

An die

Innenminister und -senatoren
der Länder

Bundesminister des Innern

Schwerin, 08. April 2013

**197. Sitzung der ständigen Konferenz der Innenminister und -senatoren der Länder am
23./24. Mai 2013 in Hannover**

hier: Bericht aus dem IT-Planungsrat

Sehr geehrte Frau Bachmann,

sehr geehrte Herren Minister und Senatoren,

als Mitglied des IT-Planungsrates und in meiner Funktion des von der IMK für den IT-Planungsrat (IT-PLR) benannten Ansprechpartners möchte ich Sie über die Ergebnisse der zurückliegenden Sitzungen des IT-PLR informieren. Der IT-PLR hat seit meiner letzten Berichterstattung zwischenzeitlich zweimal getagt. Die Sitzungen fanden am 25. Oktober 2012 in Berlin und am 08. März 2013 in Hannover statt. Die wesentlichen Themen und Beschlüsse der Sitzungen lassen sich wie folgt zusammenfassen:

I. Themenbereiche

Allgemeines

In 2013 hat Bayern den Vorsitz des IT-PLR übernommen (der Vorsitz erfolgt alternierend durch Bund und Länder). Der IT-PLR will sich zukünftig verstärkt auf die Befassung politisch-strategischer Themen konzentrieren, um durch seine Themen und als Impulsgeber in Politik und Fachöffentlichkeit wahrgenommen zu werden. So soll jeweils ein politisch-strategisch relevantes Schwerpunktthema im Mittelpunkt der Beratungen stehen. Für die nächsten Sitzungen werden dies die Themen „Informationssicherheit in der öffentlichen Verwaltung – ein Standortfaktor mit wachsender Bedeutung“, „Strategie für elektronische Identitäten im eGovernment“ und eine „Digitale Agenda für Deutschland“ sein.

Schwerpunktthemen der 9. Sitzung

Die 9. Sitzung des IT-PLR am 25. Oktober 2012 stand unter keinem besonderen Leitgedanken.

Anwendungen des IT-PLR

Der IT-PLR beschloss eine bis zum 31. Dezember 2014 befristete Regelung zum Betrieb und zur Weiterentwicklung der Anwendungen. Die jeweiligen Federführer haben danach die Aufgabe, den Betrieb sowie die fachliche und technische Weiterentwicklung der Anwendung unter Einbeziehung

Hausanschrift:

Ministerium für Inneres und Sport
Mecklenburg-Vorpommern
Arsenal am Pfaffenteich
Alexandrinestraße 1 · 19055 Schwerin

Postanschrift:

Ministerium für Inneres und Sport
Mecklenburg-Vorpommern
19048 Schwerin

Telefon: +49 385 588-2005

Telefax: +49 385 588-2970

E-Mail: poststelle@im.mv-regierung.de

Internet: www.im.mv-regierung.de

der Nutzer sicherzustellen. Anwendungen des IT-Planungsrats sind IT-Lösungen, die aus Projekten oder projektähnlichen Strukturen hervorgegangen sind und deren Betrieb bzw. Pflege und Fortentwicklung auf Dauer gewährleistet werden soll. Hierzu gehören auch die von der IMK genutzten Anwendungen DVDV und Governikus.

Fachkongress des IT-Planungsrats 2013 und Zukunftskongress Staat & Verwaltung

Der 1. Fachkongress des IT-PLR wird von Bayern ausgerichtet und findet unter dem Schwerpunktthema „Die digitale Behörde der Zukunft“ am 2./3. Mai 2013 in München statt. Baden-Württemberg wird den Fachkongress im Jahr 2014, Rheinland-Pfalz im Jahr 2015 und Berlin im Jahr 2016 ausrichten.

Das BMI informierte, dass es die Kooperation mit der Messe Moderner Staat nicht mehr fortführen wird. Als Nachfolge gestaltet das BMI mit neuen Partnern einen „Zukunftskongress Staat & Verwaltung“, der erstmalig am 25./26. Juni 2013 in Berlin stattfindet.

Aktionsplan für das Jahr 2013

Der IT-PLR beschloss den Aktionsplan für das Jahr 2013. Die aus dem „Aktionsplan Deutschland-Online“ stammenden Projekte (Kfz-Wesen, Nationales Waffenregister (Stufe 1) und Personenstandswesen) wurden zum Ende des Jahres 2012 erfolgreich abgeschlossen. Aus dem Vorhaben Deutschland Online Kfz Wesen sind Vorschläge für die Online-Außerbetriebsetzung und Online-Wiederzulassung entstanden. Nunmehr ist das Bundesministerium für Verkehr, Bau und Stadtentwicklung gehalten, die noch offenen Fragen mit den Beteiligten zu erörtern und die Vorschläge aus dem Projekt des IT-PLR weiterzuentwickeln, so dass sie in ein Gesetzgebungsverfahren überführt werden können.

