

**PROGRAMME TIC-HAITI-BRH-UNITECH**

**DIPLOME D’ETUDES SUPERIEURS SPECIALISEES**

**(DESS)**

**Sécurité des Systèmes Informatiques (SSI)**

**Sujet : Étude de cas – Cyberattaque au Conseil régional de Guadeloupe**

**Wildjorphney DORVILAS**

**Jean Wismy GENEUS**

**Juverson Théodore JOSEPH**

**Jonel LUBIN**

**Judlet STANIS**

**Présenté au Professeur : Blaise Arbouet**

**Mai 2025**

Table des matières

[Introduction 3](#_Toc198315720)

[Sommaire exécutif 3](#_Toc198315721)

[Contexte (Portée) 4](#_Toc198315722)

[Enjeux de cybersécurité 4](#_Toc198315723)

# Introduction

Avant de rentrer dans le vif du sujet, on va faire un bref historique de quelques dates importantes concernant la Guadeloupe étant un archipel situé dans les Caraïbes, faisant partie des Départements et Régions d’Outre-Mer (DROM) français.

* **1493** : Découverte par **Christophe Colomb** lors de son deuxième voyage. L'île est alors habitée par les **Amérindiens Caraïbes**.
* **1635** : Colonisation par les **Français**, début de l’installation coloniale.
* **XVIIe – XIXe siècle** : Développement de plantations (canne à sucre, café, cacao) avec le **travail forcé des esclaves africains**.
* **1848** : **Abolition de l’esclavage** en Guadeloupe.
* **1946** : La Guadeloupe devient un **département français**.
* **Années 2000** : Renforcement de l'identité régionale et montée des revendications sociales, économiques et culturelles.
* **Aujourd’hui**: La Guadeloupe est un territoire français d'outre-mer avec une culture riche et métissée, mêlant influences africaines, européennes, indiennes et caribéennes. Elle fait face à des défis économiques, sociaux et environnementaux, tout en valorisant son patrimoine unique.

À l'ère numérique, les menaces informatiques ciblant les administrations publiques ou privées sont croissantes. En février 2022, le Conseil Régional de la Guadeloupe a été victime d'une cyberattaque qui, une fois de plus, a mis sous grande paralysie une majorité de ses moyens informatiques. Cet incident témoigne du désastre dans lequel se trouvent les infrastructures numériques des collectivités territoriales au regard des cybercriminels de plus en plus sophistiqués et coordonnés. En plus des conséquences purement techniques, cette attaque a, sans aucun doute, impacté la continuité de l'accès aux services publics ainsi que la protection des données d'utilisateur. Ainsi, il est désormais nécessaire d’étudier les causes et les impacts de cette attaque pour appréhender les enjeux de la cybersécurité dans les administrations publiques modernes.

# Sommaire exécutif

Ce rapport se concentre sur l'impact et la justification de cette attaque, en mettant l'accent sur les facteurs structurels et organisationnels qui ont probablement contribué à cette violation. Il examine également les réponses entreprises par le Conseil régional et les tentatives de rétablir le fonctionnement des services numériques.

L'analyse propose, enfin, un certain nombre de recommandations visant à améliorer la sécurité informatique des collectivités publiques locales : formation du personnel, mise à jour des infrastructures, rédaction de plans de continuité des activités et engagement avec des consultants en sécurité informatique.

# Contexte (Portée)

Avec la montée en puissance des outils numériques dans les services publics, les administrations sont de plus en plus dépendantes de leurs systèmes informatiques pour assurer leur bon fonctionnement. Cependant, cette dépendance les rend aussi plus vulnérables aux attaques informatiques, appelées cyberattaques.

En février 2022, le Conseil régional de Guadeloupe a été victime d’une cyberattaque de type rançongiciel (ransomware). Cette attaque a entraîné l’arrêt brutal de plusieurs services administratifs, perturbant la gestion interne et la communication avec les citoyens. Elle a mis en évidence les faiblesses en matière de cybersécurité au sein de la collectivité.

Cet événement ne concerne pas uniquement la Guadeloupe. Il reflète un problème plus large auquel sont confrontées de nombreuses institutions publiques en Haïti, en France et ailleurs. Il montre l’importance pour ces structures de renforcer leur protection informatique afin d’assurer la continuité de leurs missions.

Ce rapport vise donc à mieux comprendre cette attaque, à analyser ses impacts, et à proposer des pistes pour éviter qu’un tel incident ne se reproduise.

# Enjeux de cybersécurité

Quand on fait le point sur la cybersécurité dans une collectivité comme le Conseil régional de Guadeloupe, on pense peut-être, pour ne pas dire souvent, à des virus, des hackers ou des pares-feux. Mais la réalité va beaucoup plus loin que ce que l’on imagine. Ce que l’attaque qu’a subie la Région en novembre 2022 nous montre, c’est que la cybersécurité touche tout le fonctionnement quotidien d’une administration.

