

SUIVI DES ACTIONS CYBER-ATTAQUES

1/7

Comptable

Ordonnateur

Bloquer tous les flux informatiques entrants et sortants de la collectivité :

Supprimer dans Hélios pour tous les budgets de la collectivité les paramètres ordonnateur via le menu : Paramétrage - Échanges PES, cliquer sur « Modif » puis supprimer l'ensemble des protocoles Retour puis Aller.

3

Après détection d'une cyberattaque :

- Ne pas répondre aux sollicitations du cybercriminel.
- Débrancher le ou les poste(s) de travail infecté(s).
- Éteindre les serveurs et couper leur accès internet.
- Ne pas connecter les serveurs de sauvegarde aux ordinateurs, ni aucun autre équipement périphérique (clé USB,...).

1

Informez les interlocuteurs suivants afin de couper les échanges et accès :

- Le comptable public.
- Le tiers de télétransmission si la collectivité à recours à un tel service.

2

Puis les autres acteurs compétents :

- La Préfecture ou l'ARS.
- Déposer plainte auprès des services de police ou de gendarmerie.

Identifier l'ampleur de l'attaque, des SI des budgets impactés

Établir une liste des outils informatiques utilisés par la collectivité ou l'établissement attaqué et répertorier les collectivités utilisant également ces outils et la même infrastructure informatique.

4

4

Éviter la contamination des systèmes informatiques :

Ajuster le périmètre du blocage à l'ensemble des flux informatiques de la collectivité et des collectivités figurant sur la liste.

5

Comptable

6

Bloquer l'accès au SI de la DGFIP via le PIGP pour l'attaquant :

- Supprimer les habilitations (Passerelle, Hélios, DFTNet ...) dans Madhras pour les comptes Aspasia des ordonnateurs, Régisseurs et collaborateurs concernés par l'attaque.

Ou

- Modifier les adresses mails de contacts sur les identifiants Aspasia, puis Réinitialiser les mots de passe.

7

Alerter l'ensemble des acteurs compétents à la DGFIP :

Informer par mail avec l'objet CYBER-ATTAQUE – Nom de la collectivité, les interlocuteurs mentionnés dans la fiche 2 chap.3 Paragraphe 2 en veillant à mettre toutes les informations demandées. Cliquer sur [DECLARER UNE ATTAQUE](#)

8

Bloquer les échanges PESV2 via la passerelle :

L'ESI de Châlons assure la suppression du lien entre les comptes Aspasia et la passerelle de transmission des flux à destination d'Hélios à la lecture du mail d'Alerte du point 7.

9

Établir la situation comptable des budgets impactés :

Éditer les différents documents comptables arrêtés à la date du jour de l'incident pour l'ensemble des budgets de la collectivité concernée : une balance, un état des restes à payer, un état des restes à recouvrer

Ordonnateur

10

Dresser un état des lieux du SI :

- Le prestataire informatique de l'ordonnateur ou l'ANSSI établissent un bilan du SI suite à l'attaque : fonctionnalités et logiciels bloqués, évaluation de la durée d'indisponibilité.

11

Dresser un état des lieux des régies pouvant être impactées :

- Suspendre l'utilisation de la régie et établir un diagnostic permettant de savoir s'il faut couper ou non DFT net et DIGIFIP (Action à faire également coté Comptable, voir point 6)

Comptable

Ordonnateur

Adapter le mode de communication :

- Définir quel canal de communication peut être utilisé sans risque : téléphones fixes, téléphones portables, messagerie informatique.

En fonction, prévoir la création d'adresses mail temporaires dans le respect des règles (voir fiche 2). Communiquer par l'intermédiaire de nouveaux postes informatiques et hors réseau (éventuellement réseau via clé 4 ou 5g)

Mettre en place des points quotidiens entre les services de l'ordonnateur et du poste comptable.

12

12

Mobilisation des agents du poste comptable :

Le comptable public peut constituer une équipe particulièrement dédiée au traitement des opérations de la collectivité attaquée ou nommer des référents en recettes et en dépenses qui feraient office de relais de l'encadrement au sein des équipes.

13

Mettre en place un mode dégradé en dépenses :

Afin d'éviter les incohérences, il convient d'échanger quotidiennement un tableau permettant le suivi du niveau de trésorerie et des crédits budgétaires.

