REPORTAGE

UN PLAN DE CONTINUITÉ POUR FAIRE FACE AUX ATTAQUES DE CYBERSÉCURITÉ : TÉMOIGNAGE DU CPAS DE NAMUR

En 2024, nous avons rédigé dans le CRFInfo plusieurs articles en lien avec la cybersécurité, préoccupation essentielle dans notre société digitalisée, dans un contexte où les cyberattaques se multiplient. Les dirigeants des pouvoirs locaux et provinciaux sont de plus en plus confrontés à cette problématique : sa compréhension et son appropriation sont essentielles pour assurer la sécurité et la continuité des services. La cybersécurité implique des mesures techniques mais également organisationnelles, ainsi que la mobilisation de compétences.

Au CPAS de Namur, la cybersécurité est une réalité concrète : de la direction aux agents, tous ont bien conscience des risques et des enjeux de la cybersécurité. Les différents services sont impliqués et travaillent sur les moyens de prévenir et de vivre une cyberattaque sur base d'un plan de continuité des systèmes d'information.

Dans cet article, nous vous invitons à découvrir comment, après avoir pris conscience des risques, la DPO et le directeur IT ont élaboré un plan de continuité, obtenu le soutien de leur hiérarchie, communiqué et impliqué les différents services afin de mettre en œuvre des actions concrètes et priorisées dans le but de permettre au CPAS (ainsi qu'à ses maisons de repos) d'anticiper les conséquences potentielles d'une cyberattaque, de mettre en place des solutions lui permettant de poursuivre ses activités essentielles en situation de crise, et de se relever dans des délais raisonnables.

LA PRISE DE CONSCIENCE

« La question n'est pas de savoir si on sera attaqués mais quand ? »

Le sujet était dans l'air et le dossier sur la table de la DPO (Déléguée à la Protection des Données) et du Directeur du service IT du CPAS de Namur depuis de nombreux mois, mais la réelle prise de conscience de l'urgence de la situation est venue lorsqu'un nombre grandissant d'entreprises publiques de leur environnement direct ou aux mêmes finalités ont été victimes de cyberattaques sur une très courte période. Bien que des mesures étaient déjà en place, il a été décidé, en accord avec le Directeur général, que la protection du CPAS contre les cyberattaques et la mise en place d'un plan de continuité devenait un dossier prioritaire du CPAS.

Pour eux, la continuité des systèmes d'information du CPAS est une problématique qui concerne tant la DPO (également CSI - Conseillère en sécurité de l'information du CPAS) que le département IT. Ils y travaillent en étroite collaboration, estimant que leurs approches métier du sujet sont complémentaires. Ils portent le projet d'une même voix, ce qui amène de la cohérence au projet, lui donne « du poids » et facilite l'adhésion de l'organisation. C'est en collaboration étroite qu'ils élaborent ce projet et le suivront dans la durée.

LE PLAN DE CONTINUITÉ

LA MÉTHODOLOGIE

« Que fait le CPAS concernant ce risque ?"

Vu l'urgence de la situation, ce qui a été travaillé en priorité dans le plan de continuité des systèmes d'information, ce sont les risques en lien avec les cyberattaques. Néanmoins, les conséquences de bien d'autres risques (inondation, coupure de courant, etc.) trouvent des solutions dans les mesures envisagées pour prévenir et lutter contre les cyberattaques. Ensemble, ils ont travaillé selon la méthodologie suivante : une large documentation basée sur leurs lectures techniques, des formations, mais surtout les témoignages concrets d'organisations ayant vécu une cyberattaque, leuront permis d'élaborer un document centralisant les pistes d'actions à mener dans les différents secteurs de l'organisation, de les prioriser, puis de les décliner en actions concrètes.

Les multiples conséquences d'une cyberattaque recensées dans les exemples collectés sont parfois surprenantes. En effet, on ne pense pas forcément au fait que les numéros de téléphone des personnes à avertir ne seront plus accessibles s'ils sont uniquement disponibles sous forme digitale, que les photocopieuses ou les frigos connectés seront hors services ou que l'avenant au contrat relatif au télétravail doit être modifié afin de pouvoir annuler le télétravail en temps de crise.

