Publié le 13 octobre 2022

Cybersécurité, entre paranoïa et prévention

La première journée du Congrès des acteurs de l'économie mixte locale a été consacrée, entre autres, à une thématique qui ne laisse insensible aucun des acteurs de nos territoires. On sent même souffler dans la salle un vent de paranoïa.

Animée par **Frédéric Duval**, directeur de la publication lyonpositif.fr, la séance s'ouvre sur une interpellation des intervenants. Méfiance, peur, paranoïa, psychose… tels sont les sentiments des dirigeants des entreprises de l'économie mixte locale ! Dès lors qu'il est question d'internet, de réseaux sociaux, de mails, la prise de conscience des enjeux s'impose.

Tous parano ?!

« Serais je le prochain à faire l'objet d'une cyber-attaque ? Si oui, que faire ? Si non, pour le moment, comment me prémunir pour demain ? », pouvait-on entendre dans les travées. Avec le déploiement à grande échelle des nouvelles technologies, les cyberattaques ne cessent de s'amplifier et de se diversifier. Le climat actuel cristallise les tensions autour des enjeux de cybersécurité avec l'émergence de nouvelles menaces liées à la transformation numérique, l'usage du cloud, l'utilisation des réseaux sociaux et l'omniprésence de la cybercriminalité. Dans un monde interconnecté où la collecte d'informations et les échanges numériques explosent, **la data devient matière à rançon**. Les conflits géopolitiques ou encore économiques jouent, également, un rôle non négligeable dans l'accroissement du nombre de cyber-attaques au quotidien.

Le panorama de la Cyber malveillance effectué par **Laurent Verdier**, directeur Pédagogie et Sensibilisation de cybermalveillance.gouv.fr, interpelle et exacerbe les sentiments de paranoïa de la salle. L'effet est saisissant. Le silence de la salle est à la hauteur des chiffres et des anecdotes partagées.

Outre le retour sur l'épisode récent de la cyber-attaque subie par l'hôpital de Corbeil-Essonnes en août 2022, il est mis en exergue que 30 % des collectivités ont fait l'objet d'une cyber-attaque en

2020. Le parcours victime sur cybermalvaillance.gouv.fr a recensé une **hausse de 173 000 demandes d'assistance pour la seule année 2021.**

A ce titre, on distingue uniquement pour les entreprises et les associations, 24 % des recherches d'assistance concernent le rançongiciel, 18 % le piratage de compte et 13 % le hameçonnage

Face à ce constat, l'auditoire était avide de comprendre les mécanismes à l'œuvre et les enjeux. Il fut question de mise en place des stratégies et des outils performants pour renforcer la protection de leurs données. La problématique est humaine et non technique selon **Alain Guillotin**, directeur Général de la Spl Chartres Métropole Innovations Numériques (CM'IN)

Par conséquent, le sujet demande que l'on s'en occupe sans attendre et exige une mise à niveau de compétences, surenchérit **Christophe Barbot**, directeur général d'Eau du bassin rennais.

Que faire ?

Au registre des solutions qui s'offrent aux Epl pour se prémunir, anticiper les attaques et renforcer la protection des données, l'ancien directeur général de la Gendarmerie Nationale, actuellement Adjoint au maire de Chartres et Vice-président de l'agglomération de Chartres Métropole, le **Général d'armée Richard Lizurey** insiste sur la nécessité absolue de sensibiliser les élus notamment de petites communes. C'est, à ses yeux, « une question de gouvernance politique. »

Des intervenants prévenants…

Maitre **Arnaud Tessalonikos,** avocat et directeur associé à Fidal, recommande 4 axes:

- contractualiser les règles liées à la protection des données
- passer d'un droit à la sécurité à une obligation de se sécuriser
- faire le choix de signer une police d'assurance liée au risque cyber
- faire appel, le plus amont possible, à l'expertise d'un avocat qui saura invoquer l'article 321-1 du code pénal

Une astuce, simple et basique ?

De façon général, changez régulièrement tous vos différents mots de passe… et demeurez un paranoïaque prévenant.