Leitlinie zur Gewährleistung der Informationssicherheit in der Landesverwaltung von Mecklenburg-Vorpommern

IS-Leitlinie M-V

Schwerin, 12.05.2014

Mecklenburg Vorpommern
Ministerium für Inneres und Sport

Inhaltsverzeichnis

1. Einleitung

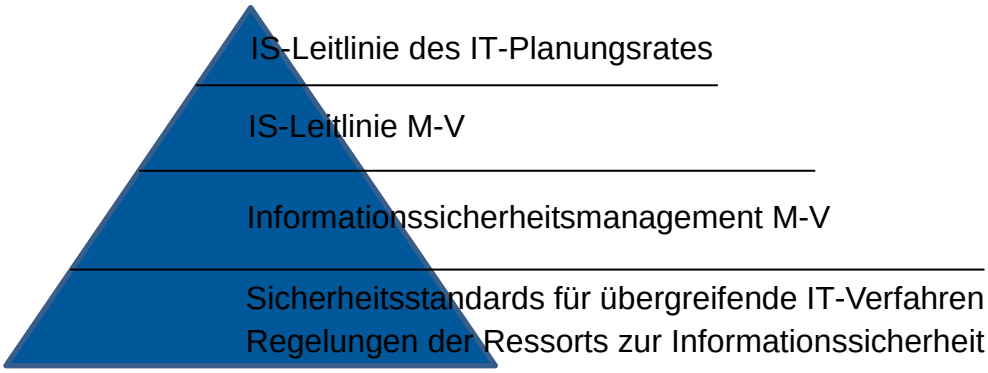
Die Geschäftsprozesse der Verwaltung werden zunehmend durch den Einsatz von Informationstechnik unterstützt. Nur wenn die Informationstechnik zuverlässig funktioniert, ist die Verwaltung heutzutage arbeitsfähig. Aus dieser Abhängigkeit ergibt sich ein hoher Anspruch an die Verfügbarkeit, die Vertraulichkeit und die Integrität der zu verarbeitenden Informationen. Um diesem Anspruch bei gleichzeitig zunehmender Vernetzung und somit wachsender Bedrohungslage gerecht werden zu können, ist eine gemeinsame IT-Sicherheitsstrategie notwendig, mit der insbesondere Festlegungen für ein übergreifend geltendes Mindestsicherheitsniveau getroffen werden. Der IT-Planungsrat hat daher entsprechende Regelungen getroffen und eine gemeinsame Leitlinie für die Informationssicherheit[1] verabschiedet, die für alle Behörden und Einrichtungen der Verwaltungen des Bundes und der Länder gilt.

2. Gegenstand und Geltungsbereich

Mit der IS-Leitlinie der Landesverwaltung von Mecklenburg-Vorpommern (IS-Leitlinie M-V) sollen die Vorgaben, die sich aus der Leitlinie des IT-Planungsrats ergeben, auf Landesebene umgesetzt werden. Sie gilt für die Staatskanzlei und die Ressorts der Landesregierung[2]. Soweit diese für ihre Geschäftsbereiche eigene Regelungen zur Informationssicherheit erarbeiten, hat dies auf der Grundlage dieser IS-Leitlinie zu erfolgen. Die IS-Leitlinie M-V versteht sich insoweit als Bestandteil eines hierarchisch abgestimmten Regelwerks (s. nachfolgende Abbildung), welches die landesweit geltenden Mindestanforderungen und die Organisationsstrukturen zur Gewährleistung der Informationssicherheit beschreibt. Der Landtagsverwaltung und dem Landesrechnungshof wird diese Leitlinie zur Anwendung empfohlen.

[1] 10. IT-Planungsrat Beschluss 2013/01

[2] Soweit die Justiz betroffen ist, sind die aus den verfassungs- und einfachrechtlich garantierten Positionen der unabhängigen Rechtspflegeorgane resultierenden Besonderheiten zu beachten, insbesondere ist die richterliche Unabhängigkeit zu wahren.



3. Ziele der Informationssicherheit und Mindestsicherheitsniveau

Aufbauend auf den in der gemeinsamen IS-Leitlinie des IT-Planungsrats beschriebenen Zielen werden mit der IS-Leitlinie M-V insbesondere folgende Informationssicherheitsziele verfolgt:

- Alle Beschäftigten der Landesverwaltung sind sich ihrer Verpflichtung zur Einhaltung der für die Informationssicherheit relevanten Gesetze, Vorschriften, Richtlinien, Anweisungen und vertraglichen Verpflichtungen bewusst und tragen durch ihr verantwortliches Handeln zur Informationssicherheit bei.
- Beim IT-Einsatz wird in jeweils angemessenem Maße die Erreichung der Schutzziele Verfügbarkeit, Vertraulichkeit, Integrität der Daten sowie die Einhaltung der Datenschutzanforderungen im Hinblick auf Transparenz, Betroffenheitsrechte und Zweckbindung gewährleistet. Die daraus abgeleiteten Sicherheitsmaßnahmen sind auch dann anzuwenden, wenn sich daraus Beeinträchtigungen für die IT-Nutzung ergeben.
- Die Sicherheit der IT-Verfahren wird neben der Leistungsfähigkeit und Funktionalität gewährleistet. Bleiben im Einzelfall trotz der Sicherheitsvorkehrungen Risiken untragbar, ist an dieser Stelle auf den IT-Einsatz zu verzichten.

