Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral des finances DFF
Centre national pour la cybersécurité NCSC
Sécurité informatique de la Confédération SEC

Version 4.5

P041 - Analyse des besoins de protection

du 19 décembre 2013 (état au 1er avril 2021)

En vertu de l'art. 11, al. 1, let. e, de l'ordonnance du 27 mai 2020 sur les cyber-risques (OPCy), le délégué à la cybersécurité édicte la directive suivante, qui s'applique à l'analyse des besoins de protection conformément à l'art. 14*b* OPCy.

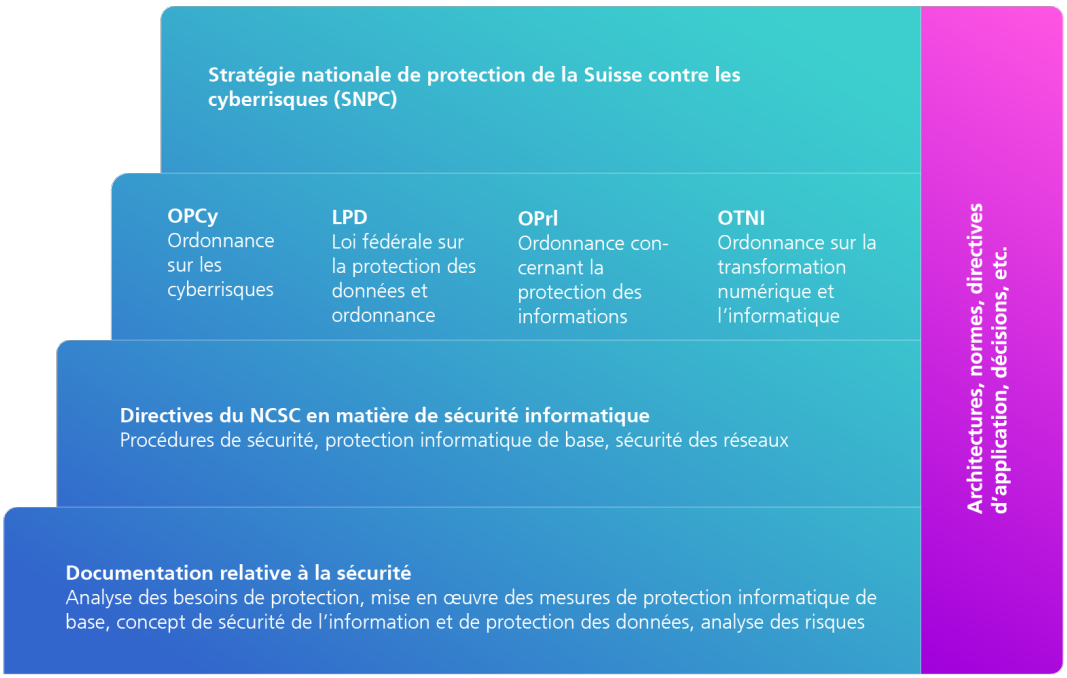

Illustration 1: Résumé des bases de la sécurité informatique

Contenu

1 Analyse des besoins de protection

L'analyse des besoins de protection consiste à définir les exigences en matière de sécurité des objets informatiques à protéger. Elle doit être contrôlée au moins par le délégué à la sécurité informatique de l'unité administrative (DSIO)[1]. Elle doit être approuvée par le mandant et par le responsable du processus d'affaires.

Les aspects suivants au moins doivent être définis dans l'analyse des besoins de protection:

1.1 Indications relatives à l'objet informatique à protéger

- Nom du projet, nom de l'objet à protéger (si l'objet à protéger existe déjà)
- Département, office
- N° du projet, ID du projet
- Processus d'affaires pris en charge
- Classification du présent document (aucune classification, INTERNE, CONFIDENTIEL, SECRET)
- Responsable du processus d'affaires (nom, UA)
- Chef de projet (du bénéficiaire de prestations) (nom,UA)
- Responsable de la sécurité de l'information et de la protection des données (nom, UA), si déjà défini
- DSIO (nom, UA)
- Document rempli par (nom, UA)

- Résultat de l'évaluation (issu de la feuille de calcul «Évaluation»)

- Contrôle des modifications

- Signatures
    - Contrôlé par: DSIO (date, nom, UA)
    - Approuvé par: mandant (date, nom, UA)
    - Approuvé par: responsable du processus d'affaires (date, nom, UA)

D'autres indications peuvent être exigées au cas par cas.

