



# BUNDESVERWALTUNGSGERICHT

## BESCHLUSS

BVerwG 1 WB 62.06

In dem Wehrbeschwerdeverfahren

des Herrn Stabsunteroffizier ...,  
..., B.,

- Bevollmächtigte:  
Rechtsanwälte ...,  
... -

hat der 1. Wehrdienstsenat des Bundesverwaltungsgerichts durch

den Vorsitzenden Richter am Bundesverwaltungsgericht Golze,  
die Richterin am Bundesverwaltungsgericht Dr. Frenz,  
den Richter am Bundesverwaltungsgericht Dr. Langer,  
den ehrenamtlichen Richter Major Falk und  
den ehrenamtlichen Richter Stabsunteroffizier Thal

am 6. September 2007 beschlossen:

Der Antrag wird zurückgewiesen.

## G r ü n d e :

### I

- 1 Der 1972 geborene Antragsteller wendet sich gegen die Feststellung eines Sicherheitsrisikos. Er ist Soldat auf Zeit mit einer bis zum 30. Juni 2009 festgesetzten Dienstzeit von zwölf Jahren. Er wurde am 21. Dezember 2001 zum Stabsunteroffizier ernannt. Seit dem 9. Januar 2006 wird er als Unteroffizier Elektronischer Kampf ... beim ... am Dienstort B. verwendet. Zuvor war er ab dem 1. Dezember 2004 als IT-Systemunteroffizier beim Dienstältesten Deutschen Offizier ... Headquarter-A. R. eingesetzt.
- 2 Für den Antragsteller war zuletzt am 27. März 2002 eine erweiterte Sicherheitsüberprüfung mit Sicherheitsermittlungen (Ü 3) ohne Einschränkungen abgeschlossen worden.
- 3 Mit Schreiben vom 8. Mai 2006 teilte der Geheimschutzbeauftragte im Bundesministerium der Verteidigung dem Antragsteller folgende sicherheitserheblichen Umstände mit, die der Militärische Abschirmdienst ermittelt hatte:

„Am 10. Mai 2005 verschafften Sie sich in Ihrer Funktion als Netzwerk Administrator Zugang zum Internet, luden zwei Programme herunter und speicherten diese im dienstlichen Netz des HQ R. Dies geschah ohne Wissen und Genehmigung der zuständigen Vorgesetzten. Zusätzlich wurde festgestellt, dass Sie ebenfalls Programme zum Kopieren und Konvertieren von DVD's und CD's heruntergeladen haben.

Dieser schwerwiegende IT-Sicherheitsverstoß wurde durch ein Protokollprogramm offenkundig.

Am 11. Mai wurden Sie durch die Security Police und den Provost Marshall des HQ befragt und es wurden Ihnen die Zugriffsrechte als Administrator entzogen, was bedeutet, dass Sie das dienstliche IT-Netz nicht mehr nutzen durften.

Entgegen dieses ausdrücklichen Befehls versuchten Sie am gleichen Tag, sich erneut Zugang zu einem Rechner und dem dienstlichen IT-Netz zu verschaffen.

Hierbei wurden Sie erkannt und die erneute Anmeldung im Netz verhindert.

Aufgrund dieses Vorfalles wurden Sie am 12. Mai 2005 erneut durch die Security Police befragt.

Danach wurden Sie von Ihrem Dienstposten abgelöst und die Zugangsberechtigung zum HQ-Gebäude wurde Ihnen entzogen.

In Ihrer Befragung durch den MAD am 19. Januar 2006 gaben Sie an, dass Sie zurzeit bei Ihrer neuen Dienststelle in B. als Netzwerkadministrator eingesetzt seien.

Zum Vorwurf, ‚eigenmächtig und ohne Kenntnis von Vorgesetzten‘ eine Key-Logger-Software heruntergeladen zu haben, erklärten Sie, dass Sie sich nur über Angriffsmöglichkeiten hätten informieren wollen, um Gegenstrategien zur Abwehr solcher Programme entwickeln zu können. Dabei sei Ihnen nicht bewusst gewesen, gegen Vorschriften zu verstoßen. Sie erklärten, Ihre Vorgesetzten nicht über Ihr Vorhaben informiert zu haben, da diese beschäftigt gewesen seien und diese ‚eh keine Ahnung‘ hätten. Später räumten Sie ein, dass Ihnen sehr wohl bewusst gewesen sei, dass Ihr Handeln kompetenzüberschreitend und unzulässig gewesen sei.

Am nächsten Tag seien Sie durch den InfoSecOfficer des HQ mit dem Vorwurf konfrontiert worden. Man habe Sie vernommen und Ihnen mitgeteilt, dass es Ihnen ab sofort verboten sei, sich im Netzwerk anzumelden und Ihr Account gesperrt werde.

Sie erklärten weiter, dass Sie sich ‚Gedanken gemacht hätten, wie Sie die Ermittlungen unterstützten könnten‘, da Sie nichts zu verbergen hätten.

