Arbeitsgruppe Informationssicherheit des IT-PLR

Leitlinie für die Informationssicherheit

in der öffentlichen Verwaltung

- 2018 -

Stand 06.12.2018

Version 2.0

Inhaltsverzeichnis

1 Einleitung

Diese Leitlinie ist die Fortschreibung der Leitlinie für Informationssicherheit, die vom IT-Planungsrat (IT-PLR) am 08.03.2013 beschlossen wurde. In Umsetzung der Leitlinie 2013 wurden in den vergangenen fünf Jahren in allen Ländern und dem Bund Informationsmanagementsysteme (ISMS) etabliert. Nunmehr ist es das Ziel, diese Managementsysteme der Bundesländer weiter zu vereinheitlichen.

In Würdigung des in Bund und Ländern vorliegenden Sachstands des ISMS fokussierte die bisherige Zielsetzung im Wesentlichen auf die Initialisierung des Sicherheitsmanagements, also der Institutionalisierung der Sicherheitsorganisation und der Schaffung grundlegender Regelungen und der Erhebung des Arbeitsfeldes.

Die Fortschreibung der Leitlinie soll nunmehr verstärkt auf die Wirkung von Sicherheitsmaßnahmen, insbesondere auf die Frage einer lückenlosen Umsetzung von Sicherheitskonzepten, und deren Messbarkeit fokussiert werden.

Mit den Verpflichtungen des Online-Zugangs-Gesetzes (OZG), der Einführung elektronischer Akten-, der Schaffung von verwaltungsübergreifenden Bürgerportalen sowie dem umfassenden elektronischen Datenaustausch der Verwaltungen mit Unternehmen und Bürgern ändern sich die Anforderungen für die Informationssicherheit für staatliche IT-Infrastrukturen erheblich. Um die Chancen zu nutzen, die sich aus einer stärkeren Vernetzung der IT-Systeme von Bund und Ländern ergeben können, ist es notwendig alle beteiligten Partner auf ein angemessenes Sicherheitsniveau zu bringen. Schließlich stellt es eine besondere Herausforderung dar, die Informationssicherheit in den vernetzten, von unterschiedlichen Partnern betriebenen, ebenenübergreifenden IT-Infrastrukturen zu wahren: Das Sicherheitsniveau in diesem Verbund wird letztlich vom schwächsten Partner bestimmt.

Die Gefahren aus dem Cyberraum sind in den letzten Jahren erheblich angestiegen. Dies wird durch die Lageberichte des BSI und die zum Teil schweren Sicherheitsvorfälle bei Bund und Ländern in der jüngeren Vergangenheit belegt. Eine prosperierende Angriffsindustrie im Internet, bestehend aus staatlichen, aber auch kriminellen Organisationen sowie sonsti-

gen Aktivsten, erfordert eine fortlaufende Anpassung der informationstechnischen Abwehrmaßnahmen der Verwaltungen bei Bund und Ländern.

In Anbetracht der Aufrechterhaltung der staatlichen Ordnung bei fortschreitender Digitalisierung können die Regierungen von Bund und Ländern keine hohen Risiken in den Kernprozessen der öffentlichen Verwaltung bei der Verarbeitung von Bürger- und Unternehmensdaten eingehen.

Informationssicherheit ist ein stetiger, dauerhafter Prozess ohne Fertigstellungstermin. Die für die Sicherung und den Erhalt der Informationssicherheit notwendigen Maßnahmen sind an die jeweilige Sicherheitslage anzupassen.

Dies kann für den Bereich der ebenenübergreifenden Zusammenarbeit nur dann wirksam erfolgen, wenn effiziente Regelungsprozesse über den IT-Planungsrat betrieben werden. Um dabei 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.

2 Geltungsbereich

Auf Grundlage des IT-Staatsvertrags ist der IT-PLR zuständig für die Vereinbarung gemeinsamer Mindestsicherheitsanforderungen zwischen Bund und Ländern. Entsprechend ist er für die Erarbeitung, Verabschiedung, Weiterentwicklung und die Erfolgskontrolle der Informationssicherheitsleitlinie verantwortlich.

Soweit Handlungsfelder des IT-Planungsrats den Einsatz der Informationstechnik in der Justiz betreffen, sind diese 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 sonstigen Einrichtungen der öffentlichen Verwaltung wird die Anwendung der Leitlinie für die Informationssicherheit empfohlen.

Sofern Bund, Länder und Kommunen gemeinsam ebenenübergreifende Verfahren oder IT-Infrastrukturen betreiben oder nutzen, gelten die Regelungen dieser Leitlinie beim Anschluss an diesen Informationsverbund.

