Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Finanzdepartement EFD
Nationales Zentrum für Cybersicherheit NCSC
Informatiksicherheit Bund SEC

Version 4.5

P041 - Schutzbedarfsanalyse

vom 19. Dezember 2013 (Stand 1. April 2021)

Der Delegierte für Cybersicherheit erlässt gestützt auf Artikel 11, Absatz 1, Buchstabe e der Verordnung über den Schutz vor Cyberrisiken in der Bundesverwaltung (CyRV) vom 27. Mai 2020 nachfolgende Vorgabe. Diese stellt eine Vorgabe für die Schutzbedarfsanalyse gemäss Artikel 14*b* CyRV dar.

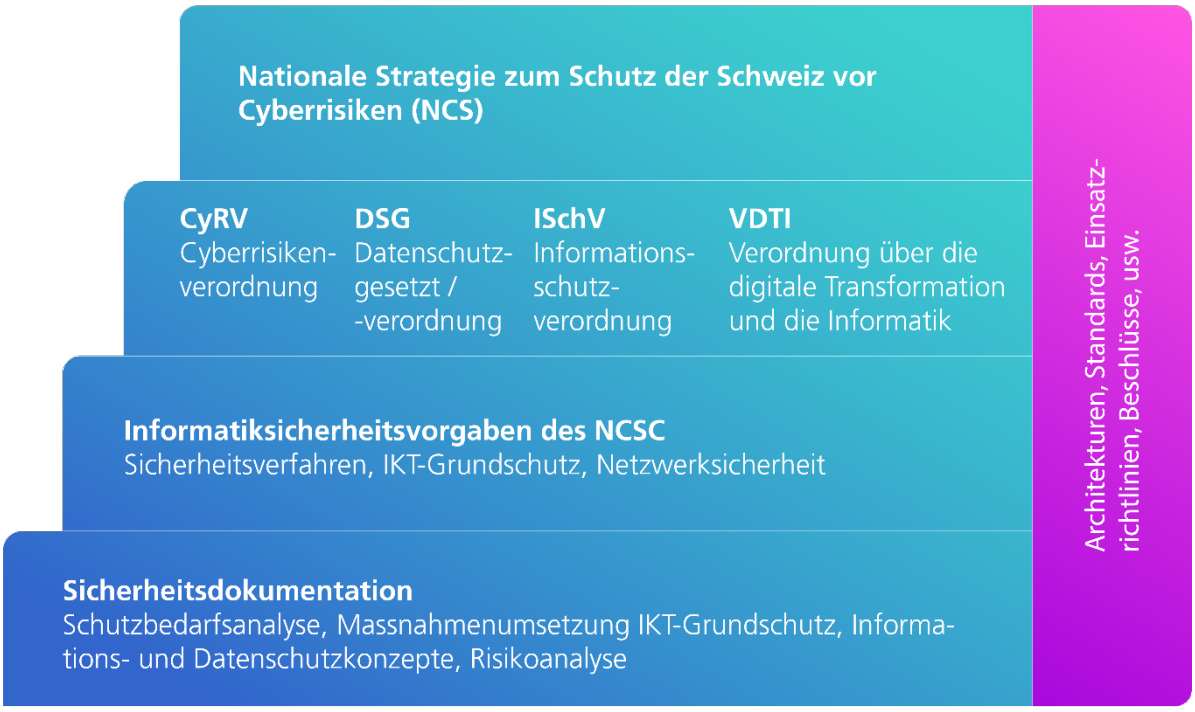

Abbildung 1: Zusammenstellung Informatiksicherheitsgrundlagen

Inhalt

1 Schutzbedarfsanalyse

Die Schutzbedarfsanalyse ist die Erhebung der Anforderungen an die Sicherheit der Informatikschutzobjekte. Sie ist mindestens durch die Informatiksicherheitsbeauftragte oder dem Informatiksicherheitsbeauftragten der Verwaltungseinheit (ISBO) zu prüfen[1]. Sie ist von der Auftraggeberin oder dem Auftraggeber und dem oder der Geschäftsprozessverantwortlichen zu genehmigen.

In der Schutzbedarfsanalyse sind mindestens festzuhalten:

1.1 Angaben zum Informatikschutzobjekt

- Projektname / Schutzobjektname (bei bestehendem Schutzobjekt)
- Departement / Amt
- Projekt Nr. / Projekt ID
- Unterstütze Geschäftsprozesse
- Klassifizierung des Dokuments (keine Klassifizierung, INTERN, VERTRAULICH, GEHEIM)
- Geschäftsprozessverantwortlicher (Name, VE)
- Projektleiter (PL LB) (Name, VE)
- Informationssicherheits- und Datenschutzverantwortlicher ISDS-V (Name, VE), *wenn schon bestimmt*
- Informatiksicherheitsbeauftragter ISBO (Name, VE)
- Dokument ausgefüllt durch (Name, VE)

- Ergebnis der Einstufung (Abbild aus Einstufung)

- Änderungskontrolle

- Unterschriften
    - Geprüft: ISBO (Datum, Name, VE)
    - Genehmigt: Auftraggeber (Datum, Name, VE)
    - Genehmigt: Geschäftsprozessverantwortlicher (Datum, Name, VE)

Weitere Angaben können individuell gefordert werden.

