Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral de la défense,
de la protection de la population et des sports DDPS

Office fédéral de la cybersécurité OFCS

Version 1.0

Guide pour l'analyse des besoins de protection

14 octobre 2024

1 Introduction

Le présent guide s'adresse aux entreprises et aux autorités qui souhaitent mettre en œuvre la procédure de sécurité de l'administration fédérale. Le texte en bleu est particulièrement important pour les unités administratives de l'administration fédérale et les autres organisations soumises à la loi du 18 décembre 2020 sur la sécurité de l'information (LSI) ou à l'ordonnance du 8 novembre 2023 sur la sécurité de l'information (OSI).

Pour l'utilisation de moyens informatiques, les autorités soumises à la LSI doivent, en vertu de l'art. 16, al. 1, LSI, élaborer une procédure de sécurité qui définit, selon l'art. 16, al. 2, let. a, LSI, les critères permettant d'évaluer le besoin de protection. Le présent guide décrit une procédure permettant de déterminer le besoin de protection d'un objet informatique à protéger (éventuellement agrégé) avant sa mise en service. Cette procédure est dénommée *analyse des besoins de protection*.

Au préalable, l'infrastructure informatique devant être prise en charge doit être divisée en un ensemble d'objets informatiques à protéger. Un objet informatique à protéger peut se composer de différents moyens informatiques (p. ex. composants matériels et logiciels) et des données qui y sont stockées, traitées et transmises. Tous ces éléments servent un but commun et défini et sont donc liés entre eux sur le plan logique (p. ex. application spécialisée pour le déroulement d'un processus d'affaires particulier). Les objets informatiques qui fournissent des services à d'autres objets informatiques à protéger sont considérés comme des plateformes et constituent eux-mêmes des objets à protéger. À cet égard, les exemples incluent le système eIAM, les infrastructures de serveurs virtualisées et les offres de *software as a service* (SaaS).

En règle générale, un objet informatique à protéger ne se limite pas aux informations, car il ne serait guère judicieux de procéder à une analyse des besoins de protection pour chaque type de document.

Dans la procédure de sécurité de l'administration fédérale, les besoins de protection doivent en principe être déterminés et identifiés pour chaque objet informatique à protéger. Leur évaluation tient uniquement compte des conséquences possibles d'une compromission. La menace à laquelle cette dernière peut conduire n'est pas prise en considération[1]. En d'autres

[1] Par exemple, s'agissant d'une perte de données, il importe peu que celle-ci soit due à l'absence de copies de sauvegarde, à une cyberattaque ou à un collaborateur malintentionné : dans tous les cas, les données sont perdues.

termes, l'analyse des besoins de protection vérifie s'il existe un risque qu'il convient de réduire.

Le besoin de protection des informations est identifié comme *accru* ou *non accru*, une indication qui s'effectue par objectif de protection (confidentialité, intégrité, disponibilité, traçabilité et protection des données). Les catégories de sécurité sont également spécifiées conformément à l'art. 17 LSI. En cas de besoin de protection accru, il sera ainsi plus facile de choisir des mesures à mettre en œuvre de manière judicieuse.

2 Procédure permettant de déterminer le besoin de protection

La procédure décrite ci-après[2] permet de déterminer le besoin de protection et la catégorie de sécurité d'un objet informatique à protéger tout en évaluant si ce besoin est accru ou non. Elle se compose de deux étapes. La première sert à décrire l'objet informatique à protéger et à établir un inventaire des informations. La seconde vise quant à elle à évaluer les conséquences possibles d'une violation des objectifs de protection (confidentialité, disponibilité, intégrité, traçabilité et protection des données[3]).

Étape 1

L'objet informatique à protéger et sa configuration technique doivent être décrits de manière aussi détaillée que possible. Il est recommandé de préciser les données suivantes (lesquelles peuvent toujours être complétées par la suite) :

a) objet et buts de l'objet informatique à protéger, avec mention des processus d'affaires concernés et des identificateurs[4] ;

b) bénéficiaires et fournisseurs de prestations impliqués (s'ils sont connus), personnes dont le rôle est concrètement assigné (p. ex. DSIO, responsable de l'objet à protéger, responsable de projet) ;

c) configuration technique (y c. environnement de développement et éventuels services de plateforme utilisés), avec des esquisses d'architecture aussi précises que possible, notamment en ce qui concerne la situation du réseau ;

d) droits d'accès (pour les personnes, les groupes, les rôles et les processus) ;

e) cadre géographique (p. ex. dans quels pays les informations sont stockées et à partir de quel endroit elles sont accessibles).