Da man Ihnen nur den Zugang zum Netzwerk untersagt hatte, hätten Sie versucht, auf der Festplatte im Papierkorb nach vorhandenen Daten zu suchen. Dieser sei allerdings schon geleert gewesen. Ein Dienststellenangehöriger habe Ihre Arbeit am PC bemerkt und Sie bei der SecPolice gemeldet, woraufhin Sie erneut vernommen wurden.

Sie gaben an, dass Ihnen nach der Vernehmung der Zugang zum HQ verboten und die Zutrittsberechtigung entzogen worden sei. Eine Vernehmung im nationalen Bereich habe sich angeschlossen und eine Kompetenzüberschreitung sei festgestellt worden.

Aufgrund des bekannt gewordenen Verstoßes gegen die IT-Sicherheit und die Gefährdung des Netzwerkes des HQ, als äußerst sicherheitssensibler Dienststelle, liegen begründete Zweifel an Ihrer Eignung als Geheimnisträger bei der Bundeswehr vor.

Ihr eigenmächtiges Verhalten, entgegen eindeutiger Befehle und im Wissen gegen bestehende Vorschriften zu verstoßen, ist ein tatsächlicher Anhaltspunkt, der bei der sicherheitsrechtlichen Bewertung schwer wiegt.

Der wiederholte Verstoß gegen die IT-Sicherheitsbestimmungen im Zusammenhang mit Ihrer dargelegten Kompetenzüberschreitung begründen Zweifel an Ihrer Eignung als Geheimnisträger und damit die Feststellung eines Sicherheitsrisikos gemäß § 2414 Abs. 1 ZDv 2/30. Ihre nicht glaubhafte Aussage, nur Gegenstrategien zur Abwehr solcher Programme entwickeln zu wollen, verstärken diese Zweifel noch.“

- 4 Dem Antragsteller wurde Gelegenheit zur Äußerung gegeben.
- 5 In seiner Stellungnahme vom 22. Mai 2006 teilte der Antragsteller im Wesentlichen mit, dass er sich keinen Zugang „verschafft“, sondern wie jeder andere NATO-Angehörige das unklassifizierte Internet-Netzwerk benutzt habe. Der Download einer Datei sei nicht generell gesperrt gewesen. Nach dem Verhör durch den Provost Marshall habe es zu keinem Zeitpunkt einen ausdrücklichen Befehl gegeben, dass er das Netzwerk nicht mehr benutzen dürfe. Das Netzwerk sei zu keiner Zeit gefährdet gewesen, weil er die Programme nicht installiert, sondern Vorbereitungen getroffen habe, um diese auf dem Test-Netzwerk auszuprobieren. Die Sicherheit und Stabilität „seines“ Netzwerkes habe für ihn Priorität.
- 6 Mit Schreiben vom 25. Juli 2006 teilte der Geheimschutzbeauftragte dem Antragsteller die bevorstehende Feststellung eines Sicherheitsrisikos mit und führte zur Begründung u.a. aus, die Behauptung, ihm sei nach dem Verhör durch den Provost Marshall die Nutzung des Netzwerkes nicht ausdrücklich untersagt worden, sei eine Verdrehung von Tatsachen. Der Antragsteller habe sich auf einen am Netzwerk angeschlossenen Rechner mit einem lokalen Passwort eingeloggt, woraufhin ihm die Zutrittsberechtigung entzogen worden sei, um weitere Übergriffe seinerseits auszuschließen. Seine Erklärung des Vorfalls mit dem Vorsatz, dem Provost Marshall die heruntergeladenen Programme zeigen zu wollen, sei nicht nachvollziehbar, da jener bei der besagten Anmeldung weder zugegen gewesen sei noch vorher von seinem Vorhaben in Kenntnis gesetzt worden sei. Die Vertrauensstellung als Netzwerk-Administrator sei von ihm dazu missbraucht worden, wissentlich eine Sicherheitssperre zu umgehen; das begründe erhebliche Zweifel an seiner Zuverlässigkeit als Geheimnisträger.

Dieses Schreiben enthielt eine Rechtsbehelfsbelehrung, derzufolge nach Eröffnung des Ergebnisses der Sicherheitsüberprüfung durch die personalbearbeitende Dienststelle das Bundesverwaltungsgericht - Wehrdienstsenate - in Leipzig angerufen werden könne.

- 8 Mit Bescheid vom 26. Juli 2006, der an den Sicherheitsbeauftragten des ... Coordination Centers B., ... Waffensysteme, in T. gerichtet war, schloss der Geheimschutzbeauftragte die erweiterte Sicherheitsüberprüfung mit Sicherheitsermittlungen (Ü 3/W 3) mit der Feststellung eines Sicherheitsrisikos ab. Dieser Bescheid wurde dem Antragsteller nach Mitteilung des Bundesministers der Verteidigung am 16. August 2006 eröffnet.
  
