Auszug aus

Denkschrift 2016

zur Haushalts- und Wirtschaftsführung
des Landes Baden-Württemberg

Beitrag Nr. 8

Informationssicherheit in der Landesverwaltung

Baden-Württemberg

RECHNUNGSHOF

Informationssicherheit in der Landesverwaltung

Die Landesverwaltung sollte Belange der Informationssicherheit künftig stärker beachten. Informationssicherheit ist eine Managementaufgabe. Beim Aufbau des Informationssicherheitsmanagements sollten Kompetenzen gebündelt werden.

1 Ausgangslage

Die Landesverwaltung nutzt in allen Bereichen für die Aufgabenerledigung IT-Systeme unterschiedlicher Art. Der Durchdringungsgrad ist in den letzten Jahren immer größer geworden. Er wird in Anbetracht von E- und Open-Government, der demografischen Entwicklung in der Bevölkerung und bei den Beschäftigten der öffentlichen Verwaltung und deren zunehmend mobileren Arbeitsplätzen weiter steigen. Infolgedessen nahm und nimmt die Abhängigkeit von IT-Systemen stark zu. Die in letzter Zeit bekannt gewordenen Zugriffe auf vermeintlich geschützte vertrauliche Daten fokussieren gleichzeitig aber auch den Schutzbedarf der in IT-Systemen verarbeiteten Daten von Bürgerinnen und Bürgern, der Wirtschaft und der öffentlichen Verwaltung.

1.1 Vorgaben für Informationssicherheit

Seit vielen Jahren gibt die Verwaltungsvorschrift über die Standards des E-Government-Konzepts Baden-Württemberg auch Vorgaben für die Informationssicherheit in der Landesverwaltung. Das Innenministerium aktualisiert die Vorschrift in regelmäßigen Abständen nach Abstimmung mit allen Ressorts.

Die Standards in der aktuellen Fassung legen u. a. fest, dass

- der Datenschutz und die Informationssicherheit bei allen IT-Maßnahmen von Anfang an zu beachten sind,
- die IT-Leitstellen und die IT-Dienstleister sicherstellen, dass der Datenschutz und die Informationssicherheit beachtet werden,
- der Schutzbedarf eines IT-Systems im Rahmen der Einsatzplanung festzustellen ist und
- für eingesetzte IT-Systeme ein Sicherheitskonzept zu erstellen ist, das sich an den Handlungsanleitungen und Standards des Bundesamts für Sicherheit in der Informationstechnik (BSI) orientiert.

Im Zuge der Föderalismusreform II wurde die Zusammenarbeit von Bund und Ländern bei der IT-Sicherheit verstärkt. Das zuständige Bund-Länder-Gremium, der IT-Planungsrat, kann verbindlich Standards und Anforderungen zur IT-Sicherheit festlegen (Artikel 91c Grundgesetz). Der IT-Planungsrat hat auch mit der Stimme Baden-Württembergs die Leitlinie zur Informationssicherheit in der öffentlichen Verwaltung (Beschluss 2013/01 des IT-Planungsrats) verabschiedet. Sie weitet den Blick von einer reinen IT-Sicherheit hin zu einem generellen Schutz von Informationen auch außer-

halb von IT-Systemen. Informationssicherheit umfasst auch immer den Schutz personenbezogener Daten nach dem geltenden Datenschutzrecht.

Die vorstehend benannte Informationssicherheitsleitlinie und der dazu verabschiedete Umsetzungsplan bindet auch Baden-Württemberg. Demnach sind bis März 2018

- ein Informationssicherheitsmanagement im Land einzuführen,
- ein Landes-IT-Sicherheitsbeauftragter und IT-Sicherheitsbeauftragte für die wesentlichen Behörden zu benennen und
- eine verbindliche Leitlinie für die Informationssicherheit im Land einzuführen.

