CPAS DE COURCELLES – Victime Ransomware

Plateforme des DPD – 29.03.2022

PREVOST Laurence – Directrice générale
GIANNONE Giovanna – Responsable RH
DHENIN Amandine – Juriste & DPO

Préambule

Il faut savoir que :

- Le CPAS ne pensait pas être victime (aussi rapidement) d'un ransomware car la politique informatique interne depuis plus de 10 ans met au centre des intérêts : **LA SECURITE !** Parfois même au détriment d'habitudes plus pratiques qui auraient permis de faciliter le travail des agents.
  - Ex : Accès full internet pour uniquement quelques agents sur demande motivée ; aucune clé USB ; …
- Dès 2018, le CPAS a pris à cœur les obligations liées au RGPD et a mis en œuvre (et continue à mettre en oeuvre) toute une série de mesures afin de s'y conformer du mieux possible
  - Ex : Plusieurs documents et procédures écrites (Charte informatique ; Gestion des incidents ; etc.) et désignation d'un DPO (d'abord externe, ensuite interne).

Introduction

- Ransomware survenu le 13 juillet 2021
- Contexte difficile
  - Inondations (> retard assurance + CIVADIS sous eaux + autres organismes sollicités)
  - Vacances annuelles (dont D.G.)
  - Pandémie (télétravail + maladie/quarantaine)
- DPO externe (mais relai interne)
  - En vacances (> DPO « f.f »)
- Journalisation de l'évènement très importante

- /!\ **Journalisation de l'incident** /!\
  - Tableau (feu tricolore) > Exemples disparates :

N°	Date	Heure	Action/Constat	Pers. Réf.	Doc.
1.0	13/07	7H30	1) Imprimantes connectées au réseau : impressions suspectes + messages d'erreur 2) Accès au serveur bloqués (plus de connexion à distance, ni en présentiel)	DPO adjoint	Photos
29.0	19/07	8H00	1) Nettoyage PC DG f.f. 2) Mise à disposition d'une connexion par câble sécurisée (DG f.f.) 3) Mise à disposition d'une imprimante (DG f.f.)	DPO adjoint	/
34.0	22/07	16H	1) Quelques PC internes sont rendus « safe » aux agents (mail, nv réseau opérationnel, suite office)	DPO adjoint	/

- Phase critique (conséquences directes du ransomware)
- Phase de continuité (assurer un travail minimum dans des conditions et avec des méthodes particulières)
- Phase de restauration (reprendre le travail dans des conditions normales)

Description – étape par étape

Le jour J : 13/07

- **Divers constats** :
  - Les imprimantes connectées au réseau ont sorti des documents avec des smileys et signes de ponctuation + elles affichent un message d'erreur.
  - Le personnel en présentiel, ainsi qu'en télétravail n'a plus eu accès au serveur, ni aux logiciels.
  - Les 4 serveurs sont cryptés (plus tard dans la journée)
    - L'analyse se poursuit sur les 2 serveurs Linux

Le jour J : 13/07 (suite)

- **Diverses actions :**
  - Contacts avec divers membres du personnel
    - Responsable IT
    - DF
    - DPO
    - DG f.f. (+ DG en congé, + tard dans la journée)
    - Présidente
  - Avertissements auprès des membres du personnel + ordre d'éteindre/débrancher tous les PC et matériels connectés
    - *Rem. : communication très chaotique en pratique.*
  - Procédure de paiements urgents mise en place (RIS ; AS ; Salaires ; Secours)
  - Mise en place d'une cellule de crise
    - IT
    - DG f.f. + Présidente
    - DPO adjoint + DPO
  - Notification à l'APD [début]
    - *Rem. : en pratique, pas facile car pas assez d'infos concernant l'incident à déclarer (impact, étendue?). Formulaire inapproprié.*

Le jour J : 13/07 (suite et fin)

- **Diverses actions (suite et fin) :**
  - Investigations IT
    - Comment? À cause de quoi ? Ampleur ?
  - Début du nettoyage des PC
  - Maintien du CSSS du 13/07

