Rechnungshöfe des Bundes und der Länder

Grundsatzpapier zum Informationssicherheits-management

8. bis 10. Juni 2015

Entwurf des Arbeitskreises Organisation und Informationstechnik

Inhaltsverzeichnis

0 Präambel

Der digitale Wandel stellt den Staat[1] vor neue Herausforderungen:

Die Ausübung der verfassungsrechtlich garantierten Aufgaben der judikativen, legislativen und exekutiven Staatsgewalten setzt einen sicheren und zuverlässigen Betrieb der Informationssysteme des Staates voraus.

Die Gewährleistung eines effektiven Rechtsschutzes gegen Akte der öffentlichen Gewalt nach Artikel 19 Abs. 4 GG und des Rechtsstaatsprinzips nach Artikel 20 Abs. 3 GG erfordern in der öffentlichen Verwaltung eine lückenlose und gegen Manipulationen geschützte Kommunikation und eine Dokumentation des Verwaltungshandelns.

Das Vertrauen der Bürger und Unternehmen in die Integrität des digitalen Staates wird erschüttert, wenn sie ihren Aufgaben wegen funktionsunfähiger Informationssysteme nicht mehr nachkommen können. Die Informationssysteme in den Staatsgewalten sind dadurch zu kritischen Infrastrukturen für das Gemeinwesen geworden.

Aktuelle Berichterstattungen in den Medien über nationale und internationale Spionage und Cyber-Kriminalität zeigen, dass die Sicherheit von Daten Dritter gefährdet ist und dass das staatliche Gemeinwesen neuartigen Gefährdungslagen ausgesetzt ist.

Die elektronische Verwaltungsarbeit geht mit der Speicherung von elektronischen Daten auf Netzlaufwerken, E-Mail-Systemen und Dokumentenmanagementsystemen einher. Aktuelle Sicherheitsgefährdungen wie Schadsoftware können die unberechtigte Kenntnisnahme, Veränderung und Löschung von Kerndaten zur Folge haben. Die europaweiten Schäden durch Schadsoftware schätzte Interpol für das Jahr 2012 auf ca. 750 Milliarden Euro.[2]

[1] Die unmittelbare und mittelbare Staatsverwaltung und alle seine Untergliederungen.

[2] Eröffnungsrede des Interpol Präsidenten Khoo Boon Hui auf der 41. Europäischen Regional Konferenz in Tel Aviv am 8. Mai 2012

Mit dem fortschreitenden digitalen Wandel in den Staatsgewalten entwickeln sich parallel dazu die Hacking-Angriffe weiter. Ohne ein darauf ausgerichtetes Informationssicherheitsmanagement (ISM) bzw. eingerichtete Informationssicherheitsmanagementsysteme (ISMS) könnte dies die Staatsgewalten in ihren Handlungen einschränken bzw. handlungsunfähig machen. Dies gilt umso mehr, je weiter in der Verwaltung die Einführung von elektronischen Akten voranschreitet. Wird das Dokumentenmanagementsystem in einem zentralen Rechenzentrum betrieben, so befindet sich auf diesem das gesammelte Verwaltungswissen der angeschlossenen Organisationseinheiten.

Die Rechnungshöfe haben das Thema Informationssicherheit in den vergangenen Jahren immer wieder aufgegriffen und eine Weiterentwicklung des Informationssicherheitsmanagement[3] aktiv begleitet und befördert. Mit dem vorliegenden Grundsatzpapier und dessen Anlagen werden die Prüfungserkenntnisse der Rechnungshöfe zusammengefasst und zu ausgewählten Aspekten Empfehlungen für eine zukünftige Ausgestaltung der ISMS in Bund, Ländern und Kommunen abgegeben. Dieses Papier ergänzt damit die Mindestanforderungen der Rechnungshöfe zum Einsatz von Informations- und Kommunikationstechnik vom November 2011. Darüber hinaus stellen die Rechnungshöfe Empfehlungen für die Prüfung der Informationssicherheit bereit.[4]

[3] Unter Informationssicherheitsmanagement bzw. dem Informationssicherheitsmanagementsystem wird der Teil des gesamten Managementsystems verstanden, welcher auf Basis eines Risikoansatzes die Entwicklung, Implementierung, Durchführung, Überwachung, Überprüfung, Instandhaltung und Verbesserung der Informationssicherheit abdeckt (DIN ISO/IEC 27001:2009-08, S. 9).