1.2 Gegenstand der Prüfung

Der Rechnungshof hat sich in der aktuellen Orientierungsprüfung auf die allgemeine Innenverwaltung beschränkt. Ansprechpartner waren damit das Innenministerium und die Regierungspräsidien. Der Themenkreis IT-Sicherheit ist zudem Bestandteil der meisten IT-Prüfungen. Hier hat der Rechnungshof in der Vergangenheit einzelfallbezogen Defizite aufgezeigt. Sie reichen von einer unzureichenden Ausfallvorsorge der IT im Falle von Großschadensereignissen bis hin zu getrennten Zuständigkeiten und Vorgehensweisen für sicherheitsrelevante IT-Komponenten.[1] Bei der Orientierungsprüfung wurde für den Bereich des Innenministeriums und der Regierungspräsidien beispielhaft untersucht, für welche Dienststellen und Fachverfahren Sicherheitskonzepte vorliegen. Basis dafür war eine Liste von IT-Verfahren, welche im Rahmen eines Migrationsprojekts der IT-Systeme der Regierungspräsidien erstellt wurde. Sie enthielt insbesondere Angaben zu IT-Standardprogrammen und IT-Fachverfahren. Durch den Bündelungscharakter der Regierungspräsidien konnten so viele der vom Land erstellten und beim Land eingesetzten IT-Fachverfahren in die Betrachtungen einbezogen werden. Zusammen mit dem Innenministerium und den Regierungspräsidien wurde diese Liste im Hinblick auf Fragestellungen der Informationssicherheit ergänzt, validiert, verdichtet und hinsichtlich der fachlichen Verantwortung zusammen mit dem Innenministerium und den Regierungspräsidien gruppiert.

2 Prüfungsergebnisse

2.1 Sachstand des Informationssicherheitsmanagements

Das Land hat seit vielen Jahren einen landesweit zuständigen IT-Sicherheitsbeauftragten im Innenministerium bestellt. Eine der Anforderungen der

---

[1] Zum Beispiel Beitrag Nr. 4 der Denkschrift 2009 „IuK-Ausfallvorsorge für Großschadensfälle“ (Landtagsdrucksache 14/4704), Beitrag Nr. 7 der Denkschrift 2014 „Das Informatikzentrum Landesverwaltung Baden-Württemberg“ (Landtagsdrucksache 15/5407) und Beitrag Nr. 11 der Denkschrift 2015 „IT-Neuordnung im Geschäftsbereich des Ministeriums für Finanzen und Wirtschaft“ (Landtagsdrucksache 15/7011).

Informationssicherheitsleitlinie ist damit erfüllt. Der IT-Sicherheitsbeauftragte muss diese Funktion jedoch neben vielen anderen zentralen Aufgaben der landesweiten IT-Koordination ausüben.

Unter der Federführung des IT-Sicherheitsbeauftragten der Landesregierung entstand in einer Arbeitsgruppe eine Informationssicherheitsleitlinie Baden-Württemberg als Entwurf einer „Verwaltungsvorschrift der Landesregierung zur Informationssicherheit (VwV Informationssicherheit)". Sie war bis Juni 2016 noch nicht verabschiedet und in Kraft gesetzt.

Im Ergebnis erfüllt das Land im Hinblick auf die vorstehend angeführten drei Punkte der Informationssicherheitsleitlinie bislang nur einen Aspekt, nämlich die formale Bestellung des Landes-IT-Sicherheitsbeauftragten. Vorgaben zur Informationssicherheit beschränken sich bislang nur auf wenige Ausnahmen. Eine Basis für ein funktionsfähiges Informationssicherheitsmanagement in Baden-Württemberg ist deshalb nicht gelegt. In Anbetracht der bereits vor drei Jahren verabschiedeten Informationssicherheitsleitlinie und dem Zeithorizont bis 2018 gibt es deshalb erheblichen Handlungsbedarf.

Neben den vorgenannten formalen Aspekten, welche die Informationssicherheitsleitlinie formuliert, gibt es viele weitere konkrete Aufträge. Sie setzen weitgehend entsprechende Strukturen für ein Informationssicherheitsmanagement voraus oder sind Aufgabe der Landesoberbehörde Informationstechnik Baden-Württemberg (BITBW). Letztere muss dafür teilweise noch Ressourcen bündeln, die Aufgaben strukturieren und weiteres Know-how aufbauen, z. B. im landesweiten Computer Emergency Response Team (CERT).

2.2 Sicherheitskonzepte

Zum Zeitpunkt der Erhebung gab es 50 IT-Fachverfahren im Innenministerium und 561 IT-Fachverfahren aus unterschiedlichen Ressorts bei den vier Regierungspräsidien.

Die Erkenntnisse lassen sich wie folgt zusammenfassen: Es fehlen bisher einheitliche Vorgaben und ein abgestimmtes Vorgehen für die Erstellung, laufende Prüfung auf Fortschreibungsbedarf und Pflege von Sicherheitskonzepten. Eine Übersicht über bestehende und fehlende Sicherheitskonzepte an zentraler Stelle, etwa beim IT-Sicherheitsbeauftragten der Landesverwaltung, ist bisher nicht vorhanden. Sowohl auf der Basis der E-Government-Standards Baden-Württemberg als auch im Hinblick auf die im IT-Planungsrat verabschiedete Informationssicherheitsleitlinie besteht dringender Handlungsbedarf, ein Informationssicherheitsmanagement zu etablieren und aufrechtzuerhalten.

