LAND BRANDENBURG

Ministerium des Innern und für Kommunales

Sicherheitsrechtliche Hinweise für die Nachnutzung von EfA-Online-Diensten - eine Handreichung -

Stand: 01.12.2023

Inhalt

1. Einleitung

Dieses Dokument soll Ihnen sicherheitsrechtliche Hinweise für die Nachnutzung von EfA-Diensten näherbringen.

Unbeschadet dieser Hinweise dient dieses Dokument lediglich als Empfehlung für eine Vorgehensweise und entlastet nicht die einzelnen Behörden davon eine entsprechende Risikobewertung und Risikoabwägung im Sinne der Informationssicherheit vorzunehmen.

Im Rahmen der Umsetzung des Onlinezugangsgesetzes (OZG) entwickeln so genannte Themenfeldführer Online-Dienste nach dem „Einer für Alle“-Prinzip (EfA). Eine Stelle / Behörde / Einrichtung, die einen EfA-Online-Dienst (nach-)nutzt, stellt sich der besonderen Herausforderung, die Informationssicherheit in den vernetzten, von unterschiedlichen Partnern betriebenen, Ebenen übergreifenden IT-Infrastrukturen zu wahren. Das Sicherheitsniveau wird vom schwächsten Partner im Verbund bestimmt. Mit dem bundesweiten EfA-Prinzip sollen bei der OZG-Umsetzung kostenintensive Mehrfachentwicklungen vermieden werden. Ein Anbieter entwickelt und betreibt einen Dienst und bietet diesen bundeweit allen Behörden zur Nutzung an. Damit vergrößert sich der zu betrachtende Informationsverbund um die Komponenten des EfA-Dienstes und die zwischenliegenden Netze. Eine elementare Idee und Funktion des Portalverbundes ist es, dass Verwaltungskunden mit nur einem Servicekonto bundesweit alle Verwaltungsdienste nutzen können und keine erneute Registrierung notwendig ist. Meldet sich ein Bürger beispielsweise beim Amt „A“ mit einer dem Nutzerkonto Bund zugehörigen Identität an, so lässt sich Amt „A“ die Authentisierung vom Bundesportal als Identitätsprovider bestätigen.

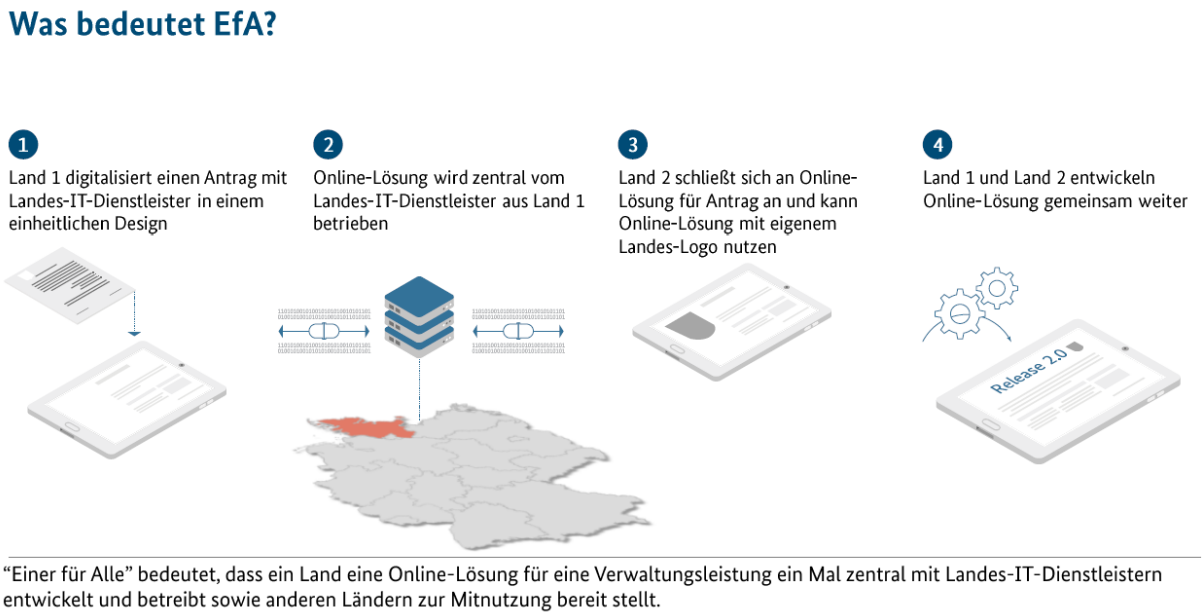

Abbildung 1: EfA-Prinzip (https://leitfaden.ozg-umsetzung.de/display/OZG/11.2.1+Konzeptionelle+Kernaspekte+der+EfA+Nachnutzung)

Die Gefahren aus dem Cyberraum sind in den letzten Jahren erheblich angestiegen. Durch die Lageberichte des BSI und die zum Teil schweren Sicherheitsvorfälle bei Bund und Ländern in der jüngeren Vergangenheit belegen diese Gefahr. Eine prosperierende Angriffsindustrie im Internet, bestehend aus staatlichen, aber auch aus kriminellen Organisationen sowie sonstige Aktivisten, erfordert eine fortlaufende Anpassung der informationstechnischen Abwehrmaßnahmen der Verwaltung bei Bund und Ländern.

