

# Geheimchutz in der Sicherheitsforschung

## Aktuelle Entwicklungen und Trends im Geheimchutz

Bedingt durch die in den letzten Jahren aufkommende asymmetrische Bedrohung ist von staatlichen Stellen eine vermehrte Aktivität zur Gefahrenabwehr im Bereich der öffentlichen Sicherheit zu beobachten. Hinweise hierfür gibt das neue vom BMBF vorbereitete Programm zur zivilen „Sicherheitsforschung“. Es zielt auf einen bisher noch nicht ausreichend abgedeckten Bereich ab, Forschung für Sicherheit vor Terrorismus, Kriminalität oder Sabotage und den Folgen von Naturkatastrophen oder Unfällen besonderen Ausmaßes zu leisten<sup>1</sup>.

Auch im Rahmen der europäischen Union ist die Gefahrenabwehr ein Thema von steigendem Interesse. So liegt ein wesentlicher Schwerpunkt des kommenden 7. Forschungsrahmenprogramms im Bereich der Sicherheitsforschung<sup>2</sup>.

Künftige Projekte im Bereich der Sicherheitsforschung werden, wie auch schon heute Projekte aus dem Bereich der Verteidigungsforschung, häufig sicherheitssensible Aktivitäten beinhalten. Hierfür ist mit dem Geheimchutzverfahren die Möglichkeit gegeben, solche Projekte als Verschlusssache (VS) einzustufen<sup>3</sup>. Eine Einstufung erfolgt bereits, wenn die Kenntnisnahme durch Unbefugte für die Interessen der Bundesrepublik Deutschland oder eines ihrer Länder nachteilig sein kann.

Viele verteidigungsbezogene F&E-Projekte sind bereits heute als Verschlusssache eingestuft. Rüstungsunternehmen und verteidigungsbezogene Forschungsinstitute haben daher Infrastrukturen zur Bearbeitung von Verschlusssachen aufgebaut.

Es ist zu erwarten, dass auch künftige Projekte im Bereich der zivilen Sicherheitsforschung zunehmend einer VS-Einstufung unterliegen werden. Um diese VS-Aufträge akquirieren zu können sind vorab organisatorische und informationstechnische Maßnahmen nach dem Geheimchutzhandbuch notwendig.

Die informationstechnischen Maßnahmen zur Bearbeitung von Verschlusssachen mit IT werden bedingt durch den Fortschritt im Bereich der Informationstechnologie preiswerter und komfortabler. Hierfür sind im Folgenden drei Beispiele aufgeführt.

Für die geforderte mehrfache Überschreibung beim Löschen von Datenträgern gibt es derzeit preisgünstige, von BSI empfohlene Produkte<sup>4</sup>.

Waren strahlungsabgeschirmte Rechner noch vor wenigen Jahren klobig und kosteten bei gleicher Leistung das 10 fache von herkömmlichen Rechnern, so ist heute ihr Äußeres nicht mehr von herkömmlichen Rechnern zu unterscheiden. Die Kosten sind auf das 1,5 bis 2 fache gefallen<sup>5</sup>.

---

<sup>1</sup> Vgl. Rede der Bundesministerin für Bildung und Forschung, Dr. Annette Schavan, MdB zu "Sicherheitsforschung - Herausforderung und Notwendigkeit zum Schutz der Gesellschaft" anlässlich der Konferenz "Future Security" am 04. Juli 2006 (URL: <http://www.bmbf.de>)

<sup>2</sup> Vgl. 7. Rahmenprogramm (URL: <http://www.cordis.lu>)

<sup>3</sup> Vgl. Geheimchutzhandbuch (URL: <http://www.bmwi-sicherheitsforum.de/>)

<sup>4</sup> Vgl. VS-Clean (URL: <http://www.bsi.de/>)

<sup>5</sup> Vgl. URL: <http://www.eglgmbh.de/>

Das Versenden von VS-eingestufter Information über das Internet ist erst seit 4 Jahren möglich. Vorher konnte dies nur über eine Standleitung (oder alternativ durch einen Boten) erfolgen<sup>6</sup>.

Der Aufbau einer VS-Infrastruktur für den niedrigsten Einstufungsgrad „VS – Nur für den Dienstgebrauch“ ist relativ preisgünstig realisierbar. Damit sind die Möglichkeiten geschaffen um VS-Aufträge dieser Einstufung akquirieren zu können.

Ein Einstieg in die VS-Infrastruktur könnte sich auch für diejenigen lohnen, die keine VS-Aufträge annehmen, denn die Aussage „Wir dürfen auch staatliche Verschlusssachen bearbeiten“ schafft beim Kunden die Gewissheit, dass mit seinen Daten auch vertrauensvoll umgegangen wird.

Dirk Thorleuchter  
Fraunhofer Institut für Naturwissenschaftlich-Technische Trendanalysen (FhG INT)  
Appelsgarten 2

53879 Euskirchen

---

<sup>6</sup> Vgl. SINA (URL: <http://www.secunet.com/>)