Als neues Steuerungsprojekt wurde die „Weiterentwicklung des Deutschen Verwaltungsdienstverzeichnisses (DVDV 2.0)“ aufgenommen. Mit DVDV steht den Verwaltungen von Bund, Ländern und Kommunen ein zentrales Verzeichnis mit technischen Verbindungsparametern für die verwaltungsübergreifende, sichere Kommunikation zur Verfügung, das die Basis für den Datenaustausch verschiedener Fachverfahren im deutschen Verwaltungsraum bildet. Dazu gehören unter anderem das Meldewesen, Pass- und Ausweiswesen, Personenstandswesen, sowie das Ausländerwesen. Auf Grund der allgemeinen technischen Entwicklung ist eine Weiterentwicklung von DVDV notwendig.

Als Koordinierungsprojekte des IT-PLR wurden die „Neuentwicklung eines EDV-Grundbuchs“, die „Online-Sicherheitsprüfung“, die „Elektronische Rechnungsbearbeitung in der Verwaltung“ und die „Cloud-E-Mail“ aufgenommen. Zudem wurde als neue Maßnahmen zur Verbesserung der Rahmenbedingungen im E-Government die „IT- und E-Government-Ausbildung von Fach- und Führungskräften der Verwaltung“ eingeordnet.

Der IT-PLR hat den Bund, die Länder und die Kommunen gebeten, neue Vorhaben anzuzeigen. An Hand eines Kriterienkataloges wird dann über die Aufnahme in den Projekt- und Anwendungsplan des IT-PLR entschieden.

Schwerpunktthemen der 10. Sitzung

Die 10. Sitzung stand unter dem Schwerpunktthema „IT-Sicherheit“.

Verabschiedung der „Leitlinie für die Informationssicherheit in der öffentlichen Verwaltung“

Der IT-Planungsrat ist gemäß dem IT-Staatsvertrag für die Vereinbarung gemeinsamer Mindestsicherheitsanforderungen zwischen Bund und Ländern zuständig und hat demgemäß eine Informationssicherheitsleitlinie erarbeitet. Diese wurde in der 10. Sitzung verabschiedet. Die Leitlinie bezieht sich auf die Schutzziele der Informationssicherheit Verfügbarkeit, Vertraulichkeit und Integ-

rität der Daten sowie die technisch-organisatorische Umsetzung der Datenschutzerfordernungen im Hinblick auf Transparenz, Betroffenenrechte und Zweckbindung. Ziel ist es eine kontinuierliche Verbesserung des sicheren Umgangs mit Informationen und Informationstechnik in den jeweiligen Verantwortungsbereichen zu erreichen.

Die Leitlinie gilt für alle Behörden und Einrichtungen der Verwaltungen des Bundes und der Länder verbindlich. Den Kommunen, den Verwaltungen des Deutschen Bundestages und der Landesparlamente, den Rechnungshöfen von Bund und Ländern sowie den BfD/LfD wird die Anwendung der Leitlinie für die Informationssicherheit empfohlen. Verantwortlich für die Informationssicherheit einer Behörde ist die Behördenleitung als Teil der allgemeinen Leitungsverantwortung.

Die Vorgaben der Leitlinie sind von Bund und Ländern im jeweiligen Zuständigkeitsbereich in eigener Verantwortung umzusetzen. Die Festlegung des Mindestsicherheitsniveaus erfolgt einheitlich orientiert am IT-Grundschutz des BSI. Hierdurch wird auch eine verbesserte Vergleichbarkeit des Sicherheitsniveaus erreicht.

Die Leitlinie für Informationssicherheit sieht vor, dass bei ebenen-übergreifenden IT-Verfahren die Umsetzung der Vorgaben der Leitlinie durch den jeweiligen IT-Verfahrensverantwortlichen auch über Bund und Länder hinaus im notwendigen Umfang auf die jeweiligen Verfahrensbeteiligten auszudehnen ist. Für beteiligte Dritte (z.B. als Auftragnehmer) gilt die Leitlinie im notwendigen Umfang.

Auch im Bereich der Sicherheit der Datennetze verlangt die Leitlinie weitreichende Maßnahmen. So sollen für ein direkt an das DOI-Netz angeschlossenes Netz grundsätzlich die BSI-Standards 100-1, 100-2, 100-3 und 100-4 umgesetzt werden.

Die Vorgaben der Leitlinie betreffen den Aufbau eines Informationssicherheitsmanagements (ISMS), die Absicherung der Netzinfrastrukturen der öffentlichen Verwaltung, einheitliche Sicherheitsstandards für ebenen-übergreifende IT-Verfahren, die gemeinsame Abwehr von IT-Angriffen sowie die Standardisierung und Produktsicherheit.

