Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Weisungen des Bundesrates über die IKT-Sicherheit in der Bundesverwaltung

vom 16. Januar 2019

Der Schweizerische Bundesrat
erlässt folgende Weisungen:

1 Allgemeine Bestimmungen

1.1 Gegenstand

Diese Weisungen regeln in Ausführung von Artikel 14 Buchstabe d der Bundesinformatikverordnung vom 9. Dezember 2011[1] (BinfV) die organisatorischen, personellen und technischen Anforderungen und Massnahmen, um für die Schutzobjekte der Informations- und Kommunikationstechnik (IKT) der Bundesverwaltung den angemessenen Schutz der Vertraulichkeit, Verfügbarkeit, Integrität und Nachvollziehbarkeit zu gewährleisten.

1.2 Geltungsbereich

Der Geltungsbereich dieser Weisungen richtet sich nach Artikel 2 BinfV[2].

1.3 Begriffe

In diesen Weisungen bedeuten:

a. *IKT-Schutzobjekte:* Anwendungen, Services, Systeme, Netzwerke, Datensammlungen, Infrastrukturen und Produkte der IKT; mehrere gleiche oder zusammenhängende Objekte können zu einem IKT-Schutzobjekt zusammengefasst werden;

b. *Sicherheitsverfahren:* Prozesse und Massnahmen zur Gewährleistung einer angemessenen IKT-Sicherheit im gesamten Lebenszyklus eines IKT-Schutzobjektes;

c. *Schutzbedarfsanalyse:* Erhebung der Anforderungen an die Sicherheit der IKT-Schutzobjekte;

1 SR **172.010.58**
2 SR **172.010.58**

d. *Informationssicherheits- und Datenschutz-Konzept (ISDS-Konzept):* Beschreibung der Schutzmassnahmen und ihrer Umsetzung für die IKT-Schutzobjekte sowie der Restrisiken;

e. *Netzwerk:* Einrichtung, welche die Kommunikation verschiedener IKT-Systeme untereinander ermöglicht;

f. *Zone:* logischer Verbund von IKT-Systemen, die sich durch ähnliche Sicherheitsanforderungen auszeichnen und der gleichen Zonenpolicy unterliegen;

g. *Zonenpolicy:* vom Inhaber einer Zone erstellte Beschreibung von Anforderungen und Vorgaben an die IKT-Systeme der Zone, an die Zone selbst sowie an die für die Zone zulässige interne und externe Kommunikation;

h. *Zonenmodell Bund:* generisches Modell für die Zonenbildung in der Bundesverwaltung;

i. *IKT-Portfolio:* einheitliche Zusammenstellung der geplanten und der laufenden IKT-Projekte und Anwendungen in einem bestimmten Zuständigkeitsbereich.

2 Zuständigkeiten

2.1 Informatiksicherheitsbeauftragte

1 Die Departemente und die Bundeskanzlei bestimmen je eine Informatiksicherheitsbeauftragte oder einen Informatiksicherheitsbeauftragten (ISBD).

2 Die ISBD haben namentlich die folgenden Aufgaben:

a. Sie koordinieren die IKT-Sicherheitsaspekte innerhalb des Departements oder der Bundeskanzlei sowie mit den überdepartementalen Stellen und sind im Rahmen der IKT-Sicherheit die primären Ansprechpartnerinnen und -partner des Informatiksteuerungsorgans des Bundes (ISB).

b. Sie erarbeiten die notwendigen Grundlagen für die Umsetzung der IKT-Sicherheitsvorgaben und für die Organisation auf Stufe Departement oder Bundeskanzlei.

3 Die Verwaltungseinheiten bestimmen je eine Informatiksicherheitsbeauftragte oder einen Informatiksicherheitsbeauftragten (ISBO).

4 Die ISBO haben namentlich die folgenden Aufgaben:

a. Sie koordinieren die IKT-Sicherheitsaspekte innerhalb der Verwaltungseinheit sowie mit den departementalen Stellen und sind die primären Ansprechpartnerinnen und -partner der oder des ISBD und der Sicherheitsorganisationen der Leistungserbringer.

b. Sie erarbeiten die notwendigen Grundlagen für die Umsetzung der IKT-Sicherheitsvorgaben und für die Organisation auf Stufe Verwaltungseinheit.

c. Sie informieren die Leiterin oder den Leiter ihrer Verwaltungseinheit mindestens halbjährlich über den aktuellen Stand der IKT-Sicherheit in ihrer Verwaltungseinheit.

