

Sommaire

Avant-propos	p.9
Introduction	p.11

Partie 1

COMPRENDRE les défis numériques actuels et futurs

Chapitre I

Vulnérabilités du service public local face aux cyberattaques	p.15
A - État des lieux de la menace cyber dans le secteur public	p.15
1. L'évolution des cyberattaques	p.15
2. L'impact sur les collectivités territoriales	p.16
3. La transformation numérique du secteur public	p.17
4. L'évolution rapide des menaces	p.18
B - Les fragilités structurelles des collectivités	p.21
1. Le manque de ressources dédiées	p.21
2. Les vulnérabilités spécifiques	p.24
C - Étude de cas : récit fictif d'une cyberattaque municipale	p.26
D - Les principales formes d'attaques	p.29
1. Rançongiciel (<i>ransomware</i>)	p.29
2. Hameçonnage (<i>phishing</i>) et ingénierie sociale (<i>social engineering</i>)	p.31
3. Attaques par déni de service (DDoS)	p.32
4. Compromission des systèmes d'information	p.34
E - Les impacts sur le service public	p.34
1. Interruption des services essentiels et défis de la reprise d'activité	p.35
2. Conséquences financières	p.37
3. Défis de confiance et réputation	p.41
4. Dimension stratégique	p.42

Chapitre II

Cadre légal et réglementaire de la cybersécurité des collectivités p.47

A - L'adaptation des obligations selon la taille et les moyens	p.48
1. Communes de moins de 3 500 habitants	p.49
2. Communes entre 3 500 et 30 000 habitants	p.50
3. Structures soumises à NIS 2	p.52
4. Cas particuliers et spécificités	p.54
5. Tableaux synthétiques	p.56
B - Du légal à l'opérationnel	p.60
1. Le principe de responsabilité	p.61
2. La contractualisation avec les prestataires	p.66
3. La couverture des risques	p.69
4. La question du paiement des rançons	p.72
5. Les sanctions pénales	p.77
6. Les sanctions administratives	p.78
7. Les ressources mobilisables	p.85

Partie 2

CONSTRUIRE

son PCA-cyber en 100 jours

Étape 1

Structurer et lancer le projet (jours J à J+7) p.99

A - Clarifier les concepts clés : PSSI simplifiée et PCA-cyber	p.100
1. La politique de sécurité des systèmes d'information (PSSI) simplifiée	p.100
2. Le plan de continuité d'activité cybersécurité (PCA-cyber)	p.101
B - Obtenir le soutien politique et l'implication de la direction	p.101
1. Sensibiliser les élus aux enjeux de la cybersécurité	p.102
2. Présenter les bénéfices du projet à la direction	p.102
3. Obtenir l'engagement formel des décideurs	p.103
C - S'appuyer sur un référent cybersécurité	p.103
1. Privilégier les compétences transversales plutôt que l'expertise technique	p.104
2. Identifier la personne adéquate au sein de la collectivité	p.104
D - Constituer le comité de pilotage (Copil) et organiser la première réunion	p.105
1. Identifier les membres clés et répartition des rôles	p.105
2. Définir les critères de sélection des participants	p.106
3. Préparer l'ordre du jour et inviter les participants	p.106
E - Animer la réunion de lancement du Copil (J+7)	p.107
1. Présentation des objectifs du projet	p.108
2. Définition de la gouvernance et des rôles des présents	p.108
3. Validation de la méthodologie et du calendrier	p.108

Étape 2

Construire le PCA-cyber avec son équipe (jours J+8 à J+59) p.111

A - Utiliser le tableau PCA-cyber comme outil central p.111

1. La cartographie de l'existant (colonnes 1 à 5) p.112
2. L'organisation de la continuité (colonnes 6 à 10) p.113
3. Choix de la plateforme de gestion de ce fichier partagé p.115

B - Organiser trois réunions pour bâtir le plan ensemble p.116

1. Constitution du groupe de travail p.117
2. Première réunion (J+17) : lancement et méthode p.118
3. Deuxième réunion (J+38) : validation et continuité p.120
4. Troisième réunion (J+59) : finalisation p.121

Étape 3

Valider et formaliser la démarche (jours J+60 à J+68) p.125

A - Organiser la réunion de validation du Copil (J+60) p.126

1. Examen des documents produits p.126
2. Phase de validation et projections p.127
3. Conclusion et perspectives p.127

B - Préparer les documents officiels et les transmettre aux conseillers (J+61) p.127

1. Documents requis pour la délibération p.127
2. Présentation en CST p.128
3. Présentation en commission politique p.128
4. Note de synthèse explicative p.128
5. Projet de délibération p.129
6. Organisation des annexes p.131
7. Convoquer les conseillers pour approbation (J+61) p.131

C - Présenter la PSSI simplifiée au conseil (J+67) p.131

D - Rédiger une note interne (J+68) p.133

1. Identification d'un risque p.133
2. Solution proposée p.134
3. Approche méthodologique p.134
4. Format et adaptation p.134
5. Contenu et objectifs p.135
6. Suivi et évaluation p.135

E - Finaliser le PCA-cyber ainsi validé p.135

1. Organiser la documentation p.135
2. Déployer et rendre accessible le PCA p.136
3. Intégrer le risque cyber au plan communal de sauvegarde (PCS) p.136

Étape 4

Mettre en œuvre et évaluer la démarche (jours J+70 à J+100) p.139

A - Organiser la séance de sensibilisation collective (J+70) p.140

1. Préparer le contenu de la formation p.140
2. Planifier la logistique de la séance p.141
3. Réaliser la formation (J+70) p.142
4. Accompagner la transformation des pratiques professionnelles p.143

