La protection des systèmes d'information est aujourd'hui une nécessité à tous les niveaux.

Christophe GUILLOTEAU
Président
Département du Rhône

Dans le Rhône, le 15 février 2021, le centre hospitalier de Villefranche-sur- Saône a été la cible d'une cyberattaque.

Ce jour-là, le centre hospitalier de Villefranche-sur- Saône a été la cible d'une cyberattaque d'une grande ampleur, paralysant une grande partie de son système d'information et provoquant le report de plusieurs interventions. Il aura fallu plus de 15 semaines pour un retour à la normale.

Les attaques informatiques se multiplient : pas une seule semaine sans information sur une attaque majeure.

Escroqueries en ligne, cyberattaques, hameçonnages ou rançongiciels : quelles que soient les formes qu'elles prennent, les criminalités numériques font désormais partie de notre quotidien.

Et pire encore, elles ne cessent de se multiplier dans le contexte de crise sanitaire actuel avec une augmentation significative en 2020 liée aux confinements (télétravail, achats en ligne…).

En deux ans, le nombre d'attaques informatiques par des pirates réclamant une rançon a explosé en France comme dans le reste de l'Europe. Selon l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), en 2020, le nombre de ces attaques aux « rançongiciels » aurait augmenté de 255% rien que sur les grandes entreprises publiques et privées y compris celles qui relèvent de la sécurité nationale, selon l'AFP.

Les attaques informatiques constituent donc aujourd'hui un vrai fléau qui touche aussi bien les particuliers que l'ensemble des entreprises ou administrations.

Face à ce contexte, la cyberdéfense est devenue une priorité pour les collectivités territoriales.

Rappelons que les collectivités traitent de nombreuses données fiscales, sociales et gèrent de nombreuses prestations… La divulgation ou le vol de ces données serait une atteinte majeure à la vie privée des citoyens, une atteinte très dommageable.
À titre d'exemple le Département du Rhône traite environ 25000 prestations par mois.

Pour faire face de manière efficace aux nombreuses menaces qui pèsent sur les données dématérialisées, les collectivités territoriales ont l'obligation de se soumettre à un cadre

réglementaire solide de protection des données des usagers.

Ce cadre légal a sensiblement évolué depuis 2018, afin de prendre en compte les avancées digitales et une multitude et variété de canaux de diffusion (réseaux sociaux, cloud, etc..).

De plus les collectivités ont entrepris elles-mêmes une transformation numérique profonde.

En effet elles ont besoin de ces nouveaux moyens pour moderniser leurs actions, pour accompagner le développement de leur territoire et améliorer la qualité de service aux usagers : accès facilité aux services, efficacité et gain de temps dans le traitement des dossiers…
Ces mutations impliquent une augmentation des services en ligne, impliquant plus de risques, plus de répercussions sur le fonctionnement de l'administration et sur le service à l'usager.

Enfin, force est de constater que les données du territoire sont de plus en plus nombreuses et variées du fait d'une multiplication des sources (smartphone et réseaux sociaux, capteurs …). Ces nouvelles données sont difficilement exploitables avec les outils informatiques traditionnels.

Tout cela amène nous amène à repenser notre schéma de système d'information pour nous moderniser tout en assurant la protection des données.

Pour répondre à cette nécessité, les collectivités doivent être en capacité de se défendre, d'assurer la souveraineté des données pour lutter contre les cybermenaces. Trouvons une alternative en nous dotant d'outils innovants, en sensibilisant et formant les agents.
L'arrivée massive de nouveaux moyens de communication et le développement de l'internet ont nécessité une refonte complète de nos usages numériques en 2017.

Le Département de Rhône applique en son sein une stratégie transverse de cybersécurité et de protection des systèmes d'informations et des données afin de protéger les données des agents, des collaborateurs, des citoyens, et de maintenir l'exploitation des services en ligne et de son système d'information.

Au Département du Rhône nous avons mis en place un dispositif de cyberdéfense technique, opérationnel et organisationnel. Nous complétons actuellement ce plan d'actions en élaborant une politique globale de sécurité pour protéger nos systèmes d'information.

Dans ce cadre nous avons produit un livret des usages numériques.

Ce document, que nous réactualisons périodiquement, est la charte d'utilisation des outils informatiques mis à disposition des agents pour exercer leurs missions.

Parallèlement à ces bons usages nous avons mené une campagne de sensibilisation auprès de l'ensemble des agents. Dans ce cadre, une base documentaire est accessible à tous les agents sur l'intranet du Département avec des fiches pratiques adaptées aux situations.

Plus concrètement, le Département met en avant sur son site intranet les gestes simples (choix des mots de passe, séparation données personnelles et privées, utilisation restreinte de la messagerie électronique) qui permettent d'accroitre de manière significative la sécurité des données professionnelles de l'ensemble des agents départementaux.

Nous poussons également les agents intéressés par le sujet à s'inscrire sur la plateforme de l'ANSSI pour suivre une formation d'initiation à la cybersécurité.

Enfin, nous veillons à la pertinence des systèmes de protection en les faisant évoluer selon l'état de l'art et les préconisations de l'ANSSI.

Le monde de la cybersécurité et de la cybercriminalité évolue sans cesse et très rapidement.
Dans la démarche d'amélioration continue de ses outils de protection face aux cybermenaces, le Département du Rhône, comme d'autres collectivités territoriales, étudie de près l'usage de solutions de protection et de défense « nouvelles générations » tirant partie des avancées technologiques apportées par l'univers de l'informatique en Nuage telles que l'Apprentissage Machine et l'Intelligence Artificiel.

Incontestablement, cette sensibilisation à la cybersécurité ne pourra se mettre en place sans l'appui de sociétés prestataires de confiance certifiés pour le choix et l'intégration de ces outils, et grâce à une formation poussée de tous les agents concernés par ce secteur aux enjeux considérables dans un monde 2.0 qui ne cesse de s'agrandir.