Datendiebstahl im Nachrichtendienst

27. September 2012

Im Mai 2012 hat ein Informatiker, der für den Nachrichtendienst des Bundes (NDB) arbeitet, in grossem Stil geheime Daten gestohlen. Auf diversen Festplatten liess er mehrere Terabyte (1024 Gigabyte oder mehr als eine Million Megabyte) klassifiziertes Material mitlaufen und lagerte es zu Hause ein.

Der Mitarbeiter des NDB wurde am 25. Mai 2012 auf Antrag der Bundesanwaltschaft verhaftet und für sechs Wochen in Untersuchungshaft genommen. Er wollte die Daten, die angeblich vollständig sichergestellt werden konnten, ins Ausland verkaufen.

Die Festplatten enthalten den gesamten Mailserver des NDB innerhalb des speziell gesicherten internen SILAN-Netzes, darunter auch Mails des militärischen Nachrichtendienstes (Mil ND) und der Führungs- und Unterstützungsbasis der Armee (FUB). Diese betreibt das Satelliten-Überwachungssystem Onyx, mit dem ausländische Telefonnummern oder Internetanschlüsse abgehört werden. Zu den Mails gehören auch unzählige Anhänge: vertrauliche Berichte an den Bundesrat, geheime Berichte ausländischer Polizei- und Nachrichtendienste über Terroristen, Waffenhändler und laufende nachrichtendienstliche Operationen. Das Mail-System des NDB ist nicht verschlüsselt.

Das VBS und die Bundesanwaltschaft informierten die Öffentlichkeit erst, nachdem Ende September 2012 die Presse der Sache auf die Spur kam.

Obwohl der Informatiker erst eine Woche, nachdem via UBS eine Meldung erfolgte, verhaftet wurde, behauptete Ueli Maurer, das Datenleck wäre intern ohnehin festgestellt worden. Gemäss Medienberichten besteht aber im NDB gar kein Sicherheitskonzept, welches diesen Namen verdienen würde.

Am 2. Oktober 2012 wurde bekannt, dass zwei kritische Mitarbeiter der Aufsicht des NDB von Ueli Maurer versetzt resp. entlassen wurden.

Am 16. Oktober 2012 führte die GPDel Aussprachen mit Bundesrat Maurer und NDB-Direktor Markus Seiler. Sie erkundigte sich namentlich nach Massnahmen für die Sicherheit der Informatiksysteme. Ebenso wollte sie wissen, wie das VBS seine Aufsicht ausgeübt hat respektive ausüben wird. Die GPDel will nun ihre bisherigen Abklärungen in eine formelle Inspektion überführen. Im Frühling 2013 will sie dem Bundesrat einen Bericht vorlegen.

Am 21. Oktober 2012 berichtete der «Sonntag», dass Markus Seiler in Spiez diverse Ämter bekleidet und auf der Webseite der reformierten Kirchgemeinde Spiez seine Telefonnummer vom Büro in Bern als Kontakt angibt. Unter diesen Umständen ist verständlich, dass Markus Seiler keine Zeit hat, um im NDB nach dem Rechten zu sehen .

Eine Woche später, am 28. Oktober 2012, wusste der «Sonntag», dass Markus Seiler mit seiner im Internet auffindbaren Mobilnummer zwar nicht erreichbar ist, dass aber kurz nach einem Anruf eine Rückfrage vom NDB kommt. Am selben Tag wurde bekannt, dass Markus Seiler

einen per Anfang 2013 geplanten Lehrauftrag an der HSG sistiert hat.

Im April 2013 präsentierte das VBS den Bericht *«Verhinderter Datenabfluss im Nachrichtendienst des Bundes»*. Auf 18 Seiten wird dargelegt, dass *«für die Schweiz und ihre Sicherheit keinerlei Schaden entstanden ist»*. Ziemlich frech ist die Schlussfolgerung auf Seite 18: *«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»*. Wie wenn andere Dienststellen der Bundesverwaltung terabyteweise Daten verhühnert hätten...

Anfang September 2013 wurde unter dem Titel «Informatiksicherheit im Nachrichtendienst des Bundes» der Bericht der Geschäftsprüfungsdelegation vom 30. August 2013 vorgestellt, wobei für die Öffentlichkeit nur eine 16-seitige Zusammenfassung erhältlich ist. Aber auch diese gekürzte Version ist vernichtend. So gab es im NDB kein Risikomanagement, obwohl der Bundesrat im Jahre 2010 die «Weisungen über die Risikopolitik des Bundes» erlassen und für die gesamte Bundesverwaltung als verbindlich erklärt hat. Unter dem Titel «Vorkehrungen für die Informatiksicherheit im NDB vor dem Datendiebstahl» ist im Bericht zu lesen: *«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.»*. Auf Seite 8 wird dann der ganze Dilettantismus im NDB offenkundig: *«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.»* und *«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.»* Kurz nach dem Bekanntwerden dieses Berichts wurde auch schon der Rücktritt von NDB-Chef Markus Seiler gefordert.

Mitte Dezember 2013 wurde die Stellungnahme des Bundesrats zum Bericht der GPDel veröffentlicht.

Er nahm so viele Daten nach Hause, wie er kriegen konnte

Stellungnahme des Bundesrats zum Bericht GPDel

Bericht GPDel «Informatiksicherheit im Nachrichtendienst des Bundes»

Medienmitteilung VBS

NZZ online vom 27. September 2012

Geheimdienst: Chaos in der Informatik-Abteilung

Maurer brachte kritische Aufsicht des Geheimdienstes zum Schweigen

Tätigkeitsbericht des Kontrollorgans über den Staatsschutz im Kanton Basel-Stadt 2011 (Auszug)

Tätigkeitsbericht des Kontrollorgans über den Staatsschutz im Kanton Basel-Stadt 2011 (PDF)

Medienmitteilung GPDel vom 16. Oktober 2012

Markus Seiler kandidiert in Spiez als FDP-Gemeinderat

Geheimdienstchef Markus Seiler aufs Handy anrufen - ein Kinderspiel

Koller kontrolliert die Kontrolleure

Bericht VBS: Verhinderter Datenabfluss im Nachrichtendienst des Bundes