[4] sh. Checkliste der Rechnungshöfe des Bundes und der Länder zur Prüfung der Informationssicherheit in der öffentlichen Verwaltung vom Juni 2015 (Anlage)

1 Informationssicherheitsmanagement

Die Informationssysteme und Netzwerke der öffentlichen Verwaltung in Deutschland sind Sicherheitsbedrohungen unterschiedlichster Art ausgesetzt. Im deutschen Regierungsnetz geht täglich eine Vielzahl mit Schadsoftware behaftete E-Mails[5] ein. Zudem beobachtet das BSI täglich gezielte Spionageangriffe[6] von hochprofessionellen Angreifern auf die Bundesverwaltung.

Die öffentliche Verwaltung hat in den letzten Jahren auf diese Bedrohung mit dem Aufbau und Ausbau von ISMS reagiert.

Die derzeit im Bund und in den Ländern implementierten ISMS orientieren sich im Grundsatz an den Empfehlungen der DIN ISO/IEC 2700x-Reihe[7] sowie den IT-Grundschutz-Standards des Bundesamt für Sicherheit in der Informationstechnik (BSI).

Der IT-Planungsrat[8] hat zur weiteren Standardisierung des Informationssicherheitsmanagements in Deutschland im März 2013 eine Leitlinie für die Informationssicherheit in der öffentlichen Verwaltung[9] einschließlich eines Umsetzungsplans[10] beschlossen. Diese Leitlinie definiert für den Bund und die Länder einen Rahmen, welche Anforderungen bestehen und welche organisatorischen Aspekte und Maßnahmen mindestens realisiert werden müssen.

---

[5] BSI, Fokus IT-Sicherheit 2013 vom Juli 2013, S. 2

[6] sog. „fortgeschrittene, andauernde Bedrohung" (Englisch: Advanced Persistent Threats – APT)

[7] Vgl. DIN ISO/IEC 27001:2008-09, Informationssicherheits-Managementsysteme – Anforderungen (ISO/IEC 27001:2005) vom September 2008

[8] Der IT-Planungsrat ist in Deutschland das zentrale Gremium für die föderale Zusammenarbeit des Bundes, der Länder und der Kommunen in der Informationstechnik (Artikel 91c GG). Er verwaltet u. a. das Verbindungsnetz der öffentlichen Verwaltungen und kann verbindliche IT-Interoperabilitäts- und IT-Sicherheitsstandards beschließen.

[9] Vgl. http://www.it-planungsrat.de/SharedDocs/Downloads/DE/Entscheidungen/10._-Sitzung/Leitlinie_Informationssicherheit_Hauptdokument.html?nn=1852114

[10] Vgl. http://www.it-planungsrat.de/SharedDocs/Downloads/DE/Entscheidungen/10.-Sitzung/Leitlinie_Informationssicherheit_Umsetzungsplan.html?nn=1852114

Im Hinblick auf die Grundsätze der Wirtschaftlichkeit und Sparsamkeit hat die Verwaltung bei der Realisierung der Informationssicherheit widerstreitende Aspekte zu beachten. Ein ISMS bindet personelle und finanzielle Ressourcen. Es ist trotzdem notwendig, um hohe materielle und immaterielle Schäden abzuwenden, die der öffentlichen Verwaltung durch Datenverlust, Datenmanipulation oder das Ausspähen von Daten entstehen würden.

Absichtserklärungen, wie die digitale Agenda für Europa, die digitale Agenda 2014-2017 oder das IT-Sicherheitsgesetz[11], messen der IT-Sicherheit einen hohen Stellenwert zu.

Der Arbeitskreis Organisation und Informationstechnik der Rechnungshöfe des Bundes und der Länder hat deshalb im Juni 2014 beschlossen, durch ein Grundsatzpapier Anregungen für eine Weiterentwicklung des ISM bzw. der ISMS zu geben.

[11] Gesetzentwurf der Bundesregierung zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) vom 17. Dezember 2014

2 Organisation der Informationssicherheit

Folgend aus der allgemeinen Leitungsverantwortung[12] ist die Behördenleitung auch für die Informationssicherheit ihrer Behörde verantwortlich. Sie hat die notwendigen technischen und organisatorischen Maßnahmen zu veranlassen, die notwendig sind, um dem ermittelten Schutzbedarf Rechnung zu tragen und ein ISMS einzurichten.

Eine hundertprozentige Informationssicherheit ist nicht erreichbar. Die vorhandenen Restrisiken müssen deshalb ermittelt sowie deren Auswirkungen beschrieben und bewertet werden.

Eine angemessene Aufbauorganisation und Ressourcenausstattung stellen wichtige Voraussetzungen für ein wirkungsvolles ISMS dar.