2.3 IT-Sicherheit und IT-Standardisierung

Die Prüfung zeigt aber auch Folgendes deutlich: Insbesondere bei den Regierungspräsidien müssen für gleiche Aufgabenstellungen unterschiedliche Programme oder unterschiedliche Versionen gleicher Programme funktionsfähig bereitgestellt werden. Ursache ist, dass entsprechende Vorgaben aus den Fachverwaltungen formuliert werden. Hinzu kommen unterschiedliche

Grafikwerkzeuge oder verschiedene, teilweise auch stark überalterte Software-Versionen. Diese Vielfalt verteuert den IT-Betrieb. Es müssen unnötigerweise mehr Programme installiert und betrieben werden als notwendig. Die Vielfalt wirkt sich aber auch auf die Informationssicherheit aus. Eine Vielzahl von - unnötigen - Programmen erhöht die Komplexität des IT-Systems und die potenziellen Angriffsmöglichkeiten. Die Pflege der Programme sowohl hinsichtlich der laufenden Aktualisierung von Versionsständen bei Bekanntwerden von Schwachstellen, als auch der zugehörigen Sicherheitsdokumentation gestaltet sich erheblich aufwendiger, als dies bei einer geringeren Anzahl standardisierter Programme der Fall wäre. Eine Standardisierung und eine Beschränkung auf das notwendige Maß der einzusetzenden Programme und Fachverfahren sind anzustreben, um die Komplexität des IT-Systems und die potenziellen Angriffsmöglichkeiten zu minimieren.

2.4 Bündelung von Know-how

Der Rechnungshof hat bereits in den Denkschriften 2005 und 2008 gefordert, den Betrieb des Datennetzes und der Firewall-Systeme zu bündeln. Diese Bündelung ist zwar vorangeschritten, aber bei Weitem noch nicht abgeschlossen.

Im CERT des Landes werden bereits IT-Sicherheitsthemen zentral für die Landesverwaltung wahrgenommen. Bislang war es jedoch als virtuelles, d. h. auf mehrere Dienststellen verteiltes CERT ohne Weisungs- oder konkrete Handlungsbefugnisse tätig.

Das seit 01.07.2015 in Kraft getretene Gesetz zur Errichtung der Landesoberbehörde IT Baden-Württemberg (BITBWG) ordnet die vorstehenden Aufgaben jetzt landesweit einer Stelle, der BITBW, zu.

Diese beiden Einzelmaßnahmen reichen jedoch nicht aus, für ein angemessenes Niveau der Informationssicherheit zu sorgen. Es ist insbesondere zu beachten, dass die Fragestellungen und Lösungsansätze vielfältig sind, müssen sie doch sowohl rechtliche, organisatorische und technische Aspekte „unter einen Hut" bringen. Dafür ist teilweise sehr spezifisches Wissen notwendig. Verantwortlich für die Einhaltung der Informationssicherheit ist nach aktueller Rechtslage die jeweilige Dienststellenleitung. Sie kann sich jedoch durch die Bestellung eines Informationssicherheitsbeauftragten in dieser Aufgabe beraten und unterstützen lassen. Bei kleinen Dienststellen und Organisationseinheiten wäre es dennoch unwirtschaftlich, das Wissen hinreichend wirtschaftlich aufzubauen und vorzuhalten. Zumindest Dienststellen mit gleichartigen Aufgaben sollten entsprechende Kompetenzen bündeln. Nur so kann die Aufgabe inhaltlich kompetent und gleichsam wirtschaftlich erledigt werden.

Auch aus Wirtschaftlichkeitsgründen sollte eine Bündelung von Wissen und Methoden einer integrierten Informationssicherheit auch für die Entwicklung und Pflege von IT-Fachverfahren angestrebt werden. Heute befassen sich noch viele verschiedene Stellen in der Landesverwaltung mit der Entwicklung und Pflege von IT-Verfahren. Die entsprechende Dienstleistung soll nach dem BITBWG erst in den nächsten Jahren in der BITBW weitgehend konzentriert werden.

2.5 Auditierung und Zertifizierung

Die vom IT-Planungsrat verabschiedete Informationssicherheitsleitlinie gibt vor, dass „zur Absicherung der Netzinfrastrukturen" als Maßnahme der Qualitätssicherung ein „Prozess der gegenseitigen Auditierung" vorgesehen werden soll. Damit ist nicht festgelegt, welche Einrichtungen wie oft auditiert werden sollen.