Als Mindestsicherheitsniveau gilt einheitlich der IT-Grundschutz des Bundesamtes für die Sicherheit in der Informationstechnik (BSI)[3].

[3] Gültig sind die jeweils aktuelle Fassung der IT-Grundschutzkataloge sowie die aktuellen Fassungen der BSI-Standards.

4. Umsetzungsstrategie

Die Umsetzungsstrategie beruht auf den in der gemeinsamen IS-Leitlinie des Planungsrats beschriebenen 5 Säulen:

- Informationssicherheitsmanagement
- Absicherung der Netz- und Kommunikationsinfrastrukturen
- Einheitliche Sicherheitsstandards für übergreifende IT-Verfahren
- Gemeinsame Abwehr von IT-Angriffen
- Standardisierung und Basisinfrastruktur

Die nachfolgenden Kapitel enthalten zu jeder der Säulen entsprechende Erläuterungen und Festlegungen.

4.1 Informationssicherheitsmanagement

Zur Gestaltung des Informationssicherheitsprozesses wird ein ressortübergreifendes Informationssicherheitsmanagement (ISM) aufgebaut. Zentrales Kernelement des ISM ist die Etablierung einer ressortübergreifenden IT-Sicherheitsorganisation. Einzelheiten dazu, insbesondere hinsichtlich der Verantwortlichkeiten, sind im „Konzept zum Aufbau und Betrieb eines Informationssicherheitsmanagements in der Landesverwaltung von Mecklenburg-Vorpommern“ (ISM-Konzept) enthalten. Dieses Konzept basiert auf den Standards des BSI und berücksichtigt insbesondere folgende Anforderungen:

- Festlegung der Struktur der ressortübergreifenden Informationssicherheits-organisation der Landesverwaltung M-V sowie der von den Beteiligten wahrzunehmenden Aufgaben
- Regelungen zur Meldung und Behandlung von Sicherheitsvorfällen und zu weiteren Berichtspflichten
- Regelungen zur Durchführung von Informationssicherheitsrevisionen sowie Sensibilisierungs- und Schulungsmaßnahmen

4.2 Absicherung der Netz- und Kommunikationsinfrastrukturen

Sichere Netz- und Kommunikationsinfrastrukturen bilden die unverzichtbare Basis für IT-Verfahren, elektronische Kommunikation und Telefonie. Angriffe oder

Bedrohungen können über Behördengrenzen hinweg alle angeschlossenen Teilnehmer gefährden und damit die Handlungsfähigkeit der Landesverwaltung insgesamt beeinträchtigen. Die Landesverwaltung M-V nutzt das Corporate Network LAVINE (CN LAVINE) als Netz- und Kommunikationsinfrastruktur. Das CN LAVINE stellt den Zugang zu landesweiten Kommunikationsdiensten, zentralen Datenbanken sowie ressortspezifischen und –übergreifenden Fachverfahren und Intranetanwendungen bereit sowie darüber hinaus den Zugang zum Internet und der Deutschland-Online-Infrastruktur (DOI). Für den Anschluss der Behörden an das CN LAVINE gelten aufgrund der DOI-Anschlussbedingungen, der vertraglichen Regelungen mit der DVZ M-V GmbH und insbesondere der Festlegungen im Sicherheits- und Notfallkonzept u. a. folgende Regelungen:

- Behörden, die an das CN LAVINE angeschlossen sind, müssen über ein Sicherheitskonzept, das auf den IT-Grundschutzkatalogen des BSI beruht, verfügen.
- Die gemäß dem IT-Sicherheits- und Notfallkonzept des CN LAVINE erforderlichen zentralen und dezentralen Sicherheitsmaßnahmen sind umzusetzen.
- Die Wirksamkeit der Sicherheitsmaßnahmen ist im Sinne eines kontinuierlichen Verbesserungsprozesses regelmäßig zu kontrollieren, zu dokumentieren und weiterzuentwickeln.