3 Ziele der Leitlinie

Die gemeinsame Leitlinie für Informationssicherheit bezieht sich auf die Schutzziele der Informationssicherheit Verfügbarkeit, Vertraulichkeit und Integrität von Daten und Informationen.

Durch die gemeinsame Leitlinie für Informationssicherheit soll sichergestellt werden, dass dem jeweiligen Schutzziel angemessene und dem Stand der Technik entsprechende Sicherheitsmaßnahmen ergriffen werden, um das Eintreten von Sicherheitsvorfällen weitestgehend zu verhindern. Es wird ein Sicherheitsniveau angestrebt, das keine hohen Risiken akzeptiert.

Bund und Länder verfolgen mit dieser Leitlinie insbesondere:

- die zuverlässige Unterstützung der Geschäftsprozesse oder sonstigen Verwaltungsaufgaben durch die IT,
- die Sicherstellung der Kontinuität der Arbeitsabläufe der öffentlichen Verwaltung,
- die Schaffung von Rahmenbedingungen für eine sichere und vertrauenswürdige Realisierung der Digitalisierungsagenda,
- sichere Vernetzung bei ebenenübergreifender Zusammenarbeit,
- die Gewährleistung der aus verfassungsrechtlichen oder gesetzlichen Vorgaben resultierenden Anforderungen,
- die Wahrung von Dienst- oder Amtsgeheimnissen,
- einen kontinuierlichen Verbesserungsprozess bei der Qualität von IT-Fachverfahren,
- die Reduzierung der bei einem Sicherheitsvorfall entstehenden materiellen und immateriellen Schäden,
- die Begrenzung der Ausweitung von Schadensereignissen,
- die Gewährleistung vertraulicher Kommunikation sowie
- die Bewältigung von IT-Krisen.

Das gemeinsame Vorgehen zielt u.a. darauf ab, die notwendigen Sicherheitsmaßnahmen wirtschaftlicher realisieren zu können, als es jeder Einzelne für sich könnte und das Risiko

hoher Folgekosten aufgrund von Sicherheitsvorfällen zu reduzieren. Die Etablierung eines einheitlichen Mindestsicherheitsniveaus definiert für die elektronische Kommunikation und für IT-Verfahren einen Anforderungsrahmen, der unter Berücksichtigung der fachlichen Anforderungen auszugestalten ist. Die gemeinsame Nutzung standardisierter technischer Lösungen verhindert den Aufbau kostenintensiver Einzelmaßnahmen. Das gemeinsame Vorgehen etabliert zudem Ebenen übergreifend ein einheitliches Verständnis über Informationssicherheit und führt zu vergleichbaren Sicherheitsniveaus.

Zum Erreichen der Ziele dieser Leitlinie entwickelt die AG-Informationssicherheit einen Umsetzungsplan.

4 Arbeitsgruppe Informationssicherheit des IT-PLR

Die ständige Arbeitsgruppe „Informationssicherheit“ des IT-PLR hat sich als ein wirksames Instrument der bundesweiten Umsetzung der Infomationssicherheitsziele und der Abstimmung in Fragen der Informationssicherheit in den vergangenen fünf Jahren nachhaltig bewährt.

Jedes Mitglied des IT-PLR benennt einen Vertreter für die Arbeitsgruppe. Dieser ist zentraler Ansprechpartner für die Umsetzung der Informationssicherheitsziele im jeweiligen Verantwortungsbereich des Mitglieds.

Die Arbeitsgruppe setzt sich aus den benannten Vertretern der Mitglieder des IT-PLR zusammen. Sie erarbeitet gemeinsam Vorschläge zur Umsetzung und Weiterentwicklung der Leitlinie sowie berichtet jährlich an den IT-PLR zur Erfolgskontrolle. Ebenso regt sie durch Vorlagen anlassbezogen zu Diskussionen aktueller Themen der Informationssicherheit an. Sie dient außerdem dem regelmäßigen Austausch zu Themen der Informationssicherheit. Die Arbeitsgruppe berücksichtigt die Standardisierungsagenda des IT-PLR und kooperiert mit dem BSI in Fragen der Standards für Informationssicherheit.

Die ständige Arbeitsgruppe koordiniert die Aufgaben eines länderübergreifenden Informationssicherheitsmanagements. In dieser Aufgabe berät sie den IT-PLR hinsichtlich der Absicherung der IT-Netzinfrastrukturen der öffentlichen Verwaltung sowie hinsichtlich der einheitlichen Sicherheitsstandards für ebenenübergreifende IT-Verfahren. Die Arbeitsgruppe unterstützt die gemeinsame Abwehr von IT-Angriffen und legt die Grundsätze für die Einführung eines einheitlichen Notfallmanagements fest.

