DEUTSCHER LANDKREISTAG

Bundesamt für Sicherheit in der Informationstechnik

Informationssicherheit für Landrätinnen und Landräte IT-Grundschutz in den Landkreisen

Das nachfolgende Papier wurde vom Deutschen Landkreistag in Zusammenarbeit mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) erstellt.

Sie finden im Dokument zunächst eine kurze Einleitung zur Funktion der Verwaltungsspitze in der Informationssicherheit und darauf folgend die konkreten, einzuleitenden Schritte. Zu Ihrer vertiefenden Information wurden im Anschluss Erläuterungen zu einem Managementsystem für Informationssicherheit, den möglichen Arten der Absicherung nach IT-Grundschutz sowie zu den im Kapitel zuvor genannten IT-Grundschutz-Profilen zusammengestellt. Die weiterführenden Dokumente und Links bilden den Abschluss des Dokuments.

I. Funktion der Verwaltungsspitze im IT-Grundschutz

Die Landrätin bzw. der Landrat ist verantwortlich für das zielgerichtete und ordnungsgemäße Funktionieren der Kreisverwaltung und damit auch für die Gewährleistung der Informationssicherheit nach innen und außen. Daher muss die Verwaltungsspitze den Sicherheitsprozess initiieren, steuern und kontrollieren. Dazu gehören strategische Leitaussagen zur Informationssicherheit, konzeptionelle Vorgaben und auch organisatorische Rahmenbedingungen sowie ausreichende Ressourcen, um Informationssicherheit innerhalb aller Geschäftsprozesse erreichen zu können.

Informationssicherheit ist Aufgabe der Leitungsebene. Die Leitung selbst ist nicht die ausführende Stelle, hat aber durch Unterstützung, Kommunikation und Vorbildfunktion maßgeblichen Einfluss auf eine adäquate Umsetzung und trägt am Ende die Verantwortung.

II. Konkrete Schritte zur Steigerung der Informationssicherheit als Landrätin/Landrat

a) <u>Initiierung und wesentliche Eckpunkte zur Steigerung der Informationssicherheit</u>

- Übernahme der abschließenden Gesamtverantwortung der Behördenleitung, dazu Sicherstellung des Informationsflusses zu folgenden Themen:
    - Darstellung der Sicherheitsrisiken für die Kreisverwaltung und die dort verarbeiteten Informationen sowie die damit verbundenen Auswirkungen und Kosten,
    - Einschätzung zu Auswirkungen von Sicherheitsvorfällen auf die kritischen Geschäftsprozesse,

- Klärung/Umsetzung der Sicherheitsanforderungen, die sich aus gesetzlichen und vertraglichen Vorgaben ergeben (z. B. i-KfZ, EU-Zahlstelle),
- Umsetzung der für die Landkreisverwaltung typischen Standardvorgehensweisen zur Informationssicherheit,
- Information über den aktuellen Stand der Informationssicherheit im Sinne eines Reifegrades und daraus abgeleitete Handlungsempfehlungen

- Ernennung einer/s Informationssicherheitsbeauftragten

  Die Informationssicherheitsbeauftragten sind zuständig für die Wahrnehmung aller Belange der Informationssicherheit innerhalb der Kreisverwaltung. Eine der Hauptaufgaben der Informationssicherheitsbeauftragten besteht darin, die Behördenleitung bei deren Aufgabenwahrnehmung bezüglich der Informationssicherheit zu beraten. Eine gegenseitige Unterstützung bei den jeweiligen Aufgaben innerhalb der Sicherheitsorganisation ist daher unerlässlich. Hierfür ist es bedeutsam, dass ein direkter Zugang zur Hausleitung besteht. Die Stelle erfordert bei der Größe einer Landkreisverwaltung regelmäßig eine Besetzung in Vollzeit.

- Initiierung der Erstellung und Fortschreibung einer Informationssicherheitsleitlinie

  Die Leitlinie zur Informationssicherheit beschreibt allgemeinverständlich, für welche Zwecke, mit welchen Mitteln und mit welchen Strukturen Informationssicherheit innerhalb der Kreisverwaltung hergestellt werden soll. Sie beinhaltet die von der Kreisverwaltung angestrebten Informationssicherheitsziele sowie die verfolgte Sicherheitsstrategie. Die Leitungsebene muss die Inkraftsetzung der Sicherheitsleitlinie veranlassen.

- Unterstützung der Informationssicherheitsbeauftragten mit dem Ziel der Einbindung in die relevanten Aktivitäten der Fachabteilungen/Dezernate

  Die Aufgaben der Informationssicherheitsbeauftragten erfordern Kommunikation und Zusammenarbeit mit verschiedenen Fachabteilungen/Dezernaten und dabei auch mit verschiedenen Hierarchiestufen. Es ist Aufgabe der Verwaltungsspitze, auf die Fachabteilungen/Dezernate einzuwirken, damit die Informationssicherheitsbeauftragten auch dort bei ihren Aufgaben ausreichend unterstützt werden.