1.2 Validité de l'analyse des besoins de protection

L'analyse des besoins de protection est valable durant cinq ans au maximum.

[1] Pour les services standard, elle doit être contrôlée par le délégué à la sécurité informatique des services standard.

1.3 Évaluation

Les aspects suivants doivent être définis dans l'analyse des besoins de protection:

Évaluation concernant...	*Question*	*Réponses*	*Textes d'aide*
la confidentialité	L'objet à protéger traite-t-il des données personnelles au sens de la législation sur la protection des données? Si oui, quels types de données personnelles sont concernés?	Aucune donnée personnelles	
		Données personnelles	On entend par «données personnelles» toutes les données se rapportant à une personne identifiée ou identifiable. Elles sont considérées à caractère personnel non sensible lorsqu'elles ne nécessitent pas de protection particulière.
		Données personnelles et profils de personnalité particulièrement sensibles	Les «données personnelles sensibles» sont des données personnelles sur les opinions ou activités religieuses, philosophiques, politiques ou syndicales, la santé, la sphère intime ou l'appartenance à une race, des mesures d'aide sociale, ainsi que des poursuites ou sanctions pénales et administratives. Le «profil de la personnalité» est un assemblage de données qui permet d'apprécier les caractéristiques essentielles de la personnalité d'une personne physique.
		Données personnelles dont l'utilisation abusive peut représenter un danger pour la vie et l'intégrité corporelle de la personne concernée	Lorsque la divulgation de données personnelles sensibles peut représenter une menace, en particulier pour la vie et l'intégrité corporelle de la personne concernée, on parle alors de «données personnelles hautement sensibles».

	L'objet à protéger traite-t-il des informations classifiées au sens de l'ordonnance concernant la protection des informations (OPrI)? Si oui, quels niveaux de classification (cf. art. 5 à 7 OPrI) sont concernés?	Non classifié	*Remarque:* Les prescriptions détaillées concernant le traitement des données en vue de la protection des informations (directives relatives au traitement des données) et les directives concernant la classification (catalogue de classification) requièrent une attention particulière[2]. *Aide:* Concernant la classification de données, le délégué à la protection des informations du département ou le service de coordination pour la protection des informations de la Confédération (rattaché au DDPS) peuvent vous conseiller.
		Classification: INTERNE	Sont classifiées «INTERNE» les informations dont la prise de connaissance par des personnes non autorisées peut porter atteinte aux intérêts du pays et qui ne doivent pas être classifiées à un niveau plus élevé (art. 7 OPrI).
		Classification: CONFIDENTIEL	Sont classifiées «CONFIDENTIEL» les informations dont la prise de connaissance par des personnes non autorisées peut porter préjudice aux intérêts du pays (art. 6 OPrI).
		Classification: SECRET	Sont classifiées «SECRET» les informations dont la prise de connaissance par des personnes non autorisées peut porter un grave préjudice aux intérêts du pays (art. 5 OPrI).

[2] Voir les prescriptions du DDPS relatives à la protection de l'information (document 52.064 d, indisponible en français).