Une fois la phase de collecte d'informations et de pistes de solutions finalisée, les éléments recensés ont été confrontés avec la réalité de terrain du CPAS de Namur. Quels sont les outils et solutions qui sont déjà en place ? Quels sont les chantiers informatiques, techniques et organisationnels à mener avec plus ou moins de célérité ?

Il est ressorti de ce travail d'analyse des actions à mener (identifiées comme des « chantiers ») qui concernent les différents secteurs de l'organisation avec des mesures à prendre en matière de dispositifs informatiques, de gestion des bâtiments, de copies papier des documents essentiels de l'organisation, de gestion de crise, mais aussi et surtout en matière de gestion des ressources humaines.

Il est néanmoins impossible d'être exhaustif : la spécificité d'une cyberattaque est son incertitude, ce qui accroit la difficulté de prévoir le risque et de le gérer. Puisque l'incertitude ne peut être levée, il s'agit de s'y préparer au mieux.

Les chantiers identifiés ont été priorisés en fonction des risques qui y sont associés tout en donnant la priorité aux chantiers visant à limiter le risque que le CPAS soit attaqué.

Ces chantiers ont pour vocation, outre la résolution des problèmes, d'impliquer les différents services concernés. Les chantiers seront confiés aux services en fonction de leurs spécificités : le service travaux travaillera par exemple sur le chantier des accès aux bâtiments alors que le département RH travaillera à la répartition du personnel en cas de crise, la direction à la formation des agents de la cellule de crise et le département IT à la recherche de solution de consolidation de l'infrastructure informatique.

L'objectif est de faire de ce plan de continuité un projet d'entreprise vivant, utile et qui parle à chaque membre du personnel, et non un document purement administratif validé au plus haut niveau et rangé dans une armoire. Il s'agit de répondre concrètement aux défis que posent les cyberattaques en matière d'anticipation et de gestion.

LES APPUIS

Pour que le plan de continuité puisse être mené, les porteurs de projets ont d'abord obtenu le soutien de leur hiérarchie. La réalité de la menace, l'importance d'élaborer une stratégie en matière de cybersécurité ainsi que les différentes pistes d'action identifiées ont été présentées à M. Sorée, le Directeur général du CPAS de Namur. Convaincu de l'importance de la démarche, il a accordé sa confiance et son appui aux porteurs de projets. L'ensemble du Bureau Permanent puis du Codir a ensuite été sensibilisé et convaincu. La démarche, puis le plan d'actions, ont ainsi été validés et soutenus,ce qui a permis aux porteurs de projet de disposer de temps, de légitimité et de moyens.

L'IMPLICATION DES CHEFS DE SERVICE ET DES « AGENTS RESSOURCES »

Une fois la hiérarchie acquise au projet, l'étape suivante a été de sensibiliser la quarantaine de personnes ressource qui ont été identifiées par les chefs de département pour mener la réflexion au sein des différents services et secteurs de l'organisation. Pour être efficace, la stratégie de cybersécurité doit absolument tenir compte de la réalité de terrain. Le recours aux personnes ressources est très utile car elles connaissent parfaitement les activités de leur service et son fonctionnement, tout en limitant le nombre d'intervenants afin de rationaliser et personnaliser les échanges et la mise en œuvre.

Concrètement, chaque secteur d'activité a rempli une fiche visant à guider sa réflexion sur la manière d'anticiper les conséquences d'une cyberattaque sur ses activités. Les réflexions portent sur l'identification et la poursuite des activités strictement obligatoires du secteur, sur la manière de contacter ses utilisateurs, de disposer en toutes circonstances des documents de référence indispensables à la poursuite de ses activités, … La question de la réaffectation potentielle des agents est également posée à chaque secteur via cette fiche : aura-t-il besoin d'agents supplémentaires pour réaliser des tâches rendues plus chronophages sans informatique ou, au contraire, sera-t-il en mesure de mettre des agents à disposition d'autres secteurs ? Cette étape permet à chacun de réfléchir à partir d'un questionnaire structuré à ce qui peut être anticipé.

