Arbeitsgruppe des IT-Planungsrats „Informationssicherheit“

Leitlinie für die Informationssicherheit in der öffentlichen Verwaltung 2018

Umsetzungsplan

VERSION 1.0 vom 05.02.2020

Inhalt

Einleitung

In Umsetzung der Leitlinie für Informationssicherheit für die öffentliche Verwaltung 2018 werden mit dem Umsetzungsplan die Handlungsfelder mit konkreten Maßnahmen und messbaren Zielen unterlegt. Aus den 26 Kennzahlen zum Umsetzungsfortschritt bei den Maßnahmen soll ein fortlaufendes jährliches Berichtswesen der AG-Informationssicherheit an den IT-Planungsrat ausgebildet werden.

Die Verwaltungen des Bundes und der Länder haben seit mehreren Jahren Informationssicherheitsmanagementsysteme (ISMS) etabliert und entwickeln diese stetig weiter. Die Wahrung der Informationssicherheit in den Verwaltungen ist eine Daueraufgabe, die in Bund und Ländern mit unterschiedlichen Haushaltsansätzen unterlegt ist. Für die Umsetzung der aus der Leitlinie für Informationssicherheit für die öffentliche Verwaltung 2018 abzuleitenden Maßnahmen werden Personal- und Sachmittel erforderlich, deren Höhe sich nach der individuellen Ausgangslage im Bereich der Informationssicherheit bei Bund und Ländern unterscheidet und nicht pauschal festgelegt werden können.

Handlungsfeld 1: Informationssicherheitsmanagement

Die Mindestanforderungen an ein ISMS sind unter Berücksichtigung der besonderen Verhältnisse bei Bund und Ländern gemäß Leitlinie, Kapitel 5.1, festgelegt: Zu jeder Mindestanforderung sind nachfolgend Kennzahlen festgelegt.

1.1. Festlegung und Dokumentation von Verantwortlichkeiten aller Rollen des Informationssicherheitsmanagements

Umsetzungstermin: 2020

- Die Rollen und deren Aufgaben sind festgelegt und dokumentiert. (Kennzahl 1: J/N)
- Die Rollen für alle Behörden und Einrichtungen sind tatsächlich besetzt. (Kennzahl 2: Umsetzung in %)

KOSTEN:
Die Kosten sind abhängig von der konkreten personalwirtschaftlichen Umsetzung.

1.2. verbindliche Leit- und Richtlinien für die Informationssicherheit

Für die Entwicklung und Fortschreibung des ISMS sind Richtlinien grundlegend. Daher ist vorrangig ein Prozess zur Initiierung, Verabschiedung, Überprüfung und Fortschreibung von Richtlinien zu etablieren.

Umsetzungstermin: 2020

- Die Leitlinien sind in Kraft gesetzt und regeln den jeweiligen Zuständigkeitsbereich verbindlich. (Kennzahl 3: J/N)
- Der Prozess zur Erstellung von Richtlinien für den jeweiligen Zuständigkeitsbereich ist etabliert. (Kennzahl 4: J/N)
- Der Prozess zur regelmäßigen Überprüfung der Richtlinien ist etabliert. (Kennzahl 5: J/N)

KOSTEN:
Die entstehenden Kosten sind abhängig vom bestehenden Umsetzungsgrad des notwenigen individuellen ISMS. Eine konkrete Kostenangabe ist nicht möglich.

1.3. flächendeckende Erstellung und Umsetzung von Sicherheitskonzepten (SiKo)

Sicherheitskonzepte für Verwaltungsprozesse, IT-Services, Fachverfahren sowie Behörden und Einrichtungen sind sukzessive zu erstellen und zu leben. Die Reihenfolge der Erstellung soll nach Schutzbedarf und damit dem Risiko gestaffelt werden. Die Erstellung, Umsetzung und Fortschreibung der Sicherheitskonzepte sind Aufgabe der Verantwortlichen für die Fachverfahren und die IT-Services (Eigentümerrolle). Die Informationssicherheits-beauftragten initiieren und begleiten den Prozess.

Umsetzungstermin: 2022

- SiKo für geschäftskritische oder für OZG-Verfahren sind erstellt und werden turnusmäßig fortgeschrieben. (Kennzahl 6: Gesamtzahl/ Anteil mit SiKo an Gesamtzahl)

Umsetzungstermin: 2024

- SiKo für sonstigen Verwaltungsprozesse und Bestandsverfahren sind erstellt und werden turnusmäßig fortgeschrieben. (Kennzahl 7: Anzahl/ Anteil an Gesamtzahl)

KOSTEN:

Die anfallenden Kosten sind abhängig vom individuell notwendigen ISMS der Einrichtungen und Behörden und sind Teil der Erstellungs- und Betriebsaufwände von Services und Fachverfahren. Eine konkrete Kostenangabe ist nicht möglich.