- Bereitstellung der erforderlichen Software als Dokumentations- und Prozesssteuerungswerkzeuge

  Für den Einstieg können zunächst bereits vorhandene Tools und Software genutzt werden. Es empfiehlt sich jedoch, zeitnah die Beschaffung von speziellen Tools anzugehen, die auch von weiteren Bereichen genutzt werden können und damit einen organisationsinternen Mehrwert generieren (z. B. Datenschutzbeauftragte, Compliance-Beauftragte, Notfallbeauftragte). Die Bereitstellung von Ressourcen für deren Beschaffung liegt in der Verantwortung der Leitungsebene.

- Aktives und widerspruchsfreies Vorleben von Informationssicherheit

  Informationssicherheit kann nicht ausschließlich als Top-Down-Prozess gelebt werden. Die Vorbildfunktion der Leitungsebene spielt eine wesentliche Rolle bei der Akzeptanz von

Sicherheitsmaßnahmen bei den Beschäftigten und ist damit wesentlicher Faktor für die erfolgreiche Umsetzung von Informationssicherheit innerhalb der Organisation.

b) Organisation des Sicherheitsprozesses

- Qualifikation der Informationssicherheitsbeauftragten durch regelmäßige Schulungen

  Um die Aufgaben geeignet wahrnehmen zu können, ist es notwendig, dass die Informationssicherheitsbeauftragten ein geeignetes initiales Schulungsprogramm durchlaufen und ein individuelles, auf deren Kenntnisse zugeschnittenes Fortbildungskonzept erarbeitet wird. Damit kann die kontinuierliche Weiterbildung in diesem sich stetig wandelnden Arbeitsfeld gewährleistet werden.

- Sensibilisierung der Beschäftigten (z. B. Sensibilisierungs-Kampagnen, Meldewege)

  Beschäftigte der Institution müssen anlassbezogen und regelmäßig sensibilisiert werden, welche Regelungen für sie relevant sind und wie sie zum Gelingen des Informationssicherheitsprozesses beitragen können. Es zeigt sich regelmäßig, dass Beschäftigte Einfallspunkt für Sicherheitsvorfälle sind – in den meisten Fällen jedoch unbeabsichtigt.

c) Dokumentation des Sicherheitsprozesses

- Initiierung eines Managementberichts der/des Informationssicherheitsbeauftragten an die Landrätin/den Landrat

  Damit die Behördenleitung die richtigen Entscheidungen bei der Steuerung und Lenkung des Sicherheitsprozesses treffen kann, benötigt sie Eckdaten zum Stand der Informationssicherheit. Diese Eckpunkte sollten in Managementberichten aufbereitet werden, die unter anderem folgende Punkte abdecken:

  - Status und Umsetzungsgrad des Sicherheitskonzepts
  - Ergebnisse von Audits und Datenschutzkontrollen
  - Berichte über Sicherheitsvorfälle
  - Berichte über bisherige Erfolge und Probleme im Informationssicherheitsprozess
  - Berichte über die Reduzierung bestehender Umsetzungsdefizite und der damit verbundenen Risiken

d) Erstellung einer Sicherheitskonzeption

- Initiierung der Einführung des IT-Grundschutz-Profils „Basis-Absicherung Kommunalverwaltung“ (Einführung in die Basis-Absicherung, teilweise Standard-Absicherung)

  - 15-20 Tage Aufwand für eine/n erfahrene/n Informationssicherheitsbeauftragte/n
  - Nach 3-12 Monaten Umsetzung in der Organisation möglich
  - Behördenleitung, Büroleitung, Personalrat und die weiteren Schlüsselakteure unterstützen den Prozess aktiv
  - Informationssicherheitsbeauftragte, Organisation, IT, Gebäudemanagement etc. erhalten die notwendigen zeitlichen, finanziellen und personellen Ressourcen

- Möglichkeit des Nachweises zur Umsetzung des IT-Grundschutzes gemäß Basis-Absicherung durch ein Testat, welches bspw. zur Kommunikation mit Dritten genutzt werden kann, um deutlich zu machen, dass die Institution aktiv daran arbeitet, eine geeignete Absicherung zu erreichen.

- Als Zielstellung Umsetzung der Standard-Absicherung nach IT-Grundschutz aufbauend auf dem IT-Grundschutz-Profil „Basis-Absicherung Kommunalverwaltung“

III. Managementsystem für Informationssicherheit

Der Schlüssel zur Informationssicherheit ist ein übergreifendes und systematisches Managementsystem für Informationssicherheit (ISMS).

Um ein solches System aufzubauen, stellt das Bundesamt für Sicherheit in der Informationstechnik (BSI) mit dem IT-Grundschutz eine etablierte und übertragbare Methodik zur Verfügung. Darüber hinaus behandelt der IT-Grundschutz auch das Thema Notfallmanagement. Der IT-Grundschutz zeigt einen systematischen Weg, um ein ISMS und ein Notfallmanagement in einer Behörde aufzubauen.