4.3 Einheitliche Sicherheitsstandards für übergreifende IT-Verfahren

Übergreifende IT-Verfahren sind dadurch gekennzeichnet, dass sie nicht nur innerhalb der eigenen Behörde, sondern durch mehrere Behörden genutzt werden. Analog zu den Netz- und Kommunikationsinfrastrukturen besteht auch bei übergreifenden IT-Verfahren ein erhöhtes Risiko, dass sich Angriffe oder Bedrohungen von einem Nutzer auf die anderen Nutzer ausbreiten können. Um das Risiko für alle beteiligten Behörden zu minimieren und ein einheitliches und angemessenes Sicherheitsniveau zu gewährleisten, gelten für die Planung und den Betrieb übergreifender IT-Verfahren folgende Regelungen:

- Die übergreifenden IT-Verfahren, insbesondere die kritischen[4] IT-Verfahren, sind zu erfassen und beschreiben.
- Bei der Planung, dem Betrieb und der Pflege von übergreifenden IT-Verfahren sind die IT-Grundschutz-Standards des BSI anzuwenden.
- Die in den zu erstellenden IT-Sicherheitskonzepten festgelegten Sicherheitsmaßnahmen sind von allen am Verfahren beteiligten Stellen umzusetzen.
- Die Wirksamkeit der Sicherheitsmaßnahmen ist im Sinne eines kontinuierlichen Verbesserungsprozesses regelmäßig zu kontrollieren, zu dokumentieren und weiterzuentwickeln.
- Bei kritischen übergreifenden IT-Verfahren sind Rückfallebenen vorzusehen.

4.4 Gemeinsame Abwehr von IT-Angriffen

Um IT-Angriffe und Bedrohungen frühzeitig zu erkennen und ihnen wirkungsvoll begegnen zu können, sind eine enge Zusammenarbeit und ein effizienter Informationsaustausch zwischen den beteiligten Stellen erforderlich. Dies betrifft auch die gegenseitige Information über Bedrohungen und die gemeinsame Bewältigung von IT-Krisen. Der IT-Planungsrat hat daher den Aufbau eines VerwaltungsCERT-Verbunds (VCV) von Bund und Ländern beschlossen.
Dies bedingt zwingend den Aufbau eines CERTs[5] in der Landesverwaltung von Mecklenburg-Vorpommern. Einzelheiten dazu sind im ISM-Konzept des Landes beschrieben.

Das CERT M-V ist in das ISM des Landes eingebunden und nimmt insbesondere folgende Aufgaben wahr:

- Die Entwicklung und strukturierte Verteilung von vorbeugenden Handlungsempfehlungen zur Vermeidung von Sicherheitsvorfällen
- Die Koordinierung und Umsetzung von Maßnahmen bei Sicherheitsvorfällen mit ressortübergreifender Bedeutung

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

[5] CERT steht für Computer Emergency Response Team (Computer-Notfall-Team).

- Die Entwicklung und Durchführung von nachhaltigen Maßnahmen zum Aufbau und zur weiteren Verbesserung des Sicherheitsbewusstseins
- Die Beratung der Kommission für Informationssicherheit der Landesverwaltung[6]
- Die regelmäßige Erstellung und Bekanntgabe von Sicherheitslageberichten
- Die Zusammenarbeit im Rahmen des VerwaltungsCERT-Verbunds (VCV) auf Bund-Länder-Ebene
- Die Unterstützung der Arbeit der Informationssicherheitsbeauftragten der Behörden

4.5 Standardisierung und Basisinfrastruktur

Der Einsatz von Standards und gemeinsamer Basisinfrastruktur ermöglicht kostengünstige, sichere und interoperable Lösungen und vereinfacht damit die Planung und den Betrieb von IT-Verfahren. Die notwendige Basisinfrastruktur mit zentral von der DVZ M-V GmbH betriebenen Netzwerkdiensten steht den Behörden zur Nutzung zur Verfügung. Einzelheiten dazu sind im IT-Strukturrahmen des Landes beschrieben.

- Der IT-Strukturrahmen ist fortzuschreiben.
- Die im IT-Strukturrahmen des Landes enthaltenen Regelungen zur Nutzung von Standards und zentral zur Verfügung stehenden Diensten sind einzuhalten.

5. Fortschreibung und Umsetzung der IS-Leitlinie

Die Informationssicherheitsleitlinie M-V wird anlassbezogen fortgeschrieben, mindestens aber alle 2 Jahre einer überprüfenden Revision unterzogen.

6. Inkraftsetzung

Diese Leitlinie tritt am Tag nach ihrer Veröffentlichung in Kraft.

[6] Die Aufgaben, die Zusammensetzung und organisatorische Einbindung dieser Kommission in die Informationssicherheitsorganisation der Landesverwaltung sind im ISM-Konzept, Kapitel 5.1 beschrieben.