27 octobre 2025 | Office fédéral de la cybersécurité OFCS

Gestion coordonnée des cyberincidents : processus de la Confédération

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

Contenu

1 Contexte 3

2 Processus-clés de la gestion coordonnée des cyberincidents 3

3 Classification des cyberincidents 5

4 Processus de la Confédération pour la gestion coordonnée des cyberincidents 6

4.1 Processus pour les cyberincidents de portée mineure 6

4.2 Processus pour les cyberincidents de moyenne portée 6

4.3 Processus pour les cyberincidents de portée importante 7

4.4 Processus pour les cyberincidents de portée majeure 8

5 Application du concept 8

1 Contexte

Le 1er mai 2024 (EXE 2024.0416), le Conseil fédéral a mandaté le Département fédéral de la défense, de la protection de la population et des sports (OFCS ; SEPOS) pour mettre en évidence la manière dont s'organise la coordination entre la Confédération, les cantons et les fournisseurs en matière de gestion des cyberattaques et les critères de classification de ces dernières.

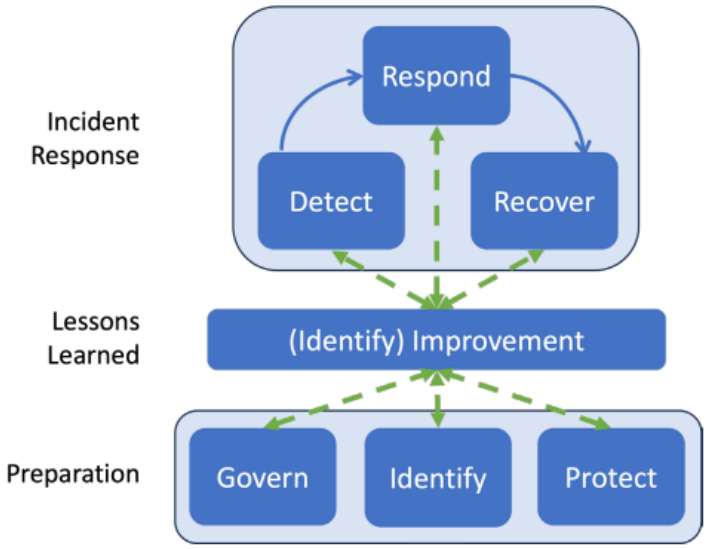
Ce mandat fait partie du train de mesures adopté après la cyberattaque contre l'entreprise Xplain SA et la fuite de données sensibles de la Confédération et des cantons qui s'en est suivie. Pour maîtriser les conséquences de cet événement, le Conseil fédéral avait formé un état-major de crise politico-stratégique « Fuite de données » qui a pu être dissous le 1er mai 2024. Il ressort de son travail que deux points sont à préciser: les cyberincidents pour lesquels il faut mettre en place un état-major de crise politico-stratégique et la manière dont il convient d'impliquer les cantons et d'autres acteurs éventuels.

La loi sur l'information (LSI) (RS 128), l'ordonnance sur la cybersécurité (OCyS) (RS 128.51) et l'ordonnance sur l'organisation de crise de l'administration fédérale (OCAF) (RS 172.010.8), entrées en vigueur en 2024 pour la première et en 2025 pour les deux autres, apportent les bases légales nécessaires pour mieux coordonner la gestion des cyberincidents. Le présent concept présente la classification des cyberincidents par ordre de gravité et les mécanismes correspondants de coordination entre organisations. Il émet en outre des recommandations sur le degré de gravité à partir duquel il convient de mettre sur pied un état-major de crise politico-stratégique.

2 Processus-clés de la gestion coordonnée des cyberincidents

À l'art. 5 de la LSI, les cyberincidents sont définis comme des événements survenant lors de l'utilisation de moyens informatiques et ayant pour conséquence une atteinte à la confidentialité, à la disponibilité ou à l'intégrité d'informations ou encore à la traçabilité de leur traitement. Quant aux cyberattaques, ce sont des cyberincidents provoqués intentionnellement. En font partie l'intrusion dans un système informatique par un logiciel malveillant ou par l'exploitation d'une faille, mais aussi des attaques par saturation (DDoS) affectant la disponibilité des services.