1.4. Beschreibung und Umsetzung eines kontinuierlichen Verbesserungsprozesses zur Gewährleistung von Umsetzung, Wirksamkeit und Beachtung der Informationssicherheitsmaßnahmen

Es sind etablierte Informationssicherheitsprozesse (z. B. für das Berichtswesen oder Sensibilisierungsmaßnahmen) auf die Wirksamkeit zu prüfen sowie notwendige neue Prozesse zu etablieren.

Umsetzungstermin: 2021

- Der KV-Prozess ist etabliert und wird angewandt. (Kennzahl 8: J/N)

KOSTEN:

Die anfallenden Kosten sind Teil des allgemeinen Betriebs- und Organisationsaufwands von Behörden und können nicht konkret beziffert werden.

1.5. Festlegung und Dokumentation der Abläufe bei der Bewältigung von Informationssicherheitsvorfällen.

Umsetzungstermin: 2020

- Meldepflichtige Ereignisse, Meldestellen und Meldeabläufe (insb. Meldewege) sind unter Beachtung des Meldestandards des IT-PLR für alle Behörden und Einrichtungen festgelegt und dokumentiert. (Kennzahl 9: J/N)

KOSTEN:

Die anfallenden Kosten sind Teil des allgemeinen Betriebs- und Organisationsaufwands von Behörden und können nicht konkret beziffert werden.

1.6. Regelmäßige Aus- und Weiterbildung der Informationssicherheitsbeauftragten (ISB), wobei eine BSI-Zertifizierung angestrebt wird

Umsetzungstermin: 2020

- Ein Aus- und Fortbildungsprogramm wird regelmäßig angewendet. (Kennzahl 10:J/N)
- Die kontinuierliche Fortbildung der ISB findet statt. (Kennzahl 11:J/N)

KOSTEN:

Die anfallenden Kosten sind Teil der fachlichen Qualifikation und beruflichen Fortbildung von Bediensteten in der öffentlichen Verwaltung.

1.7. Information, Weiterbildung und Sensibilisierung aller Beschäftigten der öffentlichen Verwaltung zu Themen der Informationssicherheit für eine kontinuierliche Verbesserung des sicheren Umgangs mit Informationen und Informationstechnik.

Umsetzungstermin: 2021

- Es sind Konzepte für unterschiedliche Zielgruppen (z.B. MA, Führungskräfte, IT-Fachkräfte) vorhanden. (Kennzahl 12: J/N)

Umsetzungstermin: 2023

- Die zielgruppenbezogenen Konzepte sind als kontinuierliche Fortbildung etabliert und die in den Konzepten beschriebenen Maßnahmen werden umgesetzt. (Kennzahl13: J/N)

KOSTEN:

Die anfallenden Kosten sind abhängig von der konkreten Ausgestaltung, insbesondere dem Umfang einer Sensibilisierungskampagne und der eingesetzten Werbemittel.

Handlungsfeld 2: Absicherung IT-Netzinfrastruktur öffentliche 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 entsprechend Schutzbedarf und Bedrohungslage fortzuschreiben.

Die Länder und der Bund sichern ihre IT-Netzinfrastruktur auf dem Stand der Technik und auf Grundlage eines Informationssicherheitsmanagements ab.

2.1. Überarbeitung der Anschlussbedingungen

Die Festlegung der Anschlussbedingungen (AB) für das Verbindungsnetz obliegt dem IT-Planungsrat (§ 4 Abs. 1 Nr. 4 i.V.m. § 1 Abs. 3 IT-NetzG).

2.2. Einhaltung der Anschlussbedingungen an das Verbindungsnetz in Bund und Ländern

Umsetzungstermin: 2022

- Der Bund und die Länder gewährleisten die Umsetzung und Aufrechterhaltung der AB in der jeweils geltenden Fassung. (Kennzahl 14: J/N)
- Ein Erfahrungsaustausch der Teilnehmer am Verbindungsnetz wird durchgeführt. (Kennzahl 15: J/N)

KOSTEN:

Die Kosten hierfür sind abhängig vom Ausbaustand des ISMS der Teilnehmer und werden maßgeblich durch die Anforderungen der AB gesetzt.

Handlungsfeld 3: Einheitliches Sicherheitsniveau für Ebenen übergreifende IT-Verfahren

Die Etablierung eines einheitlichen und angemessenen Sicherheitsniveaus ist notwendig, um ein akzeptables verbleibendes Risiko für alle Beteiligten zu erreichen.

