CYBERATTAQUE

AU SEIN D'UN POUVOIR LOCAL

JUDITH DUCHÊNE
Conseillère

Effet collatéral de la pandémie et de l'utilisation encore plus massive des technologies de l'information, le nombre de cyberattaques en Belgique n'a cessé d'augmenter ces derniers mois. Les administrations publiques et le secteur des soins de santé sont particulièrement ciblés.

Contexte

Sur le terrain, au sein d'un pouvoir local, comment se passe une cyberattaque ? Quelles sont les premières actions à entreprendre ? Comment gérer l'urgence et la continuité des services ? Comment assurer la communication vers les agents ? Vers l'extérieur ? Vers les usagers ?

Lors de la Plateforme des DPD de CPAS du 19 mars dernier, nous avons demandé à deux administrations locales qui ont été récemment piratées - le CPAS de Courcelles[1] et la Ville de Liège[2] - de venir partager leurs expériences.

Dans cet article, sur base de leurs interventions, nous reprendrons les actions de court/moyen/long termes qu'elles ont dû entreprendre, ainsi qu'une réflexion critique par rapport à celles-ci et aux ressources qui peuvent être mobilisées en pareille circonstance.

Nous espérons, en partant d'exemples concrets et « parlants », contribuer à mieux faire comprendre aux CPAS les risques encourus et les préparer à parer au mieux aux menaces dont ils peuvent être la cible.

Caractéristiques des cyberattaques concernées

Tant à Courcelles qu'à Liège, les cyberattaques se sont déroulées en plusieurs phases.

- Vol d'identité d'un utilisateur légal permettant à l'attaquant d'obtenir un accès à distance. Pour ce faire, l'attaquant peut utiliser plusieurs moyens. Le plus courant est le phishing qui consiste à voler le mot de passe d'un utilisateur légal.
- Accès au système et travail de reconnaissance. L'attaquant va essayer de découvrir la façon dont le réseau est organisé et surtout y élever ses privilèges, c'est-à-dire devenir administrateur d'une ou plusieurs machines et, à partir de là, se propager.
- Mouvement latéral et exfiltration de données. L'attaquant va répandre l'attaque dans le réseau ciblé et attaquer l'ensemble des systèmes qui pourraient contrevenir à l'attaque (antivirus par exemple). C'est seulement dans cette phase que l'on découvre la partie visible de l'attaque : le ransomware qui va paralyser les ordinateurs et, éventuellement, crypter les données.

Les attaquants se réservent des portes d'accès aux systèmes attaqués pour contrer les éventuelles mesures de restauration qui seraient prises par l'institution.

Vraisemblablement, les attaquants sont déjà bien présents avant le déclenchement de l'attaque, ce qui peut expliquer que celle-ci se passe pendant la nuit, à un moment où il n'y a pas d'activité, afin de minimiser le risque de réponse face à l'incident. Les institutions locales n'étant pas en capacité d'assurer des gardes continues 7 jours/7 et 24h/24h pour surveiller les systèmes, cela les rend plus vulnérables à ce type de menace.

Manifestations concrètes et conséquences

Dans le cas des témoignages concernés, les manifestations concrètes de l'attaque ont pris les formes suivantes[3] :

- indisponibilité de certains systèmes et présence d'erreurs dans le comportement de plusieurs services ;
- dépôt d'un message sur les ordinateurs avec la marche à suivre pour les débloquer ;
- prise d'accès et chiffrement à distance ;

[1] Laurence Prévost, Directrice générale ; Giovanna Giannone, Responsable RH ; Amandine Dhenin, Juriste et DPD.

[2] Danielle Adriaenssens, Directrice en Chef - Audit et qualité - DPD ; Benoit Joseph, Directeur du DSI.

[3] Celles-ci n'étant pas cumulatives.

- incapacité à utiliser son propre ordinateur et les applicatifs ;
- impressions qui sortent des imprimantes pendant la nuit, avec des smileys et des symboles ;
- plus d'accès au serveur, ni aux téléphones.

Premières réactions

Faire le constat de l'attaque informatique est généralement assez rapide et la réactivité par rapport aux problèmes est un élément déterminant dans la prise en charge.

