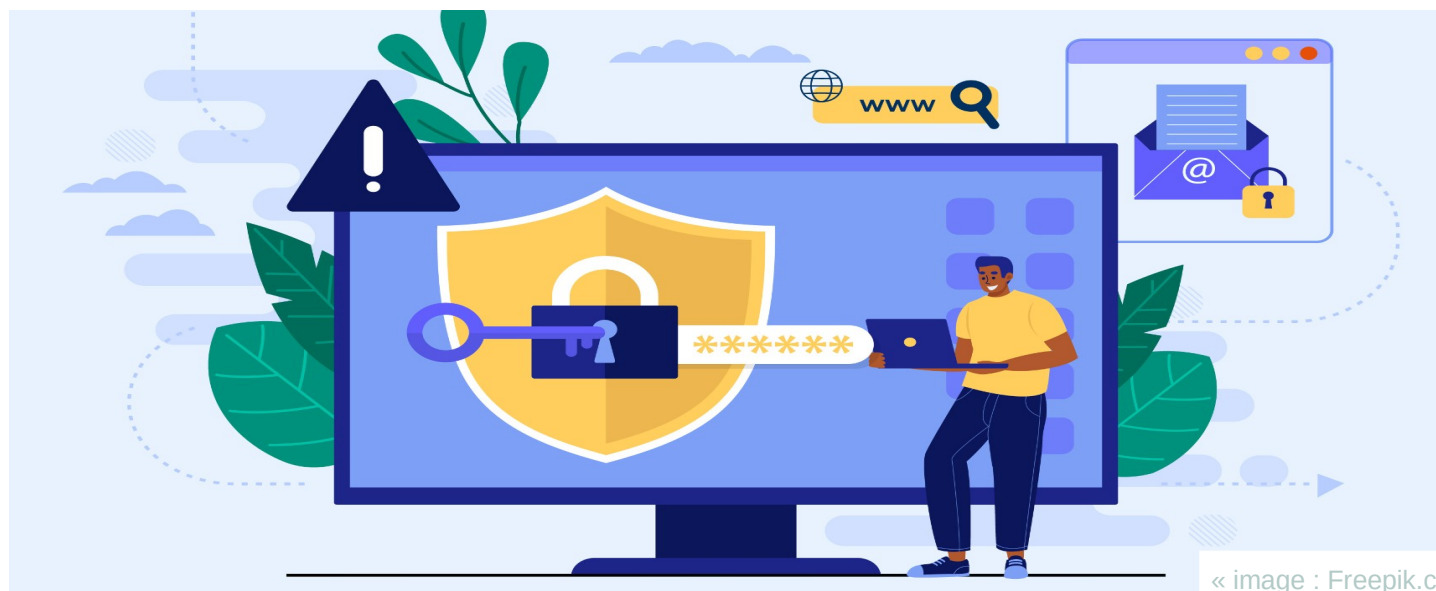


QUE FAIRE LORSQUE L'ATTAQUE EST TERMINÉE ?



Que faire une fois l'attaque définitivement traitée ?

À la suite à une cyber-attaque, la remise en état du système d'information de la collectivité est suivie par la volonté des acteurs de reprendre les échanges entre l'ordonnateur et le comptable. Cependant, cette reprise dépend de l'accord du RSSI de la DGFIP. Malgré la fin apparente de la crise, la reprise de l'activité devient critique pour le comptable public. La durée de l'événement et l'ampleur des opérations en mode dégradé impactent le temps de régularisation, avec des risques de double paiement. Les services ordonnateurs cherchent à rattraper le temps perdu en mandatant davantage, créant ainsi une charge accrue pour les services du comptable. La vigilance est cruciale en raison des risques de mauvais typages des mandats, d'une justification insuffisante des dépenses et de possibles tentatives d'escroquerie aux faux virements.

PLAN DE REPRISE D'ACTIVITÉ

REPRENDRE LES ÉCHANGES AVEC L'ORDONNATEUR

VÉRIFIER LES BALANCES COMPTABLES

RÉGULARISER LES COMPTES D'IMPUTATION PROVISOIRE (CIP)

RESTAURER LES DONNÉES DE LA COLLECTIVITÉ

> REPRENDRE LES ÉCHANGES AVEC L'ORDONNATEUR

[Obtenir l'accord de reprise des échanges

La reprise de la transmission des flux est soumise à l'engagement écrit de l'ordonnateur attestant de la fin de l'incident et la transmission du rapport forensique* au RSSI de la DGFIP.

