RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

LES COLLECTIVITÉS FACE AUX ENJEUX DE CYBERSÉCURITÉ

Cadre juridique applicable

Camille Dubedout – Doctorante, ANSSI
Valentin Schabelman – Doctorant, Examin

SAVIEZ-VOUS QUE

30 %

des collectivités territoriales ont déjà été victimes d'un rançongiciel ?

Étude du Clusif, juin 2020

Les rançongiciels (ransomware en anglais) sont des logiciels malveillants qui bloquent l'accès à l'ordinateur ou à des fichiers en les chiffrant et qui réclament à la victime le paiement d'une rançon pour en obtenir de nouveau l'accès.
Source : **www.cybermalveillance.gouv.fr**

QUELS SONT LES IMPACTS ?

DIRECTS

Vol de données, chiffrement des données, interruption des services administratifs durant plusieurs jours voire plusieurs semaines.

INDIRECTS

Coûts financiers de rétablissement des services numériques, atteinte à la réputation, conséquences juridiques, etc.

QUE FAUT-IL PROTÉGER ?

DES DONNÉES

Données d'état civil, données personnelles issues des prestations sociales, données financières, etc.

DES SERVICES

Services en ligne de paiement de cantine, de déclaration d'imposition, de cantine scolaire, d'inscription scolaire, etc.

DES SYSTÈMES & DES INFRASTRUCTURES

Systèmes d'information et de communication, réseaux d'énergie, etc.

En 2020, les signalements d'attaques par rançongiciel ont été multipliés par 3,5 par rapport à 2019. Toutes les collectivités sont concernées, quelle que soit leur taille.
Source : ANSSI

ÉVOLUTION DU CADRE RÉGLEMENTAIRE

MAI 2010 (revisé en 2014)
Le référentiel général de sécurité (RGS) fixe le premier cadre français de la confiance numérique pour les téléservices et au sein de l'administration.

DÉCEMBRE 2013
La loi de programmation militaire (LPM) garantit la protection des activités d'importance vitale.

AVRIL 2016 (entrée en vigueur le 25 mai 2018)
Le Règlement général sur la protection des données (RGPD) responsabilise les acteurs publics et privés quant à la protection des données personnelles.

JUILLET 2016
La directive *Network and Information Security* (NIS) garantit la protection des services essentiels au sein de l'Union européenne.

OCTOBRE 2016
La loi pour une République numérique (LRN) introduit de nouvelles dispositions relatives à l'Open data et confirme les dispositions du RGPD en matière de protection des données personnelles.

QUELS SONT LES OBJECTIFS DE CES RÉGLEMENTATIONS ?

Renforcer la confiance des usagers dans les services numériques.

Garantir la protection des données personnelles et des infrastructures qui les hébergent.

Renforcer la sécurité des activités d'importance vitale et des services essentiels.

SAISISSEZ-VOUS DE L'ENJEU CYBER !

Les collectivités territoriales sont responsables de la sécurité des données qu'elles traitent et de leurs services numériques vis-à-vis des autorités et des citoyens.

Les normes de cybersécurité et de protection des données instaurent une **logique de prévention des risques.** Elles impliquent une mise en conformité permanente et dynamique. Les collectivités doivent donc démontrer qu'elles offrent un niveau optimal de protection.

QUELLES SONT LES MESURES GÉNÉRALES À METTRE EN PLACE ?

CADRE JURIDIQUE

À SÉCURISER : TÉLÉSERVICES
TEXTE RÉGLEMENTAIRE ASSOCIÉ : RGS

- Analyse de risques et définition des mesures de sécurité adaptées aux enjeux et aux menaces
- Homologation de sécurité du téléservice
- Suivi opérationnel et amélioration continue

À SÉCURISER : DONNÉES PERSONNELLES
TEXTE RÉGLEMENTAIRE ASSOCIÉ : RGPD

- Nomination d'un délégué à la protection des données
- Établissement d'un registre de traitement
- Analyse d'impact lorsqu'un traitement peut impliquer un risque élevé pour les droits et les libertés des personnes concernées
- Mise en place des clauses relatives à la protection des données personnelles avec ses fournisseurs et ses sous-traitants
- Notification des violations de données personnelles

À SÉCURISER : SYSTÈMES D'INFORMATION D'IMPORTANCE VITALE OU ESSENTIELS
TEXTES RÉGLEMENTAIRES ASSOCIÉS : LPM & DIRECTIVE NIS

- Définition d'une politique de sécurité des systèmes d'information
- Cartographie des systèmes d'information
- Analyse de risques des activités d'importance vitale ou des services essentiels
- Homologation des systèmes d'information
- Audit de sécurité

Des services et des produits qualifiés par l'ANSSI permettent de répondre à certaines exigences réglementaires comme celles du RGS :
www.ssi.gouv.fr/administration/visa-de-securite

LES FONDAMENTAUX POUR PROTÉGER SES SERVICES NUMÉRIQUES

SOCLE DE SÉCURITÉ
« MESURES D'HYGIÈNE INFORMATIQUE »

Exemples : sauvegardes régulières, gestion des droits d'accès, gestion des mots de passe, dispositifs de chiffrement, cloisonnement des réseaux, application des correctifs et des mises à jour et détection des incidents.

POUR FAIRE LA DIFFÉRENCE

- Nommer un responsable de la sécurité numérique
- Organiser des formations régulières au bénéfice des agents
- S'entraîner à la gestion d'incidents de type rançongiciel
- Mettre en place des clauses de sécurité avec ses fournisseurs et ses sous-traitants
- Mettre en place un dispositif de gestion de crise et de continuité d'activité en cas de sinistre
- Adhérer à un dispositif de supervision et de réponse à incident

POUR ALLER PLUS LOIN

- *Sécurité numérique des collectivités territoriales : l'essentiel* de la réglementation, ANSSI, 2020.
- Kit de sensibilisation, **www.cybermalveillance.gouv.fr**
- *Cybersécurité : toutes les communes et intercommunalités sont concernées*, Association des maires de France et des présidents d'intercommunalités, 2020.
- *Guide de sensibilisation au RGPD pour les collectivités territoriales*, CNIL, 2019.
- *Attaques par rançongiciels, tous concernés*, ANSSI, 2020.
- Prestataires de sécurité : le label ExpertCyber, **www.cybermalveillance.gouv.fr**
- *Guide pratique pour une collectivité et un territoire numérique de confiance*, Banque des territoires, 2020.

Version 1.0 - Avril 2021
Licence Ouverte/Open Licence (Etalab — V1)
AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION
ANSSI – 51, boulevard de la Tour-Maubourg – 75700 PARIS 07 SP
www.ssi.gouv.fr – communication@ssi.gouv.fr