5 Umsetzungsstrategie

Die Digitalisierung von Verwaltungsprozessen kann nur auf Basis sicherer IT-Infrastrukturen erfolgen. Die Vorgaben dieser Leitlinie sind daher von grundlegender Bedeutung für die innovativen Digitalisierungsprojekte und werden von Bund und Ländern im jeweiligen Zuständigkeitsbereich in eigener Verantwortung umgesetzt.

Bund und Länder sorgen dafür, dass zur Erfüllung der Aufgaben des Informationssicherheitsbeauftragten (ISB) sowie für die Aufgaben des Informationssicherheitsmanagements angemessene finanzielle und personelle Ressourcen zur Verfügung gestellt werden.

Um das einheitliche Mindestsicherheitsniveau nicht zu gefährden, ist bei ebenenübergreifenden IT-Verfahren durch den jeweiligen IT-Verfahrensverantwortlichen die Umsetzung der Vorgaben der Informationssicherheitsleitlinie im notwendigen Umfang auf die jeweiligen Verfahrensbeteiligten auszudehnen.

Soweit Dritte als Auftragnehmer für die öffentliche Verwaltung Leistungen erbringen, sind diese bei der Auftragserteilung auf die verbindlichen Vorgaben der Leitlinie zur Informationssicherheit im notwendigen Umfang zu verpflichten und zu kontrollieren.

Die Festlegung des Mindestsicherheitsstandards orientiert sich am IT-Grundschutz des BSI, dem IT-Grundschutz-Kompendium in der jeweils aktuellen Fassung sowie der ISO 2700x-Reihe.

Ausgehend von der individuellen Ausgangslage im jeweiligen Zuständigkeitsbereich von Bund und Ländern, sind für die Umsetzung der aus der Leitlinie abzuleitenden Maßnahmen Investitionen notwendig. Erforderliche Ausgaben stehen unter Haushaltsvorbehalt.

Verantwortlich für Schaffung und Einhaltung der notwendigen Informationssicherheit einer Behörde ist die Behördenleitung.

Das einvernehmliche Vorgehen in der Informationssicherheit umfasst fünf Handlungsfelder:

- Informationssicherheitsmanagement,
- Absicherung der IT-Netzinfrastrukturen der öffentlichen Verwaltung,
- Einheitliche Sicherheitsstandards für ebenenübergreifende IT-Verfahren,
- Gemeinsame Abwehr von IT-Angriffen sowie
- IT-Notfallmanagement.

5.1 Informationssicherheitsmanagement

In den Einrichtungen von Bund und Ländern ist ein angemessenes Informationssicherheitsmanagement zu betreiben.

Ein Informationsmanagementsystem ist ein Rahmenwerk zur Etablierung und Fortführung eines kontinuierlichen Prozesses zur Planung, Durchführung und Kontrolle und Verbesserung der Konzepte und Aufgaben, die auf die Wahrung der Ziele der Informationssicherheit in einer Institution gerichtet sind. Zur Wahrung der Ziele der Informationssicherheit ist es notwendig, ein angemessenes und ausreichendes Sicherheitsniveau umzusetzen und dieses zu erhalten.

„Ein angemessenes Sicherheitsniveau ist in erster Linie abhängig vom systematischen Vorgehen und erst in zweiter Linie von einzelnen technischen Maßnahmen. Die folgenden Überlegungen verdeutlichen diese These und die Bedeutung der Leitungsebene im Sicherheitsprozess:

- *Die Leitungsebene trägt die Verantwortung dafür, dass gesetzliche Regelungen und Verträge mit Dritten eingehalten werden und dass wichtige Geschäftsprozesse störungsfrei ablaufen.*
- *Die Leitungsebene ist diejenige Instanz, die über den Umgang mit Risiken entscheidet.*
- *Informationssicherheit hat Schnittstellen zu vielen Bereichen einer Institution und betrifft wesentliche Geschäftsprozesse und Aufgaben. Nur die Leitungsebene kann daher für eine reibungslose Integration des Informationssicherheitsmanagements in bestehende Organisationsstrukturen und Prozesse sorgen.*
- *Die Leitungsebene ist zudem für den wirtschaftlichen Einsatz von Ressourcen verantwortlich.*

