INTERVIEW. En février dernier et en pleine pandémie de Covid-19, le groupe Afnor a vécu une cyberattaque. Retour d'expérience avec Laurence Breton-Kueny, DRH du groupe Afnor, vice-présidente nationale de l'ANDRH, experte de la continuité d'activité et du management des risques RH[1].

Cybersécurité

Groupe Afnor : réagir efficacement à une cyberattaque

Propos recueillis par Anaïs Coulon, ANDRH

Nous avons communiqué très tôt sur ce que nous vivions, auprès de nos salariés et clients notamment, en toute transparence. »

Vous avez subi une cyberattaque en février dernier. En quoi a-t-elle consisté ?

Laurence Breton-Kueny : Le 18 février 2021 matin, nous avons été attaqués par un *ransomware* et certains collaborateurs ont vu leurs écrans d'ordinateur se crypter. La direction générale a pris la décision de stopper le système d'information du groupe. Nous n'avions donc plus de messagerie, plus de sites internet fonctionnels, plus de réseau interne… et les ordinateurs qui étaient connectés au réseau ont dû être fermés. Cette décision courageuse est la seule possible quand on subit une cyberattaque car on ne connaît pas l'ampleur des dégâts et quels sont les domaines infectés. Le bon réflexe est donc de tout couper en souhaitant sauvegarder le système d'information. L'origine de l'attaque, identifiée par la suite, vient d'une pièce jointe ouverte par une personne salariée, ce que l'on appelle un « phishing ». Il s'agit d'un « vers » qui est un programme qui remonte ensuite vers des machines des administrateurs et les serveurs (le cœur du système).

Une fois les systèmes d'information coupés, comment avez-vous continué votre activité ?

L.B.-K. : À la suite de cette décision, plusieurs équipes ont travaillé en parallèle. La première, composée notamment de la direction des systèmes d'information interne, de notre cabinet spécialisé en cybersécurité que nous avions dans le cadre de notre démarche NF EN ISO/IEC 27001 et de l'Agence nationale de la sécurité des systèmes d'information (Anssi), a eu pour premier objectif d'établir un diagnostic de l'attaque subie pour mieux la comprendre et y réagir. La cellule de crise composée du Comex plus le responsable de la sécurité des systèmes d'information, la responsable communication et la responsable juridique a été activée avec pour objectif de continuer l'activité. La priorité a été de rétablir la communication avec les salariés et les clients. Il a été mis en place un nouveau système de messagerie, de nouvelles adresses e-mail, d'outils collaboratifs, de plateforme de stockage de données… afin de poursuivre notre activité dans les meilleures conditions possible. Les salariés ont ainsi utilisé leur ordinateur portable personnel lorsqu'ils en avaient un et chaque direction s'est organisée pour que l'activité puisse continuer. Cependant, une partie de nos salariés a été placée en activité partielle parce qu'elle ne pouvait tout simplement pas travailler. Côté direction, nous nous sommes retrouvés en cellule de crise deux fois par jour tous les jours, pendant plusieurs semaines, puis à raison d'une fois par jour et enfin d'une fois tous les deux jours.

Bio express

LAURENCE BRETON-KUENY

Depuis 2006 : DRH du Groupe Afnor

2003-2006 : chef de service RH, Haute Autorité de Santé, Agence nationale d'accréditation et d'évaluation en santé

Depuis 2017 : vice-présidente nationale de l'ANDRH

Depuis 2009 : présidente de l'ANDRH Seine Saint-Denis

Comment avez-vous communiqué auprès des salariés ?