2.1 Aufbauorganisation

Empfehlungen zur konkreten Umsetzung eines ISM in der öffentlichen Verwaltung sind in der Regel nicht Gegenstand der internationalen und nationalen Normen und Standards. Ausnahme bilden die IT-Grundschutz-Standards des BSI, die als Vorgaben für die Bundesverwaltung bzw. als Empfehlungen für die Bundesländer gelten (z. B. Berufung eines IT-Sicherheitsbeauftragten).

In den öffentlichen Verwaltungen haben sich intern und übergreifend unterschiedliche Ausgestaltungen des ISM entwickelt. Befördert wurde diese Entwicklung durch den heterogenen Aufbau des IT-Managements sowie der IT-Infrastrukturen in Bund, Ländern und Kommunen.

In den Prüfungen stellen die Rechnungshöfe seit Jahren einen Trend hin zu einer stärkeren Zentralisierung der Serviceerbringung in der IT fest. Diese Entwicklung wurde durch die Virtualisierung der IT in den letzten Jahren verstärkt.

[12] Vgl. Leitlinie für die Informationssicherheit in der öffentlichen Verwaltung des IT-Planungsrats, http://www.it-planung-rat.de/SharedDocs/Downloads/DE/Entscheidungen/10._Sitzung/Leitlinie_Informationssicherheit_Hauptdokument.html , aufgerufen am 22.09.2014

Nach den Erhebungen der Rechnungshöfe hat die Vernetzung und Digitalisierung in der öffentlichen Verwaltung einen solchen Verdichtungsgrad erreicht, dass in der Bundesverwaltung und in den einzelnen Ländern perspektivisch jeweils ein zentrales ISM mit Befugnissen zum Durchgriff in die Ressortverantwortlichkeiten erforderlich wird.[13] Ein zentrales ISM schafft gemeinsame Strukturen zur verwaltungsübergreifenden Aufgabenerledigung. Es ermöglicht der Verwaltung zu kooperieren und die Aufgabenwahrnehmung zu koordinieren. Ein zentrales ISM schränkt die Ressorthoheit nicht ein. Der Notwendigkeit zur Zentralisierung wurde zum Teil mit der Vorgabe des IT-Planungsrates nach Bundes- bzw. Landes-Informationsicherheitsbeauftragten[14] entsprochen.

Eine reine dienstellenbezogene Ausrichtung des ISM, wie in den IT-Grundschutz-Standards des BSI empfohlen, ist aufgrund der fehlenden Sicht auf die Gesamtarchitektur nicht mehr zeitgemäß. Diese hat in der Vergangenheit oft genug zu kleinen, nicht vernetzten Insellösungen geführt.

Im Hinblick auf die weiter voranschreitende Zentralisierung von Dienstleistungen in der IT, ist die Entwicklung eines servicesorientierten ISM notwendig. Verantwortlichkeiten in der IT sollten daher nicht mehr primär nach Organisationsgrenzen, sondern auf Dienste bezogen festgelegt werden.

Für angemessene Informationssicherheit zu sorgen, gehört zu den Aufgaben des zentralen IT-Managements. Der IT-Sicherheitsbeauftragte muss außerhalb des IT-Managements angesiedelt sein, um Interessen- und Rollenkonflikte zu vermeiden.[15] Zusätzlich ist eine intensivere Kontrolle des ISMS durch die Prüfungsinstanzen erforderlich.

[13] In der Übergangsphase kann ein zusätzliches dienststellenbezogenes ISM erforderlich sein. Hierbei ist eine enge Kommunikation und Kooperation mit der zentralen Instanz notwendig.

[14] IT-Planungsrat bezeichnet die Rolle mit Landes-IT-Sicherheitsbeauftragten

[15] Die Aufgabenwahrnehmung könnte z. B. in der Zentralabteilung, außerhalb des IT-Referats, oder vergleichbaren Organisationseinheiten erfolgen.

2.2 Ressourcenausstattung

Die mit der Informationssicherheit in den Behörden befassten Personen[16] haben zur Sicherstellung einer ausreichenden Informationssicherheit umfangreiche Aufgaben zu erfüllen. Sie müssen z. B.

- den Informationssicherheitsprozess steuern und bei allen damit zusammenhängenden Aufgaben mitwirken,
- die Leitungsebene bei der Erstellung der Leitlinie zur Informationssicherheit unterstützen,
- die Erstellung des Sicherheitskonzepts, des Notfallvorsorgekonzepts und anderer Teilkonzepte und System-Sicherheitsrichtlinien koordinieren sowie weitere Richtlinien und Regelungen zur Informationssicherheit erlassen,
- die Realisierung von Sicherheitsmaßnahmen initiieren und überprüfen,
- der Leitungsebene über den Status quo der Informationssicherheit berichten,
- sicherheitsrelevante Projekte koordinieren,
- Sicherheitsvorfälle untersuchen,
- Sensibilisierungs- und Schulungsmaßnahmen zur Informationssicherheit initiieren und koordinieren,
- bei der Einführung neuer Anwendungen und IT-Systeme mitwirken und
- die Beachtung von Sicherheitsaspekten bei allen größeren Projekten, die deutliche Auswirkungen auf die Informationsverarbeitung haben, in den verschiedenen Projektphasen gewährleisten.