Die *BSI-Standards* und das *IT-Grundschutz-Kompendium* bilden die Hauptwerke im IT-Grundschutz. Die BSI-Standards erläutern, wie ein ISMS bestmöglich organisatorisch und systematisch aufgebaut werden kann. Der BSI-Standard 200-1 „Managementsysteme für Informationssicherheit“ beschreibt verständlich, welche grundlegenden Anforderungen ein Managementsystem für Informationssicherheit erfüllen muss. Er erläutert, welche Komponenten ein ISMS enthalten sollte und welche Aufgaben die Leitungsebene übernehmen muss. Im BSI-Standard 200-2 „IT-Grundschutz-Methodik“ werden passend dazu die Vorgehensweisen erläutert (vgl. nachfolgendes Kapitel).

Im IT-Grundschutz-Kompendium beschreiben Fachtexte, die sogenannten IT-Grundschutz-Bausteine, was Verantwortliche tun müssen, um einen bestimmten Bereich besser abzusichern.

In Kombination angewandt, bilden diese Komponenten des IT-Grundschutzes die Grundlage für eine solide Informationssicherheit.

Die rund 100 IT-Grundschutz-Bausteine erläutern neben technischen Aspekten auch solche, die Infrastruktur, Organisation und Personal betreffen. Anwender können sich

gezielt die IT-Grundschutz-Bausteine heraussuchen, die für ihre aktuellen Sicherheitsfragen relevant sind.

Beispielhafte Gefährdung und Bausteine:

Vorfälle in der jüngeren Vergangenheit zeigen, dass Landkreise Ziel von Ransomware-Attacken sind. Dabei handelt es sich um Schadprogramme, die Systeme verschlüsseln und im Anschluss eine Geldforderung stellen.

Beispielhafte Gefährdung: Schadprogramm

Potentiell betroffene Bereiche: gespeicherte Daten, Server, Arbeitsplatzrechner, E-Mail-Programm

Auswahl von IT-Grundschutz-Bausteinen für geeignete Gegenmaßnahmen: OPS.1.1.4 Schutz vor Schadprogrammen, CON.3 Datensicherungskonzept, SYS.1.1 Allgemeiner Server, SYS.2.1 Allgemeiner Client, APP.5.3 Allgemeiner E-Mail-Client und –Server

IV. Basis-, Standard- oder Kern-Absicherung

Der BSI-Standard 200-2 „IT-Grundschutz-Methodik“ beschreibt, wie ein ISMS schrittweise in einer Institution aufgebaut und aufrechterhalten werden kann. Zum Aufbau und der Aufrechterhaltung des ISMS bestehen drei Vorgehensweisen:

- Die Basis-Absicherung kann bereits mit einem vergleichsweise geringen finanziellen, personellen und zeitlichen Aufwand realisiert werden.
- Darauf aufbauend ist das Ziel einer Standard-Absicherung ein vollumfängliches ISMS.
- Bei der Kern-Absicherung werden ausgewählte, besonders wichtige Bereiche abgesichert.

Für die Kommunalverwaltung wird die Standard-Absicherung empfohlen. Das Präsidium des Deutschen Landkreistages hat dies durch einen Beschluss vom 17.12.2021 bekräftigt und sich für eine verbindliche Festlegung des IT-Grundschutzes des BSI in allen Kreisverwaltungen ausgesprochen. Um die Standard-Absicherung zu erreichen, kann der Einstieg über die Basis-Absicherung, beispielsweise mittels des IT-Grundschutz-Profils „Basis-Absicherung Kommunalverwaltung“ (siehe nachfolgendes Kapitel) erleichtert werden.

V. IT-Grundschutz-Profile

In einem IT-Grundschutz-Profil werden die einzelnen Schritte eines Sicherheitsprozesses für einen definierten Anwendungsbereich dokumentiert. Diese Blaupausen für Informationssicherheit werden in der Regel von mehreren Institutionen eines Verwaltungsbereiches oder einer Branche gemeinsam erstellt. Anwendende, die ähnliche Sicherheitsanforderungen haben, können auf der Basis eines IT-Grundschutz-Profils mit reduziertem Aufwand ihre Geschäftsprozesse absichern. Ein solches Profil wurde auf Initiative des Deutschen Landkreistages auch für die Kommunalverwaltung erarbeitet. Das IT-Grundschutzprofil „Basis-Absicherung Kommunalverwaltung“ wird regelmäßig überarbeitet und an veränderte Anforderungen angepasst.

VI. Weiterführende Dokumente:

Link zum BSI IT-Grundschutz:
https://www.bsi.bund.de/grundschutz

Link zum IT-Grundschutz-Profil „Basis-Absicherung Kommunalverwaltung“:
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Hilfsmittel/Profile/Basis_Absicherung_Kommunalverwaltung.html

Link zum „Leitfaden Basis-Absicherung“:
https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/BSI-Standards/BSI-Standard-200-2-IT-Grundschutz-Methodik/Leitfaden-Basis-Absicherung/leitfaden-basis-absicherung_node.html

Beschluss des Präsidiums des Deutschen Landkreistages vom 17.12.2021.