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

Die Ausführungen in diesem Dokument erheben keinen Anspruch auf Vollständigkeit. Es bedarf für jeden Online-Dienst einer Einzelfallprüfung, in deren Ergebnis ggf. weitere Unterlagen zu erarbeiten oder inhaltliche Änderungen geboten sind.

2. Zusammenwirken mit dem Themenfeldführer

In der Regel werden bereits informationssicherheitsrelevante Dokumente für die Erfüllung von sicherheitsrechtlichen Anforderungen vom Themenfeldführer und ggf. von dessen Dienstleister(n) erarbeitet und der nachnutzenden Stelle zur Verfügung gestellt. Soweit dies nicht der Fall ist und Unterlagen nicht ausschließlich Besonderheiten des Landesrechts (z. B. aus dem Brandenburgischen E-

Government-Gesetz – BbgEGovG) oder der nachnutzenden Stelle abbilden, wird empfohlen, vor der eigenen Erstellung von informationssicherheitsrelevanten Dokumenten auf den Themenfeldführer zuzugehen und ihn um eine Ergänzung seiner Vorarbeiten und Dokumente zu bitten.

Vom Themenfeldführer zur Verfügung gestellte Unterlagen sind von der nachnutzenden Stelle auf Plausibilität und erforderliche Anpassungen zu prüfen und ggf. fortzuschreiben. Einige Nachweise sind jedoch von der nachnutzenden Stelle selbst zu erstellen (z. B. zur Festlegung lokaler technischer und organisatorischer Maßnahmen).

Letztendlich ist der jeweilige Behördenchef der jeweils nachnutzenden Stelle für die der Informationssicherheit verantwortlich. Dem jeweils zuständige Verfahrensverantwortlichen obliegt damit die sachgerechte Umsetzung bzw. der sachgerechte Betrieb des IT-Verfahrens entsprechend der Vorgaben zur Informationssicherheit. Hierbei kann er sich durch den IT-Sicherheitsbeauftragten der jeweils nachnutzenden Stelle beraten lassen.

3. Informationssicherheitsrechtliche Vorgaben im Land Brandenburg

3.1. Brandenburgisches E-Government-Gesetz §§ 12 und 16

Das BbgEGovG regelt im § 12 grundsätzlich die Einhaltung von Beschlusslagen des IT-Planungsrates durch die Behörden des Landes Brandenburg. Dazu zählen ausweislich auch Beschlusslagen des IT-Planungsrates zu Informationssicherheitsstandards.

Das BbgEGovG regelt im § 16 grundsätzlich die Aufgaben und Befugnisse des Computersicherheits-Ereignis- und Reaktionsteam (CERT) beim ZIT-BB.

Innerhalb des BbgEGovG § 12 regelt die Informationssicherheitsleitlinie des IT-Planungsrates (als IT-Sicherheitsstandard) weitere Regelungsgegenstände für die Brandenburgische Landesverwaltung. Dazu gehören die folgenden fünf Handlungsfelder:

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

3.2. Informationssicherheitsleitlinie des Landes Brandenburg

Ableitend und präzisierend aus den unter Punkt 3.1 genannten Punkten regelt zunächst die Informationssicherheitsleitlinie der Landesverwaltung den Aufbau und die Organisation des Informationsmanagementsystems (ISMS) des Landes Brandenburg. Das brandenburgische ISMS wird durch das Informationssicherheitsmanagement-Team des Landes verkörpert. Aktuell sind die BSI-Standards 200-1, 200-2 und 200-3 und 100-4 durch die Behörden der Landesverwaltung anzuwenden.

Die Informationssicherheitsleitlinie dient der Organisation der Informationssicherheit und ist ein Grundsatzdokument zum Stellenwert, zu den verbindlichen Prinzipien und dem anzustrebenden Niveau der Informationssicherheit in der Landesverwaltung und

Justiz. Sie beschreibt den Aufbau und den Betrieb eines zentral koordinierten, Ressort übergreifenden Informationssicherheitsmanagementsystems.