- 9 Mit Schreiben seiner Bevollmächtigten vom 8. August 2006, das am 10. August 2006 beim Bundesministerium der Verteidigung einging, legte der Antragsteller Beschwerde gegen den „Bescheid“ des Geheimschutzbeauftragten vom 25. Juli 2006 ein und beantragte die gerichtliche Entscheidung durch das Bundesverwaltungsgericht - Wehrdienstsenat -. Der Bundesminister der Verteidigung- PSZ I 7 - hat diesen Antrag mit seiner Stellungnahme vom 9. November 2006 dem Senat vorgelegt.
  
- 10 Zur Begründung trägt der Antragsteller insbesondere vor:  
Tatsächliche Anhaltspunkte, die Zweifel an seiner Zuverlässigkeit bei der Wahrnehmung einer sicherheitsempfindlichen Tätigkeit und damit ein Sicherheitsrisiko begründen könnten, lägen nicht vor. Der Umstand, dass er die beiden Key Logging-Programme mit seiner Benutzerkennung heruntergeladen und Kenntnis davon gehabt habe, dass alle Downloads und der dazugehörige Benutzer gespeichert und kontrolliert würden, spreche dafür, dass er nichts Unrechtmäßiges oder Destruktives im Sinn gehabt habe. Die beiden Programme seien - wohl wegen eines „CRC-Fehlers“ - zu keinem Zeitpunkt lauffähig gewesen und hätten deshalb keine Schäden verursachen können. Nachdem sein Benutzerkonto gesperrt worden sei, habe er sich (lediglich) als lokaler Benutzer angemeldet, um nach den beiden Dateien im „Mülleimer“ auf seinem Desktop zu suchen; dafür habe er nicht sein Benutzerkonto gebraucht. Er habe dies getan, um seine Unschuld zu beweisen und zu zeigen, dass diese Dateien defekt

gewesen seien. Ein schwerwiegendes dienstliches Fehlverhalten liege nicht vor. Die von ihm angeführten entlastenden Aspekte hätten in die Beurteilung vom 25. Juli 2006 keinen Eingang gefunden.

- 11 Der Antragsteller beantragt,  
  
die Entscheidung des Geheimschutzbeauftragten (im Bundesministerium der Verteidigung) vom 25. Juli 2006 aufzuheben.
  
- 12 Der Bundesminister der Verteidigung beantragt,  
  
den Antrag zurückzuweisen.
  
- 13 Der Antrag sei unzulässig, weil er zu früh eingelegt worden sei. Der Antragsteller habe mit seinem Antrag vom 8. August 2006 das Schreiben des Geheimschutzbeauftragten vom 25. Juli 2006 angegriffen, das eine Ankündigung der Feststellung eines Sicherheitsrisikos enthalten habe; die tatsächliche Mitteilung des Ergebnisses der Sicherheitsüberprüfung und damit der originäre Beschwerdeanlass sei dem Antragsteller nachweislich jedoch erst am 16. August 2006 eröffnet worden.
  
- 14 Der Antrag sei auch offensichtlich unbegründet. Der schwerwiegende Verstoß des Antragstellers gegen IT-Richtlinien - insbesondere gegen Nr. 323 ZDv 54/100 (IT-Sicherheit in der Bundeswehr) - sei Grund genug dafür, Zweifel an seiner für eine sicherheitsrelevante Tätigkeit unabdingbaren Vertrauenswürdigkeit und Zuverlässigkeit hervorzurufen. Die damalige Dienststelle des Antragstellers habe als äußerst sensibler Bereich gesehen werden müssen. Der Antragsteller habe gegen das IT-Sicherheitskonzept seiner damaligen Dienststelle verstoßen. Danach sei u.a. der Zugriff auf und das Herunterladen von gefährlichen oder schädigenden Informationen untersagt gewesen. Der Antragsteller, der sich selbst als erfahrenen IT-Administrator bezeichne, habe in Kenntnis der Sicherheitsrisiken von fast immer Viren und Trojaner in sich bergenden speicherresistenten „Key-Logger“-Programmen und im Wissen, dass das Schutzsystem des Netzwerks seiner Dienststelle solche speicherresistenten Programme nicht erkennen kann, von einer ihm unbekanntem Internetseite

derartige Programme heruntergeladen, obwohl er deren Virenfreiheit nicht habe einschätzen können. Zudem habe er unter Ausnutzung seiner Administratorenrechte die Quarantänebox als weitere Schutzschranke ausgeschaltet. Dadurch habe die unmittelbare Gefahr eines Virenbefalls des Netzwerkes bestanden. Der Antragsteller sei bereit gewesen, für seine privaten Interessen erhebliche Risiken einzugehen und eine Schädigung des Dienstherrn in Kauf zu nehmen. Das Herunterladen der „Key-Logger“-Programme sei weder auf Befehl eines Vorgesetzten noch im Rahmen des dienstlichen Auftrags erfolgt. Ein weiterer Sicherheitsverstoß liege darin, dass er das entstandene Sicherheitsrisiko entgegen Nr. 146 ZDv 54/100 nicht unverzüglich dem zuständigen IT-Sicherheitsbeauftragten gemeldet habe.

