

I. Einleitung

Am 4. Juli 2007 habe ich dem Verteidigungsausschuss zum Datenverlust im Zentrum für Nachrichtenwesen der Bundeswehr (ZNBw) vorgetragen.

Ich rufe dazu in Erinnerung:

Im IT-System JASMIN werden die aktuellen Daten im Fileserver-System, dem „zentralen Gedächtnis“ des IT-Systems JASMIN, einer regelmäßigen Datensicherung durch einen so genannten Bandroboter unterzogen. Aus Kapazitätsgründen werden mit diesem Bandroboter allerdings auch Daten aus dem operationellen System ausgelagert, wenn sie nach Bewertung durch den zuständigen Bearbeiter für die weitere Lagebearbeitung nicht mehr relevant sind. Sie stehen damit nur noch auf den „ausgelagerten“ Speichermedien zur Verfügung, können jedoch jederzeit wieder in das Fileserver-System eingespielt werden.

Am 4. Dezember 2003 sollten im ZNBw zur routinemäßigen Optimierung der begrenzten Speicherkapazitäten des Bandroboters des IT-Systems JASMIN Daten von Magnetbandkassetten (Datenkassetten, in Erscheinungsbild und Aufbau ähnlich den Audiokassetten für herkömmliche Kassettenrekorder) zusammengeführt werden. Bei diesem Prozess wurden fünf Magnetbandkassetten beschädigt. Drei davon betrafen die Datensicherung des Fileserver-Systems. Ein konkreter Datenverlust ist hier nicht entstanden, da die Daten dieser Bänder im "aktiven" Datenbestand des Fileserver-Systems noch vorhanden waren. Die Inhalte der beiden anderen beschädigten Bänder betrafen ausgelagerte Daten.

Durch spätere Bemühungen - auch mit Unterstützung des Herstellers des Bandroboters (Firma IBM) - konnten diese beiden Bänder nicht wieder lesbar gemacht werden und wurden deshalb 2005 vernichtet. Der Datenverlust umfasst - wie wir heute wissen - rd. 20.000 Dateien = 2 x 5 Giga Byte, die zwecks Auslagerung auf diesen Bandkassetten abgespeichert waren.

Ich hatte Ihnen zugesagt, alles vertretbar Mögliche zu unternehmen, um die verloren gegangenen Daten wieder aufzufinden oder technisch zu rekonstruieren.

Bevor ich zu den diesbezüglichen Anstrengungen vortrage, möchte ich erwähnen, dass ich zusätzlich eine nochmalige umfassende Recherche in den lesbaren Datenbeständen des gesamten IT-System JASMIN anhand einer Liste mit Schlagwörtern nach Daten angeordnet habe, die für den Untersuchungsgegenstand des Verteidigungsausschusses als 1. Untersuchungsausschuss von Bedeutung sind. Dabei handelt es sich, wie ich bereits im Juli berichtet habe, um ein System, das aus ca. 100 Servern und ca. 600 Arbeitsplatzrechnern besteht. Diese Untersuchung ist zwischenzeitlich abgeschlossen. Es wurden keine für den Untersuchungsgegenstand des Verteidigungsausschusses als 1. Untersuchungsausschuss relevanten Daten gefunden. Alles, was gefunden wurde, war dem Untersuchungsausschuss bereits zur Verfügung gestellt worden.

Nun zu den einzelnen Maßnahmen in Bezug auf die verloren gegangenen Daten:

II. Wiederbeschaffung der auf den vernichteten Magnetbandkassetten abgespeicherten Daten über die Herausgeber und mögliche Adressaten

Eine Maßnahme war darauf gerichtet, die auf den vernichteten Bandkassetten abgespeicherten Daten bei den herausgebenden Dienststellen oder den möglichen Adressaten wieder zu beschaffen. Ausgangspunkt dieser Suche waren die vorliegenden Auslagerungsaufträge, die von den damaligen Nutzern zur Überführung ihrer Daten in die Auslagerung erteilt worden waren. Hieraus konnten die fünf Kategorien abgeleitet werden, die ich schon in meinem Bericht vom 4. Juli 2007 erwähnt habe, nämlich

- Meldungen des BND aus 2001 und 2002,
- Meldungen des HQ ISAF aus 2002 und teilweise 2003,
- Meldungen des HQ KMNB aus 2002 und teilweise 2003,
- Meldungen von USCENTCOM aus 2001 bis 2003 und
- verschiedene eigene Produkte des ZNBw aus 1999 bis 2002.

Bei der Suche nach Dokumenten, die sich den fünf Kategorien zuordnen lassen, wurden die herausgebenden Stellen eingebunden mit der Ausnahme des USCENTCOM, dessen Meldungen bei Fü S vorlagen und von dort zur Verfügung gestellt werden konnten.