Il convient d'établir un inventaire contenant toutes les informations qui sont créées, stockées, traitées ou transmises par l'objet informatique à protéger ou qui sont nécessaires à sa mise à disposition. Ces informations doivent être regroupées d'une manière pertinente. Les données ci-dessous doivent être précisées et enregistrées pour chaque groupe d'informations :

a) description du groupe d'informations ;

b) classification actuelle ou requise selon les art. 18, 19 et 20 OSI[5] ;

c) indication si un groupe d'informations contient aussi des données personnelles et, le cas échéant, de quelles données il s'agit.

---

[2] La procédure s'inspire de l'évaluation rapide des risques (*Rapid Risk Assessment*) de Mozilla (en anglais : https://infosec.mozilla.org/guidelines/risk/rapid_risk_assessment).

[3] https://www.bj.admin.ch/bj/fr/home/staat/datenschutz/info-bundesbehoerden.html

[4] Nom du projet, numéro ou identifiant du projet, etc.

[5] Pour les informations classées INTERNE, CONFIDENTIEL ou SECRET, le groupe des personnes autorisées devrait aussi être indiqué. Cet élément est important pour identifier les risques et, par la suite, opter pour des mesures appropriées.

Étape 2

Pour chaque groupe d'informations de l'inventaire des informations établi à l'étape 1, il convient de clarifier les conséquences qu'aurait une compromission de l'objet informatique à protéger. À cette fin, il faut répondre au moins aux quatre questions ci-dessous.

a) Que se passerait-il si les informations étaient divulguées ou interceptées par des services de renseignement ou des organisations similaires[6] ? (violation de la confidentialité)

b) Que se passerait-il si les informations étaient indisponibles durant une période prolongée ? (violation de la disponibilité)

c) Que se passerait-il si les informations étaient modifiées sans autorisation ? (violation de l'intégrité)

d) Que se passerait-il s'il était impossible de savoir clairement par qui les informations ont été modifiées après leur saisie initiale ? (violation de la traçabilité)

Pour la catégorisation, il convient ensuite d'examiner si :

a) ces conséquences peuvent entraîner une violation de la sécurité de l'information ou un dommage financier d'après les critères de l'art. 28 OSI ;

b) des lois ou des ordonnances (loi sur les produits thérapeutiques, secrets d'entreprise, etc.) justifient ou exigent un besoin de protection accru ;

c) la personne préposée à la protection des données estime qu'il existe un risque accru de violation des droits fondamentaux des individus concernés au sens de l'art. 22, al. 1, de la loi fédérale du 25 septembre 2020 sur la protection des données (LPD)[7] ;

d) les conséquences sont inacceptables pour l'organisation[8].

3 Résultats de l'analyse des besoins de protection

La procédure esquissée au chap. 2 combine les groupes d'informations et les conséquences possibles qui ont une importance pour l'objet à protéger. Les effets potentiels sont identifiés et évalués en fonction des objectifs de protection (confidentialité, intégrité, disponibilité, traçabilité, protection des données).

Conformément à l'art. 17 LSI, la catégorie de sécurité (d'un objet à protéger) est évaluée au moyen des critères suivants :

a) la catégorie de sécurité *protection de base* s'applique, à moins que l'objet informatique à protéger ne relève d'une catégorie supérieure ;

b) la catégorie de sécurité *protection élevée* s'applique si un impact considérable au sens de l'art. 28, al. 1, OSI est identifié au moins à un endroit ou que des informations classées CONFIDENTIEL sont traitées ;

c) la catégorie de sécurité *protection très élevée* s'applique si un grave impact au sens de l'art. 28, al. 2, OSI est identifié au moins à un endroit ou que des informations classées SECRET sont traitées.

---

[6] Pour les informations classifiées, il est possible de répondre à cette question au moyen du catalogue de classification.

[7] Au sein de l'administration fédérale, l'évaluation est réalisée au moyen de l'instrument d'examen préalable des risques de l'Office fédéral de la justice.

[8] À cette fin, l'organisation devrait réaliser une analyse d'impact (*business impact analysis*) et fixer des critères pertinents pour ses processus d'affaires.

L'objet informatique à protéger et son besoin de protection sont inventoriés comme des actifs.