- 15 Eine wiederholte bestimmungswidrige Nutzung der ihm im Vertrauen auf seine Zuverlässigkeit und Vertrauenswürdigkeit übertragenen Rechte liege in dem Versuch, das ihm am 11. Mai 2006 erteilte Verbot des Zugangs zu jeglichem Rechner zu umgehen. In der Vernehmung an diesem Tag sei dem Antragsteller nicht nur der Zugang zu „PA-Lan“, sondern auch der Zugang zum sogenannten „Nato-Secret Account“ („NS-Account“), also zum lokalen Rechner, untersagt worden. Auch unter Berücksichtigung von Fürsorgegesichtspunkten ließen die vorliegenden Erkenntnisse keine andere Bewertung zu.
- 16 Wegen des Vorbringens im Einzelnen wird auf den Inhalt der zwischen den Beteiligten gewechselten Schriftsätze und der Akten Bezug genommen. Die Verfahrensakte des BMVg - PSZ I 7 - 578/06 - und die Personalgrundakte des Antragstellers haben dem Senat bei der Beratung vorgelegen.

## II

- 17 Mit seinem Antrag auf gerichtliche Entscheidung vom 8. August 2006 wendet sich der Antragsteller in der Sache ausdrücklich gegen die Feststellung eines Sicherheitsrisikos. Insoweit hat er - anwaltlich vertreten - die Aufhebung der „Entscheidung“ des Geheimschutzbeauftragten vom 25. Juli 2006 beantragt, in der allerdings die Feststellung eines Sicherheitsrisikos erst angekündigt worden ist. Der Senat legt den Antrag sach- und interessengerecht dahin aus, dass der

Antragsteller die Aufhebung des Bescheids des Geheimschutzbeauftragten vom 26. Juli 2006 begehrt, in dem diese Feststellung förmlich getroffen wurde. Denn bei objektiver Betrachtung sind der Antragsteller bzw. seine Bevollmächtigten irrtümlich davon ausgegangen, dass schon in dem Schreiben des Geheimschutzbeauftragten vom 25. Juli 2006 die endgültige Entscheidung enthalten sei. Es besteht kein Zweifel, dass der Antragsteller allein den Bescheid vom 26. Juli 2006 angegriffen hätte, wenn ihm seine Fehlvorstellung bewusst geworden wäre. Der Bundesminister der Verteidigung - PSZ I 7 - hat in seinem Vorlageschreiben vom 9. November 2006 das Rechtsschutzbegehren auch im vorgenannten Sinn verstanden. Er ist außerdem zutreffend davon ausgegangen, dass es sich bei dem gleichzeitig als „Beschwerde“ bezeichneten Antrag um einen Antrag auf gerichtliche Entscheidung handelt.

- 18 Der Antrag ist im Ergebnis zulässig.
- 19 Zwar ist er verfrüht und damit nicht fristgerecht eingelegt worden.
- 20 Die Zwei-Wochen-Frist des § 17 Abs. 4 Satz 1 i.V.m. § 21 Abs. 2 Satz 1 WBO beginnt bei einem Antrag gegen eine (Erst-)Maßnahme des Bundesministers der Verteidigung (im Sinne des § 21 Abs. 1 WBO) - in Anlehnung an § 6 Abs. 1 WBO - mit der Kenntnis des Antragstellers von dem Beschwerdeanlass (vgl. u.a. Beschlüsse vom 23. Februar 1972 - BVerwG 1 WB 1.70 - BVerwGE 43, 308 <310>, vom 27. April 2005 - BVerwG 1 WB 8.05 - und vom 1. September 2005 - BVerwG 1 WB 16.05 -; Böttcher/Dau, WBO, 4. Aufl. 1996, § 17 Rn. 80).
- 21 Beschwerdeanlass ist - entsprechend § 17 Abs. 4 Satz 1 WBO - im Regelfall die Bekanntgabe dieser (Erst-)Maßnahme oder Entscheidung des Ministers bzw. des Bundesministeriums der Verteidigung. Das ist bei der Feststellung eines Sicherheitsrisikos durch den Geheimschutzbeauftragten im Bundesministerium der Verteidigung die förmliche Eröffnung dieser Feststellung auf dem Formularblatt nach Anlage C 10 zu Nr. 2710 ZDv 2/30 Teil C. Denn erst die förmliche Eröffnung der Feststellung eines Sicherheitsrisikos begründet die Wirksamkeit dieser Entscheidung (vgl. § 43 Abs. 1 Satz 1 VwVfG). Die Eröffnung des Bescheids über die Feststellung eines Sicherheitsrisikos vom 26. Juli



2006 erfolgte nach der nicht in Frage gestellten Mitteilung des Bundesministers der Verteidigung am 16. August 2006. Der bereits am 10. August 2006 eingegangene Antrag auf gerichtliche Entscheidung vom 8. August 2006 ist damit verfrüht eingelegt worden.