3.1. Erfassung aller Ebenen übergreifenden Verfahren

Bund und Länder erfassen die in der jeweiligen Verantwortung betriebenen Ebenen-übergreifenden IT-Verfahren nach einem einheitlichen Prozess und auf einheitlicher Datenstruktur. Die Datenstruktur enthält auch Informationen hinsichtlich des tatsächlichen Sicherheitsstandards.

Umsetzungstermin: 2020

- Der Prozess für die Erfassung der Verfahren und die dafür erforderliche Datenstruktur ist erarbeitet.(Kennzahl 15: J/N)

Umsetzungstermin: 2021

- Die Verfahren wurden erfasst und der Prozess zur regelmäßigen Überprüfung wurde festgelegt. (Kennzahl 16: Reifegrad des Sicherheitsniveaus der erfassten Verfahren in %)

KOSTEN:
Die Kosten für die Erstellung des Erfassungsprozesses und der Datenstruktur werden mit ca. 30.000 Euro geschätzt und sind im Budget der AG-Informationssicherheit enthalten. Daneben entsteht ein nicht bezifferbarer Aufwand bei der tatsächlichen Erfassung und Pflege der Daten bei Bund und Ländern.

3.2. Anwendung des IT-Grundschutzes auf Ebenen übergreifende IT-Verfahren

Bei der Planung, Aufbau und Anpassung Ebenen übergreifender IT-Verfahren ist der IT-Grundschutz des BSI in seiner jeweils gültigen Fassung anzuwenden. Der Verantwortliche für das Verfahren legt dabei die IT- Architektur und die Anforderungen nach IT-Grundschutz unter Berücksichtigung der zu erwartenden Zielgruppe in der Verwaltung für die Nutzung der Anwendung fest. Die Umsetzung der Anforderungen erfolgt durch den Nutzer in eigener Verantwortung.

Für die tatsächliche Umsetzung des IT-Grundschutzes wird durch den Verantwortlichen für das IT-Verfahren ein geeigneter Nachweis (ggf. qualifizierte Eigenauskunft/ Grundschutz Testat/Zertifikat) geführt. Die Nutzer des IT-Verfahrens sind zur Mitwirkung bei der Erfassung des Umsetzungsstandes des IT-Grundschutzes verpflichtet. Der Verantwortliche für das IT-Verfahren kann insbesondere Auskunft über den Stand der Umsetzung der Anforderungen vom Nutzer verlangen.

Umsetzungstermin: 2023

- Für die erfassten Ebenen übergreifenden Verfahren werden die SiKo entsprechend IT-Grundschutz weiterentwickelt. (Kennzahl 17: Reifegrad des Sicherheitsniveaus in %)

KOSTEN:

Die entstehenden Kosten sind abhängig vom konkreten IT-Verfahren und dem bereits bestehenden Sicherheitsniveau und können nicht genau beziffert werden. Die Pflicht zur Anwendung des IT-Grundschutz besteht seit 2013.

3.3. Anwendung der Mindeststandards des BSI

Die AG-InfoSic prüft die Möglichkeit der verbindlichen Anwendung der Mindeststandards des BSI nach § 8 Abs. 1 Satz 1 BSI-Gesetz als Ergänzung und Konkretisierung des IT-Grundschutzes für die Länder. Dabei ist die Aufnahme in die Standardisierungsagenda des IT-PLR zu bewerten.

Umsetzungstermin: 2021

- Die AG Informationssicherheit hat die bestehenden Standards geprüft. (Kennzahl 18: Anzahl der geprüften Mindeststandards)

KOSTEN:

Die Prüfung der Mindeststandards auf ihre Anwendbarkeit und das Konsultationsverfahren erfolgen im Rahmen der allgemeinen Tätigkeit der AG.

Handlungsfeld 4: Gemeinsame Abwehr von IT-Angriffen

Zur Stärkung der Analyse-, Detektions-, Reaktions- und Handlungsfähigkeit sowie der Zusammenarbeit und des aktiven Informationsaustauschs im VerwaltungsCERT-Verbund sind die im VerwaltungsCERT-Verbund organisierten CERT's weiterzuentwickeln.

4.1. Erarbeitung eines gemeinsamen, verbindlichen Mindeststandard CERT

Die AG-InfoSic erarbeitet einen gemeinsamen, verbindlichen Standard für CERT, der die personellen, technischen, infrastrukturellen und organisatorischen Anforderungen an ein Verwaltungs-CERT mit definierten Kompetenzen und CERT-Diensten beschreibt. Diese Anforderungen werden von den Mitgliedern in den jeweiligen CERT´s umgesetzt.