Eine der wichtigsten Maßnahmen ist der Aufbau eines VerwaltungscERT-Verbund (VCV) von Bund und Ländern zur frühzeitigen Erkennung und Abwehr von IT-Angriffen und zur gegenseitigen Information, Warnung und Alarmierung sowie zur gemeinsamen Bewältigung von IT-Krisen. Dies bedingt die Schaffung geeigneter landes- und bundesinterner Strukturen.

Der Umsetzungsplan zur Leitlinie sieht eine schrittweise Umsetzung der einzelnen Maßnahmen in den jeweiligen Zuständigkeitsbereichen vor. Der erreichte Stand der Umsetzung ist jährlich intern zu evaluieren und im Rahmen der Erfolgskontrolle dem IT-PLR vorzulegen.

NEGS-Maßnahme „Evaluierung der Kieler Beschlüsse“

Der IT-PLR hat im Rahmen einer Evaluierung der in der Vergangenheit vielfach genutzten „Kieler Beschlüsse“ ein Gutachten erstellen lassen. Im Ergebnis dessen ist für eine Weiterentwicklung der Kieler Beschlüsse vorrangig die Betrachtung von institutionalisierten Kooperationen zur Sicherstellung einer vergaberechtskonformen, gemeinsamen Entwicklung und Pflege von Software und die Entwicklung von Gestaltungsvarianten für einen gemeinsamen Betrieb von Softwarelösungen erforderlich. In Ergänzung der fortentwickelten Kieler Beschlüsse soll außerdem ein Leitfaden entstehen, der die verschiedenen Kooperationsmodelle darstellt.

Geodateninfrastruktur Deutschland (GDI-DE)

Der IT-PLR sieht in der Geodateninfrastruktur Deutschland (GDI-DE) eine wesentliche Komponente der föderalen IT- und E-Government-Infrastrukturen, die eine wichtige Rolle bei der Umsetzung der Nationalen E-Government Strategie (NEGS) spielt. Der IT-PLR beauftragte daher das Len-

kungsgremium GDI-DE ein Konzept zur Integration der GDI-DE in die föderalen IT- und E-Government-Infrastrukturen mit Verknüpfungen zu anderen Infrastrukturen zu erarbeiten.

II. Zusammenarbeit von IMK und IT-Planungsrat

Mit der Realisierung der ersten Stufe wurde das Vorhaben Nationales Waffenregister als Steuerungsprojekt des IT-PLR zum 31.12.2012 erfolgreich beendet. Eine Fortführung als Steuerungsprojekt des IT-PLR ab 2013 ist auf Grund anderer Prioritätensetzung nicht vorgesehen, wenn gleich nunmehr die Umsetzung der Stufe 2 und 3 ansteht. In der Funktion des von der IMK für den IT-PLR benannten Ansprechpartners setze ich mich für eine weitergehende Unterstützung des übergreifenden Vorhabens Nationales Waffenregister ein. Das Anliegen der IMK wurde dem IT-PLR entsprechend vorgetragen. Nach derzeitigem Stand ist für 2013 mit einer finanziellen Unterstützung des Projektes durch den IT-PLR in Höhe von 230 T€ zu rechnen.

Die IT-Sicherheit ist mittlerweile ein wichtiges Thema im Bereich der inneren Sicherheit und damit der IMK. So ist augenfällig, dass sich die vom IT-PLR verabschiedete „Leitlinie für die Informationssicherheit in der öffentlichen Verwaltung“ auch auf Themenfelder und Aufgabengebiete der IMK auswirken wird. Berührungspunkte sind hier in erster Linie gemeinsam betriebene IT-Verfahren, gemeinsam genutzte Netze und die gemeinschaftliche Gefahrenabwehr bei übergreifenden IT-Angriffen. Die IMK hat eine AG Cybersicherheit eingesetzt, die sich seit 2011 mit den Fragen der IT-Sicherheit und im Speziellen mit der Cybersicherheit befasst. Es ist naheliegend, dass zukünftig eine Zusammenarbeit zwischen der AG Cybersicherheit der IMK und der vom IT-PLR eingerichteten AG IT-Sicherheit angestrebt werden sollte, um Synergien zu heben und Doppelarbeit zu vermeiden. Die Abstimmung von geplanten Maßnahmen, wie z.B. der Aufbau des deutschlandweiten VerwaltungscERT-Verbundes, sollte im beiderseitigen Interesse liegen und voran getrieben werden.