- 22 Indessen ist dieser Antrag durch das Schreiben des Geheimschutzbeauftragten vom 25. Juli 2006 ausgelöst worden, das die Feststellung eines Sicherheitsrisikos ankündigt. Diese Ankündigung stellt zwar noch nicht die - im Sinne des § 17 Abs. 3 WBO anfechtbare - Maßnahme selbst dar. In der Ankündigung wird die bevorstehende Feststellung eines Sicherheitsrisikos dem Antragsteller als dem Betroffenen jedoch in einer Form bekannt gegeben, die keinen Zweifel daran lässt, dass die Entscheidung endgültig ist und vor ihrer förmlichen Bekanntgabe vom Antragsteller nicht mehr beeinflusst werden kann; die Ankündigung enthält zudem für die bereits getroffene Entscheidung über die Feststellung eines Sicherheitsrisikos die - ausschließliche und einzige - Begründung, die dann im Formblatt nach Anlage C 10 zu Nr. 2710 ZDv 2/30 Teil C nicht mehr enthalten ist. Zu berücksichtigen ist schließlich, dass die - ansonsten nicht übliche - „Aufspaltung“ der Entscheidung in ein Ankündigungsschreiben mit Mitteilung der Gründe einerseits und die formblattmäßige Eröffnung des Entscheidungstenors andererseits durch die Besonderheiten des Sicherheitsüberprüfungsverfahrens bedingt ist. Die „Aufspaltung“ bezweckt, dass allein der Betroffene auch die Entscheidungsgründe, seine Dienstvorgesetzten dagegen nur das für sie maßgebliche Ergebnis der Sicherheitsüberprüfung erfahren. Dem - gerade auch dem Schutz des Betroffenen dienenden - Zweck dieser Vorgehensweise entspricht es, dass sich Fehler bei der Einlegung von Rechtsbehelfen, die durch diese „Aufspaltung“ veranlasst sind, nicht zulasten des Betroffenen auswirken sollen, sofern nicht vorrangige andere Interessen einer Korrektur oder Heilung des Fehlers entgegenstehen (vgl. dazu auch Urteil vom 31. August 1966 - BVerwG 5 C 42.65 - BVerwGE 25, 20 <21 f.>).

- 23 Bei einer derartigen Sachlage kann ein Soldat mit der Kenntnisnahme von der Ankündigung und der Mitteilung der Gründe davon ausgehen, dass über die Feststellung bereits eine abschließende Entscheidung gefallen ist. Der daraufhin - vorzeitig - gestellte Antrag auf gerichtliche Entscheidung wird zulässig, wenn die förmliche Bekanntgabe des Feststellungsbescheids spätestens im Zeitpunkt der Rechtshängigkeit des Antrags auf gerichtliche Entscheidung erfolgt ist, d.h. im Zeitpunkt der Vorlage des Antrages beim Wehrdienstgericht (Beschlüsse vom 30. Juli 1974 - BVerwG 1 WB 46.73 - BVerwGE 46, 294 <296>, vom 8. Juli 1980 - BVerwG 1 WB 134.79 - BVerwGE 73, 24 <25> und vom 14. Juni 2006 - BVerwG 1 WB 60.05 - Buchholz 450.1 § 17 WBO Nr. 60 <insoweit nicht veröffentlicht>). Dann liegt auch die erforderliche Beschwer des betroffenen Soldaten vor (vgl. zu dieser Voraussetzung generell: Urteil vom 31. August 1966 a.a.O., Beschluss vom 8. Dezember 1977 - BVerwG 7 B 76.77 - MDR 1978, 600). Der betroffene Soldat ist nach der förmlichen Eröffnung des Feststellungsbescheides nicht genötigt, den Antrag auf gerichtliche Entscheidung noch einmal zu wiederholen.
- 24 Der Antrag ist jedoch unbegründet.
- 25 Der Bescheid des Geheimschutzbeauftragten vom 26. Juli 2006 ist rechtmäßig und verletzt den Antragsteller nicht in seinen Rechten.
- 26 Über den Anfechtungsantrag des Antragstellers ist nach der im Zeitpunkt der Vorlage durch den Bundesminister der Verteidigung - PSZ I 7 - maßgeblichen Sach- und Rechtslage zu entscheiden (Beschluss vom 9. November 2005 - BVerwG 1 WB 19.05 - Buchholz 402.8 § 5 SÜG Nr. 19 <insoweit nicht veröffentlicht>).
- 27 Ob ein Sicherheitsrisiko vorliegt, das einer sicherheitsempfindlichen Tätigkeit eines Soldaten entgegensteht, entscheidet die zuständige Stelle. Die dazu notwendige Überprüfung von Angehörigen der Bundeswehr auf Sicherheitsbedenken ist eine vorbeugende Maßnahme, die Sicherheitsrisiken nach Möglichkeit ausschließen soll (stRspr, u.a. Beschluss vom 9. November 2005 - BVerwG 1 WB 19.05 - a.a.O. m.w.N.). Ein Sicherheitsrisiko im Sinne des § 5 Abs. 1

