion zum NDB nicht behoben wurde, musste dieser mit den Informatikressourcen des bisherigen Auslandnachrichtendienstes auskommen. Dies führte dazu, dass beim Ausfall des einzigen internen Datenbankadministrators die Betriebssicherheit der Datenbanken nur gewährleistet werden konnte, solange keine gravierenden Probleme auftauchten. Diese Personalsituation erschwerte es auch, die Integrität der Datenbankprogramme zu überprüfen.

Wegen der wachsenden Zahl an Informatikprojekten, die auch als Folge der Fusion anstanden, ist ausserdem die Abhängigkeit des NDB von externen Informatikern gestiegen. Diese werden jedoch in der Regel nicht der höchsten Stufe der Personensicherheitsprüfung unterzogen, wie sie heute für alle Mitarbeitenden des NDB vorgeschrieben ist. Obwohl seit Mai 2012 vorgeschrieben, können bis heute nicht alle Mitarbeitenden des NDB eine solche Personensicherheitsprüfung vorweisen. Die Ursachen dafür liegen nicht beim NDB sondern in den Kapazitätsengpässen der zuständigen Fachstelle im VBS.

Die GPDel stellte auch fest, dass der NDB verschiedene Vorschriften für die Informatiksicherheit auf Stufe Bund und VBS nicht eingehalten hatte. Für die Wahrnehmung der Aufgabe des Informatiksicherheitsbeauftragen (ISBO) stand, wenn überhaupt, nur in ungenügendem Ausmass Personal zur Verfügung. Die vorgeschriebenen Sicherheitskonzepte für die Anwendungen und Systeme waren mehrheitlich ungenügend oder fehlten. Der NDB war weiter aus Kapazitätsgründen nicht in der Lage, seine Systeme im Hinblick auf interne Sicherheitsvorfälle ausreichend zu überwachen. Um den Betrieb aufrechterhalten zu können, wurde in der Informatik des NDB auch darauf verzichtet, die Zugriffsmöglichkeiten auf den Systemen einzuschränken.

Die Informatiksicherheit war nicht in ein Risikomanagement eingebettet, welches die Konsequenzen der ungenügenden Personalressourcen und der fehlenden Sicherheitsmassnahmen aufgezeigt und eine gezielte Risikoverminderung ausgelöst hätte.

Während sich der NDB zwar in den letzten Jahren vermehrt in das Risikoreporting des Departements einbrachte, wurden im Rahmen des interne Risikomanagements - auch für die Informatik - die Risiken weder definiert und bewertet, noch einem Risikoeigner zugeordnet. Zudem fehlte eine Notfallplanung für den Fall eines Hinweises oder Verdachts auf eine Gefahr für die Integrität oder die Vertraulichkeit der NDB-Daten.

Diese Ausgangsituation trug dazu bei, dass der NDB vorgängig zum Datendiebstahl im Mai 2012 nicht angemessen auf verschiedene Anzeichen einer Gefährdung der Verfügbarkeit und Integrität seiner Daten reagieren konnte. Als Folge von Problemen mit dem einzigen internen Datenbankadministrator stand die Leitung der Abteilung, zu welcher die Informatik, die Sicherheitszelle sowie der Rechts- und Personaldienst gehörten, vor dem Dilemma, entweder mit seiner Freistellung die Verfügbarkeit der Systeme zu gefährden oder bei seinem weiteren Einsatz ein Risiko für die Integrität und - wie es sich nachträglich auch zeigte - die Vertraulichkeit der Daten in Kauf zu nehmen. Letztlich erlaubte indes die ungenügende Reaktion der zuständigen Abteilung in Sachen Personalführung und Risikomanagement den Datendiebstahl. Der Direktor des Dienstes erfuhr von diesen Problemen erst, nachdem der Datendiebstahl aufgrund eines externen Hinweises intern bestätigt wurde.

Nach dem Datendiebstahl reagierte der NDB mit einer ganzen Reihe von technischen und organisatorischen Massnahmen, um erkannte Mängel in der Informatiksicherheit rasch zu beheben. Diese punktuellen Massnahmen erfolgten indes nicht im Rahmen eines umfassenden Risikomanagements. Das volle Ausmass der Ressourcenproblematik in der Informatik wurde von der Leitung des NDB erst ein halbes Jahr nach dem Vorfall erkannt. Über die notwendigen Personalkredite entschied der Bundesrat auf Antrag des VBS erst im Frühling 2013, also etwa ein Jahr nach dem Datendiebstahl.

Im Herbst 2012 erhielt der NDB einen vollamtlichen ISBO. Die Bereinigung der Informatiksicherheitskonzepte befand sich jedoch erst in den Anfängen. Ein funktionierendes Risikomanagement muss erst noch aufgebaut werden.

Aus Sicht der GPDel hat der Direktor NDB seine Aufsicht nach dem Vorfall zu wenig konsequent wahrgenommen und die internen Untersuchungen nicht den richtigen Stellen im Dienst anvertraut. Der Vorsteher VBS begnügte sich seinerseits zu lange mit den NDB-internen Abklärungen. Erst im Spätsommer 2012 zog er die VBS-internen Aufsichts- und Vorgabestellen mit ein. Die Informationsrechte der ND-Aufsicht wurden dabei vom NDB nicht immer vorbehaltslos respektiert und der Vorsteher VBS sorgte zu wenig für eine Klärung der Rollenverteilung zwischen dem Aufsichtsorgan und dem zu beaufsichtigenden Dienst.

Als Folge des Datendiebstahls im NDB veranlasste der Vorsteher VBS im Herbst 2012 auch eine ad hoc Untersuchung zur Informationssicherheit auf Stufe Bund. Diese Abklärungen überschnitten sich mit dem vom Bundesrat seit Jahren institutionalisierten

Reporting zur Informations- und Informatiksicherheit. Den Weg zur Verbesserung der Informatiksicherheit auf Stufe Bund erkennt die GPDel weniger in solchen isolierten Reaktionen auf einen Vorfall, als viel mehr in einer Intensivierung der systematischen Massnahmen, welche der Bundesrat seit 2009 umsetzen und kontrollieren lässt.

Im April 2013 publizierte das VBS in eigener Verantwortung seine abschliessende Würdigung zum Datendiebstahl im NDB. Die Inspektion der GPDel hat zum Teil andere Erkenntnisse ergeben. Die GPDel konnte auch die Schlussfolgerungen des VBS zur Informationssicherheit auf Stufe Bund nicht alle teilen.

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.

Für die Information der Öffentlichkeit hat die GPDel am 30. August 2013 einen Kurzbericht mit einer Zusammenfassung der Erkenntnisse aus der Inspektion und ihren Empfehlungen

verabschiedet. Am 4. September 2013 erhielt die GPDel die Zustimmung beider GPK zur Publikation des Kurzberichts am 5. September 2013.121 Am 30. Oktober 2013 legte der Bundesrat in seiner Stellungnahme122 dar, wie er die Empfehlungen der GPDel umsetzen wird.