Le 20 mai 2025, le département des Hauts-de-Seine a été frappé par une cyberattaque de grande ampleur, entraînant la mise hors service de l'ensemble de ses systèmes informatiques : réseau, messagerie, applications métiers.

Problématique

Les collectivités territoriales françaises sont-elles suffisamment préparées pour faire face à des cyberattaques de plus en plus fréquentes et sophistiquées ?

Déclenchement de l'attaque le matin du 20 mai 2025, les équipes du département des Hauts-de-Seine détectent une activité anormale. En réponse, tous les systèmes informatiques sont désactivés pour éviter une propagation ou une exfiltration de données. Une Réponse immédiate a été prise, le département a mobilisé ses équipes internes et ses prestataires pour limiter les dégâts, diagnostiquer l'origine de l'attaque et restaurer progressivement les services il y a des enjeux pour les usagers cette attaque perturbe potentiellement l'accès aux aides sociales, aux inscriptions scolaires, aux services d'action sociale ou de voirie. Les cyberattaques contre les hôpitaux, mairies, départements ou régions se multiplient. L'ANSSI recense chaque année des dizaines d'incidents majeurs, avec parfois des fuites de données sensibles ou des paralysies de services critiques.

Les collectivités françaises ne sont pas encore suffisamment préparées, bien que des efforts soient en cours.

L'attaque contre les Hauts-de-Seine montre que même des départements bien équipés peuvent être vulnérables, en l'absence de plans de continuité opérationnelle robustes cela peut être résolu ou diminuer par des simulations régulières de crise pour entraîner les équipes, sensibilisation des agents publics, qui sont souvent les premières cibles via des e-mails piégés.

Pour que la résilience numérique des services publics locaux progresse réellement, il faut que la cybersécurité cesse d'être perçue comme une dépense technique, et devienne une priorité stratégique et politique.

Le parisien, ANNSI, France inter