Abschließend schlage ich für die anstehende Sitzung der IMK am 23./24.05. 2013 folgenden Beschluss vor:

1. Die IMK nimmt den Bericht des Ansprechpartners der IMK für den IT-Planungsrat über die Sitzung des IT-Planungsrates vom 25. Oktober 2012 und vom 8. März 2013 zur Kenntnis.
2. Die IMK begrüßt die durch den IT-Planungsrat am 8. März 2013 verabschiedete „Leitlinie für die Informationssicherheit in der öffentlichen Verwaltung“.
3. Die IMK bittet seine AG Cybersicherheit, sich zukünftig mit der neu eingerichteten AG IT-Sicherheit des IT-Planungsrates bezüglich Planung und Umsetzung von Maßnahmen abzustimmen.

Mit freundlichen Grüßen



Thomas Lenz

**Leitlinie für die Informationssicherheit
in der öffentlichen Verwaltung**

- Hauptdokument -

Stand 19.02.2013

Version 1.8 (Beschlussvorschlag IT-Planungsrat nach AL-Sitzung München)

Inhaltsverzeichnis

1	Einleitung	3
2	Geltungsbereich und Umsetzung	5
3	Ziele der Informationssicherheit und Umsetzungsstrategien	6
3.1	Informationssicherheitsmanagement.....	8
3.2	Absicherung der Netzinfrastrukturen der öffentlichen Verwaltung.....	9
3.3	Einheitliche Sicherheitsstandards für Ebenen-übergreifende IT-Verfahren.....	11
3.4	Gemeinsame Abwehr von IT-Angriffen.....	11
3.5	Standardisierung und Produktsicherheit.....	12

1 Einleitung

Modernes Verwaltungshandeln ist heute ohne elektronische Kommunikationsmedien und IT-Verfahren nicht mehr denkbar. Mit deren Nutzung verbunden war und ist aber immer auch die Frage nach einer angemessenen Sicherheit von IT-Infrastrukturen und -Verfahren der öffentlichen Verwaltungen zum Schutz der enthaltenen und übertragenen Daten. In zunehmendem Maße nutzen Bund und Länder nun auch Ebenen-übergreifende Kommunikation und IT-Verfahren. Damit erwächst eine neue Herausforderung: Die Verlässlichkeit der vernetzten, von unterschiedlichen Partnern betriebenen Infrastrukturen. Die getroffenen Schutzmaßnahmen der einzelnen Kommunikationspartner haben Auswirkungen auf alle.

Um hier für alle Beteiligten ein hohes Maß an Verlässlichkeit zu erzielen, ist als gemeinsame Strategie die Etablierung eines einheitlichen und einvernehmlichen Mindestsicherheitsniveaus unter Berücksichtigung des Grundsatzes der Wirtschaftlichkeit notwendig, wie sie in dieser für Bund und Länder verbindlichen Informationssicherheitsleitlinie beschrieben wird.

Diese Informationssicherheitsleitlinie ist u.a. aus folgenden Gründen notwendig:

- Ein unzureichendes Sicherheitsniveau oder Sicherheitslücken bei einer Behörde und Einrichtung können über die Netzinfrastrukturen und Ebenen-übergreifenden IT-Verfahren¹ die Sicherheit aller beeinträchtigen. Ein einheitliches Mindestsicherheitsniveau gewährleistet, dass sich alle Beteiligten auf ein gemeinsames Basisniveau für Informationssicherheit einigen und dadurch dieses Risiko minimieren.
- Es müssen Ebenen-übergreifend im Rahmen der elektronischen Kommunikation oder im Rahmen von IT-Verfahren auch sensible und eingestufte Informationen vom Absender bis zum Empfänger mit einem einheitlichen Sicherheitsniveau ausgetauscht werden können.

¹ Ebenen-übergreifende IT-Verfahren im Sinne dieser Informationssicherheitsleitlinie sind IT-Verfahren, die über Verwaltungsgrenzen hinweg angeboten bzw. genutzt werden sollen (z.B. Bund-Länder-übergreifend oder von mehreren Bundesländern genutzte IT-Verfahren), siehe § 3 Abs. 1 IT-Staatsvertrag, .

- Zur gemeinsamen Abwehr von IT-Angriffen ist eine rasche Reaktionszeit von Bund und Ländern unerlässlich. Ein einheitliches Mindestsicherheitsniveau bei allen Beteiligten senkt das Risiko, dass die für die Zusammenarbeit vorgesehenen elektronischen Kommunikationskanäle zwischen Bund und Länder bei IT-Angriffen ausfallen oder kompromittiert werden.

Das gemeinsame Vorgehen zielt u.a. darauf ab, die notwendigen Sicherheitsanforderungen wirtschaftlicher realisieren zu können, als es jeder Einzelne für sich könnte und das Risiko hoher Folgekosten aufgrund von Sicherheitsvorfällen zu reduzieren. Durch Etablierung eines einheitlichen Mindestsicherheitsniveaus können neue IT-Verfahren oder die elektronische Kommunikation auf diesem aufbauen und vorhandene Sicherheitsmaßnahmen gemeinsam genutzt werden. Kostenintensive Einzelmaßnahmen werden vermieden. Das gemeinsame Vorgehen etabliert zudem Ebenen-übergreifend ein einheitliches Verständnis und Wissen über Informationssicherheit.