B - Déployer la double authentification pour tous (J+80)	p.145
1. L'importance de la double authentification	p.146
2. Les méthodes de double authentification	p.147
3. Défis et solutions pour l'adoption	p.147
4. Étapes de mise en place	p.148
C - Déployer le gestionnaire de mots de passe sécurisé (J+80)	p.148
1. La nécessité d'un gestionnaire de mots de passe	p.149
2. Fonctionnalités d'un gestionnaire de mots de passe	p.149
3. Choix d'un gestionnaire de mots de passe	p.149
4. Défis et solutions pour l'adoption	p.150
5. Étapes de mise en place	p.150
D - Réaliser le bilan des 100 jours (J+100)	p.151
1. Bilan des actions menées	p.152
2. Plan d'action pour les six prochains mois	p.153
3. Conclusion et prochaines étapes	p.153

Partie 3

GÉRER

une situation de crise

Chapitre I

Réaction immédiate à la cyberattaque	p.159
A - Détection et qualification de l'incident	p.159
1. Identification des signes d'attaque	p.159
2. Première évaluation technique	p.162
3. Documentation initiale	p.164
B - Actions immédiates	p.165
1. Mesures conservatoires techniques	p.165
2. Activation des procédures d'urgence	p.167
3. Préservation des preuves	p.168
C - Mise en œuvre de la cellule de crise	p.169
1. Organisation du dispositif	p.169
2. Configuration hybride	p.172
3. Chaîne d'alerte interne	p.173

Chapitre II

Gestion opérationnelle de la crise	p.175
A - Coordination des actions	p.175
1. Maintien de l'efficacité du pilotage	p.175
2. Gestion des ressources humaines et matérielles	p.176
3. Adaptation continue et apprentissage en temps réel	p.177
B - Investigation technique	p.178
1. Analyse de l'attaque	p.178
2. Recherche de preuves	p.179
3. Qualification des impacts	p.179

C - Relations avec les autorités et avec l'écosystème de réponse aux incidents	p.180
1. Forces de l'ordre	p.180
2. L'Anssi et son réseau de proximité	p.183
3. Autres autorités ou partenaires	p.184
Chapitre III	
Communication de crise	p.187
A - Application du plan de communication	p.187
1. Mise en œuvre de la stratégie	p.187
2. Adaptation au contexte	p.188
B - Relations avec les médias	p.188
1. Gestion des sollicitations	p.188
2. Communication proactive	p.189
3. Gestion de la communication numérique	p.189
C - Communication interne	p.190
1. Information des agents et des élus	p.190
2. Animation du dispositif	p.190
3. Gestion du stress	p.191
Chapitre IV	
Reprise et retour à la normale	p.193
A - Stratégie de reprise	p.193
1. Évaluation des prérequis	p.194
2. Planification du redémarrage	p.194
3. Processus de validation	p.194
B - Mise en œuvre de la reprise	p.195
1. Exécution du plan de reprise	p.195
2. Gestion des anomalies	p.195
3. Stabilisation du fonctionnement	p.196
C - Normalisation de l'activité et levée progressive du dispositif de crise	p.196
D - Retour d'expérience et renforcement postcrise	p.196
1. Documentation de crise	p.196
2. Retour d'expérience	p.197
3. Renforcement du dispositif	p.198
Conclusion	p.201
Bibliographie	p.203
Chroniques historiques de la cybersécurité	p.205
Chronique 1	
Les fondations (1974-1999)	p.207
Épisode 1 : 1978 – loi Informatique et Libertés (FR)	p.207
Épisode 2 : 1982 – lois de décentralisation (FR)	p.209
Épisode 3 : 1988 – loi Godfrain (FR)	p.211

Chronique 2

L'essor de la dématérialisation (2000-2009) p.213

Épisode 1 : 2000 – loi sur la preuve électronique (FR) p.213

Épisode 2 : 2004 – loi pour la confiance dans l'économie numérique (LCEN) (FR) p.215

Épisode 3 : 2005 – ordonnance relative aux échanges électroniques administratifs (FR) ... p.217

Chronique 3

Structuration et renforcement (2010-2015) p.219

Épisode 1 : 2009-2010 – la naissance de la cybersécurité française, Anssi et RGS (FR) p.219

Épisode 2 : 2013 – loi de programmation militaire (FR) p.222

Épisode 3 : 2015 – loi Notre (FR) p.224

Épisode 4 : 2015 – DSP2 (directive sur les services de paiement 2) (EU) p.226

Chronique 4

L'émergence du cadre européen (2016-2020) p.227

Épisode 1 : 2016 – le règlement général sur la protection des données (EU) p.227

Épisode 2 : 2016 – loi pour une République numérique (loi Lemaire) (FR) p.230

Épisode 3 : 2016 – directive NIS (EU) p.232

Épisode 4 : 2019 – *Cybersecurity Act* (EU) p.234

Chronique 5

L'accélération des enjeux cyber (2021-2025) p.236

Épisode 1 : 2021 – stratégie nationale de cybersécurité (FR) p.236

Épisode 2 : 2021 – ordonnance sur la publicité des actes des collectivités territoriales (FR) .. p.238

Épisode 3 : 2022 – loi 3DS (FR) p.239

Épisode 4 : 2022 – NIS 2 (EU) p.241

Épisode 5 : 2023 – loi d'orientation et de programmation du ministère de l'Intérieur (FR) .. p.245

Épisode 6 : 2024 – règlement IA (EU) (ou *AI Act*) p.247Épisode 7 : 2024 – *Cyber Resilience Act* (EU) p.249Épisode 8 : 2025 – loi relative à la résilience des infrastructures critiques
et au renforcement de la cybersécurité (FR) p.251