**Introduction**

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

**Quelques dates clés :**

* **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.

En février 2022, le Conseil régional de Guadeloupe a subi une cyberattaque majeure qui a perturbé ses opérations administratives. Tous les systèmes d'information de la collectivité ont été entièrement fermés, affectant la gestion des dossiers, la communication interne et les relations avec les citoyens ainsi qu'avec les partenaires. Cette attaque par ransomware s'inscrit dans un schéma global caractérisé par une montée des menaces cybernétiques contre les institutions publiques.

**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.

Ce rapport cherche à utiliser le focus de cette attaque comme un moyen d'encourager une approche proactive pour une préparation plus efficace afin de faire face aux menaces numériques en perpétuelle évolution en accord avec la résilience du service public et la protection.

**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 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**

La cybersécurité est aujourd’hui un enjeu majeur pour toutes les organisations, y compris les administrations publiques. Elle désigne l’ensemble des moyens mis en œuvre pour protéger les systèmes informatiques, les données et les communications contre les attaques ou les intrusions malveillantes.

Dans le cas du **Conseil régional de Guadeloupe**, la cyberattaque subie en 2022 montre à quel point une institution peut être fragilisée lorsque sa sécurité informatique est compromise. Plusieurs enjeux importants se dégagent de cette situation :

1. **Protection des données sensibles**  
   Les administrations traitent de nombreuses informations personnelles, financières et administratives. En cas d’attaque, ces données peuvent être volées, détruites ou utilisées à des fins illégales.
2. **Continuité du service public**  
   Une cyberattaque peut paralyser l’activité d’une collectivité, empêchant la population d’accéder aux services essentiels (aides, subventions, documents administratifs, etc.).
3. **Confiance des citoyens**  
   Lorsque les données ou les services sont compromis, la confiance des usagers dans les institutions peut être fortement affectée.
4. **Coûts financiers et organisationnels**  
   La gestion d’une cyberattaque engendre des coûts importants : réparation des systèmes, perte de productivité, recours à des prestataires externes, etc.
5. **Obligations légales**  
   Les collectivités ont l’obligation de protéger les données personnelles conformément au **Règlement Général sur la Protection des Données (RGPD)**. Une faille peut entraîner des sanctions juridiques.

Ces enjeux montrent qu’il est essentiel pour les institutions publiques de mettre en place des stratégies de cybersécurité solides, incluant la prévention, la détection, la réponse aux incidents, et la sensibilisation du personnel.

**Classification des données — *Définition simple***

La **classification des données**, c’est le fait de **trier et organiser les données en catégories** selon leur nature, leur sensibilité ou leur usage, afin de mieux les gérer et les utiliser.

**🔹 Types de classification (exemples)**

1. **Selon la nature des données :**
   * **Données numériques** : vitesses de véhicules, temps de trajet
   * **Données textuelles** : avis des usagers, rapports d’incidents
   * **Données visuelles** : images de caméras de surveillance
2. **Selon la source des données :**
   * Capteurs de circulation
   * GPS des véhicules
   * Applications mobiles
   * Réseaux sociaux
3. **Selon la sensibilité :**
   * **Données publiques** : info trafic, horaires de bus
   * **Données personnelles** : localisation des utilisateurs, trajets individuels
   * **Données confidentielles** : données internes des opérateurs de transport
4. **Selon l’usage prévu :**
   * Analyse en temps réel
   * Prévisions et modélisations
   * Prise de décision automatisée

**✅ Pourquoi classifier ?**

* Pour **protéger les données sensibles**
* Pour **gagner en efficacité** dans leur traitement
* Pour **adapter les outils** aux bons types de données