2 Geltungsbereich und Umsetzung

Auf Grundlage des IT-Staatsvertrages ist der IT-PLR zuständig für die Vereinbarung gemeinsamer Mindestsicherheitsanforderungen zwischen Bund und Ländern. Entsprechend ist er für die Erarbeitung, Verabschiedung, Weiterentwicklung und Erfolgskontrolle der Informationssicherheitsleitlinie verantwortlich. Änderungen an dieser Leitlinie sind ebenfalls durch den IT-PLR zu verabschieden.

Soweit Gegenstände des IT-Planungsrats den Einsatz der Informationstechnik in der Justiz betreffen, sind die aus den verfassungs- und einfachrechtlich garantierten Positionen der unabhängigen Rechtspflegeorgane resultierenden Besonderheiten zu beachten. Die richterliche Unabhängigkeit ist zu wahren.

Die Leitlinie für die Informationssicherheit gilt nach Verabschiedung durch den IT-PLR für alle Behörden und Einrichtungen der Verwaltungen des Bundes und der Länder. Den Kommunen, den Verwaltungen des Deutschen Bundestages und der Landesparlamente, den Rechnungshöfen von Bund und Ländern sowie den Beauftragten für den Datenschutz in Bund und Ländern wird die Anwendung der Leitlinie für die Informationssicherheit empfohlen.

Die Vorgaben der Leitlinie sind von Bund und Ländern im jeweiligen Zuständigkeitsbereich in eigener Verantwortung umzusetzen.

Um das einheitliche Mindestsicherheitsniveau nicht zu gefährden, ist bei Ebenenübergreifenden IT-Verfahren durch den jeweiligen IT-Verfahrensverantwortlichen die Umsetzung der Vorgaben der Informationssicherheitsleitlinie auch über Bund und Länder hinaus im notwendigen Umfang auf die jeweiligen Verfahrensbeteiligten auszudehnen.

Soweit Dritte als Auftragnehmer für die öffentliche Verwaltung Leistungen erbringen, sind bei der Auftragserteilung auf die Vorgaben der Leitlinie zur Informationssicherheit im notwendigen Umfang zu verpflichten. Dies ist über einzelvertragliche Regelungen oder Rahmenverträge sicher zu stellen und vom Auftraggeber zu kontrollieren.

Ausgehend von der individuellen Ausgangslage im jeweiligen Zuständigkeitsbereich von Bund und Ländern, ist für die Umsetzung der Leitlinie (z.B. Aufbau Informationssicherheitsmanagement, LandesCERTs) mit entsprechenden Kosten zu rechnen. Mögliche Kosten stehen generell unter Haushaltsvorbehalt. Sofern eine pauschale Abschätzung möglich ist, wird diese im Umsetzungsplan zur Leitlinie aufgeführt.

Der IT-PLR setzt eine ständige Arbeitsgruppe zur Informationssicherheit ein. Jedes Mitglied des IT-PLR benennt einen Vertreter für die Arbeitsgruppe. Dieser ist zentraler Ansprechpartner für die Umsetzung der Informationssicherheitsleitlinie im jeweiligen Verantwortungsbereich des Mitglieds.

Die Arbeitsgruppe setzt sich aus den benannten Vertretern der Mitglieder zusammen und erarbeitet gemeinsam Vorschläge zur Weiterentwicklung der Leitlinie und sowie einen jährlichen Bericht zur Erfolgskontrolle für den IT-PLR. Sie dient außerdem dem regelmäßigen Austausch zu Themen der Informationssicherheit unterhalb des IT-PLR. Die Arbeitsgruppe berücksichtigt die Standardisierungsagenda des IT-PLR und kooperiert mit dem BSI bzgl. Standards für Informationssicherheit.

3 Ziele der Informationssicherheit und Umsetzungsstrategien

Die gemeinsame Leitlinie für Informationssicherheit bezieht sich auf die Schutzziele der Informationssicherheit Verfügbarkeit, Vertraulichkeit und Integrität der Daten **sowie die technisch-organisatorische Umsetzung der Datenschutzanforderungen im Hinblick auf Transparenz, Betroffenenrechte und Zweckbindung.**

Mit den Festlegungen zu den Mindestanforderungen und zum gemeinsamen Vorgehen in der Informationssicherheit werden insbesondere folgende Ziele verfolgt:

- Unterstützung bei der Erfüllung der aus **datenschutzrechtlichen und sonstigen gesetzlichen Vorgaben resultierenden Anforderungen** an die Sicherheit der Informationsverarbeitung.