1.2 Gültigkeit der Schutzbedarfsanalyse

Die Gültigkeit einer Schutzbedarfsanalyse beträgt maximal 5 Jahre.

[1] Bei den Standarddiensten ist sie von der oder dem Informatiksicherheitsbeauftragten für die Standarddienste zu prüfen.

1.3 Einstufung

In der Schutzbedarfsanalyse sind zu beurteilen:

Beurteilung betreffend der ...	*Frage*	*Antworten*	*Hilftexte*
Vertraulichkeit	Sollen [mit diesem Schutzobjekt] Personendaten nach der Datenschutzgesetzgebung bearbeitet werden? Wenn ja, welche Art von Personendaten sind betroffen?	Keine Personendaten	
		Personendaten	Alle Angaben, die sich auf eine bestimmte oder bestimmbare Person beziehen, sind *Personendaten*. Sie werden als *nicht-sensible Personendaten* bezeichnet, wenn sie keine besondere Schutzwürdigkeit aufweisen.
		Besonders schützenswerte Personendaten oder Persönlichkeitsprofile	*Besonders schützenswerte („sensible") Personendaten* sind Daten über religiöse, weltanschauliche, politische oder gewerkschaftliche Ansichten oder Tätigkeiten, über die Gesundheit, die Intimsphäre oder die Rassenzugehörigkeit, über Massnahmen der sozialen Hilfe und über administrative oder strafrechtliche Verfolgungen und Sanktionen. Ein *Persönlichkeitsprofil* ist eine Zusammenstellung von Daten, die eine Beurteilung wesentlicher Aspekte der Persönlichkeit einer natürlichen Person erlaubt.
		Personendaten, deren Missbrauch für den Betroffenen Gefahren für Leib & Leben bedeuten	Wenn das Bekanntwerden von besonders schützenwerten Daten zur Bedrohung, insbesondere an Leib und Leben der betroffenen Person führen kann, dann spricht man von *hochsensiblen (lebenswichtigen) Personendaten*.

	Sollen [mit diesem Schutzobjekt] klassifizierte Informationen nach der Informationsschutzverordnung (ISchV) bearbeitet werden? Wenn ja, Informationen aus welchen Klassifizierungsstufen (vgl. Art. 5 bis 7 ISchV) sind betroffen?	Nicht klassifiziert	*Hinweis*: Zu beachten sind hier insbesondere die Weisungen über die detaillierten Bearbeitungsvorschriften zum Informationsschutz (Bearbeitungsweisungen) und die Weisungen über die Klassifizierung (Klassifizierungskatalog).[2] *Hilfestellung*: Bezüglich der Klassifizierung von Daten kann Sie der/die Informationsschutzbeauftragte des Departements oder die Koordinationsstelle für den Informationsschutz im Bund (dem VBS zugeordnet) beraten.
		Klassifizierung: INTERN	Als *INTERN* werden Informationen klassifiziert , deren Kenntnisnahme durch Unberechtigte den Landesinteressen einen Nachteil zufügen kann und die nicht höher klassifiziert werden müssen (Art. 7 ISchV).
		Klassifizierung: VERTRAULICH	Als *VERTRAULICH* werden Informationen klassifiziert, deren Kenntnisnahme durch Unberechtigte den Landesinteressen Schaden zufügen kann (Art. 6 ISchV).
		Klassifizierung: GEHEIM	Als GEHEIM werden Informationen klassifiziert, deren Kenntnisnahme durch Unberechtigte den Landesinteressen einen schweren Schaden zufügen kann (Art. 5 ISchV).

[2] Siehe die Informationsschutzvorschriften vom VBS (Dokumentation 52.064 d).