Die eingeschalteten Stellen haben insgesamt 46.099 Dateien bereitgestellt. Aus diesen 46.099 Dateien konnte das ZNBw 19.861 Dateien herausfiltern, die einen deutlichen Bezug zu den genannten Kategorien aufweisen.

Rein zahlenmäßig könnte damit davon ausgegangen werden, dass die im ZNBw verloren gegangenen Dateien zu einem Großteil wiederbeschafft sind. Dies kann jedoch nicht mit letzter Gewissheit angenommen werden, weil die Namen der verloren gegangenen Dateien nicht bekannt sind.

Die wieder zur Verfügung gestellten Dateien sind darauf überprüft worden, ob sich darunter Dokumente befinden, die dem Verteidigungsausschuss als 1. Untersuchungsausschuss auf Grund des Untersuchungsauftrags und den dazu ergangenen Beweisbeschlüssen vorzulegen sind. Die Überprüfung führte zu dem Ergebnis, dass dies nicht der Fall ist. Alles Relevante war dem Verteidigungsuntersuchungs-ausschuss bereits zur Verfügung gestellt worden.

III. Technische Rekonstruktion der verloren gegangenen Daten

Parallel zu meiner Anweisung, die verloren gegangenen Daten bei den herausgebenden Stellen oder den Adressaten wieder zu beschaffen, wurde versucht, die Daten durch technische Rekonstruktion auf noch vorhandenen Datenträgern wieder zu gewinnen. Diese Arbeiten erstreckten sich auf folgende Komponenten des IT-Systems JASMIN im ZNBw in Gelsdorf, auf denen noch Kopien oder Fragmente der verloren gegangenen Daten vermutet werden konnten:

- a. der Laptop, der bei Spezialoperationen genutzt wurde, mit einer Festplatte,
- b. das Fileserver-System mit 45 Festplatten,
- c. die Arbeitsplatzrechner mit 471 „aktiven“ Festplatten und 212 ausgesonderten Festplatten,
- d. 453 sonstige Festplatten,

Hierunter fallen 429 aktive und 24 ausgesonderte Festplatten, die für unterschiedliche Zwecke, z.B. Internet-, E-mail-, Druck- und Kommunikationsdienste, eingesetzt sind oder waren und systembedingt nur als Zwischenspeicher dienen.

- e. 125 Festplatten ohne Zuordnung,

Hierunter fallen 106 Festplatten, die in der VS-Registatur lagern und deren früherer Einsatzbereich nicht mehr konkret bestimmt werden kann, sowie 19 werkneue Festplatten.

also zusammen 1307 Festplatten.

Ziel der Untersuchung war, Daten, die auf diesen Datenträgern einmal abgespeichert waren, zwischenzeitlich aber gelöscht wurden, zu rekonstruieren. Hierfür wurde eine in der Fachwelt anerkannte, leistungsstarke Spezialsoftware, die gelöschte, aber noch nicht überschriebene Daten einer Festplatte ganz oder in Fragmenten wieder lesbar machen kann, eingesetzt.

Solche Untersuchungen mit forensischen Mitteln sind mit einem hohen technischen, zeitlichen, personellen und auch finanziellen Aufwand verbunden. Insgesamt standen also 1307 Datenträger für Untersuchungen zu Verfügung.

Bei den 471 Festplatten der Arbeitsplatzrechner („aktive“ Festplatten) und den 212 noch vorhandenen, früher in den Arbeitsplatzrechnern verwendeten Festplatten konnte die Überprüfung auf eine 10%-ige Stichprobe (gleich insgesamt 70 Festplatten) beschränkt werden. Dies deshalb, weil nach der Weisungslage Lageinformationen nur auf den Fileservern und nicht auf den Arbeitsplatzrechnern abgespeichert werden dürfen, so dass ein Auffinden von einschlägigen Daten auf diesen Festplatten höchst unwahrscheinlich ist. Nur wenn weisungswidrig gehandelt worden wäre, was man nicht unterstellen kann, könnte es überhaupt zu Abspeicherungen gekommen sein.

In gleicher Weise wurde bei den 429 aktiven und 24 ausgesonderten Festplatten vorgegangen (10%-ige Stichprobe gleich 46 Festplatten), die für unterschiedliche Zwecke, z.B. Internet-, E-mail-, Druck- und Kommunikationsdienste, eingesetzt sind oder waren und systembedingt nur als Zwischenspeicher dienen. Auch bei diesen Zwischenspeicher-Festplatten ist mit hoher Wahrscheinlichkeit davon auszugehen, dass auf ihnen keine für den Untersuchungsausschuss relevanten Daten gespeichert sind.