Le lendemain : 14/07

- **Diverses actions :**
  - Signalement au CERT
  - Notification APD (fin) (mandat au DPO car aucun accès à internet)
  - Démarches pour PC « safe » en prêt
  - Communication du CPAS -> Mise en place de numéros d'urgence
  - Communiqué de presse (Présidente) -> suite à une fuite …
  - Utilisation de PC/GSM/Mails personnels

Les jours suivants: 15/07

- **Diverses actions :**
  - Mise en place d'une réunion interservices
    - Présidente + DG f.f.
    - 1 représentant de chaque service
    - But :
      - Point sur la situation
      - Liste de priorité pour le nettoyage des PC
      - Décisions relatives à la continuité des services
        - urgences
        - min. 1 agent/service en présentiel (Dispense de service pour les autres agents)
        - Suppression du télétravail
      - Annulation BP du 20/07 mais maintien BP 30/07 + CAS du 26/07
      - Boite mail générale du CPAS : réponse automatique « Joindre uniquement par téléphone ».
  - Plainte déposée auprès de la police
  - Rapatriement physique de tous les PC auprès du service IT -> pour nettoyage
  - Contacter certains organismes (pour les subsides notamment)
    - UVCW
    - FEDASIL
    - SPPIS
    - CPAS Charleroi
    - Fédération Wallonie-Bruxelles

Les jours suivants: 16/07

- **Diverses actions :**
  - Communiqué papier interne (via les bacs à courrier -> point sur la situation + n° d'urgence mis en place)
  - Communiqué de presse n°2
  - Début de la rédaction de la journalisation de l'incident

Les jours suivants: 19/07

- Diverses actions :
  - Entraide entre services et agents (ex : transfert temporaire d'agent pour renforcer les services critiques + échange de documents)
  - PC DG f.f. lui est rendu safe (+ Câble Ethernet - réseau externe ; + imprimante d'appoint copie/scan/impression via câble USB)
  - Dispatching de petites imprimantes d'appoint dans différents services critiques (copie/scan/impression)
  - Adresse mail générale du CPAS est à nouveau opérationnelle
  - La fonction copie des imprimantes professionnelles est disponible (1 imprimante/service)
  - Etablissement d'une liste de distribution des PC safe en location

Les jours suivants: 20/07

- **Action :**
  - **Mise en place de 2 PC safe au service IT pour tout le personnel (Accès aux mails + impression + internet)**

Les jours suivants: 22/07

- Diverses actions :
  - Régénération partielle de documents de paiements (grâce à Belfius)
  - Certains PC nettoyés sont rendus safe aux agents (email ; nouveau réseau ; suite Office)
    - 8 PC

Les jours suivants: 23/07

- Diverses actions :
  - Mise en place d'une réunion interservices
    - Suppression des dispenses de service
    - Liste de priorisation des applicatifs à remettre en route
    - Prévenir les gens pour les retards dans les facturations (SAFA/IDESS)
  - Distribution des PC loués
    - 19 PC
  - Connexion internet (via câble) dans les boxes de permanences sociales
  - Mise au point d'une procédure temporaire pour les commandes et pour les factures d'hébergement
  - Récupération totale des données de GESDOS
  - Notification de l'incident à la BCSSS

Les jours suivants: 26/07

- **Action:**
  - **Récupération acropole salaire (applicatif + données)**
  - **Récupération acropole compta (applicatif + données)**
  - **Récupération Bureautique (applicatif + données)**

Les jours suivants: d'août à nos jours (début)