Satz 1 SÜG liegt u.a. dann vor, wenn tatsächliche Anhaltspunkte Zweifel an der Zuverlässigkeit des Soldaten bei der Wahrnehmung einer sicherheitsempfindlichen Tätigkeit begründen (Nr. 1). Die Beurteilung des Sicherheitsrisikos, die zugleich eine Prognose der künftigen Entwicklung der Persönlichkeit des Soldaten und seiner Verhältnisse darstellt, obliegt der zuständigen Stelle, die ihre Entscheidung aber nicht auf eine vage Vermutung oder eine rein abstrakte Besorgnis stützen darf, sondern auf der Grundlage tatsächlicher Anhaltspunkte zu treffen hat. Dabei gibt es keine „Beweislast“, weder für den Soldaten dahingehend, dass er die Sicherheitsinteressen der Bundeswehr bisher gewahrt hat und künftig wahren wird, noch für die zuständige Stelle, dass der Soldat diesen Erwartungen nicht gerecht geworden ist oder ihnen künftig nicht gerecht werden wird (stRspr, u.a. Beschluss vom 9. November 2005 a.a.O.). Der zuständigen Stelle steht bei der ihr hiernach obliegenden Entscheidung ein Beurteilungsspielraum zu. Die gerichtliche Rechtmäßigkeitskontrolle hat sich darauf zu beschränken, ob sie von einem unrichtigen Sachverhalt ausgegangen ist, den anzuwendenden Begriff oder den gesetzlichen Rahmen, in dem sie sich frei bewegen kann, verkennt, allgemein gültige Wertmaßstäbe nicht beachtet, sachfremde Erwägungen angestellt oder gegen Verfahrensvorschriften verstoßen hat (stRspr, u.a. Beschluss vom 9. November 2005 a.a.O. m.w.N.). Im Zweifel hat das Sicherheitsinteresse Vorrang vor anderen, insbesondere persönlichen Belangen (§ 14 Abs. 3 Satz 2 SÜG).

- 28 Die Feststellung eines Sicherheitsrisikos und das damit verbundene Verbot einer (weiteren) Betrauung des Antragsstellers mit einer sicherheitsempfindlichen Tätigkeit im Bescheid des Geheimschutzbeauftragten im Bundesministerium der Verteidigung vom 26. Juli 2006 steht im Einklang mit den gesetzlichen Vorschriften.
- 29 Der Geheimschutzbeauftragte hat den gesetzlichen Begriff des Sicherheitsrisikos im Sinne des § 5 Abs. 1 SÜG sowie den zu beachtenden Rahmen nicht verkannt. Er hat in seinem Anhörungsschreiben vom 8. Mai 2006, auf das er im Schreiben vom 25. Juli 2006 inhaltlich Bezug nimmt, an Nr. 2414 Abs. 1 ZDv 2/30 Teil C und damit inhaltlich an § 5 Abs. 1 Satz 1 Nr. 1 SÜG angeknüpft und dabei richtigerweise das Tatbestandsmerkmal „Zweifel an der Zuverlässig-

keit“ in den Mittelpunkt der rechtlichen Erwägungen gestellt. Die Wertung, dass derartige Zweifel vorliegen, wenn jemand in einem besonders sicherheitsrelevanten Bereich eines NATO-Hauptquartiers unter Missbrauch seiner Vertrauensstellung als Netzwerk-Administrator gegen IT-Richtlinien, Befehle und Kompetenzregelungen verstößt und damit das Netzwerk der Dienststelle (potentiell) gefährdet, ist rechtlich nicht zu beanstanden. Denn der Begriff der Zuverlässigkeit, der sich in § 5 Abs. 1 Satz 1 Nr. 1 SÜG auf die (jeweilige) ausgeführte sicherheitsempfindliche Tätigkeit bezieht, beinhaltet allgemein, dass sich der betroffene Soldat - auch ohne ständige Kontrolle im Rahmen der Dienstaufsicht - an vorgegebene Regeln hält und dass seine Vorgesetzten darauf vertrauen dürfen, dass er keine eigenmächtige Handlungen vornimmt, die zu Sicherheitsrisiken führen können.

