

Cybercriminalité

Sensibiliser et prévoir

La Cybercriminalité

A

Les victimes des cyberattaques

B

Les textes et obligations

C

La DGFiP, acteur et partenaire

D

Communiquer auprès des ordonnateurs

E

La reprise d'activité

Les types de collectivités victimes

Toutes les collectivités et les établissements publics de santé sont des cibles potentielles, quelle que soit la taille : commune rurale, très grande commune urbaine, conseil départemental, conseil régional ;

Ça n'arrive pas qu'aux autres. **La question n'est plus de savoir si vous allez être victime ou non d'une cyberattaque mais quand** et comment s'en protéger ;

Toutefois selon l'enquête de cybermalveillance.gouv.fr, **les communes et EPCI de moins de 25 000 hab sont les plus touchées.**

Notre constat, les collectivités et établissements publics locaux touchés ont tous des **logiciels** de GF, facturation et RH **opérés localement.**

Quels sont les chiffres ?

Proportionnellement, les collectivités et établissements publics locaux sont plus attaqués que les entreprises. Le site Cybermalveillance.gouv.fr a assisté 1 entreprise en 2022, 34 collectivités l'ont été proportionnellement ;

La DGFIP dénombre une **moyenne de 10 signalements par mois** et recense des d'attaques par vagues.

L'objectif des attaques est d'obtenir le **paiement d'une rançon** mais aussi de **générer une déstabilisation** générale. La **recrudescence des attaques dans les mois prochains** est un risque annoncé et fort ;

Les **impacts** d'une attaque sont **plus ou moins conséquents en fonction de la taille de la collectivité** ; une petite collectivité pourra redémarrer plus rapidement qu'une structure conséquente, en raison de la complexité du SI, et cela malgré des moyens supérieurs.

Les obligations faites aux collectivités

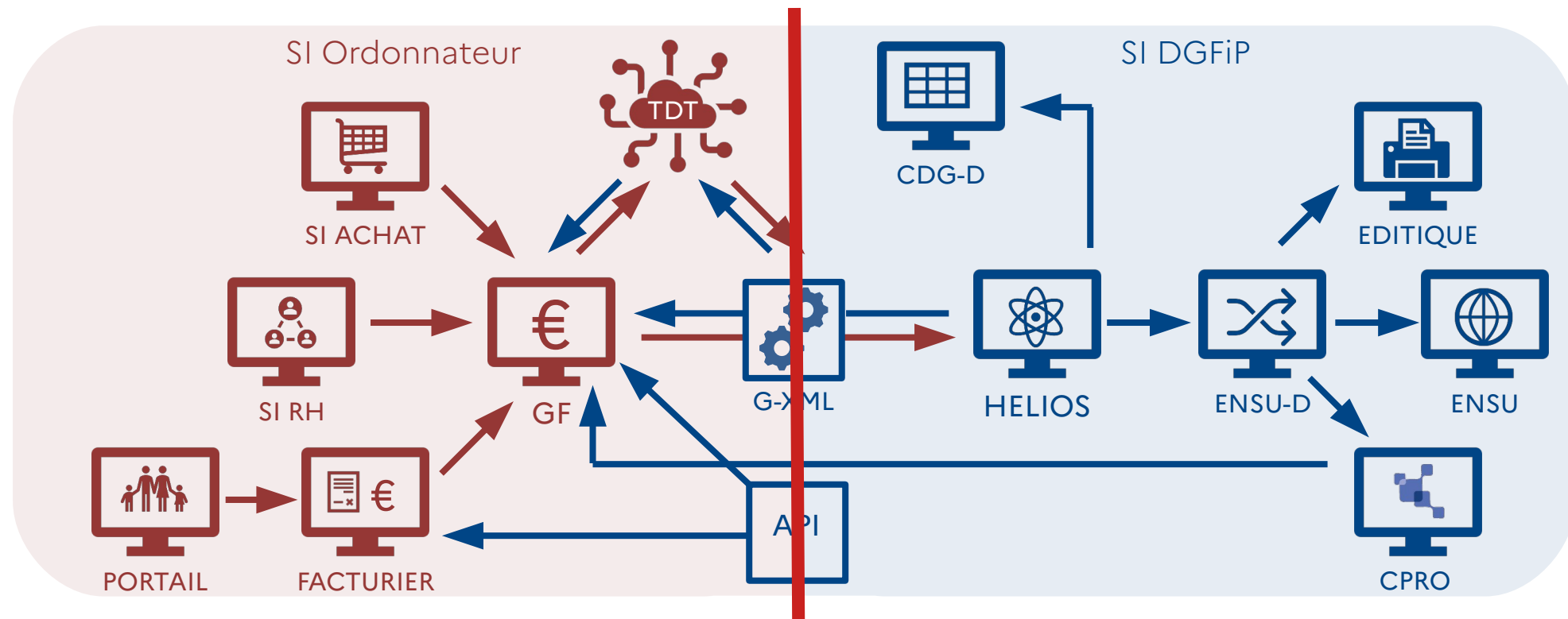
Dans le **Règlement Général de Sécurité (RGS)** :

- Homologation de sécurité du téléservice, **conduire une analyse de risques et définition des mesures de sécurité adaptées aux enjeux et aux menaces** (Classification des informations sensibles, Mise en place de mesures de sécurité adaptées à la classification), Suivi opérationnel et amélioration continue, **Gestion des incidents** de sécurité, **Sécurisation des échanges** électroniques.