- Récupération des données jusqu'à 2017
  - Aucune récupération de données postérieures à 2017 sur le serveur.
- Récupération intégrale des données contenues dans les applicatifs civadis.
  - Aucune récupération des données liées aux autres applicatifs (3P, maison de repos, …).
- Réinstallation progressive des divers programmes (Salto, 3P, Corilus, Copieurs, Pointeuse, …)
  - Avec à la clé à chaque fois des devis et des délais
- Tous les membres du personnel ont récupéré un PC safe (fin location des PC en août) avec accès internet, mail, nouveau réseau et applicatifs utiles.
- Reconstitution de nombreux dossiers/documents en version électronique toujours en cours + alimentation en données du nouveau réseau (mise à jour des divers accès aux fichiers partagés).
- La connexion RDS à distance est réinstallée fin octobre ; Télétravail possible mi-novembre
- Le retard accumulé par les différents services n'est toujours pas rattrapé.
- Toujours aucun retour de l'APD …
- Contact avec assureur Ethias > **N'a pas encore rendu sa décision**
  - Le CPAS n'a pas souscrit à l'« Ethias CyberProtection »
  - Mais souscription à l'assurance « Tous risques – informatique » > Garantit risque de malveillance
    - Prise en charge **potentielle** de reconstitution de l'information
    - Prise en charge **potentielle** de la location de matériel
    - Normalement, non prise en charge des honoraires du DPO

Les jours suivants: d'août à nos jours (suite et fin)

- **La maison de repos est le service le plus touché** : impossible de récupérer les données contenues sur l'applicatif utilisé au quotidien là bas
  - Concerne : MR ; MRS ; Centre de Jour et Résidence-services
  - Très dangereux en pratique car contient le régime alimentaire, les médicamentations etc. des résidants.
  - Aucune facturation n'était plus possible > Encoder facture par facture une fois l'applicatif réinitialisé
  - Les horaires du personnel soignant n'étaient plus disponibles
  - Situation apaisée depuis **fin 01/2022.**

Constats – Journalisation

Constats

- Du 13/07 au 16/07
  - -> phase critique majoritaire
  - -> amorçage de la phase de continuité
  - -> quasi inexistence de la phase de restauration
- A partir du 19/07
  - -> Phase de continuité majoritaire
  - -> Accroissement de la phase de restauration
  - -> Quasi-disparition de la phase critique

Constats – Tirer des leçons de nos erreurs

- Avoir du matériel IT « SAFE » de stock
  - PC (min. 1/service + direction) configuré pour travailler en cas d'urgence
  - Câbles Ethernet
  - Imprimantes (copie/scan/impression)
- Avoir plusieurs listings
  - Listing numéros des agents à contacter (avec priorisation)
  - Listing papier avec priorisation des personnes/services/activités -> Par exemple pour le nettoyage PC
- Prévoir un doublon du responsable du service IT
- Prévoir des notes internes-types disponibles sur clé USB
  - Ex : Procédure paiement urgent, émission de facture, etc.
- Commencer la journalisation dès le 1e constat
- Vérifier le formulaire APD (est-il à jour ?)
- Sensibilisation du personnel > Un agent est la cause qui a rendu possible le ransomware

To do list – Récapitulative

- 1. Ordonner l'arrêt des traitements IT + le débranchement des appareils connectés au réseau
  - -> Communiquer l'information à tous les agents
- 1bis. Commencer les investigations
- 2. Réunion de crise + fréquence des réunions ultérieures si nécessaire
  - Mettre en place toutes les procédures d'urgence prévues en amont
- 3. Procéder au nettoyage des PC/restauration données etc.
- 3bis. Notifications
  - Police
  - Assurance
  - APD
  - CERT
  - nomoreransom
  - Organismes utiles (ex : SPP IS / BCSS / UVCW / …)
- 4. Communication externe « contrôlée »

Conclusion

- Le CPAS a travaillé pendant plusieurs jours « à l'ancienne »
  - Pas de PC (sauf PC personnel de certains agents mais pas toujours de suite office)
  - Pas d'accès aux mails
  - Pas de téléphone fixe (assez vite résolu)
  - Pas d'imprimante > Faire les notifications des décisions du Comité (CSSS) **à la main** !
  - Pas d'accès à Internet
  - Pas d'accès aux applicatifs utiles au quotidien
  - Plus aucun document numérisé …
- 2 constats importants :
  - Le retour à la normale prend du temps
  - Le retour à la normale coûte de l'argent
- Pas prêts … mais on espère que cela nous a servi et qu'à vous aussi.