5 Die Departemente, die Bundeskanzlei und die Verwaltungseinheiten sorgen dafür, dass die Informatiksicherheitsbeauftragten ihre Aufgaben ohne Interessenkonflikte wahrnehmen. Sie regeln das Verhältnis zwischen der oder dem ISBD und den ISBO, namentlich die fachliche Führung in Sicherheitsfragen.

6 Das ISB bestimmt eine Informatiksicherheitsbeauftragte oder einen Informatiksicherheitsbeauftragten für die Standarddienste (ISB SD). Sie oder er nimmt die Aufgaben nach Absatz 4 für die IKT-Standarddienste wahr.

2.2 Leistungsbezüger

1 Als Leistungsbezüger sorgen die Verwaltungseinheiten für die Anwendung des Sicherheitsverfahrens.

2 Die Personen, die in der Verwaltungseinheit für eine Anwendung, für einen Geschäftsprozess oder für eine Datensammlung verantwortlich sind, legen zusammen mit der oder dem ISBO die Sicherheitsanforderungen für ihre IKT-Schutzobjekte fest. Die Verwaltungseinheiten führen das IKT-Portfolio mit den sicherheitsrelevanten Angaben. Die Sicherheitsanforderungen sind mit den Leistungserbringern sowohl für die Entwicklung und den Betrieb als auch für die Ausserbetriebnahme von IKT-Mitteln schriftlich zu vereinbaren. Die Verwaltungseinheiten dokumentieren und überprüfen die Umsetzung der Sicherheitsmassnahmen sowie deren Wirksamkeit.

3 Die Verwaltungseinheiten überprüfen periodisch den Schutzbedarf der IKT-Schutzobjekte und passen sowohl die Sicherheitsdokumentation als auch die Sicherheitsmassnahmen an.

4 Sie sorgen dafür, dass die Mitarbeiterinnen und Mitarbeiter die Zuständigkeiten sowie die Abläufe der IKT-Sicherheit in ihrem Arbeitsumfeld je nach Stufe und Funktion kennen.

5 Die Mitarbeiterinnen und Mitarbeiter der Bundesverwaltung, die IKT-Mittel nutzen, sind für deren sichere Handhabung verantwortlich. Die Verwaltungseinheiten haben sie bei Stellenantritt sowie periodisch für Themen der IKT-Sicherheit zu sensibilisieren und zu schulen.

6 Die Verwaltungseinheiten sorgen dafür, dass Personen, auf die die BinfV[3] nicht anwendbar ist, nur dann Zugriff auf die IKT-Infrastruktur des Bundes erhalten, wenn sie sich verpflichten, die IKT-Sicherheitsvorgaben einzuhalten.

7 Sie erlassen unter Beizug des oder der ISBO oder ISBD weitergehende oder spezifische Vorgaben zur sicheren Nutzung der IKT-Mittel und halten diese aktuell; insbesondere definieren sie einen Sicherheitsvorfallbearbeitungsprozess.

3 SR **172.010.58**

2.3 Leistungserbringer

1 Die Vorgaben für Leistungsbezüger nach Ziffer 2.2 gelten für Leistungserbringer sinngemäss.

2 Die Leistungserbringer setzen die erforderlichen Sicherheitsmassnahmen beim Betrieb von IKT-Mitteln um, dokumentieren und überprüfen sie. Sie bringen die Ergebnisse den betroffenen Leistungsbezügern in geeigneter Form zur Kenntnis.

3 Die Verantwortlichkeiten und der Schutzbedarf auf der betrieblichen Ebene sind in den Projekt- und Leistungsvereinbarungen zwischen den Leistungserbringern und den Leistungsbezügern festzuhalten. Insbesondere sind die Entscheidungskompetenzen für Sofortmassnahmen bei einem Vorfall zu regeln.