- Utiliser ou adapter une maquette d'Ordre de Paiement (OP)
- Définir les PJ que l'ordonnateur est en capacité de fournir (a minima les factures et les RIB)

- Transmettre le tableau recensant les OP payés, ce qui permettra de régulariser les Comptes d'Imputation Provisoire (CIP) lorsque l'attaque sera maîtrisée.

- Éditer les OP qui seront validés par l'ordonnateur et visés par le comptable public.

14

14

Comptable

Ordonnateur

15

Déterminer un processus pour l'envoi des flux de paie, aide sociale :

Vérifier que la DSPL a bien informé GP1A de l'impossibilité pour la collectivité d'émettre les flux de paie. GP1A donne son accord par une lettre de couverture autorisant la duplication des fichiers de payes. Cette demande doit être reconduite chaque mois.

Si le flux de virement peut être correctement établi, définir une modalité de transfert vers Hélios (Cf Fiche 3)

16

Mettre en place une stratégie commune dans la gestion des recettes :

- Peuvent être encaissés sur des CIP, les recettes par virement ou avis de règlement et les recettes payées avant émission des titres.

- Les encaissements et le recouvrement contentieux sont maintenus de façon ordinaire.

16

17

Surveiller l'évolution de la trésorerie de la collectivité attaquée :

-L'encaissement des recettes étant de priorité inférieure dans ce contexte, il convient de prêter attention à l'évolution de la trésorerie et d'évaluer avec l'ordonnateur la pertinence de recourir à une ligne de trésorerie.

17

Constater la fin de l'attaque :

L'ordonnateur adresse un engagement écrit au comptable public affirmant que l'incident est terminé.

18

Comptable

20

Informez les équipes SI :

Transmettre le rapport au RSSI de la DGFIP (SI3) et attendre la confirmation de reprise possible des échanges

21

Réactivation des paramètres Hélios :

Réactiver les paramètres Hélios des flux aller

22

Réactivation des habilitations sous Madhras :

Réactiver les habilitations Madhras du personnel de la collectivité si elles ont été supprimées ou réinitialiser les mots de passe (après avoir remis les adresses mails ou de communiquer ces mots de passe par téléphone)

23

Pointage des balances éditées avant l'incident :

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

24

Examen des CCA pour les collectivités impactées :

Le comptable public lance des demandes d'édition de CCA sur Hélios pour relever les possibles incohérences comptables.

Ordonnateur

19

Transmettre un rapport sur l'état du SI :

Demander au prestataire un rapport sur la situation de la collectivité et le transmettre au comptable. Ce rapport détaille l'origine de l'incident et les actions de sécurisation entreprises par la collectivité.

25

Tester l'envoi d'un premier flux :

Envoyer un flux PES dépense et un flux PES recettes pour s'assurer de la bonne reprise des échanges via le Gxml.

SUIVI DES ACTIONS CYBER-ATTAQUES

6/7

Comptable

Ordonnateur

Régulariser les comptes d'imputation provisoire en dépense :
Produire les mandats de régularisation en exploitant les données de l'état « Liste des dépenses à régulariser ».

26

Comparer les données à l'aide d'éditions :
S'assurer de la correspondance des données des mandats avec les éditions demandées dans hélios des OP et des CIP à régulariser.

27

27

Être vigilant sur le typage des mandats :
Les mandats doivent être correctement typés « mandat émis après paiement » et doivent porter les références à la pièce de dépense (ordre de paiement).

28

28

Rassembler l'ensemble des pièces de régularisation des dépenses :
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 PEC, émarger manuellement les mandats avec les OP.

29

Apporter une attention particulière sur les mises en paiement :
Être particulièrement vigilant sur les mises en paiement afin d'éviter de payer des mandats qui auraient dû être émargés avec des OP.

30

30

SUIVI DES ACTIONS CYBER-ATTAQUES

7/7

Comptable

31

Régulariser les comptes d'imputation provisoire en recette :

Le comptable public transmet le détail des soldes des CIP aux services ordonnateurs afin que les titres correspondants soient émis.

32

Vérifier les crédits consommés :

L'ordonnateur et le comptable public s'ajustent sur les crédits consommés en dépense et en recette.

32

Ordonnateur

33

Restaurer les données de la collectivité :

Dans le cas où les données de l'ordonnateur ont été endommagées, et si nécessaire, demander au comptable la mise à disposition des flux transmis. La demande est transmise au bureau GP2B.