L.B.-K. : Nous avons communiqué très tôt sur ce que nous vivions, auprès de nos salariés et clients notamment, en toute transparence. Le plan de continuité de l'activité pandémie grippale de 2009 du groupe Afnor, que j'avais mis en place, avait été réactivé et réactualisé au début de l'épidémie de Covid-19 en 2020. Il était prévu, dans ce plan de continuité d'activité, un système d'envoi de SMS (SMS factor) qui me permet de communiquer avec tous les salariés du groupe. Nous possédons un portail RH depuis 2010 qui permet un stockage des données salariés confidentielles. Nous avons envoyé un SMS pour les prévenir et les orienter vers un site d'information back up où les informations générales et par métiers étaient mises en ligne. Par la suite, tous les PC ont été analysés afin d'établir un diagnostic et identifier les ordinateurs contaminés par ce virus comme tous les serveurs…

Au bout de deux mois, 95 % de notre système d'information était de retour grâce aux équipes internes et au cabinet de cybersécurité. Il est important de rappeler que dès le départ il y a eu un refus de payer la rançon demandée, dont nous ne connaissons pas le montant. Chaque …

La question des cyberattaques place sur le devant de la scène deux sujets parfois oubliés par les RH : la continuité de l'activité et le management des risques. »

ransomware (dans notre cas Ryuck) communique ce montant de façon différente et, dans notre cas, il fallait aller le voir dans le dark net. Il s'agit de la position de l'Anssi, partagée par notre conseil d'administration.

La personne ayant fait cette erreur a-t-elle été mise au courant ?

L.B.-K. : Non, et c'est là un point très important : l'une des règles en cybersécurité dans ce cas de figure est de ne pas prévenir la personne concernée, car il s'agit d'un élément qui pourrait être traumatisant pour elle. De plus, la pièce jointe du mail en question était trompeuse car elle contenait le nom de l'Afnor.

Qu'est-ce que cette cyberattaque a impliqué pour les RH ?

L.B.-K. : Nous avons été extrêmement présents pour réagir et accompagner le collectif face à cette cyberattaque : mobiliser tous les salariés, mettre en place l'activité partielle, collaborer à la cellule de crise, garantir la continuité d'activité...

L'une des principales difficultés a été la paie, car dans ce domaine aussi, nos outils étaient hors service. Le 18 février la paie du mois n'était pas partie et nous ne pouvions plus y avoir accès. Nous avons donc dû retrouver le fichier du mois précédent en travaillant de concert avec la direction financière avant qu'il soit crypté, le retravailler et ensuite la direction financière a dû trouver une banque qui accepte que nous effectuions des paiements par virement à destination des salariés. Nous avons utilisé cette technique trois mois de suite. Impossibilité de payer les charges sociales, il a fallu prévenir tous les organismes. C'était une situation inédite !

Quels sont vos conseils à destination des professionnels RH à ce sujet ?

L.B.-K. : Renseignez-vous bien en amont sur les assurances cybersécurité (il y a un volet RH) et faites-vous accompagner par un cabinet spécialisé cybersécurité, formez bien les salariés au risque du phishing et regardez bien la norme ISO 27001.

Ce qui est important lorsque vous êtes attaqué, c'est de réagir très vite et être bien accompagné permet d'avoir une longueur d'avance. Rapprochez-vous également de l'Anssi, organisme public de lutte contre les cyberattaques, qui vous permettra d'avoir la réponse la plus adaptée à votre situation et de trouver des formations.

De manière plus générale la question des cyberattaques, tout comme celle de la pandémie de Covid-19, place sur le devant de la scène deux sujets parfois oubliés par les RH : la continuité de l'activité et le management des risques. Il est essentiel de prévoir et d'anticiper des plans de continuité de l'activité afin de ne pas être pris de cours lorsque des situations comme celles-ci surviennent. Il faut également être en capacité en tant que DRH d'avoir une vision globale des risques encourus par l'entreprise dans tous les domaines. Au niveau de mon groupe, nous souhaitons témoigner et partager notre expérience, et en interne continuer de sensibiliser et de former chacun aux bons réflexes pour diminuer les risques. Cependant, nous savons également que cette situation peut se reproduire à l'avenir, car l'erreur est humaine, d'où l'intérêt d'être vigilant.

1 *Réaliser un PCA Pandémie grippale dans une organisation : Pourquoi et comment ?* Édition Afnor 2008, Sandrine Segovia-Kueny, Laurence Breton-Kueny.