4 Die Leistungserbringer stellen sicher, dass sie IKT-Sicherheitsvorfälle mit ständigen oder Ad-hoc-Sicherheitsorganisationen rasch und effektiv bewältigen können. Diese sind zuständig für vorfallbezogene technische Analysen und für die Koordination der Behebung des Vorfalls. Sie sammeln technische Informationen und werten diese aus, unter Berücksichtigung allfälliger verwandter Ereignisse, und informieren den zuständigen ISBD oder ISBO.

3 Sicherheitsverfahren

3.1 Sicherheitsvorgaben

1 Das ISB erlässt ergänzend zu diesen Weisungen Vorgaben zum Sicherheitsverfahren und zu den dazugehörenden Hilfsmitteln auf Stufe Bund, namentlich für:

a. die Schutzbedarfsanalyse;

b. einen Prüfprozess zur Reduktion nachrichtendienstlicher Ausspähung;

c. den IKT-Grundschutz;

d. das ISDS-Konzept.

2 Es legt das Zonenmodell Bund fest.

3.2 Schutzbedarfsanalyse, ISDS-Konzept und Risikobeurteilung

1 Bei IKT-Vorhaben ist vorab eine Schutzbedarfsanalyse durchzuführen. Dabei sind auch die risikorelevanten Fälle zur Reduktion nachrichtendienstlicher Ausspähung gemäss einem entsprechenden Prüfprozess (Ziff. 3.1 Abs. 1 Bst. b) zu ermitteln.

2 Bestehende IKT-Schutzobjekte müssen über eine gültige Schutzbedarfsanalyse verfügen.

3 Die minimalen Sicherheitsvorgaben (IKT-Grundschutz) sind für alle IKT-Schutzobjekte umzusetzen; die Umsetzung ist zu dokumentieren.

4 Ergibt die Schutzbedarfsanalyse einen erhöhten Schutzbedarf, so ist zusätzlich zur Dokumentation der Umsetzung des IKT-Grundschutzes ein ISDS-Konzept mit Risi-

koanalyse zu erstellen. Bei der Erstellung des ISDS-Konzepts darf auf bestehende themenspezifische Sicherheitskonzepte verwiesen werden.

5 Werden gemäss dem Prüfprozess zur Reduktion nachrichtendienstlicher Ausspähung risikorelevante Fälle ermittelt, so muss der Prüfprozess vollständig durchlaufen werden; die Umsetzung ist zu dokumentieren.

6 Die Schutzbedarfsanalysen, die Dokumentation der Umsetzung des IKT-Grundschutzes, die Dokumentation des Prüfprozesses zur Reduktion nachrichtendienstlicher Ausspähung und die ISDS-Konzepte sind mindestens von der oder dem ISBO zu prüfen; bei den IKT-Standarddiensten sind sie von der oder dem ISB SD zu prüfen. Sie sind von der Auftraggeberin oder dem Auftraggeber und dem oder der Geschäftsprozessverantwortlichen zu genehmigen.

7 Zeigt bei einer IKT-Leistungserstellung der Prüfprozess zur Reduktion nachrichtendienstlicher Ausspähung eine Vernetzung mit anderen IKT-Systemen auf und ergibt sich daraus ein Bedrohungspotenzial, so müssen die zuständigen Verwaltungseinheiten das ISB informieren.

8 Will eine Verwaltungseinheit neue Informations- und Kommunikationstechnologien (Hard- und Software) oder bestehende Technologien in einem neuen Einsatzgebiet einsetzen, so muss sie die Technologien vor dem Einsatz einer Risikobeurteilung unterziehen. Das Ergebnis der Risikobeurteilung ist der oder dem zuständigen Informatiksicherheitsbeauftragten und dem ISB vorzulegen.

9 Die Sicherheitsdokumentationen haben eine Gültigkeit von höchstens fünf Jahren. Bei sicherheitsrelevanten Änderungen am IKT-Schutzobjekt oder an der Bedrohungslage sind sie unverzüglich zu aktualisieren.

