

QUE FAIRE PENDANT LA CYBER-ATTAQUE ?



« image : Freepik.com »

Que faire tant que l'attaque n'est pas traîtée ?

Le plan de continuité de l'activité (PCA) pour assurer la résilience face aux cyber-attaques doit être mis en œuvre. Il sera d'autant plus aisé d'assurer cette continuité de service que celle-ci aura été préparée entre les services ordinateurs et comptables.

Tout en assurant le paiement des fournisseurs et du personnel pour leur éviter des conséquences financières, cette période particulière reposant sur des mesures exceptionnelles du traitement des dépenses publiques, ne doit pas laisser place à l'absence de contrôles ou à la baisse de vigilance, bien au contraire.

La cyber-attaque, souvent liée au chiffrement des données et à la demande de rançon, peut également impliquer le vol de données, nécessitant une vigilance continue contre les fraudes et les faux virements, même après la reprise d'activité.

PLAN DE CONTINUITÉ D'ACTIVITÉ

ORGANISER LE TRAVAIL DU POSTE COMPTABLE

GÉRER LA PAYE

EXÉCUTER LES RECETTES

➤ ORGANISER LE TRAVAIL DU POSTE COMPTABLE

[Établir la situation comptable des budgets attaquées

Pour faciliter les contrôles sur les données Hélios et la reprise d'activité à l'issue de la période de crise, il convient d'éditer une balance, un état des restes à payer et un état des restes à recouvrer, arrêtés à la date du jour du piratage du système d'information pour l'ensemble des budgets de la collectivité ou de l'établissement concerné.

[Recevoir un premier diagnostic de l'ordonnateur

Dans la mesure du possible le comptable se fera communiquer un bilan de l'attaque sur le SI de l'ordonnateur : date de l'attaque, quels SI touchés (facturation, paie, ...), évaluation de la durée d'indisponibilité. Ce bilan peut être établi par le prestataire informatique de la collectivité ou par l'Agence nationale de la sécurité des systèmes d'information (ANSSI) (secretariat.anssi@ssi.gouv.fr).

La date de l'attaque a une importance vis-à-vis des décisions à prendre concernant les dépenses transmises au comptable et en attente de prise en charge et de paiement dans Hélios.

En fonction du diagnostic établi, le comptable et l'ordonnateur mettent en place une stratégie pour assurer la continuité de service.

Il s'agit de définir :

- quel canal de communication peut être utilisé sans risque (réseau téléphonique mobile, clé 4 ou 5G, ordinateurs sains basés en dehors du réseau attaqué)
- des adresses mails temporaires (des adresses peuvent être créées auprès de fournisseurs respectant la souveraineté numérique, Proton mail, La Poste.net ou encore en ayant recours à l'acquisition d'un nouveau nom de domaine). L'ordonnateur donnera la liste restreinte des interlocuteurs et adresses mails. Le but est que le comptable puisse être certain de l'identité des interlocuteurs lors des futurs échanges.

Les services de l'ordonnateur et du comptable doivent échanger quotidiennement pour avoir un état des lieux de la situation de l'attaque, connaître la priorisation des dépenses à payer en urgence par ordre de paiement ou encore transmettre la situation de trésorerie.

[Identifier les dépenses prioritaires

La mise en œuvre d'un fonctionnement dégradé impose de sélectionner les dépenses dont l'exécution ne peut pas attendre le traitement définitif de l'attaque. Cette sélection doit être réalisée en commun par l'ordonnateur et le comptable. Ce dernier contribue à éclairer la décision de l'ordonnateur en l'informant :

- des dépenses concernées notamment :
 - Payes, charges, prélèvements à la source ;
 - Échéances d'emprunt (débit d'office ou non) ;
 - Paiements de sommes importantes (marchés publics...) et/ou sensibles (fournisseurs de médicaments, dépenses stratégiques pour les budgets de sites industriels sensibles ...);
 - Paiement auprès de créanciers en situation financière délicate.
- de la situation de trésorerie.