Éteindre tous les appareils liés au serveur

Il s'agit de la première action à entreprendre dès le constat de l'attaque. Dans une grande administration qui comprend plusieurs bâtiments administratifs, salles de machines, salles de serveurs, l'arrêt d'urgence de tous les systèmes ne se met pas en place si rapidement en raison notamment de la difficulté à faire circuler l'information.

Faire circuler l'information en interne

Sans ordinateurs et téléphones fonctionnels, faire circuler l'information, aussi bien aux agents sur place qu'aux agents qui travaillent dans d'autres implantations et à ceux qui télétravaillent, est un véritable défi.

Dans les cas présentés, cela s'est fait :

- en communiquant prioritairement vers le président/directeur général (DG)/directeur financier (DF)/délégué à la protection des données (DPD) / DPD adjoint/responsable IT ;
- en communiquant prioritairement vers les « référents informatiques » qui sont des utilisateurs de référence pour le service informatique dans les différents départements ;
- en passant des appels, sur base des numéros privés des agents connus par chacun(e) et par les secrétariats ;
- par un message sur la boite mail privée des agents ;
- par l'utilisation d'une application de communication collaborative (ex. : Teams…).

Mettre en place une procédure de paiements urgents (RIS, aides sociales, salaires, secours)

Commencer à journaliser l'incident

La journalisation de l'incident est intéressante à mettre en place dès les premières heures. Il s'agit concrètement de répertorier dans un tableau les actions entreprises (date/heure/action - constat/personne de référence de l'action/documentation de l'action) et de les classer.

Ce tableau permet de répertorier les actions dans un premier temps mais également, par la suite, de prendre un certain recul, d'identifier là où les choses pourraient être améliorées si un tel incident devait se reproduire.

Au CPAS de Courcelles, les actions entreprises ont été classées de la manière suivante :

➔ 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)

N°	Date	Heure	Action/Constat	Pers. Réf.	Doc.
1.0	13 / 07	personne	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	personne	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	/

Mettre en place une cellule de crise

La cellule de crise réunit les personnes les plus impliquées dans le fonctionnement du CPAS. Elle permet de faire le point sur la situation et de planifier l'ordre dans lequel les différentes urgences doivent être traitées.

Ouvrir un sinistre auprès de l'assurance

Pour les institutions qui sont couvertes par une assurance « cyber risques », une déclaration de sinistre doit être faite.

Le risque est généralement couvert sur base d'un audit préalable qui doit pouvoir attester d'un niveau de sécurité au minimum satisfaisant.

Une fois prévenue et selon les modalités contractuelles, la compagnie d'assurance peut dépêcher sur place une équipe d'experts le jour même afin de déterminer les premières actions techniques ; notamment la vérification que l'attaquant n'ait plus accès aux systèmes en vue de pouvoir commencer la partie « réparation/restauration » en repartant sur des bases les plus saines possibles.

Débuter la procédure de notification à l'APD

Dans les 72 heures de la prise de connaissance d'une fuite de données, le responsable du traitement doit en informer l'Autorité de Protection des Données (APD) par le biais d'un formulaire en ligne.

Les deux pouvoirs locaux concernés ont éprouvé de nombreuses difficultés à le faire, pour plusieurs raisons :

difficulté pratique de remplir un formulaire en ligne sans disposer d'un ordinateur et d'une connexion internet fonctionnelle ;

difficulté de déclarer l'incident à temps alors que les informations arrivent au compte-goutte et qu'il est impossible de cerner immédiatement l'ampleur du problème (identification des données touchées, nombre de personnes touchées, durée de l'indisponibilité, description des actions/décisions prises…) ;

la mobilisation des services (et notamment de l'ICT) est plutôt orientée sur le rétablissement des activités.

Les pouvoirs locaux concernés n'ont reçu aucun retour de l'APD à la suite de leur déclaration.

Déposer une plainte auprès de la police locale et signaler l'incident au CERT[4]

[4] CERT = Federal Cyber Emergency Team.

En cas d'incident de sécurité, une plainte peut être déposée auprès de la police locale. Celle-ci pourra ensuite transférer l'information auprès des autorités de police compétentes : la Federal Computer Crime Unit (FCCU) ou la Regional Computer Crime Unit (RCCU).