	L'objet à protéger traite-t-il des informations ou données devant être particulièrement protégées pour une autre raison (législations spécifiques[3])? Si oui, quel est le degré des exigences en matière de protection?	Pas d'exigences accrues en matière de confidentialité	*Sensibilité des données:* • Les informations et les données à traiter sont-elles soumises à des prescriptions de droit spéciales relatives à la protection de la confidentialité, telles que l'art. 11, let. e, de la loi fédérale sur les marchés publics, l'art. 21 de la loi sur l'organisation du gouvernement et de l'administration ou l'art. 110 de la loi fédérale sur l'impôt fédéral direct? • L'objet à protéger traite-t-il des informations ou des données dont la confidentialité doit être assurée conformément à des accords avec un ou plusieurs partenaires contractuels? • La prise de connaissance non autorisée des informations ou des données traitées constitue-t-elle une violation pénalement répréhensible du secret de fonction, du secret professionnel, du secret d'affaires ou du secret de fabrication? *Pas d'exigences spéciales:* les mesures en matière de protection informatique de base sont déjà appliquées.
		Exigences accrues en matière de confidentialité	Les «exigences accrues» doivent être fixées selon la situation. Elles comprennent au minimum les mesures en matière de protection informatique de base. Elles peuvent également comprendre les mesures supplémentaires suivantes: • aucune publication sur Intranet ou Internet; • protection des accès au moyen de mots de passe uniques, d'une connexion SMS (l'identifiant d'utilisateur et le mot de passe ne suffisent plus), voire de l'A2F (hard crypto token); • cryptage de la transmission; • cryptage des données…
la disponibilité	Durée de défaillance maximale admissible	Plus de 12 heures	Les durées de défaillance sont fixées selon le catalogue des services standard du secteur Transformation numérique et gouvernance de l'informatique (secteur TNI)[4].
		Maximum 12 heures	Catalogue des services: classe de disponibilité 1

[3] Dispositions légales concernant les systèmes sanitaire, financier, etc.
[4] Disponible sur: intranet.dti.bk.admin.ch > Directives informatiques > Services standard > SD100 - Catalogue des services standard

		Maximum 8 heures	Catalogue des services: classe de disponibilité 2
		Maximum 2 heures	Catalogue des services: classe de disponibilité 3
	Heures de service[5]	Heures de service standard (11/5)	Lun-ven, 7h00-18h00, selon les dispositions du SLA. Voir également le catalogue des services informatiques du fournisseur de prestations.
		Heures de service étendues (11/5 CF)	Lun-ven, 7h00-18h00, prolongé jusqu'à 21h00 la veille des séances du Conseil fédéral. Décrire les exigences en matière d'horaire de service étendu.
		Heures de service 24 heures sur 24 et 7 jours sur 7	Service assuré 24 heures sur 24. S'il s'agit des heures de service standard d'une UA ou d'un FP, un concept SIPD supplémentaire n'est pas nécessaire. Les exigences spécifiques doivent figurer en détail dans un SLA.
	Gestion de la continuité des services informatiques (ITSCM) importante [pour l'objet à protéger] en tant que partie de la gestion de la continuité des affaires (BCM) pour les processus critiques?	ITSCM / BCM non nécessaire	*Questions auxiliaires:* • Que se passe-t-il si votre centre de calcul n'est plus opérationnel, par exemple pour cause d'incendie? • Que se passe-t-il si vos postes de travail (bâtiment administratif) ne sont plus disponibles? • Existe-t-il des solutions de secours en cas de catastrophe? • Existe-t-il des scénarios d'urgence? *Conséquences possibles:* • Des mesures régissant l'organisation en cas d'urgence (panne d'un ordinateur isolé) doivent être prises. En cas de catastrophe (panne de longue durée de centres de calculs entiers), les données doivent être stockées sur un troisième site séparé.
		ITSCM / BCM nécessaire	
l'intégrité	L'authenticité, l'exactitude et/ou l'intégrité des données doivent-elles pouvoir être garanties?	Pas d'exigences spéciales	*Pas d'exigences spéciales:* les mesures en matière de protection informatique de base sont déjà appliquées. *Questions auxiliaires:* • Que se passe-t-il si les données sont incomplètes? • Le traitement ou l'analyse des données est-il en danger?

