Favoriser le recrutement et les carrières cybersécurité dans les fonctions publiques territoriales et hospitalières : un impératif de sécurité nationale.

Philippe LOUDENOT
Senior advisor
CyberCercle

Si 66% des Français - soit 2 Français sur 3 - attendent aujourd'hui de leur collectivité qu'elles leur proposent des services numériques personnalisés, seul un tiers d'entre eux est prêt à leur confier ses données personnelles. Garantir la confiance numérique est aujourd'hui un enjeu majeur.

La dématérialisation engagée par l'ensemble des acteurs et accélérée par la crise sanitaire participe à la profonde transformation numérique de la société. Mais elle s'accompagne aussi de l'essor des menaces cyber, désormais permanentes et capables de désorganiser de nombreuses structures privées comme publiques, petites comme grandes, que ce soit au niveau national ou de tous les niveaux territoriaux. C'est dans ce contexte que les acteurs concernés doivent faire face à l'explosion de cyberattaques : vol de données confidentielles, interruption des fonctions critiques de l'entreprise ou de la collectivité, actes frauduleux. Ces cyberattaques sont d'ailleurs de plus en plus relayées par les médias.

Sur l'ensemble des incidents ou attaques numériques, les TPE/PME et collectivités représentent près de 80 % des victimes, souvent sans ressources pour y faire face. A titre d'exemples, plusieurs attaques récentes ont ainsi impacté des administrations territoriales mais également des structures de santé ou médico-sociales révélant un phénomène d'ampleur, celui de l'oubli par ces structures de la protection des données et de la sécurité numérique de premier niveau.

Cet « oubli » pouvant se révéler dramatique, est induit par une méconnaissance des risques pesant sur la protection des données et des enjeux de la sécurité du numérique. Certes, une pléthore de spécialistes communique sur ce sujet, mais uniquement via des menaces dont l'origine annoncée est située dans des contrées lointaines ou du fait de cybercriminels en recherche d'argent facile et éloignés de la justice : ce sont des méchants et il y en a plein ! Si ce type de discours est toujours écouté très poliment, il est souvent vite oublié face à des interrogations, de fait, légitimes : « pourquoi moi ? », « pourquoi ma structure ? ». **Par trop souvent il n'est pas fait état des risques et particulièrement des impacts sur les organisations mêmes.**

Pour se prémunir, car, comme en médecine, le préventif coûte moins cher que le curatif (si tenté que l'on puisse traiter), **différents acteurs proposent un certain nombre d'actions et particulièrement celle de nommer un responsable de la sécurité des systèmes d'information (RSSI).** Si le règlement européen de la protection des données à caractère personnel, le fameux RGDP, fait obligation de nommer un délégué à la protection des données personnelles (DPO), précisant toutefois que celui-ci peut être interne, mutualisé ou externalisé, cette vision ne l'est pas pour le RSSI.

Alors que les entreprises et les administrations françaises prennent conscience de l'enjeu de la cybersécurité, plus de 5 000 postes sont actuellement à pourvoir dans ce domaine dans l'Hexagone. De nouvelles formations se mettent en place, certes, mais cela ne semble pas suffire. Le RSSI est donc une ressource « rare ». Sans paraphraser le sophisme « ce qui est rare est cher », l'énorme difficulté pour certaines structures de proposer un poste de RSSI et de trouver la personne qualifiée est un constat permanent.

Le Livre blanc sur la défense et la sécurité nationale place la sécurité et la défense des systèmes d'information au cœur des priorités stratégiques de la Nation. Néanmoins, au regard des besoins existant sur le terrain, les annonces faites en février 2021 par le Président de la République pour muscler la filière de cybersécurité française et annoncer un plan national consacré à la cybersécurité se heurtent au manque de moyens des structures des fonctions publiques hospitalières ou territoriales.

En effet, face aux besoins accrus en matière de Ressources humaines cyber, la fonction publique d'État dispose aujourd'hui de deux textes, pour renforcer ou attirer des talents, spécialistes de domaines ou les ressources manquent :

- La circulaire du Premier ministre du 21 mars 2017 relative à la gestion des ressources humaines dans les métiers du numérique et des systèmes d'information et de communication. Elle se traduit par la création d'un corps des ingénieurs des systèmes d'information et de communication. Elle propose de favoriser le recrutement et la mobilité. A cet effet il est proposé, même en l'absence d'un corps de fonctionnaires, de pouvoir, pour les métiers à compétences rares, procéder directement à un recrutement en CDI.

- La note « Référentiel de rémunération des 56 métiers de la filière numérique et des systèmes » du 15 décembre 2021 (annexe 2), co-signée par la directrice générale de l'administration et de la fonction publique, la directrice du budget et le directeur interministériel du numérique d'information et de communication. Cette note vise une meilleure prise en compte de l'expertise et des compétences détenues par les candidats et d'identifier le niveau adapté de rémunération au regard des différents seuils que propose le référentiel, du niveau de complexité du poste, des compétences détenues par le candidat et de son expérience.

En revanche, concernant la fonction publique hospitalière ou territoriale, où les besoins en spécialistes cyber sont criants, force est de constater la pénurie de spécialistes en cybersécurité, renforcée par une faible attractivité : niveaux de salaires incompatibles au regard du marché, postes à durée limité et aucune visibilité sur un éventuel plan de carrière.

S'il est souhaité une prise en compte et un accompagnement cyber de l'ensemble des échelons de ces fonctions publiques, il peut être envisagé, à l'instar des délégués à la protection des données, la possibilité de disposer de RSSI internes, mutualisés ou externalisés. Sans préjudice de ces deux dernières possibilités, il pourrait être étudié la mise en place de leviers identiques à ceux existants dans la fonction publique d'État et ainsi favoriser le recrutement de ressources rares, en prenant en compte également les moyens pour garder, maintenir et élever le niveau de connaissance mais aussi de proposer une carrière aux candidats.

Engager une réflexion sur la dimension ressources humaines en cybersécurité pour les fonctions publiques hospitalières et territoriales est un enjeu de sécurité nationale.