- 30 Der Antragsteller hat auch tatsächlich gegen IT-Sicherheitsbestimmungen, gegen eine Weisung sowie gegen eine Kompetenzregelung verstoßen. Er hat die in seiner damaligen Dienststelle geltenden IT-Sicherheitsinstruktionen („Security Operating Procedures“) Anhang A missachtet, indem er - nach seiner eigenen Einlassung so eingestufte - gefährliche Informationen in Form der sogenannten Key Logging-Programme aus dem Internet in das Netzwerk des Hauptquartiers herunterlud. Ferner hat er entgegen Nr. 146 ZDv 54/100 (IT-Sicherheit in der Bundeswehr) das dadurch verursachte und insbesondere durch das Einstellen der Key Logging-Programme in eine sogenannte Quaratänebox sichtbar gewordene IT-Sicherheitsvorkommnis nicht dem zuständigen IT-Sicherheitsbeauftragten gemeldet. Außerdem hat der Antragsteller gegen das im Entzug der Zugangsberechtigung zu jeglichem Rechner liegende - konkludente - Verbot vom 11. Mai 2005 verstoßen, indem er sich unmittelbar nach der Vernehmung am selben Tag über den ihm zugewiesenen dienstlichen Rechner lokal anmeldete und im „Papierkorb“ auf dem Desktop nach den heruntergeladenen Key-Logging-Programmen suchte. Eine Kompetenzüberschreitung durch den Antragsteller ist darin zu sehen, dass er ohne ausdrücklichen Auftrag seiner Vorgesetzten und trotz fehlender Zuständigkeit dafür als Systemadministrator zwei speicherresistente Key Logging-Programme aus dem Internet herunterlud, um sie - so zumindest seine Einlassung - im Test-Netzwerk des Hauptquartiers „auszuprobieren“.

- 31 Es sind keine Anhaltspunkte dafür ersichtlich, dass im vorliegenden Fall allgemein gültige Wertmaßstäbe verletzt worden sind. Insbesondere ist nach der Art und Nachhaltigkeit der vorgeworfenen Verstöße nicht erkennbar, dass die ermittelten tatsächlichen Anhaltspunkte von so geringem Gewicht sind, dass eine Subsumtion unter den Begriff des Sicherheitsrisikos im Sinne des § 5 Abs. 1 SÜG offensichtlich nicht vertretbar wäre. Nicht zuletzt die Schlüsselfunktion des Antragstellers als IT-Systemunteroffizier schließt es aus, den ihm vorgehaltenen Verstößen lediglich geringfügiges Gewicht beizumessen.
- 32 Der Geheimschutzbeauftragte ist auch nicht von einem unvollständigen oder unrichtigen Sachverhalt ausgegangen. Entgegen der Ansicht des Antragstellers ist davon auszugehen, dass ihm in seiner Vernehmung am 11. Mai 2006 sowohl der Zugang zum Netzwerk als auch zum lokalen Rechner untersagt wurde. Seine ursprüngliche Äußerung im Schreiben vom 22. Mai 2006, es habe nach der Vernehmung durch den Provost Marshall (am 11. Mai 2006) zu keinem Zeitpunkt einen ausdrücklichen „Befehl“ gegeben, dass er das Netzwerk nicht mehr benutzen dürfe, korrigierte er bereits selbst im Schreiben seiner Bevollmächtigten vom 8. August 2006 dahin gehend, dass sein Benutzerkonto gesperrt worden sei. Dem Antragsteller ist damals aber auch der Zugang zu jeglichem Rechner verboten worden. Das ergibt sich eindeutig aus der Vernehmungsniederschrift - in englischer Sprache - vom 12. Mai 2005, die vom Antragsteller unterschrieben wurde. Darin heißt es: „... after being informed that both my NS and PA Lan accounts had been suspended.“ „NS Account“ steht nach unwidersprochen gebliebener Auskunft des Bundesministers der Verteidigung für „Nato-Secret Account“, worunter der allgemeine Zugang zum lokalen Rechner zu verstehen sei. Den Antragsteller entlastet insoweit nicht, dass die Vernehmung nicht in seiner Muttersprache Deutsch, sondern auf Englisch geführt wurde. Es liegen keine Anhaltspunkte dafür vor, dass der in der Vernehmungsniederschrift wiedergegebene Inhalt der Vernehmung vom 12. Mai 2005 unrichtig ist; dies hat auch der Antragsteller nicht behauptet. Überdies ist davon auszugehen, dass dem Antragsteller als in einem NATO-Hauptquartier eingesetzten IT-Systemadministrator der oben genannte englische Fachbegriff in seiner Bedeutung bekannt war; Gegenteiliges hat er nicht vorgetragen.