	Sollen [mit diesem Schutzobjekt] Informationen oder Daten bearbeitet werden, die aus einem sonstigen Grund (spezielle Gesetzgebungen[3]) besonders geschützt werden müssen? Wenn ja, wie hoch sind die Schutzanforderungen?	Keine erhöhten Anforderungen an die Vertraulichkeit	*Schutzwürdigkeit der Daten*: • Unterstehen die zu bearbeitenden Informationen oder Daten spezialgesetzlichen Vorgaben zum Schutz der Vertraulichkeit wie beispielsweise Art. 11 Bst. e des Bundesgesetzes über das öffentliche Beschaffungswesen, Art. 21 des Regierungs- und Verwaltungsorganisationsgesetzes oder Art. 110 des Bundesgesetzes über die direkte Bundessteuer? • Sollen mit dem Schutzobjekt Informationen oder Daten bearbeitet werden, deren Vertraulichkeit aufgrund von Vereinbarungen mit einem oder mehreren Vertragspartnern zu schützen sind? • Kann eine unberechtigte Kenntnisnahme der zu bearbeitenden Informationen oder Daten als strafrechtlich relevante Verletzung des Amts-, Berufs-, Geschäfts- oder Fabrikationsgeheimnisses gelten? *Keine speziellen Anforderungen*: Die IKT-Grundschutz Massnahmen sind schon enthalten.
		Erhöhte Anforderungen an die Vertraulichkeit	*Erhöhte Anforderungen* müssen situativ festgelegt werden. Sie beinhalten mind. die Massnahmen des IKT-Grundschutzes. Es können folgende weitergehende Massnahmen sein: • Keine Veröffentlichung im Intranet/Internet; • Zugriffsschutz mittels One Time Password, SMS-Login (User-ID und PW reichen nicht aus) oder sogar mittels 2 FA (Hard Crypto Token); • Verschlüsselung des Transportweges; • Verschlüsselung der Daten: • …
Verfügbarkeit	Max. zulässige Ausfalldauer	Ausfalldauer grösser 12 Std.	Die Angaben zur Ausfalldauer richten sich nach den Definitionen des Servicekatalogs der Standarddienste des DTI.[4]
		Ausfalldauer max. 12 Std.	Servicekatalog: Verfügbarkeitsklasse 1
		Ausfalldauer max. 8 Std.	Servicekatalog: Verfügbarkeitsklasse 2

[3] Gesetzliche Bestimmungen zu Gesundheits-, Finanzwesen, usw.
[4] Zu finden unter: intranet. dti.bk.admin.ch > IKT-Vorgaben > Standarddienste > SD 100 - Servicekatalog SD

		Ausfalldauer max. 2 Std.	Servicekatalog: Verfügbarkeitsklasse 3
	Servicezeiten[5]	Servicezeiten Standard (11/5)	Mo – Fr 07:00- 18.00 Uhr; gemäss Vereinbarung in SLA / siehe auch IKT-Servicekatalog des LE
		Servicezeiten erhöht (11/5BR)	Mo – Fr 07:00 – 18:00 Uhr, Verlängerung bis 21:00 Uhr jeweils vor BR-Sitzungen; Anforderungen an erhöhte Servicezeiten beschreiben
		Servicezeiten 24/7	7 x 24 Stunden Betrieb; falls eine solche Betriebszeit für eine VE/LE Standard ist, so ist kein zusätzliches ISDS-Konzept erforderlich. Die genauen Anforderungen müssen in einer SLA im Detail festgelegt werden.
	IT Service Continuity Management (ITSCM) relevant [für dieses Schutzobjekt] als Teil des Business Continuity Management (BCM) für geschäftskritische Prozesse?	ITSCM / BCM nicht notwendig	*Hilfsfragen*: • Was geschieht, wenn ihr Rechenzentrum nicht mehr operativ ist ? Bsp. Brand des RZ. • Was geschieht, wenn ihre Arbeitsplätze (Bürogebäude) nicht mehr verfügbar sind? • Bestehen Ausweichlösungen für den Katastrophenfall ? • Gibt es Notfallszenarien ? *Mögliche Auswirkungen*: • Notfallvorsorge (Ausfall eines einzelnen Rechners) muss in jedem Fall getroffen werden. • Im Katastrophenfall (Ausfall für längere Zeit von ganzen Rechenzentren) müssen die Daten an einem dritten, externen Standort gelagert werden.
		ITSCM / BCM notwendig	
Integrität	Muss die Echtheit, Korrektheit und/oder Unversehrtheit der Daten gewährleistet werden können?	Keine speziellen Anforderungen	*Keine speziellen Anforderungen*: Die IKT-Grundschutz Massnahmen sind schon enthalten. *Hilfsfragen*: - Was passiert, wenn die Daten unvollständig sind? - Ist die Verarbeitung / Auswertung der Daten gefährdet?