Demgegenüber sind neben der Festplatte des Laptops ausnahmslos alle 45 Festplatten des Fileserversystems und alle 106 Festplatten, die in der VS-Registatur

des ZNBw lagern und früher für nicht mehr feststellbare Zwecke verwendet wurden, überprüft worden.

Geprüft wurde auch, gelöschte und erneut überschriebene Daten auf unterster physikalischer Ebene („Restmagnetismus“) wieder lesbar zu machen. Das IT-AmtBw hat dazu bei unterschiedlichen - wegen der VS-Einstufung - deutschen Stellen die Frage geklärt, ob, durch wen, mit welchem Aufwand bis wann und mit welchem Ergebnis ggf. Untersuchungen dieser Art durchgeführt werden könnten. Eingeschaltet wurden als staatliche Institutionen das Bundesamt für Sicherheit in der Informationstechnik (BSI), das Bundeskriminalamt (BKA), der Bundesnachrichtendienst (BND), als Industrieverbände der Bundesverband Informationswirtschaft Telekommunikation und neue Medien e.V. (BITKOM), der Zentralverband Elektrotechnik- und Elektronikindustrie e.V. (ZVEI) und verschiedene Fachfirmen.

Keine der angefragten Stellen und Fachfirmen konnte Möglichkeiten aufzeigen, wie gelöschte und überschriebene Daten wieder lesbar gemacht werden können. In seinem Kurzgutachten vom 16. August 2007 kommt das BSI zu dem Schluss: „Von der Möglichkeit einer Auswertung durch Überschreiben gelöschter Daten wird zwar häufig gesprochen, es gibt aber nirgends einen Hinweis auf eine erfolgreiche Auswertung.“

Auch Herr Bernd Melchers, Leiter der Datensicherung im Rechenzentrum der Freien Universität Berlin, der sich in der Presse dahin geäußert hat, dass „Datenbänder auch nach 20 Jahren noch ausgelesen oder deren beschädigte Daten wieder hergestellt werden können“, konnte hier nicht weiter helfen. Seine in der Presse wiedergegebene Aussage bezog sich lediglich auf Datenbänder. Die Datenbänder der beiden Magnetbandkassetten sind jedoch – wie bereits erwähnt - physisch vernichtet worden. Soweit es – wie hier - um die Wiederherstellung von Daten auf Festplatten auf unterster physikalischer Ebene („Restmagnetismus“) geht, sieht auch Herr Melchers – so das Ergebnis eines Telefonats mit ihm am 6. September 2007 - keine Möglichkeit einer Rekonstruktion von Daten auf dieser Ebene.

Nach dem derzeitigen Stand der Technik ist eine Rekonstruktion verwertbarer Daten zumindest auf Festplatten auf der Ebene des Restmagnetismus somit auszuschließen.

Von Versuchen, mit Hilfe des Restmagnetismus weitere Daten zu rekonstruieren, wurde daher nach intensiver Erörterung mit externen Fachleuten Abstand genommen.

Zu den Ergebnissen:

Soweit noch lesbare Dateien erneut durchsucht wurden, wurden keine zusätzlichen für den Untersuchungsausschuss relevanten Dateien gefunden.

Die Ergebnisse der Untersuchungen der vorerwähnten 1307 Datenspeicher mit forensischen Mitteln im Einzelnen:

a) Laptop

Hier darf ich noch einmal in Erinnerung rufen:

In dem vom Datenverlust betroffenen Zeitraum wurden vom ZNBw zwei Laptops im Rahmen der Unterstützung von Spezialoperationen genutzt. Von diesen wurden möglicherweise Daten in das IT-System des ZNBw übertragen.

Einer dieser Laptops ist bereits ausgesondert und seine Festplatte vernichtet. Insofern ist eine Rekonstruktion von Daten unmöglich.

Der zweite Laptop war zunächst bei der German National Intelligence Cell HQ SFOR im Einsatz. Ab etwa Juli 2004 bis Juli 2006 wurde er im ZNBw Dezernat SpezOp für einen möglichen Einsatz bereit gehalten und ab Januar 2007 der Verbindungsstelle beim Joint Force Command NEAPEL übergeben. Von dort wurde er im Juli diesen Jahres zwecks Überprüfung seiner Festplatte angefordert.