Dans le **Règlement Général sur la Protection des Données (RGPD)** :

- Protection des données personnelles du personnel et de mes administrés. Identification et documentation des données personnelles traitées, **Mesures de sécurité appropriées pour protéger les données et notification des violations** de données à l'autorité de contrôle.

Rompre les échanges ordonnateur - comptable



Pourquoi la DGFiP se positionne sur ce sujet ?

Le nombre des attaques à l'encontre des collectivités et établissements publics locaux n'a cessé de croître, impactant de plus en plus les comptaibles publics.

Afin de couper tous les risques, il est nécessaire d'**isoler le SI de la DGFiP** ;

Le constat a été fait que **les comptaibles sont non identifiés** dans toutes les documentations cybersécurité à destination des collectivités. **Pourtant le comptable public est un partenaire à prévenir** ;

Les comptaibles, eux mêmes dépourvus, **devaient être plus sensibilisés, mieux documentés**, mieux informés, avec une amélioration des process ;

La DGFiP, au travers d'**API**, expose des données aux collectivités qui doivent respecter les obligations de sécurité informatique. **La DGFiP vérifie le respect de ces obligations**.

Pourquoi la DGFIP se positionne sur ce sujet ?

Les cyber-attaques ont de nombreux **effets collatéraux sur les missions du comptable**. Celui-ci ne reçoit plus de données numériques de l'ordonnateur ; il est cependant nécessaire d'**assurer la continuité de service notamment avec les dépenses urgentes**.

Il est donc important de sensibiliser nos partenaires collectivités et établissements publics de santé sur les effets de telles attaques.

La première des dépenses urgentes est celle **des rémunérations des personnels** de la collectivité, les charges et autres obligations.

L'ordonnateur **devra prioriser les dépenses**. La priorité n'est pas nécessairement le montant, mais plus la **sensibilité de la dépense** (en fonction de sa nature) **ou celle de l'entreprise** (la mise en difficulté d'une entreprise en cas d'absence de paiement).

Pourquoi la DGFIP se positionne sur ce sujet ?

Les **dépenses** obligatoires et urgentes devront être payées par **Ordre de Paiement**.
Les modalités de paiement des **rémunérations** seront à déterminer en **fonction du périmètre de l'attaque subie**.

Les dépenses et Recettes sont réalisées dans des **conditions dégradées** ;

La régularisation des opérations comptables est longue et les **risques de doubles paiements sont forts**. Toutes les pièces comptables devront être correctement typées avec référencement aux OP.

Les recettes ne font plus l'objet de titres, ce qui peut générer des soucis de trésorerie, des soucis de liquidation des recettes, d'impayés des usagers, les sommes demandées étant plus importantes en rattrapage et le recouvrement éloigné du fait générateur.

Sensibiliser et prévoir

Le risque zéro n'existe pas, malgré toutes les précautions et respects des règles de sécurité.

Il faut rappeler la nécessité de **sauvegarder** (isoler les sauvegardes et les vérifier)

Mais il faut aussi **anticiper la création d'une cellule de crise** si le risque devait survenir.

Un plan de continuité de l'activité doit être élaboré. Il faut dresser les processus métier et définir une analyse des risques pour chacun en fonction de la durée de la crise.

Le **serveur mail est corrompu**, quelle solution externe est envisagée ? Qui a droit d'échanger avec le comptable, à partir de quel fournisseur, quelle normalisation des adresses mails pour "identifier" mes interlocuteurs ?

Le **serveur de téléphonie ToiP** est corrompu. Comment communiquer ? Identification des personnes, et numéro de portable ?

Sensibiliser et prévoir

La GF est corrompue : Il faut prioriser les dépenses urgentes, puis je transmettre des pièces à mon comptable ?

La RH est corrompue, le périmètre du personnel de la collectivité est très fluctuant (nombreuses vacations par exemple). Quelles conséquences ?

La RH est externalisée, et est en capacité de réaliser une liquidation au juste prix. Puis je assurer le juste paiement ? Qu'en est il du respect des obligations de paiement des charges et obligations fiscales (PAS) ?

L'ANSSI propose **des exercices à destination des collectivités**. Il faut s'entraîner pour mieux se protéger et réagir. Le comptable peut être associé et cela peut être inclus au travers des **conventions signées** entre la collectivité et le SGC.

La reprise des échanges ordo-comptable ?

Les **échanges PES V2 sont interrompus** dès réception de l'information de la cyber-attaque.

La reprise des échanges n'est **pas à la main du comptable**.

Une reprise des échanges est soumise à **validation du RSSI de la DGFIP**.

Le RSSI attend une **analyse Forensique** (date de compromission et conditions) ainsi que le **détail des mesures correctrices prises**.

Merci de votre attention