Seul le bureau SI3 (RSSI de la DGFIP) donne son accord de reprise à la lecture du rapport (Cf définition en fin document) transmis par l'ordonnateur et établit par le prestataire sur la situation de la collectivité vis à vis de cette attaque.

Ce rapport détaille l'origine de l'incident afin d'identifier le canal d'infection et les actions de sécurisation prises par la collectivité ou l'établissement public victime.

Pour des raisons de confidentialité, le rapport sera transmis aux seules boîtes :

- bureau.si3-dmocss@dgfip.finances.gouv.fr
- soc@dgfip.finances.gouv.fr

La reprise peut se faire au fur et à mesure de la restauration des données chez l'ordonnateur. Le mode dégradé peut se poursuivre partiellement sur certains services (par exemple réouverture des échanges entre la Gestion Financière et Hélios, tandis que le serveur de messagerie reste en cours d'analyse).

Le comptable public ou la personne référente en direction locale informe et demande la reprise des échanges (demande formulée à la boucle de mails) afin que chacun des acteurs soit informé et puisse rétablir les connexions pour les échanges de flux.

[Paramétrage Hélios

Le comptable paramètre les échanges PES dans Hélios à l'identique de ceux supprimés lors de la déclaration de l'attaque.

En cas de doute, il peut être préconisé à l'ordonnateur d'envoyer un flux PES dépense et un flux PES recette pour s'assurer de la bonne reprise des échanges. A l'issue de cette phase l'envoi des flux peut reprendre.

[Aspasia et Madhras

Il est nécessaire de rétablir les adresses mails des personnes sur les fiches Aspasia, à la condition que le serveur de messagerie de l'ordonnateur soit réputé sain. A défaut, les adresses mails doivent rester celles de secours.

Les mots de passe peuvent alors être réinitialisés par le SGC ou le référent en direction locale.

Si les habilitations Madhras des personnels ordonnateurs ont été supprimées par le poste, elles peuvent être remises en oeuvre.

Si les habilitations ont été invalidées par la cellule PIGP ou SIL, il convient de leur renvoyer les fiches navettes.

> VÉRIFIER LES BALANCES COMPTABLES

Le comptable public demande les différentes balances à la reprise et les compare avec celles éditées le jour de l'incident. Il vérifie la justification des mouvements comptabilisés.

Des demandes d'édition de CCA sont lancées afin de relever les éventuelles incohérences comptables.

> RÉGULARISER LES COMPTES D'IMPUTATION PROVISOIRE (CIP)

[En dépense

Selon la durée de l'attaque et du volume des opérations traitées en mode dégradé, il est nécessaire d'organiser la reprise soit en traitant prioritairement les régularisations, soit en traitant les autres dépenses pour désintéresser les autres fournisseurs. Cela dépend des volumes traités et du temps de l'attaque.

En fonction du volume, veiller à régulariser l'intégralité des sommes comptabilisées en CIP pendant la durée de l'attaque avant de reprendre l'envoi de bordereaux « normaux ». Cela permettra d'éviter les sources d'erreurs et de reprendre une activité de manière sécurisée, une fois l'ensemble des émargements effectués.

En fonction du temps de gestion en mode dégradé, la régularisation des OP manuels n'est pas forcément prioritaire : les premiers jours ou semaines post piratage peuvent être consacrés aux mandatement des factures restées en souffrance durant la crise.

Enfin il est conseillé de réaliser des ajustements fréquents entre l'ordonnateur et le comptable sur les crédits consommés.

Les ordres de paiement doivent être régularisés par des mandats correctement typés et référençant les N° d'OP, afin de mettre à jour la consommation budgétaire.