- Effiziente und effektive IT-Unterstützung der Geschäftsprozesse in Bund, Ländern und Kommunen.
- Nachhaltige Verfügbarkeit der IT-Systeme zur Gewährleistung der Kontinuität der Geschäftsprozesse in Bund, Ländern und Kommunen.
- Sicherung der in IT-Systemen getätigten Investitionen.
- Absicherung der IT-Systeme gegen Manipulation, unberechtigten Zugriff und Verlust.
- Reduzierung der im Fall eines IT-Sicherheitsvorfalls entstehenden Kosten und Aufwände zur Schadensbehebung.
- Wahrung besonderer Dienst- oder Amtsgeheimnisse.

Die Festlegung des Mindestsicherheitsniveaus erfolgt einheitlich orientiert am IT-Grundschatz des BSI².

Hierdurch wird auch eine verbesserte Vergleichbarkeit des Sicherheitsniveaus erreicht. Ein kontinuierlicher Qualitätsverbesserungsprozess ist erforderlich, der neben dem internen Qualitätsverbesserungsprozess auch eine verwaltungsübergreifende Vergleichbarkeit der einzelnen Sicherheitsniveaus ermöglicht.

Es soll eine kontinuierliche Verbesserung des sicheren Umgangs mit Informationen und Informationstechnik in den jeweiligen Verantwortungsbereichen erreicht werden. Information, Weiterbildung, Sensibilisierung aller Beschäftigten der öffentlichen Verwaltung zu Themen der Informationssicherheit sind hierbei wesentliche Eckpfeiler.

Verantwortlich für die Informationssicherheit einer Behörde ist die Behördenleitung als Teil der allgemeinen Leitungsverantwortung.

Das einvernehmliche Vorgehen soll auf folgenden fünf Säulen ruhen:

- Informationssicherheitsmanagement
- Absicherung der Netzinfrastrukturen der öffentlichen Verwaltung
- Einheitliche Sicherheitsstandards für Ebenen-übergreifende IT-Verfahren

² Gültig ist die jeweils aktuellste Fassung der IT-Grundschatzkataloge, die fortlaufend den Entwicklungen der Technik angepasst werden, sowie die zum Zeitpunkt der Verabschiedung der Leitlinie gültige Fassung der BSI-Standards.

- Gemeinsame Abwehr von IT-Angriffen
- Standardisierung und Produktsicherheit

3.1 Informationssicherheitsmanagement

„Sicherheit ist kein unveränderbarer Zustand, der einmal erreicht wird und sich niemals wieder ändert. Jede Institution ist ständigen dynamischen Veränderungen unterworfen. Viele dieser Veränderungen betreffen über Änderungen der Geschäftsprozesse, Fachaufgaben, Infrastruktur, Organisationsstrukturen und der IT auch die Informationssicherheit. Neben den unübersehbaren Änderungen innerhalb einer Institution können sich außerdem externe Rahmenbedingungen ändern, z.B. gesetzliche oder vertragliche Vorgaben, aber auch die verfügbare Informations- oder Kommunikationstechnik kann sich einschneidend ändern. Daher ist es notwendig, Sicherheit aktiv zu managen, um ein einmal erreichtes Sicherheitsniveau dauerhaft aufrechtzuerhalten.“ (Quelle: BSI-Standard 100-1: Managementsysteme für Informationssicherheit, Kapitel 3.2.1).

Ein ISMS ist ein Rahmenwerk zur Etablierung und Fortführung eines kontinuierlichen Prozesses zur Planung, Lenkung und Kontrolle der Konzepte und Aufgaben, die auf die Wahrung der Ziele der Informationssicherheit in einer Institution gerichtet sind.

Das Ziel der Leitlinie ist der Aufbau und die Etablierung eines ISMS nach einheitlichen verwaltungsübergreifenden Mindestanforderungen orientiert am IT-Grundschutz des BSI. Zur Einführung genügt im ersten Schritt ein ISMS auf Basis ISO 27001.

Die Mindestanforderungen an das ISMS umfassen:

- Festlegung und Dokumentation von Verantwortlichkeiten hinsichtlich des Informationssicherheitsmanagements (z.B. Benennung IT-Sicherheitsbeauftragte³).
- Erstellung von jeweiligen verbindlichen Leitlinien für die Informationssicherheit.

³ IT-Sicherheit wird im Dokument durch Informationssicherheit und IT-Sicherheitskonzepte durch Sicherheitskonzepte ersetzt. Der IT-Sicherheitsbeauftragte wird als feststehender Begriff (definiert z.B. in BSI-Standards) hingegen weiter verwendet.