[Créer des documents de suivi

Dans ce contexte particulier, le mode opératoire suivant peut être mis en œuvre :

- Échanger quotidiennement un tableau de suivi du niveau de trésorerie et des crédits budgétaires.
- Identifier précisément au sein des services ordonnateurs des personnes habilitées à transmettre des ordres de paiement au poste comptable et si possible identifier un référent en dépense au sein de la trésorerie.
- L'ordonnateur établira des ordres de paiement sur la base de la proposition de la maquette d'ordre de paiement (OP) jointe en annexe. Reprendre éventuellement une base de bordereau papier et indiquer sur le document papier de l'OP que le paiement est produit dans le cadre d'une cyberattaque ; Le comptable saisira les OP dans Hélios sur la base de ces informations.
- Définir les pièces justificatives que l'ordonnateur est en capacité de fournir (a minima les factures et les IBAN) au format papier ou via la messagerie mise en place à cet effet pour que le comptable puisse réaliser ses contrôles. Les pièces justificatives de la dépense devront quoi qu'il en soit être produites à l'appui des mandats de régularisation une fois la crise traitée.
- Le comptable transmettra le tableau recensant les OP payés (Hélios / Edition / Lancement Traitement / Liste des dépenses à régulariser en Pdf ou CSV) , 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.
- La cyberattaque devenue publique par voie de presse est une occasion pour d'autres escrocs opportunistes de réaliser des tentatives de détournement durant cette période de crise. La vigilance doit être accrue vis à vis de toutes les communications et demandes de changement d'IBAN.

> Gérer la paye

[Reconduire la paye du mois précédent

La direction départementale informe le bureau GP-1A d'une impossibilité pour la collectivité attaquée d'émettre des flux de paye. GP-1A donne alors son accord par une lettre de couverture autorisant la duplication des fichiers de payes. Cette demande doit être reconduite chaque mois pour chacun des budgets concernés.

La procédure de duplication des fichiers de paye prévue par le bureau GP-1A se déroule de la façon suivante : <http://nausicaadoc.appli.impots/2021/003459>

- Une fois le flux dupliqué : l'ordonnateur doit établir un OP avec le montant total à payer, dans la mesure du possible il convient de produire une liste des agents sortants pour lesquels il faut supprimer la paye ou la réduire ;
- Si le mois de payes répliqué était le mois au cours duquel la collectivité avait versé un régime indemnitaire, le comptable doit réduire manuellement chaque paye en fonction de l'état établi par l'ordonnateur ;
- Les nouveaux entrants sont payés par création d'OP manuels auxquels sont joints toutes les pièces justificatives attendues ;
- Pour les prélèvements fiscaux (PAS) et sociaux (URSSAF) : ne pas omettre de produire les DSN correspondantes si le même fichier de paye est réutilisé pour plusieurs mois. Il faut pendre contact avec le SIE compétent pour l'avertir de la situation et permettre les appariements (fichiers de déclaration/paiement). Les régularisations ne sont possibles que jusqu'au 31/12/N ;
- Si la collectivité suspend ses paiements aux organismes sociaux, elle doit les prévenir de sa situation et de l'interruption des paiements.

[Gérer la paye avec la paye liquidée pour le mois courant

La cyber-attaque peut ne pas avoir touchée le logiciel RH ou le logiciel RH peut être gérée hors du site attaqué ou être hébergée par un tiers (en mode Saas*).

Il est alors possible d'établir une liquidation des salaires à leurs justes valeurs pour le mois considéré. Le fichier des virements Paymen peut ainsi être établi pour transmission à Hélios. La transmission à Hélios : plusieurs hypothèses se présentent en fonction des établissements et collectivités concernées.

- Lorsque le logiciel RH et le TDT sont hébergés par le même éditeur en mode Saas, le fonctionnement est nominal, le fichier de virements peut être transmis à Hélios (bien que tous les paramétrages d'échanges PES soient suspendus).
- Le logiciel RH est externalisé mais la collectivité n'a pas recours à un TDT ou bien celui-ci n'est pas hébergé par le même éditeur. Il faut donc pouvoir assurer le transfert du flux vers Hélios par une autre modalité.
 - Il peut s'agir d'un transfert du flux via le PIGP et la passerelle de transmission à la condition qu'un utilisateur de la collectivité ait de tels droits. A défaut, il est possible de demander de tels droits pour une personne en établissement une fiche navette. Le poste initialise une fiche navette avec son ordonnateur. Il effectue la saisie dans Aspasia et Madhras, puis il envoie la fiche navette au SIL ou à la cellule PIGP selon le département (La durée de traitement est à J+1 de la saisie du SIL pour les flux Hopayra et PES V2). Le transfert du fichier de virements doit être opéré à partir d'un ordinateur hors du réseau attaqué. Cf lien dans l'encadré « Documentation »)
 - A défaut et en cas d'urgence, les modalités de transfert du flux sont à voir avec le niveau national (Cf boucle des destinataires de la déclaration de l'attaque). Le poste comptable transmettra un jeton « Escale » à la personne de confiance sur une adresse mail saine pour la récupération du fichier Paymen. Après accord du niveau national, le poste sera invité à transmettre le fichier pour injection dans Hélios. Il faut noter qu'une injection de flux à J ne donne accès aux données dans Hélios qu'à J+1 (si J est un vendredi, les données seront disponibles à J+3, soit le lundi).