La personne déléguée à la sécurité de l'information de l'unité organisationnelle (DSIO) doit vérifier l'analyse des besoins de protection. Il s'agit notamment de contrôler que les conséquences possibles identifiées sont plausibles et que l'évaluation est compréhensible et dûment fondée. Le cas échéant, il convient d'associer d'autres services pertinents à cet examen. En outre, la personne chargée de prodiguer des conseils en matière de protection des données devrait être impliquée s'il est question de données personnelles. Dans le cadre de projets ou de processus d'affaires, il est judicieux que le mandant ou la personne qui assume la responsabilité du processus approuve l'analyse des besoins de protection.

4 Autres étapes de la procédure de sécurité

L'analyse des besoins de protection vérifie s'il existe un risque qu'il convient de réduire. En l'absence d'un besoin de protection accru, l'organisation n'est pas confrontée à des risques extraordinaires nécessitant une analyse des risques élargie. Le minimum attendu en matière de sécurité informatique est alors couvert au moyen d'exigences de base (protection informatique de base [Si001]) qui doivent être mises en œuvre pour chaque objet informatique à protéger.

Il convient de s'intéresser en particulier aux conséquences considérables ou graves pour l'organisation, lesquelles induisent un besoin de protection accru. Il est nécessaire de les réduire à un niveau acceptable au moyen de mesures techniques et organisationnelles appropriées. En outre, les directives relatives au besoin de protection accru (P042) doivent être mises en œuvre selon un concept de sécurité de l'information et de protection des données. Les interactions entre l'analyse des besoins de protection, la protection informatique de base et le processus en cas de besoin de protection accru sont schématisées dans l'illustration 1.

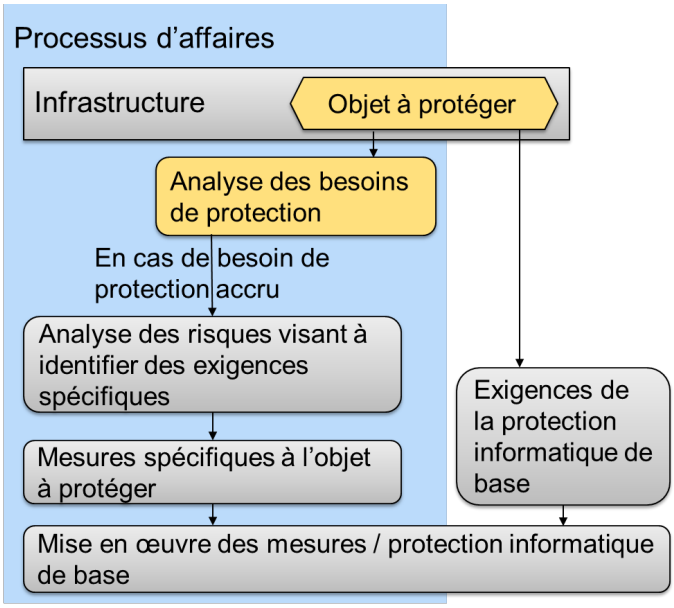

Illustration 1 L'analyse des besoins de protection au sein de la procédure de sécurité

Si des informations classées CONFIDENTIEL ou SECRET doivent être transmises à des entreprises externes ou que des entreprises externes doivent participer au développement, à la gestion, à l'exploitation, à la maintenance ou au contrôle d'un objet informatique à protéger ayant la catégorie de sécurité *protection élevée* ou *protection très élevée*, il faut lancer une

procédure de sécurité relative aux entreprises conformément à l’ordonnance du 8 novembre 2023 sur la procédure de sécurité relative aux entreprises (OPSEnt).

Si des données personnelles sont traitées avec l’objet informatique à protéger, il est possible qu’il faille également établir un registre des activités de traitement au sens de l’art. 12 LPD, ainsi qu’un règlement de traitement selon l’art. 6 de l’ordonnance du 31 août 2022 sur la protection des données (OPDo ; pour les organes fédéraux) ou l’art. 5 OPDo (pour les personnes privées).

Une analyse des besoins de protection constitue à la fois un artefact au sein des projets et une partie de la documentation de chaque objet informatique à protéger. Étant donné qu’un projet peut inclure plusieurs objets informatiques à protéger, il peut y avoir plus d’une analyse des besoins de protection (d’un objet informatique à protéger) par projet. Dans les projets, il faut achever rapidement une première version de l’analyse des besoins de protection. Il convient ensuite de la tenir à jour pour la documentation et de s’assurer qu’elle est en tout temps actuelle.