Umsetzungstermin: 2020

- Erarbeitung des verbindlichen Standards ist erfolgt. (Kennzahl 19: J/N)

Umsetzungstermin: 2022

- Die im Mindeststandard CERT definierten Anforderungen sind umgesetzt. (Kennzahl 20: Reifegrad der Umsetzung der einzelnen Anforderungen in %)

KOSTEN:
Die Kosten sind abhängig von der konkreten individuellen Ausgangslage des CERT und den festzulegenden Anforderungen und können noch nicht beziffert werden.

4.2. Weiterentwicklung der Zusammenarbeit

Die Erfüllung der Meldepflicht für Sicherheitsvorfälle im VCV sowie die Integration der Kommunen als Zielgruppe des Landes-CERTs zu prüfen. Evaluierung der Geschäftsordnung des VerwaltungsCERT-Verbunds mit Blick auf den Austausch eingestufter Informationen. Systematische Vernetzung der jeweiligen CERTs mit den anderen cybersicherheitsbezogenen öffentlichen Stellen, wie zum Beispiel den Verfassungsschutz- und Kriminalämtern, den Zentral- und Ansprechstellen Cybercrime bei den Staatsanwaltschaften, usw. Etablierung VCV-interner Standards mit dem Ziel die Abstimmungsprozesse zu beschleunigen und die Entscheidungskompetenzen des VerwaltungsCERT-Verbunds zu stärken.

Umsetzungstermin: 2022

- Verbesserung der gegenseitigen Vernetzung und des praxisbezogenen Erfahrungsaustauschs zwischen den CERTs im VerwaltungsCERT-Verbund durch regelmäßige Hospitationen. (Kennzahl 21: Anzahl der Hospitationen)

KOSTEN:
Die Kosten bewegen sich im Rahmen der allgemeinen Reise- und Fortbildungskosten im CERT-Betrieb.

4.3. Standards zur gemeinsamen Erkennung und Abwehr von IT-Angriffen

Erarbeitung einer Konzeption zur Etablierung von technischen Standards und Maßnahmen zum Erkennen und zur koordinierten Abwehr von IT-Angriffen und Teilen von Informationen (z.B. Malware Information Sharing Platform (MISP)).

Umsetzungstermin: 2022

- Konzeption ist erarbeitet (Kennzahl 22: J/N)

Umsetzungstermin: 2025

- Umsetzung des Konzeptes zur Etablierung von gemeinsamen (technischen) Standards zur gemeinsamen Erkennung und Abwehr von IT-Angriffen einschließlich dem automatisierten Informationsaustausch. (Kennzahl 23: Reifegrad der Umsetzung in %)

KOSTEN:

Die konkreten Kosten sind abhängig von der individuellen CERT-Ausgangslage, Anzahl der betreuten Arbeitsplätze u.a.

Handlungsfeld 5: Teil IT-Notfallmanagement

Störungen und Sicherheitsvorfälle (incidents) können sich zu einem Notfall (major incidents) ausweiten und sind deshalb genau zu beobachten, sorgfältig zu dokumentieren und zeitnah zu beheben. Durch das Notfallmanagement (bisher BSI 100-4 künftig 200-4 BCM) sollen kritische Zustände erkannt und entsprechende Handlungspläne aktiviert werden. Im Rahmen der Etablierung des Notfallmanagements sind mit Bezug zur Informationssicherheit Geschäftsprozesse mit IT Bezug zu betrachten. Das IT-Notfallmanagement ist Teil des ganzheitlichen Notfallmanagements und darf nicht isoliert betrachtet werden. Das Informationssicherheitsmanagement unterstützt das Notfallmanagement und stimmt sich in den Prozessen ab.

5.1. Aufbau des IT-Notfallmanagements

Voraussetzung 2021

- Der übergreifende Notfallmanagementprozess, z.B. in Form einer Notfallmanagement-Leitlinie, ist initiiert.
- Die Rolle des Notfallbeauftragten und dessen Aufgaben sind festgelegt und dokumentiert.
- Die Ansprechpartnerinnen und –partner für das IT-Notfallmanagement (Notfallmanager) sind bei den wesentlichen Behörden benannt.

  (Kennzahl 24: Reifegrad – des Prozesses)

KOSTEN:
Die Kosten bewegen sich im Rahmen des allgemeinen Betriebs- und Organisationsaufwand von Behörden. Die innerorganisatorischen Aufwände sind nicht konkret bezifferbar.

Umsetzungstermin: 2023

- Erstellung IT-bezogene Notfallkonzepte
- Schnittstellen vom IT-Notfallmanagement zu Krisen- und Katastrophenschutz sind etabliert.

  Kennzahl 25: J/N)
- Das Zusammenspiel der Beteiligten wird regelmäßig beübt und die Ergebnisse bewertet. (Kennzahl 26: J/N)