Die Informationssicherheitsleitlinie der Landesverwaltung regelt insbesondere, dass

- jede Dienststellenleitung beziehungsweise Geschäftsführung verantwortlich für die Informationssicherheit in ihrem Bereich ist,
- bei der Erarbeitung von Richt- und beziehungsweise Leitlinien zum Risikomanagement beziehungsweise zum Qualitätsmanagement in der Landesverwaltung und Justiz die Regelungen der Informationssicherheitsleitlinie zu berücksichtigen sind.
- Durch die Informationssicherheitsleitlinie soll sichergestellt werden, dass dem jeweiligen Schutzzweck angemessene und dem Stand der Technik entsprechende Sicherheitsmaßnahmen ergriffen werden, um Informationswerte und personenbezogene Daten angemessen zu schützen und um die Verfügbarkeit von informationstechnischen beziehungsweise kommunikationstechnischen Verfahren zu gewährleisten.
- Die Informationssicherheitsleitlinie muss von allen Dienststellen der Landesverwaltung und Justiz entsprechend ihrer Aufgabenverantwortung umgesetzt und ausgestaltet werden.
- Die Informationssicherheitsleitlinie ist Bestandteil eines hierarchisch abgestuften Regelwerks und ist das übergeordnete Regelwerk für Informationssicherheitsrichtlinien und Informationssicherheitskonzepte der Ressorts beziehungsweise einzelner Einrichtungen.
- Dem Landtag, dem Landesrechnungshof und der Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht und den Kommunen des Landes Brandenburg wird die Anwendung der Informationssicherheitsleitlinie empfohlen.

Das Land Brandenburg verfolgt mit der oben genannten Leitlinie:

- die zuverlässige Unterstützung der Geschäftsprozesse oder sonstigen Verwaltungsaufgaben der IT,
- die Sicherstellung der Kontinuität der Arbeitsabläufe der öffentlichen Verwaltung,
- die Schaffung von Rahmenbedingungen für eine sichere und vertrauenswürdige Realisierung der Digitalisierungsagenda,

- die sichere Vernetzung bei Ebenen übergreifender Zusammenarbeit,
- die Gewährleistung der aus verfassungsrechtlichen oder gesetzlichen Vorgaben resultierenden Anforderungen,
- die Wahrung von Dienst- und 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 Informationen sowie
- die Bewältigung von IT-Krisen.

3.2.1. Absicherung der IT-Netzinfrastrukturen der öffentlichen Verwaltung

Die von Bund und Ländern beschlossenen Anschlussbedingungen gemäß § 4 des Gesetzes über die Verbindung der informationstechnischen Netze des Bundes und der Länder (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 angeschlossenen Netze, sofern ein 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 ebenen übergreifende Verwaltungsprozesse 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.

3.2.2. Einheitliche Sicherheitsstandards für Ebenen übergreifende IT-Verfahren

Es ist mit sehr hoher Wahrscheinlichkeit davon auszugehen, dass es sich im Allgemeinen bei OZG-Verfahren dem Wesen nach um sogenannte „Ebenen übergreifende IT-Verfahren“ handeln könnte.

Ebenen übergreifende IT-Verfahren sind im Sinne der Informationssicherheitsleitlinie IT-Verfahren, die über Verwaltungsgrenzen hinweg angeboten werden bzw. genutzt werden sollen (Bund-Länder übergreifende oder von mehreren Ländern genutzte IT-Verfahren).

Bei Ebenen übergreifenden IT-Verfahren werden auf Grund 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 Ebenen übergreifenden 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 Ebenen übergreifender IT-Verfahren ist der IT-Grundschutz des BSI in seiner jeweiligen Fassung anzuwenden.

Es sind die im jeweiligen Bereich betriebenen Ebenen übergreifenden 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.

4. Einheitliches IT-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.

4.1. Erfassung aller Ebenen übergreifenden IT-Verfahren

Der Bund und die 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 IT-Sicherheitsstandards. Der Prozess zur Erfassung der Verfahren ist seit 2020 umgesetzt, und seit 2021 ist der Prozess zur regelmäßigen Überprüfung der Prozesse etabliert.

4.2. 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 der jeweilig gültigen Fassung zu 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 Anforderung 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.

Der Reifegrad des Sicherheitsniveaus der Ebenen übergreifenden IT-Verfahren wird im jährlichen Turnus mit dem Fragenkatalog zur IT-Sicherheit in allen Ressorts und nachgeordneten Stellen abgefragt.

Impressum

Herausgeber:

Ministerium des Innern und für Kommunales des Landes Brandenburg (MIK)

Referat 64

Henning-von-Tresckow-Straße 9-13

14467 Potsdam

Internet: mik.brandenburg.de

Stand: Dezember 2023

Dieser Bericht ist ausschließlich im PDF-Format verfügbar.