3.3 Internationale Standards

Die IKT-Sicherheitsmassnahmen orientieren sich an aktuellen internationalen Standards, insbesondere an den ISO-Standards betreffend die IKT-Sicherheitsverfahren.

3.4 Restrisiken

1 Risiken, die nicht oder nur ungenügend reduziert werden können (Restrisiken), sind auszuweisen und der Auftraggeberin oder dem Auftraggeber, der oder dem Geschäftsprozessverantwortlichen sowie der Leitung der Verwaltungseinheit schriftlich zur Kenntnis zu bringen.

2 Der Entscheid darüber, ob bekannte Restrisiken in Kauf genommen werden, obliegt der Leiterin oder dem Leiter der zuständigen Verwaltungseinheit.

3.5 Kosten

Die Kosten für die IKT-Sicherheit sind Teil der Projekt- und Betriebskosten und bei der Planung ausreichend zu berücksichtigen.

4 Netzwerksicherheit. Zuständigkeiten und Sicherheitsvorgaben

[1] Es dürfen nur Zonen aufgebaut und betrieben werden, die konform zum Zonenmodell Bund und vom ISB genehmigt sind.

[2] Das ISB führt ein Verzeichnis aller genehmigten Zonen. Die Liste enthält namentlich:

a. Zonenname;

b. Zoneninhaberin oder -inhaber;

c. Verweis auf die anwendbare Zonenpolicy;

d. Zonenbetreiberin oder -betreiber.

[3] Alle Zonen haben über eine Zonenpolicy zu verfügen. Die Zonenpolicy bedarf der Genehmigung durch das ISB.

[4] Das ISB erlässt die weiteren Vorgaben zur Netzwerksicherheit.

5 Schlussbestimmungen

5.1 Aufhebung anderer Weisungen

Die Weisungen des Bundesrates vom 1. Juli 2015[4] über die IKT-Sicherheit in der Bundesverwaltung werden aufgehoben.

5.2 Übergangsbestimmungen

[1] Schutzbedarfsanalysen und ISDS-Konzepte, die bei Inkrafttreten dieser Weisungen bestehen, gelten weiter und sind im Rahmen von Überprüfungen und Revisionen zu aktualisieren.

[2] Das Vorgehen und der Prüfprozess zur Reduktion nachrichtendienstlicher Ausspähung gemäss den Ziffern 3.2 Absätze 1, 5, 6 und 7 sind nicht anwendbar auf IKT-Projekte, für die der Projektinitialisierungsauftrag vor dem 1. Januar 2016 ergangen ist. IKT-Schutzobjekte, die am 1. Januar 2016 bereits in einer HERMES-Phase[5] oder im Betrieb waren, müssen spätestens bis zum 1. Januar 2021 von den zuständigen Verwaltungseinheiten und ihren Leistungserstellern überprüft werden.

[3] Die Zonen, die bei Inkrafttreten dieser Weisungen die Bedingungen gemäss Ziffer 4 Absatz 1 erfüllen und über eine gemäss Ziffer 4 Absatz 3 vom ISB genehmigte Zonenpolicy[6] verfügen, können mit ihren Abweichungsbewilligungen (Ausnahmen) weiter betrieben werden.

4 BBl **2015** 5795
5 www.hermes.admin.ch
6 Dabei handelt es sich um die blaue Netzdomäne, die *Shared Service Zone* (SSZ), die *Central Access Zone* (CAZ), das AHV/IV-Netz und die Netzdomäne *Law Enforcement Monitoring Facility* (LEMF).

4 Netzwerke, die bei Inkrafttreten dieser Weisungen in Betrieb stehen und nicht Teil einer Zone gemäss den Bedingungen nach Ziffer 4 Absatz 1 sind, können weiter betrieben werden, müssen aber beim nächsten Umbau, spätestens jedoch zehn Jahre nach Inkrafttreten dieser Weisungen, in eine gemäss Ziffer 4 Absatz 1 geführte Zone überführt werden.

5.3 Inkrafttreten

Diese Weisungen treten am 15. Februar 2019 in Kraft.

16. Januar 2019

Im Namen des Schweizerischen Bundesrates

Der Bundespräsident: Ueli Maurer
Der Bundeskanzler: Walter Thurnherr