- Erstellung und Umsetzung von Sicherheitskonzepten für Behörden und Einrichtungen.
- Festlegung und Dokumentation der Abläufe bei IT-Sicherheitsvorfällen.
- Etablierung von Prozessen, mit denen Umsetzung, Wirksamkeit und Beachtung der Informationssicherheitsmaßnahmen regelmäßig kontrolliert und die Einleitung ggf. erforderlicher Maßnahmen (z. B. Fortschreibung Sicherheitskonzepte) gewährleistet wird.
- Information, Weiterbildung, Sensibilisierung aller Beschäftigten der öffentlichen Verwaltung zu Themen der Informationssicherheit. Hierzu gehört auch die Etablierung und Durchführung regelmäßiger Sensibilisierungsmaßnahmen für die oberste Leitungsebene.
- Anforderungsgerechte und einheitliche Fortbildung der IT-Sicherheitsbeauftragten. Eine Zertifizierung der IT-Sicherheitsbeauftragten wird angestrebt.
- Jahrestagungen der IT-Sicherheitsbeauftragten zum gegenseitigen Erfahrungsaustausch (Verantwortung für Organisation wechselt mit Vorsitz im IT-Planungsrat)

3.2 Absicherung der Netzinfrastrukturen der öffentlichen Verwaltung

Netzinfrastrukturen sind als elektronisches Nervensystem der öffentlichen Verwaltung die Basis für übergreifende IT-Verfahren und elektronische Kommunikation (z.B. E-Mail). Aufgrund der Vernetzung können Angriffe oder Bedrohungen über einzelne Behördengrenzen hinweg alle Behörden gefährden und im schlimmsten Fall die Handlungsfähigkeit der Verwaltung insgesamt beeinträchtigen.

Der Bund und die Länder beschließen gemäß §4 IT-NetzG gemeinsam im Koordinierungsgremium für das Verbindungsnetz (IT-PLR) u. a. die Anschlussbedingungen. Bund und Länder vereinbaren u. a. folgende Maßnahmen in den Anschlussbedingungen zu regeln:

- Errichtung eines ISMS einschließlich einer Informationssicherheitsleitlinie, IT-Sicherheitsbeauftragten und Sicherheitskonzept für direkt angeschlossene Netze, sofern ein solches ISMS nicht bereits in einem ISMS gemäß Ziffer 3.1 enthalten ist.

- Für ein direkt angeschlossenes Netz sind grundsätzlich die BSI-Standards 100-1, 100-2, 100-3 und 100-4 dem individuellen Schutzbedarf entsprechend umzusetzen. Bei Anschluss eines Netzes sind die Teile des direkt angeschlossenen Netzes, für die diese Verpflichtung gilt, festzulegen. Sollten diese Standards auch im Rahmen eines angemessenen Stufenplans nicht umsetzbar sein, werden in den Anschlussbedingungen geeignete Maßnahmen festgelegt.
- Festlegung des Schutzbedarfs für Netzwerkverbindungen, über die kritische IT-gestützte Ebenen-Übergreifende Geschäftsprozesse⁴ laufen. Die Vergleichbarkeit der Maßnahmen für einen durchgängig hohen Schutzbedarf ist mittelfristig anzustreben.
- Abweichungen von Sicherheitsanforderungen in den Anschlussbedingungen sind dem IT-Planungsrat (oder einer vom IT-Planungsrat benannten Stelle) sowie dem Betreiber für das Verbindungsnetz bekannt zu machen. Über den Umgang mit Abweichungen entscheidet der IT-Planungsrat (oder eine vom IT-Planungsrat benannte Stelle).
- Zur Qualitätssicherung ist ein Prozess der gegenseitigen Auditierung vorgesehen.

⁴ Kritische IT-gestützte Geschäftsprozesse sind solche, die für die Arbeitsfähigkeit der Verwaltung von essentieller Bedeutung sind. Sie besitzen daher einen besonderen Schutzbedarf bezüglich Verfügbarkeit und/oder Vertraulichkeit, Integrität.

3.3 Einheitliche Sicherheitsstandards für Ebenen-übergreifende IT-Verfahren

Ebenen-übergreifende IT-Verfahren im Sinne dieser Leitlinie sind IT-Verfahren, die über Verwaltungsgrenzen hinweg angeboten bzw. genutzt werden sollen (Bund-Länder-übergreifend oder von mehreren Bundesländern genutzte IT-Verfahren).

Analog zu Netzinfrastrukturen besteht auch bei Ebenen-übergreifenden IT-Verfahren das Risiko, dass sich Angriffe sowie Bedrohungen im Zuständigkeitsbereich einer nutzenden bzw. anbietenden Behörde über das IT-Verfahren auf die Zuständigkeitsbereiche der anderen beteiligten Behörden ausbreiten können. Die Etablierung von einheitlichen und angemessenen Sicherheitsniveaus ist daher notwendig, um das Risiko für alle beteiligten Behörden zu minimieren.