Die Rechnungshöfe haben in verschiedenen Prüfungen festgestellt, dass in vielen Bereichen der Verwaltung ein Mangel an ausreichend qualifizier-

[16] z. B. IT-Sicherheitsbeauftragte, IT-Sicherheitsteam, Administratoren

tem und geschultem Personal besteht, um die gestiegenen und gesetzlich verankerten[17] Anforderungen an die Informationssicherheit zu erfüllen.

Der personelle Bedarf muss nach wirtschaftlichen Aspekten erhoben und fortgeschrieben werden.

Neben dem Personal sind entsprechend der Informationssicherheitsleitlinien des Bundes und der Länder die zur Erreichung der Sicherheitsziele erforderlichen Sachmittel zur Verfügung zu stellen.

3 Das CERT als wichtiges Element des operativen Informationssicherheitsmanagements

Ein Computer Emergency Response Team (CERT) ist eine Gruppe von IT-Sicherheitsfachleuten, die bei der Lösung von konkreten IT-Sicherheitsvorfällen als Koordinatoren mitwirken, Warnungen zu Sicherheitslücken herausgeben und Lösungsansätze anbieten.

Die vom IT-Planungsrat 2013 verabschiedete Leitlinie über die Informationssicherheit in der öffentlichen Verwaltung verpflichtet die Länder, bis 2016 ein CERT aufzubauen.

In Abgrenzung zum Informationssicherheitsmanagement wird das interne oder auch behördenübergreifende CERT u. a. vom Sicherheitsmanagement genutzt, um

- Informationen über mögliche Sicherheitsvorfälle bereitzustellen,
- ggf. bereits im Vorfeld hierzu Beratungsleistungen vorzuhalten,
- Alarm- und Warnmeldungen zu generieren,
- Sicherheitswerkzeuge zu entwickeln und einzusetzen,
- ggf. befallene technische Infrastruktur zu analysieren,
- Sicherheitsvorfälle zu bearbeiten und
- ggf. bei Wiederherstellung nach Sicherheitsvorfällen mitzuwirken.

[17] Vgl. Entwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz), Referentenentwurf Stand 18.8.2014.

Die Rechnungshöfe sehen in der Einrichtung eines CERT einen wichtigen Baustein für das operative ISM. Aufgrund des erheblichen Aufwands für die Einrichtung und den Betrieb eines CERT ist eine länderübergreifende Kooperation naheliegend. Darüber hinaus ist eine enge Zusammenarbeit zwischen dem BSI, den IT-Sicherheitsbeauftragten des Bundes und der Länder sowie den CERT der Länder erforderlich.

4 Erwartungen und Prüfungsmaßstäbe der Rechnungshöfe

Die Herstellung einer angemessenen Informationssicherheit ist in der aktuellen Verwaltungsarbeit eine wesentliche Herausforderung. Die Verwaltung hat ungeachtet der bestehenden Gefährdungen vorrangig sicherzustellen, dass

- die Informationssysteme zuverlässig und kontinuierlich zur Verfügung stehen,
- die Anforderungen an die Sicherheit der Informationsverarbeitung regelmäßig ermittelt und unverzüglich umgesetzt werden,
- die in Informationssysteme getätigten Investitionen gesichert werden,
- die ISMS organisatorisch, personell und finanziell die Anforderungen erfüllen können,
- die ISMS die Auswirkungen und Kosten eines IT-Sicherheitsvorfalls reduzieren und damit zu einem wirtschaftlichen Verwaltungshandeln beitragen.

Die Rechnungshöfe werden die Ordnungsmäßigkeit und Wirtschaftlichkeit der ISMS in Bund, Ländern und ggf. Kommunen anhand von gemeinsamen Mindeststandards untersuchen. Der Arbeitskreis Organisation und Informationstechnik der Rechnungshöfe des Bundes und der Länder hat hierzu in Erweiterung des vorliegenden Grundsatzpapiers eine Checkliste (Stand Juni 2015) erarbeitet. Diese bildet zukünftig eine Grundlage für Prüfungen zur Informationssicherheit durch die Rechnungshöfe.