Bei der Auswertung der mit forensischen Methoden wieder lesbar gemachten und der ohnehin lesbaren Daten wurden keine Daten gefunden, die für den Untersuchungsgegenstand bzw. die Beweisanträge des 1. Untersuchungsausschusses von Bedeutung sind.

b) Fileserver-System

Im Rahmen der Auswertung der forensisch aufbereiteten Daten wurden auch auf den 45 Festplatten des Fileserver- Systems keine Daten gefunden, die von Relevanz für den Verteidigungsausschuss als 1. Untersuchungsausschuss sind.

c) Arbeitsplatzrechner im ZNBw

Die Auswertung der 70 der 10%-igen Prüfung unterliegenden Festplatten bestätigte die Annahme, dass auf den Festplatten der Arbeitsplatzrechner keine für den Verteidigungsausschuss als 1. Untersuchungsausschuss relevanten Daten abgespeichert waren.

d) sonstige Festplatten

Die 10%-ige Stichprobenüberprüfung mit forensischen Mitteln der 429 aktiven und 24 ausgesonderten Festplatten der Serversysteme, auf denen lediglich Zwischenablagen erfolgen, bestätigte ebenfalls, dass dort keine für den Verteidigungsausschuss als 1. Untersuchungsausschuss relevanten Daten abgespeichert waren.

e) Festplatten ohne Zuordnung

Bei der Prüfung der 106 in der VS- Registratur des ZNBw lagernden Festplatten, die momentan nicht in der Nutzung, zuvor aber für unterschiedlichste Aufgaben verwendet worden sind, wurden keine Daten gefunden, die von Relevanz für den Verteidigungsausschuss als 1. Untersuchungsausschuss sind. Die 19 werkneuen Festplatten mussten nicht überprüft werden, da sie noch nicht in Nutzung waren.

IV. Darstellung der Vorschriftenlage und Bewertung

Im Rahmen der Aufarbeitung des Datenverlusts war auch der Frage nachzugehen, wie das Vorgehen des ZNBw, das zum Datenverlust führte, vor der damaligen Vorschriftenlage zu bewerten ist.

Den Rahmen und die Grundlagen für den sicheren Betrieb des IT-Systems JASMIN hat das BMVg mit Zentralen Dienstvorschriften (ZDv) wie z.B. die ZDv 2/30 (Sicherheit in der Bundeswehr) und die ZDv 54/100 (IT-Sicherheit in der Bundeswehr) dem ZNBw vorgegeben. Diese Dienstvorschriften enthalten keine Regelungen, wie im Falle der Beschädigung einer Bandkassette mit ausgelagerten Daten vorzugehen ist. Das ZNBw hat daher gegen keine Dienstvorschriften verstoßen, als es die beschädigten, nicht lesbaren Bandkassetten physisch vernichtete, nachdem Bemühungen – auch mit Unterstützung des Herstellers des Bandroboters – erfolglos geblieben sind.

Allerdings hatte das ZNBw, entgegen ressortinternen und vorhabenbezogenen Vorgaben, bis zum Zeitpunkt der Beschädigung der zwei Magnetbandkassetten kein Datensicherungskonzept mit Regelungen zur doppelten Datensicherung in Kraft gesetzt. Im Entwurf lag dieses Konzept jedoch bereits vor und bildete den Handlungsrahmen für das ZNBw. Deshalb habe ich am 4. Juli 2007, als ich das BSI zitierte, vom „damals gültigen Datensicherungskonzept“ gesprochen.

Das ZNBw ist aber das Risiko, Daten zu verlieren, eingegangen, indem es entgegen der eigenen und auch in der Industrie üblichen Praxis temporär auf einen zweiten Satz ausgelagerter Daten verzichtet hat, um dringend benötigte Speicherkapazitäten für den laufenden Betrieb zu schaffen. Dieses Risiko wurde jedoch auf der Grundlage der bis dahin gemachten Erfahrungen im Betrieb des IT-Systems JASMIN durch die Dienststelle als tragbar bewertet. Diese Güterabwägung des ZNBw war aus damaliger Sicht vertretbar.

Gleiches gilt für die Entscheidung des ZNBw, auf weitere Versuche der Datensicherung bei den nicht mehr lesbaren Magnetbandkassetten zu verzichten. Angesichts des geringen operationellen Nutzens, der den Inhalten der Bänder damals beigemessen wurde, konnte der bekanntlich erhebliche zeitliche und finanzielle Aufwand, der zum Auslesen der beschädigten Bänder hätte betrieben werden müssen, nachvollziehbar als wirtschaftlich nicht vertretbar angesehen werden. Das mag auch heutiger Sicht anders bewertet werden, die Fairness gebietet es aber, das Verhalten und die Maßnahmen sowie die damaligen Entscheidungen auch mit damaligen Maßstäben zu bewerten.