En cas de cyberincident, des contre-mesures sont nécessaires. On parle alors de gestion de l'incident ou Incident Response en anglais. Le National Institute of Standards and Technology (NIST) a élaboré des processus de base nécessaires pour maîtriser un cyberincident (Incident Response Life Cycle Model, cf. graphique 1).



Graphique 1 : *processus de base de gestion des cyberincidents (A. Nelson and al. (2025),*

Le modèle de cybersécurité comprend trois processus-clés de gestion opérative des cyberincidents : la détection (Detect), la réaction (Respond) et la récupération (Recover). La phase de détection consiste à identifier le cyberincident (y compris potentiel) aussitôt que possible, à analyser son origine, à déterminer les acteurs qui en sont responsables et leurs motivations, et à préciser ses caractéristiques techniques (p. ex. le logiciel malveillant utilisé). La deuxième étape (réaction) comporte des contre-mesures pour mettre fin au cyberincident ou au moins pour en minimiser les dégâts. Quant à la phase de récupération, elle vise à réparer les dommages subis et à rétablir la disponibilité fonctionnelle des systèmes et des données.

Ces processus sont appliqués à chaque cyberincident, mais dans des proportions qui dépendent largement du type d'incident et de ses répercussions. Le plus souvent, l'équipe de sécurité responsable réussit à maîtriser seule la situation, sans délai. Elle lance ensuite deux autres processus pour mieux protéger l'organisation contre d'éventuels cyberincidents à venir (amélioration ou Lessons Learned et préparation ou Preparation).

La mise en réseau exponentielle accroît la fréquence des cyberincidents qui ne se limitent pas à une seule organisation, mais, à travers des interfaces ou des liens de dépendance, peuvent toucher par exemple des systèmes gérés par des tiers ou appartenant à des tiers. Les perturbations causées par les cyberincidents se propagent souvent très vite. Les entreprises ont tendance à confier la gestion de leur équipe de sécurité à des fournisseurs de services qui s'occupent de la sécurité (Managed Security Service Providers), ce qui répartit les responsabilités entre deux acteurs au moins qui doivent se coordonner ou être coordonnés. En fonction de l'incident et de ses conséquences, cette tâche est assurée par l'organisation elle-même ou une organisation qui a subi des répercussions, par une entreprise de cybersécurité mandatée par l'une de ces organisations ou par l'OFCS en cas de cyberincident de grande ampleur.

Lorsque plusieurs acteurs sont directement impliqués dans la gestion d'un cyberincident, il est essentiel d'assurer la bonne coordination des tâches. Dans ce but, il importe de déterminer au plus vite les processus à mettre en place et qui en assume la responsabilité. Une gestion efficiente passe par une classification claire et transparente des cyberincidents.

Ces démarches sont d'autant plus importantes quand l'administration fédérale est touchée puisqu'il en va de l'intérêt public. Sur la base de l'art. 73a LSI, l'OFCS réalise des analyses techniques pour évaluer et contrer les cyberincidents et les cybermenaces et aider les infrastructures critiques à y faire face. L'OFCS joue donc un rôle-clé dans la gestion coordonnée de tels cyberincidents. Mais le législateur a limité son rôle puisque l'OFCS n'apporte qu'un soutien subsidiaire, sans assumer de tâches qui peuvent être prises en charge par des fournisseurs privés dans un délai raisonnable (Art. 74, al. 3, LSI). Pour que les acteurs du secteur privé, des cantons et de la Confédération puissent assurer une gestion coordonnée des cyberincidents, il est essentiel de définir clairement le rôle de la Confédération et le type de cyberincidents qu'elle est appelée à gérer.