Der Leitungsebene kommt daher eine hohe Verantwortung für die Informationssicherheit zu. Fehlende Steuerung, eine ungeeignete Sicherheitsstrategie oder falsche Entscheidungen können sowohl durch Sicherheitsvorfälle als auch durch verpasste Chancen und Fehlinvesti-

tionen weitreichende negative Auswirkungen haben. Eine intensive Beteiligung der Führungsebene ist somit unerlässlich: Informationssicherheit ist Chefsache!"[1]

Die Mindestanforderungen an ein ISMS sind:

- die Festlegung und Dokumentation von Verantwortlichkeiten aller Rollen des Informationssicherheitsmanagements,
- verbindliche Leit- und Richtlinien für die Informationssicherheit,
- flächendeckende Erstellung und Umsetzung von Sicherheitskonzepten für Verwaltungsprozesse, IT-Services, Fachverfahren sowie Behörden und Einrichtungen,
- eingeführte und dokumentierte Informationssicherheitsprozesse,
- Etablierung eines kontinuierlichen Verbesserungsprozesses zur Gewährleistung von Umsetzung, Wirksamkeit und Beachtung der Informationssicherheitsmaßnahmen,
- Festlegung und Dokumentation der Abläufe bei Informationssicherheitsvorfällen,
- die regelmäßige Aus- und Weiterbildung der Informationssicherheitsbeauftragten (BSI-Zertifizierung der ISB wird angestrebt) sowie
- die Information, Weiterbildung und Sensibilisierung aller Beschäftigten der öffentlichen Verwaltung zu Themen der Informationssicherheit zu einer kontinuierlichen Verbesserung des sicheren Umgangs mit Informationen und Informationstechnik führen.

[1] IT-Grundschutzstandard des BSI 200-1, Seite 6

5.2 Absicherung der IT-Netzinfrastrukturen der öffentlichen Verwaltung

Die von Bund und Ländern beschlossenen Anschlussbedingungen gem. § 4 IT-NetzG an das Verbindungsnetz des Bundes sind zu erfüllen, deren Einhaltung zu überprüfen und, an Schutzbedarf und Bedrohungslage gemessen, fortzuschreiben. In einer Fortschreibung sind die jeweils aktuellen IT-Grundschutzstandards des BSI anzuwenden.

In der Fortschreibung sind die folgenden Mindestanforderungen an die Anschlussbedingungen zu erfüllen:

- Errichtung eines ISMS einschließlich einer Informationssicherheitsleitlinie, Informationssicherheitsbeauftragten und Sicherheitskonzept für direkt angeschlossene Netze, sofern ein solches ISMS nicht bereits in einem ISMS gemäß Ziffer 4.1 enthalten ist.
- 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.
- Mittelfristiges Anstreben eines durchgängig hohen Schutzbedarfs für Netzwerkverbindungen, die kritische ebenenübergreifende Verwaltungsprozesse[2] unterstützen.
- 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 Überprüfung und des Erfahrungsaustausches (z.B. Revision der Anschlussbedingungen) vorzusehen.

[2] Kritische IT-gestützte Verwaltungsprozesse sind solche, die für die Arbeitsfähigkeit der Verwaltung von essentieller Bedeutung sind. Sie besitzen daher eine über normal hinausgehende Schutzbedarfsneignung bezüglich Verfügbarkeit, Vertraulichkeit oder Integrität.

5.3 Einheitliche Sicherheitsstandards für ebenen übergreifende IT-Verfahren

Ebenenübergreifende IT-Verfahren im Sinne dieser Leitlinie sind IT-Verfahren, die über Verwaltungsgrenzen hinweg angeboten bzw. genutzt werden sollen (Bund-Länderübergreifend oder von mehreren Ländern genutzte IT-Verfahren).

Bei ebenenübergreifenden IT-Verfahren werden aufgrund der Reichweite und der Vielzahl der Beteiligten besondere Anforderungen an die Informationssicherheit gestellt. Die Etablierung eines einheitlichen und angemessenen Sicherheitsniveaus ist daher notwendig, um ein akzeptables verbleibendes Risiko für alle Beteiligten zu erreichen.

Der Datenaustausch über die Verwaltungsgrenze wird gemäß den Vorgaben des IT-NetzG über das Verbindungsnetz realisiert. Bei kritischen ebenenübergreifenden IT-Verfahren ist im Rahmen der Notfallvorsorge ein Prozess zu etablieren welcher festlegt, ob und welche gemeinsamen Rückfallebenen für das jeweilige IT-Verfahren notwendig und möglich sind.

Bei der Planung und Anpassung ebenenübergreifender IT-Verfahren ist der IT-Grundschutz des BSI in seiner jeweiligen Fassung anzuwenden.