Il convient donc de :

- Demander à l'ordonnateur de produire les mandats de régularisation en exploitant les données de l'état CO67 « État des ordres de paiement ».
- Les mandats doivent être correctement typés « mandat émis après paiement » et doivent obligatoirement porter les références à la pièce de dépense (ordre de paiement).
- Ces mandats, correctement typés « émis après paiement » ne doivent pas porter de coordonnées bancaires. Ils doivent porter un mode de règlement « Virement interne » ou « Avis de Règlement ».
- S'assurer de la correspondance des mandats avec les éditions demandées dans hélios des OP et des CIP à régulariser.
- Demander à l'ordonnateur de regrouper les mandats de régularisation sur des bordereaux de régularisations dédiés et en fonction de la nature de la dépense (fonctionnement, investissement, marchés, paye, emprunt...) en rattachant le mandat au numéro de la pièce ayant permis la dépense au préalable (OP).
- Si le rattachement automatique ne fonctionne pas ou bloque la prise en charge, émarger manuellement les mandats avec les OP.
- Être particulièrement vigilant sur les mises en paiement afin d'éviter de payer des mandats qui auraient dû être émargés avec des OP.

> RÉGULARISER LES COMPTES D'IMPUTATION PROVISOIRE (CIP)

[En Recette

Toutes les recettes enregistrées sur des CIP doivent faire l'objet d'une régularisation. Le détail des soldes des CIP doit être transmis aux services ordonnateurs afin que les titres correspondants soient émis.

Les titres doivent être correctement typés «titres émis après encaissement» et doivent obligatoirement porter les références à la pièce de recette.

Selon la durée de l'attaque et du volume des opérations traitées en mode dégradé, il est nécessaire d'organiser la reprise en traitant les régularisations et en reprenant l'encaissement des recettes.

En fonction du temps de gestion en mode dégradé, les premiers jours ou semaines post piratage peuvent être consacrés à l'émission des titres de recettes et envoi des ASAP.

Face à la nécessité de rattrapage du retard d'émission des titres de recette, il est néanmoins conseillé à l'ordonnateur et au comptable d'adopter une stratégie commune de titrage échelonné, en lissant l'émission des titres afin de ne pas submerger les services du comptable.

S'agissant des créances à échéance mensuelle (frais de cantine, crèche...) ou des créances faisant l'objet d'un prélèvement automatique, une attention particulière devra être apportée lors de la régularisation des paiements auprès des usagers. En effet, il serait préférable d'aménager la politique de recouvrement en accordant des délais de paiements afin que les usagers puissent échelonner leurs paiements et ne supportent pas une charge financière trop importante de manière simultanée. Il conviendra par conséquent d'en tenir compte dans le traitement de la chaîne des poursuites.

Concernant les prélèvements, le comptable devra systématiquement vérifier la date du prélèvement renseignée par l'ordonnateur dans le flux et la décaler le cas échéant. En effet, il se peut que le flux de prélèvement déjà signé par l'ordonnateur ait été bloqué en raison de l'attaque et soit débloqué après la date prévue initialement (lors de la prise en charge des titres permis par le déblocage des flux PES Recette).

Enfin il est conseillé de réaliser des ajustements fréquents entre l'ordonnateur et le comptable sur les crédits réalisés en recettes.

> RESTAURER LES DONNÉES DE LA COLLECTIVITÉ

Dans le cas où les données de l'ordonnateur ont été endommagées, et aucune sauvegarde ne peut être exploitée, le comptable de la collectivité demande au bureau GP-2B de lui transmettre les flux aller (dépenses, recettes, budget) qu'elle a transmis à Hélios.

Cette demande est formulée à la boîte : bureau.gp2b-communication@dgfip.finances.gouv.fr

A compter de la version 5.24 Hélios de juillet 2024, une évolution permettra à la direction locale (DSPL) de réaliser cette demande en transactionnel dans Hélios.

Il est rappelé que seuls les flux comptables sont restitués et ne comportent pas les pièces justificatives.

Pour les exercices comptables clos et validés, il est possible pour l'ordonnateur de récupérer les flux et les pièces justificatives associées via ORC.

DÉFINITION ANALYSE FORENSIQUE

- Une analyse forensique est une recherche méthodique et approfondie des actions réalisées sur un système informatique après incident (piratage, vol de données, etc.).
Une analyse bien menée permet, sous certaines conditions, de retrouver des preuves : Documents confidentiels ou sensibles effacés, Programmes de piratage exécutés, Connexions réussies, Sites internet visités, Tentatives de suppression des log, Mots de passe volés, Appels reçus, SMS envoyés,
- Mises en relation entre elles, ces preuves permettront de valider ou d'invalides des hypothèses de départ : Vol de données, Piratage, Téléchargement ou recèle de contenus illicites