dem Kultusministerium erhebliche datenschutzrechtliche Verbesserungen bei der Konzeption von ASV erreicht werden konnten.

Gegen das Gesetz zur Errichtung einer standardisierten zentralen Antiterrordatei von Polizeibehörden und Nachrichtendiensten von Bund und Ländern (Antiterrordateigesetz-ATDG) sind erhebliche verfassungsrechtliche Bedenken erhoben worden, über die bereits im 22. Tätigkeitsbericht 2006 berichtet wurde. Nun ist gegen das ATDG eine Verfassungsbeschwerde eingelegt worden, über die beim Bundesverfassungsgericht im November 2012 mündlich verhandelt worden ist. Möglicherweise wird das Verfahren auch die umstrittene Frage klären, ob und inwieweit das sogenannte Trennungsgebot einer Zusammenarbeit von Polizei und Nachrichtendiensten entgegensteht. Der Verfahrensausgang wird sich überdies auf die Beurteilung der neu errichteten Rechtsextremismusdatei auswirken.

Einen zentralen Prüfungsschwerpunkt im Berichtszeitraum bildete der Einsatz des „Staatstrojaners" durch bayerische Strafverfolgungsbehörden im Zusammenhang mit der Durchführung von Maßnahmen zur Quellen-Telekommunikationsüberwachung. Die Ergebnisse dieser Prüfung werden nochmals zusammenfassend dargestellt. Sollte an der Quellen-Telekommunikationsüberwachung weiter festgehalten werden, empfehle ich dringend, gesetzliche Bestimmungen zu schaffen, die der erhöhten Eingriffsintensität und den technischen Besonderheiten dieser Maßnahme gerecht werden.

Die Einhaltung des Personaldatenschutzrechts hat der BayLfD in mehreren Kommunen verstärkt überprüft. Regelmäßig bemühten sich die geprüften Stellen ernsthaft um die Einhaltung der datenschutzrechtlichen Bestimmungen. Im Rahmen der Kontrollen waren gleichwohl eine nicht unerhebliche Anzahl von Mängeln festzustellen.

Zudem hat der BayLfD beim Personaldatenschutz zahlreiche grundlegende Verbesserungen bewirken können: Bei der beamtenrechtlichen Beihilfe wurde endlich die – im Übrigen auch von der betroffenen Ärzteschaft seit langem geforderte – Pseudonymisierung im Psychotherapie-Begutachtungsverfahren in der Bayerischen Beihilfeverordnung fest verankert. Dies ist ein wesentlicher Fortschritt zur Wahrung der Datenschutzrechte der betroffenen Beihilfeberechtigten, aber auch ihrer Angehörigen. In den vom Bayerischen Finanzministerium erarbeiteten Leitfaden Betriebliches Eingliederungsmanagement haben die von mir aufgestellten datenschutzrechtlichen Anforderungen Eingang gefunden. Die datenschutzkonforme Ausgestaltung wird sicherlich dazu beitragen, die Akzeptanz dieses Verfahrens bei den Betroffenen zu fördern. Im staatlichen Bereich ist nun auch das Regressverfahren nach Dienst- und sonstigen Unfällen datenschutzkonform geregelt. Die Übermittlung personenbezogener (Gesundheits-)Daten an die Schadensersatzpflichtigen wird damit auf das notwendige Maß beschränkt.

Der Trend zur Zusammenfassung der IT-Ressourcen des Freistaats in wenigen Standorten hat sich ansonsten weiter fortgesetzt. In diesem Zusammenhang hat der CIO-Rat eine vom Staatsministerium des Innern und der CIO-Stabsstelle erarbeitete Musterrahmenvereinbarung zur Auftragsdatenverarbeitung gebilligt und der Staatskanzlei und den Ressorts deren Verwendung empfohlen. Sie reduziert das Risiko von widersprüchlichen Anforderungen an die Rechenzentren und den hohen Aufwand an Einzelvereinbarungen zwischen den Auftrag gebenden öffentlichen Stellen und den Rechenzentren. Der BayLfD hat die Erstellung der Musterrahmenvereinbarung begleitet und wird das Vorliegen solcher Regelungen zur Auftragsdatenverarbeitung prüfen.

Der 25. TB ist auf der Website des BayLfD verfügbar: *http://www.datenschutz-bayern.de/*

Neues IT-Sicherheitsexpertenzertifikat „TeleTrusT Engineer for System Security" (T.E.S.S.)

Der Bundesverband IT-Sicherheit e.V. (TeleTrusT) führt unter der Bezeichnung „TeleTrusT Engineer for System Security" ein neues Expertenzertifikat ein. Schulungsanbieter sind secorvo Security Consulting und isits, die Prüfungen werden durch PersCert TÜV abgenommen.

Die Zuverlässigkeit heutiger, oft sehr komplexer IT-Lösungen, Produkte oder IT-Dienstleistungen hängt von ihrer Sicherheit ab. In vielen Fällen wird mit Sicherheitsarchitekturen gearbeitet, die aus einem Bündel nicht zusammenhängender Maßnahmen bestehen. Bei der Umsetzung werden deshalb Kosten- und Zeitrahmen nicht eingehalten und die Sicherheit bleibt auf der Strecke. Moderne IT-Lösungen bestehen aus vielen Einzelkomponenten. Die Sicherheitseigenschaften eines Systems lassen sich nicht ohne weiteres aus Sicherheitseigenschaften der Einzelkomponenten ableiten, sondern ergeben sich aus deren Zusammenwirken. Security Engineering setzt mit dem Prinzip „Security by design" an der Wurzel an. Wird Sicherheit von Anfang an bei der Konzeption über alle Komponenten eines Systems mitgedacht, lässt sie sich auch wirtschaftlich in hoher Qualität implementieren. Die dafür notwendige spezielle Qualifikation wird dem neuen Expertenzertifikat nachgewiesen.

Das Personenzertifikat T.E.S.S. belegt, dass sich der Absolvent intensiv mit Security Engineering auseinandergesetzt sowie das Prinzip „Security by design" verstanden hat und umsetzen kann. Die Prüfung zum T.E.S.S. fragt ab, ob der Teilnehmer in der Lage ist, „Security by design" auf die Entwicklung unterschiedlichster Systeme anzuwenden und damit Sicherheit angemessen und erfolgreich implementieren können.

Die Einführung des T.E.S.S. ist ein wichtiger Beitrag, um in Zukunft das Thema Sicherheit besser in neue IT-Lösungen, Produkte, Systeme und IT-Services zu integrieren und somit auch ein Beitrag zur Wettbewerbsfähigkeit der Industrie.
Weitere Informationen unter: *http://www.teletrust.de/tess/*

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 25. Januar 2013

Beschäftigtendatenschutz nicht abbauen, sondern stärken!
Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder erinnert an ihre Entschließung vom 16./17. März 2011 und ihre Forderung nach speziellen Regelungen zum Beschäftigtendatenschutz. Bei einer Gesamtbetrachtung ist die Konferenz enttäuscht von dem jetzt veröffentlichten Änderungsentwurf der Koalitionsfraktionen.

Bereits der ursprünglich von der Bundesregierung vorgelegte Entwurf enthielt aus Datenschutzsicht erhebliche Mängel. Der nun