Es sind die im jeweiligen Bereich betriebenen ebenenübergreifenden IT-Verfahren, insbesondere die kritischen IT-Verfahren, zu erfassen und zu beschreiben. Hierzu soll ein einheitlicher Prozess der Erfassung und Pflege etabliert werden, bei dem auch die wesentlichen Teilaspekte der Informationssicherheit erfasst werden.

5.4 Gemeinsame Abwehr von IT–Angriffen

IT-Angriffe und Bedrohungen betreffen häufig nicht nur einzelne Bedienstete, sondern meist ganze Behörden und Einrichtungen. Solche IT-Angriffe können daher ein enormes Schadenspotenzial entfalten. So besteht in Netzverbünden einerseits die Gefahr einer internen Ausbreitung des IT-Angriffs. Anderseits werden IT-Angriffe, seien sie wahllos oder zielgerichtet ausgeführt, selten nur einen Verbundpartner treffen. Die frühzeitige Erkennung und Abwehr von IT-Angriffen erfordert eine enge Zusammenarbeit und einen effizienten Informationsaustausch zwischen den beteiligten Stellen.

Zur Umsetzung dieser Ziele wird der VerwaltungsCERT-Verbund (VCV) von Bund und Ländern zur gegenseitigen Information, Warnung und Alarmierung weiterentwickelt.

Auswertungen und Meldungen über IT-Angriffe müssen mittels Prozessen und Verfahren in den einzelnen Organisationen etabliert und umgesetzt werden. Dabei ist es notwendig, den ungehinderten Informationsfluss im VerwaltungsCERT-Verbund zu fördern und zu erhalten.

Dazu bedarf es insbesondere des Betriebs ausreichend finanziell und personell ausgestatteter CERTs. Diese arbeiten eng zusammen und tauschen sich aus. Der VCV hat zu allen relevanten Stellen ein besonderes Vertrauensverhältnis. Der Schutz von Informationen und Quellen ist ein zentrales Element für die vertrauensvolle Zusammenarbeit. Dadurch kann er bei Sicherheitsvorfällen unverzüglich Warnungen und Informationen weiterleiten. Die existierenden Verfahren für einen automatisierten Informationsfluss zwischen den CERTs sind in die internen Prozesse einzubinden und durch Einbringen eigener Erkenntnisse zu fördern. Die Verfahren und ein automatisierter Austausch sind entwickeln.

Bund und Länder verständigen sich auch auf gemeinsame technische Maßnahmen zur Abwehr von IT-Angriffen um die Reaktionsfähigkeit, die Reaktionszeit und Erkennbarkeit zu verbessern.

5.5 IT-Notfallmanagement

Um Notfällen und Krisen vorzubeugen, ist es erforderlich, in den vom Geltungsbereich dieser Leitlinie erfassten Verwaltungen angemessene Notfallmanagement-Prozesse gem. dem IT-Grundschutzstandard des BSI in der jeweils aktuell gültigen Fassung zu etablieren. Geeignete Präventivmaßnahmen erhöhen die Robustheit und Ausfallsicherheit der Geschäftsprozesse und ermöglichen ein schnelles und zielgerichtetes Agieren in einem Notfall oder einer Krise. Die Umsetzung der Maßnahmen erfolgt eigenverantwortlich im jeweiligen Verantwortungsbereich des Bundes und der Länder.

IT-Notfallmanagement, d.h. Notfallvorsorge und Notfallbewältigung, hat im Wesentlichen zum Ziel, durch Absicherung bzw. Wiederherstellung der Verfügbarkeit der IT-Services, der IT-Verfahren, der IT-Systeme und insbesondere der Informationen zu garantieren, dass die Verwaltungstätigkeiten – jedenfalls im unbedingt erforderlichen Umfang – fortgeführt werden können.

IT-Notfallmanagement ist Teil des ganzheitlichen Notfall- oder Krisenmanagements und kann somit nicht isoliert betrachtet werden. Bund und Länder sind daher gehalten, die Prozesse des IT-Krisenmanagements in angemessener Form in das allgemeine Krisenmanagement zu integrieren. Eine enge Zusammenarbeit und Abstimmung mit den Arbeitsgremien der Innenministerkonferenz ist zu suchen.

Das IT-Notfallmanagement, das IT-Krisenmanagement sowie die Zusammenarbeit mit dem allg. Krisenmanagement, ist auch länderübergreifend und mit dem Bund mit geeigneten Übungen (intern u. extern) zu verbessern.