Les mesures à prendre ne sont pas imposées même si des pistes sont suggérées, c'est à chaque secteur de trouver et d'identifier les mesures et solutions qui lui permettront de fonctionner au mieux en situation de crise. Les choix opérés par les services seront examinés et validés par l'équipe projet et la hiérarchie afin de s'assurer que les options envisagées sont réalistes et fonctionnelles.

Le plan de continuité du CPAS de Namur est donc un plan d'action coconstruit, adapté à l'organisation, respectant les spécificités métiers et prenant en compte le matériel numérique spécifique utilisé. Le plan de continuité devant intégrer les nouveaux outils, les nouvelles législations et inclure les nouveaux agents, il s'agit d'un projet qui devra sans cesse être actualisé et mis à jour. Pour être pleinement utile le jour de l'attaque, ce plan devra entrer dans les pratiques journalières et engendrer de nouveaux réflexes pour la grande majorité des travailleurs, comme veiller à systématiser l'actualisation de la copie papier de certains documents clés du service.

L'INFORMATION À L'ENSEMBLE DES AGENTS ET LA DIFFUSION D'UNE CULTURE CYBER-RÉSILIENTE

"Ce que chacun peut faire pour limiter le risque et gérer ses éventuelles conséquences."

L'ensemble des agents du CPAS de Namur ont été sensibilisés à la cybersécurité et à la gestion de crise. Le plan de continuité leur a été présenté et expliqué. Un point d'attention spécifique a été fait sur ce que chaque agent peut faire concrètement pour aider à la sécurité informatique du CPAS et à un déroulement optimal de la période de gestion de crise en cas d'attaque.

Associer les utilisateurs leur permet d'être mieux préparés à une cyberattaque et à ses conséquences. En outre, chaque nouveau collaborateur reçoit une formation lors de son entrée en fonction sur les règles RGPD et sur l'hygiène informatique à adopter.

LA MISE EN ŒUVRE

Le plan de continuité du CPAS de Namur se structure en quatre dimensions : éviter, se préparer, gérer une cyberattaque, reprendre les activités. Il doit permettre d'agir rapidement en ayant identifié au préalable les actions prioritaires à mener et les réponses à apporter. En cas de cyberattaque, la procédure est claire : constater, évaluer, contenir, atténuer (communiquer tôt et souvent), et reprendre l'activité.

De nombreuses mesures/chantiers identifiés dans la mise en place du plan de continuité sont rapides à mettre en place et n'ont pas de coût, ce sont des "quick-wins" importants car ils permettent de se sentir avancer dans le projet. Par ailleurs, d'autres chantiers comme des marchés de service ou le passage en revue systématique des solutions imaginées par les secteurs demanderont de nombreux mois de travail.

LES COMPÉTENCES MOBILISÉES

DES COMPÉTENCES MULTIPLES ET COMPLÉMENTAIRES

La conduite d'un tel projet nécessite un ensemble de compétences, qui, pour nos interlocuteurs, ne sont mobilisables qu'en travaillant en collaboration avec l'ensemble des secteurs de l'organisation (Direction, IT, DPO, RH, marchés publics, …).

La gestion de projet

Pour conduire ce plan de continuité, Mme Jedwab a principalement mobilisé et développé ses compétences en gestion de projet.

L'apprentissage continu

De son côté, Monsieur Sanzot met en évidence l'importance de l'apprentissage continu pour les agents de son département. D'ailleurs, la capacité d'auto-formation est un point d'attention lors du recrutement dans le service IT.

Le facteur humain est un élément central dans la résilience des organisations face à la cybersécurité. La formation des employés figure parmi les mesures essentielles

préconisées dans la mise en place d'un plan d'actions en matière de sécurité.

La communication

La communication est essentielle dans la mise en place du plan de continuité car elle permet d'expliquer la démarche institutionnelle à l'ensemble des agents et de les faire adhérer au projet. Il faudra veiller à ce que cette communication reste active dans le temps, sans oublier de sensibiliser les nouveaux travailleurs.