[5] Gemäss Servicekatalog Standarddienste
intranet. dti.bk.admin.ch > IKT-Vorgaben > Standarddienste > SD100 - Servicekatalog SD

		Spezielle Anforderungen	*Mögliche Auswirkungen*: a) Verstösse gegen geltende Gesetze, Vorschriften oder Verträge b) Beeinträchtigung von Ergebnissen c) Beeinträchtigung der Aufgabenerfüllung d) Negative Aussenwirkungen (z.B. Image der BV) e) Finanzielle Auswirkungen (für das Amt oder für die Bundesverwaltung, volkswirtschaftlich) f) Welche Auswirkungen hat es auf die Aufgabenerfüllung ? Beispiele von betroffenen Daten: • Gesundheitsdaten • Rechnungslegung • Rechtsverbindlichkeit • Backup • usw.
Nachvollzieh-barkeit	Müssen bestimmte Arbeitsvorgänge nachgewiesen werden können?	Keine speziellen Anforderungen	*Keine speziellen Anforderungen*: Die IKT-Grundschutz Massnahmen sind schon enthalten. *Hilfestellung*: Bezüglich der Fragen der Nachvollziehbarkeit kann Sie die EFK (Eidg.. Finanzkontrolle) oder der EDÖB (Eidg. Datenschutz- und Öffentlichkeitsbeauftragte) beraten.

		Spezielle Anforderungen	*Hilfsfragen*: • Sind es finanziell relevante Daten? (z.B. Buchhaltungs- oder Inventardaten) • Werden gemäss dem Betriebs-, Konzept- oder Organisationshandbuch Sicherheitsprüfungen durchgeführt? • Sind Belegprinzipien gefährdet? *Mögliche Auswirkungen*: • Verstösse gegen geltende Gesetze, Vorschriften oder Verträge • Beeinträchtigung der Auskunftspflicht (Persönlichkeitsrecht, Privacy) • Beeinträchtigung der Aufgabenerfüllung • Finanzielle Auswirkungen (für die BV, volkswirtschaftlich)
RINA-Relevanz	Ist dieses Schutzobjekt durch nachrichtendienstliche Ausspähung (oder ähnliche) erheblich gefährdet und/oder werden dafür sensitive Beschaffungen notwendig?	Nein - Nicht RINA-relevant	
		Ja - RINA-relevant	Wird die Frage mit Ja beantwortet, dann ist eine RINA-Relevanz gegeben. In diesem Fall sind die Kriterien gemäss Anleitung zum RINA-Prozess[6] zu prüfen und gegebenenfalls entsprechende Massnahmen vorzukehren.

Weitere Beurteilungskriterien können individuell gefordert werden.

[6] Siehe intranet.ncsc.admin.ch > Vorgaben & Hilfsmittel > Sicherheitsverfahren > Beurteilung des Schutzbedarfs > P041 - Hi02: Anleitung zum Prüfprozess RINA (Risikomanagementmethode zur Reduktion nachrichtendienstlicher Ausspähung)

2 Erhöhter Schutzbedarf

Erhöhter Schutzbedarf liegt vor, sobald eines der Felder aus der Einstufung im Bereich der Vertraulichkeit als rot gekennzeichnet wird oder wenn mehr als zwei Kriterien in den Bereichen Verfügbarkeit, Integrität oder Nachvollziehbarkeit als rot gekennzeichnet werden. Bei ausgewiesenem, erhöhtem Schutzbedarf ist gemäss Art.14d CyRV ein Informationssicherheits- und Datenschutzkonzept (ISDS-Konzept) zu erarbeiten. Darin sind, neben der Umsetzung der Sicherheitsvorgaben für den Grundschutz und basierend auf einer Risikoanalyse, weitere Sicherheitsmassnahmen spezifisch für das Projekt oder das Informatikschutzobjekt zu definieren, dokumentieren und umzusetzen.

Bei erhöhten Anforderungen nur in den Bereichen Verfügbarkeit, Integrität oder Nachvollziehbarkeit (max. zwei Kriterien) müssen zusätzliche Sicherheitsmassnahmen als Erweiterung des IKT-Grundschutzes dokumentiert werden. Dies erfolgt vorzugsweise im Dokument «Massnahmenumsetzung des IKT-Grundschutzes», zum Beispiel in Form eines zusätzlichen Kapitels.

Trifft das Kriterium RINA-Relevanz zu, ist der Prüfprozesses zur Reduktion nachrichtendienstlicher Ausspähung (gemäss Anleitung RINA[7]) zu durchlaufen. Werden gemäss dem Prüfprozess RINA risikorelevante Fälle ermittelt, so muss der Prüfprozess vollständig durchlaufen werden; die Umsetzung ist zu dokumentieren. RINA ist in erster Priorität ein Sensibilisierungsprozess. Er beleuchtet mögliche Bedrohungen betreffend einer nachrichtendienstlichen Ausspähung.

[7] Siehe İntranet.ncsc.admin.ch > Vorgaben & Hilfsmittel > Sicherheitsverfahren > Beurteilung des Schutzbedarfs > P041 - Hi02: Anleitung zum Prüfprozess RINA (Risikomanagementmethode zur Reduktion nachrichtendienstlicher Ausspähung)