Schließlich war die Vernichtung der beiden Magnetbandkassetten und der damit verbundene Datenverlust nicht meldepflichtig. Nach der ZDv 2/30 (Sicherheit in der Bundeswehr), der ZDv 54/100 (IT-Sicherheit in der Bundeswehr) und der ZDv 10/13 (Besondere Vorkommnisse) sind nur Verluste von Datenträgern (im Sinne von Verlieren oder Diebstahl) sowie unberechtigte Manipulationen und vorsätzliche Beschädigungen von Informationen zu melden. Unabhängig davon wäre allerdings - zumindest aus heutiger Sicht - eine Information des BMVg dem Vorfall angemessen gewesen. Deshalb habe ich angewiesen, in die einschlägigen Vorschriften zur

Behandlung besonderer Vorkommnisse (z.B. ZDv 10/13), die Regelung aufzunehmen, dass jegliche Art des Verlusts von VS-Daten (VS-VERTRAULICH und höher) zu melden ist. Außerdem habe ich angewiesen zu prüfen, ob die Regelungen zur jederzeitigen Verfügbarkeit von Daten (z.B. Datensicherung und Auslagerung von Daten aus operationellen Systemen) in der ZDv 54/100 ausreichend sind.

Die Nachweisführung von Verschlussachen, also auch der sorgfältige Umgang mit VS-Datenträgern, ist in der Bundeswehr eindeutig geregelt. Dennoch habe ich eine Prüfung angewiesen, ob in der ZDv 2/30 noch weiterer Regelungsbedarf besteht, um bestehende Verfahren so abzusichern, dass sich ein Vorfall wie dieser in der Bundeswehr nicht mehr wiederholt.

Zusätzlich habe ich angewiesen, die Vorschriften des Militärischen Nachrichtenwesens der Bundeswehr, u.a. die ZDv 2/1 – VS-NfD – Das Militärische Nachrichtenwesen der Bundeswehr – dahingehend zu überprüfen, ob Regelungsbedarf hinsichtlich der Bearbeitung, Aufbewahrung und Vernichtung von VS-Daten/VS-Datenträgern besteht.

Weiterhin habe ich angewiesen, dass der IT-Sicherheitsbeauftragte der Bundeswehr mit den IT-Sicherheitsbeauftragten der Organisationsbereiche die Kontrollen für die vorschriftenkonforme Behandlung von VS-Datenträgern in den Dienststellen der Bundeswehr intensiviert.

V. Zusammenfassung

Ich fasse zusammen:

- Aufgrund der Anzahl der wiederbeschafften Dateien, die sich in die fünf Kategorien der verloren gegangenen Daten einfügen lassen, kann davon ausgegangen werden, dass der weitaus überwiegende Teil der verloren gegangenen Dateien im ZNBw wieder verfügbar ist. Eine letzte Gewissheit hierüber kann es jedoch nicht geben, da die Namen der verloren gegangenen Dateien nicht bekannt sind. Unter den wiederbeschafften Dateien befanden sich keine, die dem Verteidigungsausschuss als 1. Untersuchungsausschuss vorzulegen sind. Entweder betrafen sie nicht den Untersuchungsgegenstand oder sie waren bereits vorgelegt worden.
- Die Auswertung der direkt lesbaren Daten im gesamten System JASMIN führte zu keinem für den Untersuchungsausschuss relevanten Ergebnis. Gleiches gilt für die Auswertung der Daten, die mit forensischen Mitteln aus den 1307 Festplatten im ZNBw in Gelsdorf einschließlich der Festplatte des Laptops wieder rekonstruiert worden sind. In beiden Fällen wurden keine für den Untersuchungsauftrag relevanten Dokumente gefunden, die dem Untersuchungsausschuss noch nicht vorgelegt wurden.
- Das Vorgehen des ZNBw, das zum Datenverlust führte, lag in seinem damaligen Ermessensspielraum und kann nachvollzogen werden.

- Eine Meldepflicht des Datenverlustes bestand formal nicht, eine Information an das BMVg wäre dem Vorfall allerdings – zumindest aus heutiger Sicht – angemessen gewesen.
- Um zukünftig einen solchen Datenverlust in der Bundeswehr zu vermeiden, habe ich die Prüfung und Ergänzung der einschlägigen Dienstvorschriften sowie verstärkte Kontrollen durch den IT-Sicherheitsbeauftragten der Bundeswehr und die IT-Sicherheitsbeauftragten der Organisationsbereiche angewiesen.
- Aus meiner Sicht und nach dem Urteil der Fachleute, die eingebunden wurden, ist alles Mögliche getan worden, um die möglicherweise verloren gegangenen Daten wiederzubeschaffen.