Kooperationsgruppe „Informationssicherheit des IT-PLR“

Leitlinie für die Informationssicherheit

in der öffentlichen Verwaltung

- Hauptdokument -

Stand 19.02.2013

Version 1.8 (10. IT-Planungsrat Beschluss 2013/01)

Inhaltsverzeichnis

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-Verfahren[1] 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-Grundschutz des BSI[2]. 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-Grundschutzkataloge, 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-Sicherheitsbeauftragte[3]).
- 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 Geschäftsprozesse[4] 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-Verfahren[5] 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 LandesCERTs[6], 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.