Le CERT met également à disposition, sur son site, un formulaire destiné à signaler un incident, à demander de recevoir de l'aide en cas d'incident, à transmettre un message de phishing[5].

Ces démarches ont été faites par le CPAS de Courcelles et la Ville de Liège mais elles n'ont pas abouti à un suivi de la part des institutions concernées.

Actions pour rétablir la continuité

Assurer une communication claire vers l'extérieur

Lorsqu'une institution vit ce type d'incident, la rapidité et la maîtrise de la communication est vraiment essentielle car, souvent, des fuites surviennent et la presse interpelle.

Les informations divulguées publiquement (par exemple par voie de communiqué de presse ou d'une conférence de presse) se doivent d'être précises et basées sur les informations émanant des personnes compétentes.

La manière dont le service aux citoyens va pouvoir être assuré à court terme doit être précisée.

Réunir les services et réorganiser le travail

Rapidement, il est nécessaire de réunir les services pour faire un point général de la situation et que chacun(e) puisse savoir ce qui s'est exactement passé.

Une liste des priorités doit être établie pour déterminer :

- les services pour lesquels il y a une décision de continuité de service ;
- les services pour lesquels il y a une dispense de service ;
- les obligations légales qui doivent continuer à être assurées ;
- les réunions qui doivent être organisées/celles qui peuvent être reportées ou supprimées.

Concomitamment, le télétravail est supprimé puisqu'il n'est plus possible de se connecter à distance.

Des PC peuvent être loués afin de pouvoir continuer, autant que faire se peut, à faire fonctionner le CPAS (permanences sociales, procédure temporaire pour les commandes/factures…).

Rapatrier les PC vers le service IT

Rapatrier les PC au service IT pour qu'ils puissent être testés et, éventuellement, réinstallés.

Établir la liste des PC prioritaires en fonction des priorités déterminées pour la reprise des services et la réorganisation du travail.

Faire réinstaller les applicatifs par les sociétés informatiques

Avertir les institutions partenaires

Les institutions avec lesquelles le CPAS est en contact régulier doivent être averties, ainsi que les institutions subsidiantes.

Quelques effets directs (potentiels) d'une cyberattaque sur l'organisation

- Certaines données peuvent être perdues à tout jamais.
- Erreurs dans les tâches liées à la continuité de service, dues à l'indisponibilité des données et au fait de devoir les encoder manuellement.
- Épreuve difficile pour les agents, les autorités et la hiérarchie.
- Perte de documents modèles : modèles de délibération, de notification, cahiers des charges…
- Prise de retard de plusieurs mois dans le travail dû à la restauration progressive du matériel, des applicatifs…
- Risque de fuites dans la presse à propos de l'évènement.
- Incertitude sur ce qui sera couvert ou pas par l'assurance.
- Risque de donner une image négative de l'institution et de la protection qu'elle assure vis-à-vis des données à caractère personnel qu'elle traite.

Comment se préparer au mieux?

Aucun pouvoir local n'est à l'abri d'une cyberattaque.

Si elle ne peut être évitée, les deux pouvoirs locaux qui ont témoigné dressent, avec le recul, quelques leçons à tirer de leurs expériences.

- Sensibiliser les agents est vraiment fondamental. La formation en sécurité informatique pourrait être placée par l'institution sur le même pied que les formations obligatoires.
- Insister, au sein de l'institution, sur la responsabilité collective en matière de sécurité informatique.
- Rappeler systématiquement les règles et bonnes pratiques à chaque alerte de sécurité.
- Sécuriser le réseau et l'infrastructure.
- Avoir du matériel informatique « safe » en stock (PC, imprimantes…).
- Avoir un listing des numéros et adresses privées des agents afin de pouvoir les avertir plus facilement en cas d'incident.
- Prévoir un doublon du responsable du service informatique.
- Prévoir des notes internes-types/documents-types disponibles sur clé USB (procédure paiement urgent, émission de facture, modèle de délibération, de notification, cahiers des charges…) afin de ne pas devoir repartir de zéro en cas d'incident.
- Commencer la journalisation de l'incident dès le 1er jour.
- Prévoir une communication interne et externe rapide et contrôlée (avant qu'il y ait une fuite). ■

[5] Le formulaire est disponible via le lien suivant : https://cert.be/fr/signaler-un-incident-0.