3 Classification des cyberincidents

La classification claire et transparente des cyberincidents sert à répartir les rôles de gestion en fonction du type de cyberincident. Pour autant, il est important de souligner que cette classification n'est pas valable partout et tout le temps, et de rappeler que la gestion d'un cyberincident peut évoluer en cours d'événement. Chaque organisation évalue l'incident selon sa propre perspective, forcément subjective. Il arrive régulièrement que la première appréciation soit révisée au fil des événements. Cette inévitable subjectivité et la dynamique des événements compliquent la coordination, de sorte qu'une communication continue et approfondie entre les différents acteurs impliqués a d'autant plus d'importance. En revanche, le classement en lui-même est simple. Il repose sur deux facteurs interdépendants :

- le nombre et l'importance des organisations et des systèmes ciblés directement ou indirectement ;
- et les répercussions déjà subies ou à venir.

Quand le cyberincident ne touche qu'une seule organisation, ces deux dimensions sont en général assez faciles à établir. Les équipes de sécurité sont nombreuses à appliquer intuitivement des critères pour évaluer ces deux facteurs et décider rapidement quelles structures utiliser pour gérer le cyberincident.

Mais lorsque le cyberincident atteint plusieurs organisations, il est important que tous les acteurs concernés comprennent la manière dont leurs partenaires l'évaluent. Il peut arriver également qu'un incident ne touche qu'une seule organisation, mais plusieurs systèmes, ce qui peut avoir de graves conséquences, sans que d'autres acteurs soient pour autant concernés dans l'appréciation de l'événement. Par exemple, une attaque par un rançongiciel qui chiffre les données d'un système pour les rendre inaccessibles est souvent grave pour l'organisation ciblée, mais rarement pour des tiers qui n'ont pas besoin d'y réagir (dont la Confédération puisque l'intérêt public n'est pas menacé).

À chaque incident, la Confédération doit évaluer les répercussions sur la société dans une perspective globale. L'OFCS classe les cyberincidents en fonction du nombre d'organisations touchées en Suisse et des répercussions sur le fonctionnement de l'économie ou sur le bien-être de la population. Pour jouer son rôle de coordination dans la gestion des cyberincidents, il utilise un modèle qui classe les cyberincidents en quatre catégories selon leur portée : mineure, moyenne, importante et majeure. Ce modèle vise à garantir une pratique uniforme dans la gestion coordonnée des cyberincidents, dans le respect des prescriptions légales.

Portée	Cible	Conséquences
Mineure	Personnes ou organisations (hors infrastructures critiques)	Le cyberincident n'entraîne pas de limitations fonctionnelles ou celles-ci n'affectent pas ou pratiquement pas le bon fonctionnement de l'économie ou le bien-être de la population.
Moyenne	Infrastructure critique	Le cyberincident est une cyberattaque à signaler au sens de l'art. 74*d* LSI lorsqu'il pourrait mettre en péril le fonctionnement de la ou des infrastructures critiques concernées, ou entraîner une manipulation ou une fuite d'informations.
Importante	Plusieurs infrastructures critiques	
Majeure	Nombre important d'entreprises / sous-secteurs critiques	Le cyberincident peut avoir des répercussions importantes sur le fonctionnement de l'économie ou le bien-être de la population

***Tableau 1** : classification des cyberincidents*

4 Processus de la Confédération pour la gestion coordonnée des cyberincidents

Le processus de gestion coordonnée dépend du classement du cyberincident. Ce chapitre présente les processus appliqués à chaque catégorie par l'OFCS dans son rôle de coordination de la gestion des incidents. Il est important de rappeler que le classement d'un cyberincident peut évoluer et, par conséquent, les processus aussi.

4.1 Processus pour les cyberincidents de portée mineure

Les cyberincidents de portée mineure peuvent être signalés à l'OFCS sur une base volontaire (Art. 73b, al. 1, LSI). L'OFCS reçoit le signalement et émet sur demande une recommandation quant aux mesures à prendre, pour autant qu'aucune analyse ni clarification supplémentaire ne soit nécessaire à cet effet (Art. 73b, al. 2, LSI). Dans ce cas, la responsabilité de la gestion des incidents incombe à l'organisation ou à la personne concernée. La Confédération n'assume aucun rôle de coordination.