La qualité de la communication interne et externe en cas d'attaque sera déterminante dans la gestion de crise. Le CPAS de Namur estime que les chantiers relatifs à ces aspects devront être menés en priorité afin d'anticiper tout ce qui peut l'être dans cette matière.

La bienveillance

"La bienveillance sera essentielle pour traverser la crise."

LA CYBERSÉCURITÉ EST ÉGALEMENT UNE AFFAIRE D'ATTITUDE.

Une fois l'attaque survenue, il va y avoir énormément de pressions internes et externes. Il serait totalement destructeur pour l'organisation et plus spécifiquement pour les agents qui se débattront sans relâche pour rétablir l'activité, de voir cette pression amplifiée par des remarques destructrices et des bruits de couloir déplaisants du type « Ils auraient quand même pu… », « Ils auraient dû… », « Avec tout ce qu'on entend, il aurait quand même été facile de … ». La communication large sur ce qui est en place dans le cadre du plan de continuité a également pour objectif de conscientiser l'ensemble du personnel sur le fait que ce risque est pris en charge, que le CPAS y travaille assidument. Cette communication sur le travail réalisé a pour double objectif de rassurer les travailleurs sur le fait que le problème est connu et anticipé mais également de limiter, dans la mesure du possible, les propos négatifs et cassants.

La bienveillance devra également être présente entre les services pendant la période de crise. Il est important que chacun prenne conscience que l'ensemble des secteurs et agents seront déstabilisés et qu'il faudra veiller à la qualité des relations humaines dans l'ensemble des échanges professionnels tout au long de la période de crise qui sera assurément longue.

La déstabilisation profonde que peut représenter une cyberattaque pour certains agents a également été anticipée dans le plan de continuité qui prévoit une proposition d'intervention de psychologues de la médecine du travail pour l'ensemble des services.

Il a également été identifié comme essentiel de veiller spécifiquement aubien-être des agents de l'IT en cas de cyberattaque. Il s'agit de travailleurs qui pourront ressentir, plus que d'autres, un fort sentiment de responsabilité par rapport à la crise et à sa résolution. Ils seront préservés, autant que possible, des pressions externes pour pouvoir se concentrer sur le travail de nettoyage et de reconstruction. Il s'agit d'un secteur qui sera mis à rude épreuve, il est donc essentiel d'anticiper « à froid » le travail en doublure et la gestion d'horaires de crise qui permettront à chacun de disposer de plages de repos impératives pour sa santé physique et mentale.

CONCLUSION

La mise en place d'un plan de continuité des systèmes d'information axé cybersécurité tel que le CPAS de Namur souhaite le développer nécessite une collaboration étroite entre le service IT et le DPO, ainsi que l'implication de tous les agents et des différents niveaux de la hiérarchie. Grâce à une démarche structurée et validée à tous les niveaux, les CPAS peuvent mieux se préparer aux cyberattaques et assurer la continuité des services essentiels. La sensibilisation, la formation continue et le soutien de la direction sont des éléments clés pour le succès de cette initiative.

BERNARD SANZOT

Diplômé en informatique de gestion à l'IESN, il est le premier informaticien diplômé du CPAS de Namur, entré en service en 1989. Créateur de la cellule développement au sein du département informatique et initiateur de nombreux logiciels internes complémentaires aux applications métiers acquises auprès de partenaires externes, il est, depuis 2020, Directeur du Département IT qui compte actuellement 12 agents.

CAROLINE JEDWAB

Romaniste de formation avec une licence complémentaire en gestion culturelle, Caroline Jedwab a enseigné le français des affaires à l'UHasselt pendant quelques années et aégalement travaillé au développement d'outils d'apprentissage des langues en ligne puis a été Responsable des affaires générales au sein d'hôpitaux publics pendant 18 ans. Elle travaille au CPAS de Namur depuis 2018, pour y exercer la fonction de DPO - Chargée du contrôle interne (elle a été embauchée dans le contexte de la mise en œuvre du RGPD).