Aus einer anderen Prüfung ist bekannt, dass Audits und davon abgeleitete Zertifizierungen mit nennenswertem finanziellem Aufwand extern beauftragt wurden. Die daraus generierten Zertifikate haben generell eine Befristung. Würde die Landesverwaltung zukünftig stärker auf eine externe Auditierung und Zertifizierung bauen, so würden daraus erhebliche finanzielle Aufwände folgen. Audits zur Qualitätssicherung müssen im Hinblick auf das Vorgehen wirtschaftlich durchgeführt werden.

3 Empfehlungen

Um ein angemessenes Sicherheitsniveau zu erreichen, müssen folgende Maßnahmen ergriffen werden.

3.1 Vielfalt der IT-Systeme reduzieren

Die heute noch anzutreffende Vielfalt der IT-Systeme und -Verfahren und die eingesetzten Versionen muss stark reduziert werden.

3.2 Hauptamtlichen Informationssicherheitsbeauftragten bestellen

Zur zentralen Steuerung und in Übereinstimmung mit den Vorgaben der Informationssicherheitsleitlinie des IT-Planungsrats sollte die Landesregierung einen hauptamtlichen Informationssicherheitsbeauftragten bestellen. Er sollte mit hinreichenden Ressourcen und Rechten ausgestattet werden, um seine Aufgaben erfüllen zu können.

3.3 Informationssicherheit bei IT-Fachverfahren mit betrachten

Um unnötigen Aufwand zu vermeiden, sollte die Landesverwaltung die Informationssicherheit bei der Neueinführung oder der Modernisierung von IT-Verfahren von Anfang an mit betrachten. Das Thema muss entsprechend den E-Government-Standards als integraler Bestandteil der Konzeption von Verfahren und Systemen behandelt werden.

3.4 Kenntnisse der Mitarbeiter zur Informationssicherheit verbessern

Alle in der IT und der Organisation tätigen Mitarbeiter der Landesverwaltung sollten über hinreichende Grundkenntnisse der Informationssicherheit verfügen.

Sicherheitsrisiken können auch durch menschliches Fehlverhalten entstehen. Daher sollten alle Mitarbeitenden der Landesverwaltung regelmäßig für das Thema Informationssicherheit sensibilisiert werden.

3.5 Aufgaben zentralisieren

Aufgaben, die tiefergehende Kennnisse erfordern, sollten zentral an einer Stelle wahrgenommen werden. Das CERT Baden-Württemberg ist dafür ein Beispiel. Seine Befugnisse müssen jedoch durch Weisungs- oder eigenständige Handlungsbefugnisse gestärkt werden. Die Bündelung von Netzwerk- und Firewall-Themen muss noch vollständig umgesetzt werden.

3.6 Informationssicherheit zur Managementaufgabe machen

Behördenleiter müssen sich die Aufgabe Informationssicherheit als Managementaufgabe zu eigen machen. Bei deren Umsetzung sollten sie sich der Unterstützung durch fähige IT-Sicherheitsbeauftragte innerhalb großer Dienststellen oder aus einem Kompetenzzentrum versichern.

3.7 Audits festlegen

Im Rahmen der Qualitätssicherung sollte die Landesverwaltung festlegen, ob und wie oft Einrichtungen und IT-Verfahren auditiert werden sollen. Entscheidend sind nicht formale Zertifizierungen, sondern die Einhaltung der Sicherheitsstandards. Aus Audits abgeleitete formale Zertifizierungen sollten auf das unbedingt notwendige Maß begrenzt werden. Vielfach können auch verwaltungsinterne Audits zu sachgerechten und wirtschaftlichen Ergebnissen führen. Dafür können auch ressort- oder länderübergreifende Lösungen in Betracht gezogen werden.

4 Stellungnahme des Beauftragen des Landes für Informationstechnologie

Der Beauftrage des Landes für Informationstechnologie führt in seiner Stellungnahme ergänzend aus, dass zur Qualitätssicherung von Maßnahmen der Informationssicherheit Audit-Prozesse notwendig seien. Die Beschlüsse des IT-Planungsrats sähen dazu bislang vor, dass formale Auditierungen und Zertifizierungen aus wirtschaftlichen Gründen auf die Fälle beschränkt werden sollen, in denen diese gesetzlich vorgeschrieben seien. In anderen Fällen sollen grundsätzlich gegenseitige verwaltungsinterne Auditierungen zugelassen werden. Im Übrigen teile er die Bewertungen und Empfehlungen. Einige Aspekte würden bereits entsprechend vorbereitet oder angewandt.