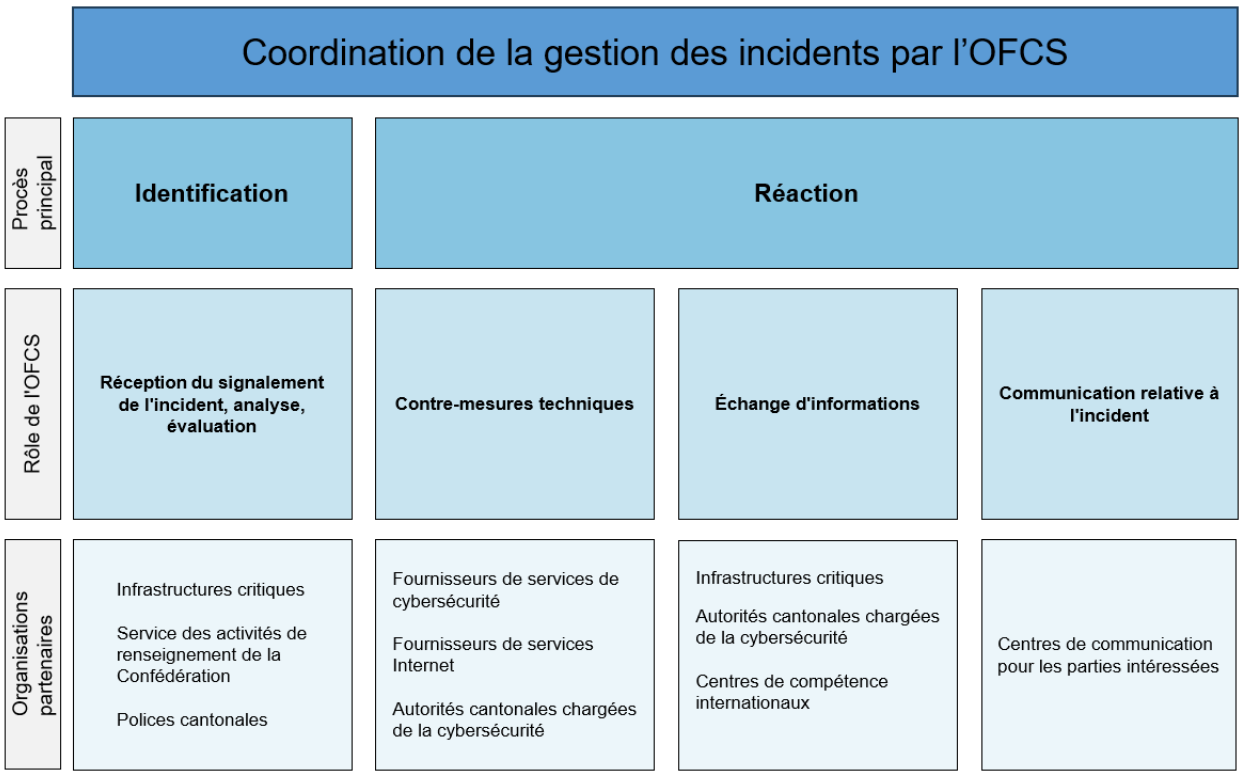
4.2 Processus pour les cyberincidents de moyenne portée

Depuis le 1er avril 2025, les exploitants d'infrastructures critiques ont l'obligation de signaler les cyberattaques selon l'art. 74a LSI. La Confédération et plus précisément l'OFCS sont tenus en contrepartie d'aider les exploitants concernés à gérer le cyberincident à la condition que les exploitants ne puissent pas obtenir en temps voulu un soutien équivalent sur le marché (Art. 74a, al. 3, LSI). Le groupe d'intervention en cas d'urgence informatique de l'OFCS (Government Computer Emergency Response Team, GovCERT) coordonne la gestion technique directement avec les entreprises concernées. Si le cyberincident touche l'administration fédérale, l'OFCS peut, en vertu de l'art. 12, al. 3, de l'ordonnance du 8 novembre 2023 sur la sécurité de l'information (OSI) (RS 128.1) aider et conseiller directement les unités administratives concernées si nécessaire, au-delà de son rôle généralement subsidiaire.