[Gérer les autres dépenses par flux Paymen

Les modes opératoires de la paye sont applicables autres dépenses payées par flux Paymen, notamment les dépenses d'aides sociales, APA, bourses etc

DÉFINITION

- **Le SaaS**, ou Logiciel en tant que Service, est un modèle de distribution de logiciel via internet. Ce modèle repose sur la technologie cloud permettant l'externalisation du système d'information. Le principe est d'accéder au logiciel sous forme de services délivrés via internet.
- Un logiciel **On-Premise ou Instancié** nécessite l'installation d'un « software » sur les postes de travail et l'achat du logiciel ou de licences. C'est un logiciel installé et hébergé dans l'environnement technique de la collectivité utilisatrice.

> Exécuter les recettes

[Assurer les recettes

En cas de cyber-attaque, la première préoccupation est d'assurer les dépenses par le traitement d'ordres de paiement.

La gestion des recettes n'intervient que dans un second temps, pourtant elle est essentielle pour assurer la trésorerie de la structure. De plus, liquider les recettes au plus proche du fait générateur est gage du bon recouvrement. Toutefois il n'existe pas dans le domaine recette de possibilité d'émettre des pièces à l'initiative du comptable : des ordres de recettes.

En effet, ces pièces comptables n'ont pas de caractère exécutoire.

Mais les recettes parvenant au SGC pour le compte du budget sont toujours comptabilisées :

- les recettes par virement ou avis de règlement ainsi que les recettes payées avant émission de titres sont encaissées sur des Comptes d'Imputation Provisoire (CIP).
- les encaissements et le recouvrement contentieux sont maintenus de façon ordinaire.

Pour un SPIC (REOMI, eau et assainissement) : le point des recettes est très sensible. La structure des recettes de ces entités est très liée aux recettes d'activité. L'impact des dotations est moins important que pour les collectivités territoriales (communes, départements, régions ou EPS...). Le retard à rattraper peut-être long et volumineux. L'impact sur la trésorerie doit faire l'objet d'une attention particulière.

[Les recettes par voie de rôles (ORMC)

La cyber-attaque peut ne pas avoir affecté le ou les logiciel(s) de facturation émetteurs d'ORMC, ou ceux ci sont hébergés en extérieur (Mode Saas*). Dès lors que l'ordonnateur a l'assurance de pouvoir émettre des fichiers sains, il est possible d'envisager un envoi à Hélios pour intégration, après échange avec le niveau national pour accord.

Cette procédure est d'autant plus privilégiée lorsque les flux ORMC portent des prélèvements sur les comptes bancaires des usagers.

Pour cela, il est nécessaire de rétablir le paramétrage des flux pour les seuls ORMC.

> Exécuter les recettes

[Les régies de recette

Les régies de recette peuvent ne plus fonctionner pendant l'attaque et le régisseur se verra momentanément retirer ses habilitations au compte DFTNet.

Ainsi, afin que ses espèces puissent être encaissées par la collectivité, il devra se rapprocher de son service teneur de compte pour lui adresser des ordres de virement dit "papier", dans la mesure où le comptable n'est pas habilité à mouvementer le compte DFT.

Par ailleurs, dans une telle situation, une information continue du service DFT en direction est à mettre en place, afin qu'il soit en mesure de suivre les opérations qui transitent sur le compte et de procéder au rétablissement ou non des accès aux comptes concernés selon l'analyse et l'ampleur de l'attaque.

[Gérer la trésorerie de la collectivité attaquée

Le paiement des dépenses, combiné à une absence d'émission de titres de recette et par conséquent un recouvrement moindre de recettes, implique de prêter une attention particulière sur l'évolution de la trésorerie et d'évaluer avec l'ordonnateur la pertinence de recourir à une ligne de trésorerie.

Pour informer l'ordonnateur sur le suivi de trésorerie, il est possible de transmettre la C5 par mail.

DOCUMENTATION

- Suivi de trésorerie : Édition / Lancement Traitement / domaine compta : la C5
- Suivi des crédits budgétaires : État de développement des soldes
- Modèle d'Ordre de Paiement,
- Tableau récapitulatif des OP, Edition / Lancement Traitement / domaine compta, Liste des dépenses à régulariser
- Tableau de bord « Suivi des actions Cyber Attaque ».
- Lien vers le circuit de la fiche navette <http://nausicaadoc.appli.impots/2020/009818>
- Lien vers la fiche navette <http://nausicaadoc.appli.impots/2020/009817>