* Le premier enjeu, c’est de pouvoir continuer à travailler.

Lorsque l’attaque a eu lieu, tous les systèmes informatiques ont été mis à l’arrêt. Impossible d’envoyer un courriel, d’accéder aux dossiers, ou même de savoir où en étaient certains projets. Tout a dû être suspendu. Et on le sait : dans une collectivité, les services publics doivent continuer, peu importe les circonstances.

Cette crise nous rappelle une chose simple : si l’informatique tombe, tout tombe avec. Sans informatique, plus de paie, plus de gestion des subventions, plus de courrier interne. D’où l’importance de penser la cybersécurité comme une condition de survie du service public.

* Le deuxième enjeu, c’est la protection des données

Dans une collectivité, on gère une énorme quantité de données : celles des agents, des élus, des entreprises partenaires, des citoyens. Ce sont des informations sensibles, parfois très personnelles.

Dans le cas de la Guadeloupe, on sait qu’un ransomware a été utilisé. Cela signifie que les données ont probablement été chiffrées par les attaquants, voire copiées. Même si on n’a pas tous les détails, on peut imaginer l’angoisse que cela a pu créer : est-ce que les données ont fuité ? Qui y a eu accès ? Et que va-t-il se passer si elles sont publiées ?

C’est un vrai rappel : protéger les données, c’est protéger les gens.

L’image de la collectivité est aussi en jeu

Dans un monde où tout va vite, une attaque informatique devient très vite un sujet médiatique. Et le risque, c’est que les citoyens ou les partenaires perdent confiance : "Est-ce que les données sont en sécurité ?", "Est-ce que la Région est bien préparée ?".

La Guadeloupe a réagi rapidement en communiquant de manière transparente, ce qui est à saluer. Mais cela montre aussi qu’il faut être prêt, pas seulement techniquement, mais aussi humainement et en termes de communication.

Et surtout, il ne faut pas oublier le facteur humain

La plupart des attaques commencent par un simple e-mail piégé. Un clic, et tout bascule. Ce n’est pas une question d’incompétence, c’est humain : on est pressé, on fait confiance, on ne voit pas le danger.

C’est pour ça que la cybersécurité ne doit pas être l’affaire des seuls informaticiens. Tout le monde doit être formé, sensibilisé, responsabilisé.

# Classification des données

Quand on parle de sécurité, on pense souvent à renforcer les protections. Mais une étape clé est souvent oubliée : savoir ce qu’on protège. Et pour cela, il faut absolument classer les données.

* Dans le cas du Conseil, il est probable que les attaquants n’aient pas fait dans le détail : ils ont chiffré tout ce qu’ils ont pu. Mais si la collectivité avait eu une bonne politique de classification, elle aurait su quelles données sont vitales, lesquelles sont sensibles, et lesquelles sont moins critiques.

Pourquoi est-ce important ?

Imaginez par exemple qu’on perde toutes les données d’un web site : embêtant, mais on peut les republier. En revanche, perdre les dossiers Ressources Humaines des agents ou les contrats en cours, c’est une tout autre histoire.

* Classer les données, c’est comme faire le tri chez soi : on ne protège pas un vieux prospectus de la même manière qu’un passeport ou un acte de naissance.

Un exemple concret appliqué à une collectivité comme la Guadeloupe

* Les documents publics (rapports, subventions publiées et autres) - peu sensibles - on veille surtout à la disponibilité.
* Les données personnelles (fiches de paiement, adresses, numéros de sécurité sociale) - très sensibles - accès restreint, chiffrement, sauvegardes séparées.
* Les projets budgétaires en cours - stratégiques - protégés contre la fuite et la manipulation.

En classifiant ses données, une collectivité peut :

* Appliquer les bonnes protections au bon endroit.
* Mieux gérer une crise en priorisant la restauration des données critiques.
* Respecter les réglementations, notamment le RGPD.

Et surtout, c’est un travail d’équipe

Ce ne sont pas que les informaticiens qui doivent savoir ce qui est sensible ou pas. Les agents métiers aussi doivent pouvoir dire : Ceci, c’est critique pour mon service, pour le fonctionnement global du système. On parle d’un travail collectif, entre les directions.

# Sources utilisées

* Conseil régional de Guadeloupe – Communiqué officiel sur la cyberattaque (novembre 2022) | regionguadeloupe.fr
* FranceInfo – Cyberattaque de grande ampleur (22 novembre 2022) | francetvinfo.fr
  + Le Monde Informatique – Détails techniques de l’attaque (22 novembre 2022) | lemondeinformatique.fr