Weisungen des Bundesrates über die IKT-Sicherheit in der Bundesverwaltung

vom 1. Juli 2015

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, technischen und baulichen 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;

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;

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;

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

f. *(Netz-)Domäne:* logischer Verbund aller Verbindungen und Komponenten eines Netzwerks;

g. *Netzdomänenpolicy:* Regelwerk der Voraussetzungen für den Anschluss und die Anforderungen für die Kommunikation von verschiedenen Netzwerken und Systemen.

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.

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

[5] Die Departemente, die Bundeskanzlei und die Verwaltungseinheiten sorgen dafür, dass die Informatiksicherheitsbeauftragten ihre Aufgaben ohne Interessenkonflikte wahrnehmen.

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 dokumentie-

ren und überprüfen die Umsetzung der Sicherheitsmassnahmen sowie deren Wirksamkeit.

3 Die Verwaltungseinheiten überprüfen laufend den Schutzbedarf und passen die Sicherheitsmassnahmen entsprechend an.

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

5 Die Mitarbeiterinnen und Mitarbeiter der Bundesverwaltung, die IKT-Mittel nutzen oder betreiben lassen, 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.

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 werden in den Projekt- und Leistungsvereinbarungen zwischen den Leistungserbringern und den Leistungsbezügern festgehalten.

3 Sicherheitsverfahren

3.1 Sicherheitsvorgaben

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 Grundschutz;

d. das ISDS-Konzept.

3 SR **172.010.58**

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 Bst. b) zu ermitteln.

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

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

[4] Ergibt die Schutzbedarfsanalyse einen erhöhten Schutzbedarf, so ist zusätzlich zum Grundschutz ein ISDS-Konzept 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] Schutzbedarfsanalysen, weitergehende Sicherheitsvorgaben, die Dokumentation des Prüfprozesses zur Reduktion nachrichtendienstlicher Ausspähung und ISDS-Konzepte sind mindestens von der oder dem ISBO zu prüfen und 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 sie vor dem Einsatz einer Risikobeurteilung unterziehen. Das Ergebnis der Risikobeurteilung ist der oder dem zuständigen Informatiksicherheitsbeauftragten und dem ISB vorzulegen.

3.3 Internationale Standards

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

3.4 Restrisiken

[1] Risiken, die nicht vollständig beseitigt werden können (Restrisiken), sind auszuweisen und den Auftraggeberinnen und Auftraggebern und den Geschäftsprozessverantwortlichen 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 sind bei der Planung ausreichend zu berücksichtigen.

4 Netzwerksicherheit. Zuständigkeiten und Sicherheitsvorgaben

[1] Das ISB führt ein Verzeichnis aller Netzdomänen, die für die Verwaltungseinheiten betrieben werden. Die Liste enthält namentlich:

a. Netzdomänenname;

b. Netzdomäneninhaberin oder -inhaber;

c. Verweis auf die anwendbare Netzdomänenpolicy;

d. Vereinbarungen der Netzdomäne mit anderen Netzdomänen.

[2] Alle Netzdomänen haben über eine Netzdomänenpolicy zu verfügen. Die Netzdomänenpolicy bedarf der Genehmigung durch das ISB.

[3] Vereinbarungen über Netzdomänen, die zwischen Bundesverwaltungseinheiten oder zwischen Bundesverwaltungseinheiten und Dritten abgeschlossen werden, bedürfen der Genehmigung durch das ISB.

[4] Werden Dritte direkt an eine Bundesnetzdomäne angeschlossen, so hat die zuständige Verwaltungseinheit die Einhaltung der IKT-Sicherheitsvorgaben nach diesen Weisungen durch eine Vereinbarung zu regeln sowie deren Einhaltung regelmässig zu überprüfen. Die Vereinbarungen bedürfen der Genehmigung durch das ISB.

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

5 Schlussbestimmungen

5.1 Aufhebung anderer Weisungen

Die Weisungen des Bundesrates vom 14. August 2013[4] über die IKT-Sicherheit in der Bundesverwaltung werden aufgehoben.

5.2 Übergangsbestimmungen

[1] Schutzbedarfsanalysen und ISDS-Konzepte, die bei Inkrafttreten der Weisungen des Bundesrates vom 14. August 2013[5] über die IKT-Sicherheit in der Bundesverwaltung bestanden haben, 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 auf alle IKT-Projekte

4 BBl **2013** 6713
5 BBl **2013** 6713

anwendbar, für die der Projektinitialisierungsauftrag nach Inkrafttreten dieser Weisungen ergeht. IKT-Schutzobjekte, die zum Zeitpunkt des Inkrafttretens dieser Weisungen bereits in einer HERMES-Phase[6] oder im Betrieb sind, müssen innert einer Frist von fünf Jahren von den zuständigen Verwaltungseinheiten und ihren Leistungserstellern überprüfen werden.

5.3 Inkrafttreten

Die Weisungen treten am 1. Januar 2016 in Kraft.

1. Juli 2015

Im Namen des Schweizerischen Bundesrates

Die Bundespräsidentin: Simonetta Sommaruga
Die Bundeskanzlerin: Corina Casanova

6 www.hermes.admin.ch