Si plusieurs organisations sont perturbées en Suisse ou que les méthodes éprouvées ne permettent pas d'assurer la gestion dans un délai raisonnable, l'OFCS cherche d'abord à établir le flux d'informations entre les organisations impliquées à travers le Cyber Security Hub (CSH), sous forme d'alertes, d'évaluations et de recommandations. Cette plateforme sert aussi aux échanges entre personnes concernées, contribuant ainsi à la gestion coordonnée des incidents.

4.3 Processus pour les cyberincidents de portée importante

À partir de cette catégorie, l'OFCS assume en première instance un rôle plus central dans la coordination de la gestion des incidents. Si le cyberincident concerne l'administration fédérale, c'est le Secrétariat d'État à la politique de sécurité (SEPOS) qui en assure la gestion. Le SEPOS peut en déléguer la direction à l'OFCS (Art. 12, al. 7, OSI), dont la coordination et le soutien technique sont importants si l'incident concerne plusieurs infrastructures critiques, ou s'il a des conséquences graves (s'il entraîne des perturbations p. ex.) ou s'il se prolonge sans que des contre-mesures efficaces puissent être prises. Le graphique 2 illustre les grandes lignes de la coordination et du soutien et l'implication des organisations partenaires.Il y apparaît clairement que l'OFCS se concentre sur les processus-clés de la détection et de la réaction. Il revient aux organisations concernées de récupérer toutes les fonctionnalités de leurs systèmes (Recovery).



***Graphique 2** : coordination de la gestion des cyberincidents par l'OFCS.*

4.4 Processus pour les cyberincidents de portée majeure

Pour être classé comme étant de portée majeure, un cyberincident doit avoir entraîné une crise ou avoir eu le potentiel d'en entraîner une. Comme il représente un danger immédiat majeur pour l'État, la société et l'économie, le Conseil fédéral met en place un état-major de crise pour le gérer et en atténuer les effets. L'ordonnance du 20 décembre 2024 sur l'organisation de crise de l'administration fédérale (OCAF) (RS 172.010.8) réglemente la mise en place et la coordination d'un tel état-major. L'organisation et plus particulièrement le choix du département qui prend la direction des opérations dépendent des secteurs critiques concernés. La priorité est de rétablir la situation dès qu'une panne importante touche un secteur critique. Les processus sont fondamentalement les mêmes pour gérer un cyberincident de portée majeure ou de portée importante. La cellule de crise politico-stratégique peut, si nécessaire, élaborer des directives d'ordre politique ou stratégique pour la gestion opérationnelle de la crise ou de l'incident (Art. 5, al. 3, let. b, OCAF).

5 Application du concept

La procédure de l'OFCS décrite dans le présent concept pour la gestion coordonnée des cyberincidents repose sur les bases légales existantes. Elle a été complétée ces derniers mois par deux éléments décisifs : l'adoption de l'OCAF et l'obligation pour les infrastructures critiques de signaler toute cyberattaque les concernant à compter du 1er avril 2025, suite à la modification de la LSI du 29 septembre 2023.

Les processus de gestion coordonnée des incidents étant déjà une pratique courante, il n'est pas nécessaire d'agir dans l'immédiat pour renforcer leur application, par exemple à travers de nouvelles bases légales. Il est toutefois important de faire mieux connaître la classification des cyberincidents et les processus de gestion correspondants. La gestion coordonnée des incidents ne fonctionne que si, dès le début, les responsabilités et le soutien attendu sont clairs pour tous les partenaires.

L'OFCS continuera donc à coordonner étroitement les processus de gestion des incidents et la classification des cyberincidents avec les cantons et les exploitants d'infrastructures critiques, et à communiquer ses tâches et ses compétences de manière transparente.