Introduction

C'est ainsi, fort de ce constat initial et de la prise de conscience partagée que la cybersécurité est désormais un enjeu stratégique pour chaque collectivité, que nous allons aborder dans ce guide les défis numériques auxquels font face nos organisations. À l'ère du numérique et de l'intelligence artificielle, nos collectivités évoluent dans un monde toujours plus connecté, où les services publics s'appuient sur des systèmes d'information et des infrastructures numériques pour fonctionner efficacement. Pourtant, cette transformation numérique, qui offre des opportunités considérables d'amélioration des services et de simplification des démarches, s'accompagne également de risques nouveaux.

Des petites communes aux grandes métropoles, aucune collectivité n'est à l'abri des cyberattaques, qui peuvent paralyser les services essentiels, compromettre des données sensibles et, malheureusement, éroder la confiance des citoyens envers leurs élus et leurs services publics. Dans ce contexte, la nécessité pour les collectivités de se doter d'une stratégie de cybersécurité n'a jamais été aussi pressante. Pourtant, face au sentiment de complexité technique et aux contraintes budgétaires, de nombreux élus et dirigeants, en particulier dans les plus petites collectivités, se trouvent démunis.

Rédigé par un dirigeant territorial expérimenté dans la gestion des enjeux numériques locaux, ce guide pratique propose des solutions accessibles et opérationnelles. Il s'adresse spécifiquement aux élus et dirigeants territoriaux, en mettant l'accent sur les collectivités qui n'ont pas d'agents ou de services dédiés à la cybersécurité.

La première partie, « **Comprendre les défis numériques actuels et futurs** », dresse un panorama des enjeux de la cybersécurité pour les collectivités territoriales.

La deuxième partie, « **Construire son PCA-cyber en 100 jours** », propose une méthodologie et un calendrier pour mettre en place un plan de continuité d'activité (PCA) cyber et faire voter une politique de sécurité des systèmes d'information (PSSI) simplifiée.

La troisième partie, « **Gérer une situation de crise cyber** », fournit un guide pratique pour réagir en cas de cyberattaque, depuis la détection initiale jusqu'au retour d'expérience postcrise.

Enfin, cet ouvrage se clôt par une série de **chroniques historiques de la cybersécurité**, présentée en annexes. Bien que leur lecture ne soit pas indispensable à la compréhension des trois parties principales, elle apporte un éclairage sur la construction progressive de notre socle législatif et réglementaire au fil des décennies. Chaque nouveau texte, chaque obligation actuelle s'inscrit en effet dans une histoire marquée par des faits générateurs qui ont motivé ces évolutions. Ces chroniques permettent ainsi aux élus et dirigeants de replacer la cybersécurité dans une perspective historique, afin de mieux saisir les origines et la finalité des dispositifs qu'ils mettent aujourd'hui en œuvre.