- 33 Anzeichen dafür, dass der Geheimschutzbeauftragte bei der Entscheidung über das Bestehen eines Sicherheitsrisikos sachfremde Erwägungen angestellt hat, sind nicht gegeben. Derartiges behauptet auch der Antragsteller nicht.
- 34 Die gesetzlichen Vorgaben für die Güterabwägung im Sinne des § 14 Abs. 3 SÜG, die im Zweifel dem Sicherheitsinteresse den Vorrang einräumen, wurden beachtet.
- 35 Auf die für die Beurteilung eines Sicherheitsrisikos notwendige Prognose der künftigen Entwicklung der Persönlichkeit des Soldaten und seiner Verhältnisse (vgl. dazu u.a. Beschluss vom 24. Januar 2006 - BVerwG 1 WB 17.05 - Buchholz 402.8 § 5 SÜG Nr. 20 = NZWehrr 2006, 153) ist der Bundesminister der Verteidigung - PSZ I 7 - im Vorlageschreiben eingegangen. Die Einschätzung, dass keine gesicherte positive Prognose gestellt werden könne, weil das Fehlverhalten nur etwa ein Jahr zurückliege und der Antragsteller erst über einen längeren Zeitraum durch eine tadellose Führung und durch sein sonstiges Verhalten zeigen müsse, dass ihm wieder uneingeschränkt Vertrauen entgegengebracht werden könne, ist rechtlich nicht zu beanstanden. Der Zeitaspekt als Anknüpfungspunkt ist zulässig, weil eine zuverlässige Prognose typischerweise einen aussagekräftigen - verstrichenen - Zeitraum zwischen dem Anhaltspunkt für ein Sicherheitsrisiko und der Entscheidung darüber voraussetzt. Die Erwägung, dass dazu ein Zeitraum von einem Jahr nicht ausreicht, ist angesichts der in § 12 Abs. 2 Satz 1 Nr. 1 SÜG zum Ausdruck kommenden (Regel-)Anforderung an die zeitliche Ermittlungstiefe zu billigen.
- 36 Schließlich sind auch keine Verfahrensverstöße ersichtlich.
- 37 Im vorliegenden Fall war die Durchführung einer Sicherheitsüberprüfung erforderlich, weil der Antragsteller nach Mitteilung des stellvertretenden Sicherheitsbeauftragten seiner damaligen Dienststelle - als IT-Systemunteroffizier - Zugang zu Unterlagen mit dem Verschlussgrad „Streng Geheim“ einschließlich vergleichbarer Geheimhaltungsgrade erhalten sollte bzw. hatte und mit einer sicherheitsempfindlichen Tätigkeit betraut werden sollte (vgl. § 2 Abs. 1 Satz 1 i.V.m. § 1 Abs. 2 Nr. 1, 2 SÜG).

- 38 Der Geheimschutzbeauftragte war auch zuständige Stelle für die Beurteilung, ob ein Sicherheitsrisiko vorliegt (§ 14 Abs. 3 Satz 1 SÜG) und ob die Betrauung mit einer sicherheitsempfindlichen Tätigkeit erfolgen kann oder abgelehnt werden muss (§ 14 Abs. 4 i.V.m. § 2 Abs. 1 Satz 1 SÜG). Das ergibt sich für Verfahren der erweiterten Sicherheitsüberprüfung mit Sicherheitsermittlungen (Ü 3) aus § 3 Abs. 1 Satz 1 Nr. 1 i.V.m. § 35 Abs. 3 SÜG und Nr. 2416 ZDv 2/30 Teil C. Grundlage für die nach § 14 Abs. 3 und 4 SÜG zu treffende Entscheidung der zuständigen Stelle sind die Ermittlungen und Maßnahmen der mitwirkenden Behörde nach Maßgabe des § 14 Abs. 1 und 2 SÜG. Mitwirkende Behörde im Sicherheitsüberprüfungsverfahren ist im Geschäftsbereich des Bundesministeriums der Verteidigung nach § 3 Abs. 2 SÜG und § 1 Abs. 3 Satz 1 Nr. 1 Buchst. a und b MADG der Militärische Abschirmdienst.
- 39 Dem Antragsteller wurde durch Schreiben des Geheimschutzbeauftragten vom 8. Mai 2006 Gelegenheit zur Stellungnahme gegeben. Seinem Anspruch auf Wahrung des rechtlichen Gehörs gemäß § 14 Abs. 3 Satz 3 i.V.m. § 6 Abs. 1 Satz 1 SÜG ist damit Rechnung getragen worden.
- 40 Ein Verstoß gegen die Prüfungspflicht nach Nr. 2709 ZDv 2/30 Teil C liegt nicht vor. Es kann dahingestellt bleiben, ob der Geheimschutzbeauftragte bei seiner Entscheidung diese Verfahrensbestimmung beachtet hat. Denn der Bundesminister der Verteidigung hat dazu noch rechtzeitig in seinem Vorlageschreiben vom 9. November 2006 Stellung genommen und dabei nachvollziehbar dargelegt, dass wegen der Uneinsichtigkeit des Antragstellers auch unter Fürsorgegesichtspunkten keine andere Bewertung in Betracht komme.
- 41 Die Ausdehnung der Feststellung eines Sicherheitsrisikos auf die Verwendung in einer sicherheitsempfindlichen Tätigkeit der Überprüfungsarten Ü 1 und Ü 2 ist ebenfalls rechtlich nicht zu beanstanden. Die Feststellung eines Sicherheitsrisikos nach Nr. 2414 Satz 1 Nr. 1 ZDv 2/30 Teil C stellt auch die Zuverlässigkeit des Betroffenen beim Umgang oder Zugang zu Verschlusssachen der Überprüfungsarten Ü 1 und Ü 2 generell in Frage.