Der Datenaustausch über die Verwaltungsgrenze wird gemäß den Vorgaben des IT-NetzG über das Verbindungsnetz realisiert. Bei kritischen Ebenen-übergreifenden IT-Verfahren⁵ ist im Rahmen der Notfallvorsorge festzulegen, ob und welche gemeinsamen Rückfallebenen (z.B. alternative Kommunikationswege über die Verwaltungsnetze und das Verbindungsnetz) für das jeweilige IT-Verfahren notwendig sind.

- Bei der Planung und Anpassung Ebenen-übergreifender IT-Verfahren ist der IT-Grundschutz nach BSI anzuwenden.
- Es sind die im jeweiligen Bereich betriebenen Ebenen-übergreifenden IT-Verfahren, insbesondere die kritischen IT-Verfahren, zu erfassen und beschreiben.

3.4 Gemeinsame Abwehr von IT-Angriffen

IT-Angriffe und Bedrohungen betreffen häufig nicht nur einzelne sondern mehrere Nutzer.

Die frühzeitige Erkennung und Abwehr von IT-Angriffen erfordert eine enge Zusammenarbeit und einen effizienten Informationsaustausch zwischen den beteiligten Stellen. Dies be-

⁵ Kritische IT-gestützte Geschäftsprozesse sind solche, die für die Arbeitsfähigkeit der Verwaltung von essentieller Bedeutung sind. Sie besitzen daher einen besonderen Schutzbedarf bezüglich Verfügbarkeit und/oder Vertraulichkeit, Integrität.

trifft auch die gegenseitige Information über Bedrohungen (z.B. Schwachstellen in Softwareprogrammen) und die gemeinsame Bewältigung von IT-Krisen.

Zur Umsetzung dieser Ziele wird ein VerwaltungsCERT-Verbund (VCV) von Bund und Ländern zur gegenseitigen Information, Warnung und Alarmierung durch Schaffung geeigneter landes- und bundesinterner Strukturen aus- bzw. aufgebaut.

Dies beinhaltet insbesondere den Aufbau entsprechender LandesCERTs⁶, die Festlegung übergreifender Prozesse, Meldeverfahren und Meldewege mit zentraler Sammelstelle im BSI, die gegenseitige Unterstützung und Hilfeleistung bei IT-Sicherheitsvorfällen, die regelmäßige Erstellung eines übergreifenden IT-Sicherheitslageberichtes und regelmäßige CERT-Treffen zur gemeinsamen Bewertung der übergreifenden IT-Sicherheitslage und der getroffenen Maßnahmen (z.B. zur Prävention weiterer IT-Angriffe). Es werden im Rahmen des VCV zudem Prozesse zur Bewältigung von IT-Krisen und deren regelmäßige Übung abgestimmt. Die für die Abwehr von IT-Angriffen zuständigen Behörden und Einrichtungen wie bspw. Nationales Cyber-Abwehrzentrum und IT-Krisenreaktionszentrum im BSI sind in den IT-Krisenreaktionsprozess geeignet einzubinden. Zudem ist eine angemessene Einbindung von Verfassungsschutzbehörden in Bund und Ländern sowie Strafverfolgungsbehörden und Behörden des Datenschutzes erforderlich.

- Zur Formalisierung der Zusammenarbeit im VCV und Umsetzung der genannten Ziele wird eine Geschäftsordnung erarbeitet und zwischen den Beteiligten abgestimmt.

Die Umsetzung der Maßnahmen erfolgt eigenverantwortlich im jeweiligen Verantwortungsbereich. Bund und Länder integrieren zudem die Prozesse des IT-Krisenmanagements in angemessener Form in das allgemeine Krisenmanagement.

3.5 Standardisierung und Produktsicherheit

Einheitliche Anforderungen und Standards zum Einsatz sicherer, datenschutzgerechter und interoperabler Lösungen stärken die Informationsinfrastrukturen von Bund und Ländern und vereinfachen die Realisierung von IT-Verfahren (insb. Ebenen-übergreifenden).

⁶ Aufbau kann auch in Kooperation zwischen Ländern erfolgen (z.B. gemeinsames LandesCERT)

Zur Vereinfachung und Stärkung Ebenen-übergreifender Verfahren sollen gemeinsame Basiskomponenten angeboten werden, die Grundfunktionen wie z. B. Verschlüsselung bereitstellen.

- Hierzu sind die Durchführung einer Bedarfsermittlung und die gemeinsame Festlegung von Mindestsicherheitsanforderungen für sichere Produkte, Systeme und Verfahren notwendig mit dem Ziel, gemeinsame Basiskomponenten einzusetzen.

ENTWURF