[5] Selon le catalogue des services informatiques standard: intranet.dti.bk.admin.ch > Directives informatiques > Services standard > SD 100 - Catalogue des services standard

		Exigences spéciales	*Conséquences possibles:* a) Violation de lois, de prescriptions ou de contrats en vigueur b) Préjudice porté à des résultats c) Préjudice porté à l'accomplissement des tâches d) Conséquences négatives (par ex. image de l'administration fédérale) e) Conséquences financières (pour l'office, pour l'administration fédérale, pour l'économie publique) f) Quelles conséquences cela a-t-il sur l'accomplissement des tâches? Exemples de données concernées: • Données de santé • Comptabilité • Caractère juridiquement contraignant • Sauvegarde • Etc.
la traçabilité	Certains processus de travail doivent-ils pouvoir être retracés?	Pas d'exigences spéciales	*Pas d'exigences spéciales:* les mesures en matière de protection informatique de base sont déjà appliquées. *Aide:* Concernant les questions de traçabilité, le Contrôle fédéral des finances ou le Préposé fédéral à la protection des données et à la transparence peuvent vous conseiller.

		Exigences spéciales	*Questions auxiliaires:* • S'agit-il de données à caractère financier (par ex. données de comptabilité ou d'inventaire)? • Des contrôles de sécurité sont-ils exécutés conformément au manuel d'exploitation, de conception ou d'organisation? • Les principes de la justification des écritures sont-ils en danger? *Conséquences possibles:* • Violations de lois, prescriptions ou contrats en vigueur • Préjudice porté à l'obligation de renseigner (droit de la personnalité, sphère privée) • Préjudice porté à l'accomplissement des tâches • Conséquences financières (pour l'administration fédérale, pour l'économie publique)
Pertinence GRAES	L'objet à protéger risque-t-il d'être compromis par des services de renseignement (ou autres) et/ou est-il nécessaire de procéder à des acquisitions de nature confidentielle?	Non - GRAES non pertinent	
		Oui - GRAES pertinent	Si la réponse à la question est oui, alors le processus d'audit GRAES est pertinent. Dans ce cas, les critères doivent être examinés selon les instructions du processus GRAES[6] et les mesures correspondantes doivent être prises.

D'autres critères d'évaluation peuvent être exigés au cas par cas.

[6] Voir intranet: intranet.ncsc.admin.ch > Directives informatiques & outils > Procédures de sécurité > Appréciation des besoins de protection > P041 - Hi02: Guide concernant le processus d'audit GRAES (méthode de gestion des risques visant à réduire les activités d'espionnage de services de renseignement)

2 Besoin de protection accru

Le besoin de protection est considéré comme accru dès que l'un des champs d'évaluation de la confidentialité est surligné en rouge ou lorsque plus de deux critères en matière de disponibilité, d'intégrité ou de traçabilité sont surlignés en rouge. Si une protection accrue est nécessaire, il convient d'élaborer au titre de l'art. 14*d* OPCy un concept de sécurité de l'information et de protection des données (concept SIPD). En plus de la mise en œuvre des directives en matière de sécurité relevant de la protection de base, d'autres mesures de sécurité spécifiques au projet ou à l'objet informatique à protéger doivent être définies sur la base d'une analyse des risques, documentées et mises en œuvre.

Si les exigences sont plus élevées uniquement dans les domaines de la disponibilité, de l'intégrité ou de la traçabilité (deux critères au maximum), des mesures supplémentaires en matière de sécurité doivent être énoncées à titre d'extension de la protection de base, de préférence dans le document «Mise en œuvre des mesures de protection informatique de base dans l'administration fédérale», par exemple par l'ajout d'un chapitre.

Si le critère de la pertinence d'un processus d'audit est rempli, il faut alors passer au processus d'audit visant à réduire les activités menées par des services de renseignement (selon le guide GRAES[7]). Si des cas à risques sont identifiés selon le processus d'audit, celui-ci doit être mené à terme; la mise en œuvre doit être documentée. Il s'agit avant tout d'un processus de sensibilisation qui met en lumière les menaces potentielles concernant des activités d'espionnage de services de renseignement.

[7] Voir intranet.ncsc.admin.ch > Directives informatiques & outils > Procédures de sécurité > Appréciation des besoins de protection > P041 - Hi02: Guide concernant le processus d'audit GRAES (méthode de gestion des risques visant à réduire les activités d'espionnage de services de renseignement)