​Plusieurs entreprises et institutions dans la Caraïbe ont été victimes de cyberattaques ces dernières années. Voici quelques exemples notables :​

* **La Martiniquaise-Bardinet (Martinique)** : En septembre 2021, le groupe français de vins et spiritueux a subi une cyberattaque par ransomware revendiquée par le cybergang BlackMatter. Les attaquants ont dérobé 30 Go de données, notamment des contrats commerciaux et des informations bancaires. La société a choisi de ne pas payer la rançon demandée et a renforcé ses mesures de cybersécurité par la suite. ​[RCI+2Le Monde Informatique+2RCI+2](https://www.lemondeinformatique.fr/actualites/lire-le-ransomware-blackmatter-fait-tituber-la-martiniquaise-bardinet-84242.html?utm_source=chatgpt.com)
* **Conseil régional de Guadeloupe (Guadeloupe)** : En novembre 2022, la région a été victime d'une cyberattaque de grande ampleur, entraînant l'interruption de tous les réseaux informatiques pour protéger les données. Une cellule de crise a été mise en place et les autorités compétentes ont été alertées. ​[KARIBINFO+4Siècle Digital+4L'Usine Digitale+4](https://siecledigital.fr/2022/11/22/la-region-guadeloupe-est-victime-dune-cyberattaque/?utm_source=chatgpt.com)
* **Collectivité Territoriale de Martinique (Martinique)** : En mai 2023, cette institution a subi une cyberattaque par ransomware, revendiquée par le groupe Rhysida. Les attaquants ont divulgué des échantillons de données dérobées, notamment des documents d'identité et des devis. Une cellule de crise a été activée pour rétablir les services et enquêter sur l'incident. ​[RCI+3INCYBER NEWS+3Outre-mer la 1ère+3](https://incyber.org/article/rhysida-revendique-la-cyberattaque-contre-la-martinique/?utm_source=chatgpt.com)
* **Entreprises guadeloupéennes (Guadeloupe)** : En novembre 2020, plusieurs dizaines d'entreprises ont été victimes de cyberattaques, touchant divers secteurs d'activité. L'UDE-MEDEF a mis en place une cellule de crise pour aider les entreprises concernées. ​[RCI](https://rci.fm/guadeloupe/infos/Economie/Des-entreprises-guadeloupeennes-victimes-de-cyberattaques?utm_source=chatgpt.com)
* **Entreprises en Haïti** : En septembre 2023, un individu spécialisé dans le piratage des cartes bancaires des entreprises, notamment la compagnie téléphonique Digicel, a été arrêté. Il était impliqué dans le vol de millions de gourdes et de milliers de dollars américains. ​[KARIBINFO+2Image7+2Le Monde Informatique+2](https://image7haiti.com/escroquerie-un-haitien-specialise-dans-le-piratage-des-cartes-bancaires-des-entreprises-en-haiti-arrete-par-la-dcpj/?utm_source=chatgpt.com)

Ces incidents soulignent la vulnérabilité des entreprises et institutions de la Caraïbe face aux cybermenaces croissantes. Il est essentiel pour ces entités de renforcer leurs mesures de cybersécurité pour se protéger contre de telles attaques.

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

**Consigne :**  
En novembre 2022, le **Conseil régional de Guadeloupe** a été victime d’une **cyberattaque de grande ampleur**, entraînant l’interruption totale de ses réseaux informatiques afin de protéger les données.

À partir de cette situation, répondez aux questions suivantes :

1. **Identifiez les enjeux liés à la cybersécurité** dans les institutions publiques.
2. **Expliquez les conséquences possibles** d’une telle attaque sur le fonctionnement de l’administration et sur les citoyens.
3. Quelles **mesures préventives** et **réactions immédiates** peuvent être mises en place pour limiter les impacts d’une cyberattaque ?
4. Selon vous, quel **niveau de sensibilité** peuvent avoir les données traitées par une collectivité territoriale comme la région Guadeloupe ?

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

**Consigne :**  
En novembre 2022, le **Conseil régional de Guadeloupe** a été victime d’une **cyberattaque de grande ampleur**, entraînant l’interruption totale de ses réseaux informatiques afin de protéger les données.

À partir de cette situation, répondez aux questions suivantes :

1. **Identifiez les enjeux liés à la cybersécurité** dans les institutions publiques.
2. **Expliquez les conséquences possibles** d’une telle attaque sur le fonctionnement de l’administration et sur les citoyens.
3. Quelles **mesures préventives** et **réactions immédiates** peuvent être mises en place pour limiter les impacts d’une cyberattaque ?
4. Selon vous, quel **niveau de sensibilité** peuvent avoir les données traitées par une collectivité territoriale comme la région Guadeloupe ?

Souhaites-tu que je prépare un document complet avec ce sujet, ou l’ajouter à un document existant ?

##### You said:

repondre aux consignes

###### ChatGPT said:

Voici une **réponse complète** aux consignes du sujet sur la cyberattaque du **Conseil régional de Guadeloupe** :

## 🛡️ **Étude de cas – Cyberattaque au Conseil régional de Guadeloupe (Novembre 2022)**

### ****1. Enjeux liés à la cybersécurité dans les institutions publiques****

Les institutions publiques, comme les collectivités territoriales, traitent une grande quantité de **données sensibles** : informations personnelles des citoyens, dossiers sociaux, données financières, documents administratifs, etc.  
Les principaux enjeux sont :

* **Protection des données personnelles** (conformité RGPD)
* **Continuité des services publics**
* **Confiance des usagers** envers l’administration
* **Prévention des pertes financières** et du vol de données
* **Résilience informatique** face aux cybermenaces croissantes (ransomwares, phishing, attaques DDoS…)

### ****2. Conséquences possibles d’une telle attaque****

Une cyberattaque de grande ampleur peut avoir des impacts graves sur plusieurs plans :

* **Interruption des services publics** (dossiers bloqués, démarches impossibles)
* **Atteinte à la confidentialité des données** (fuite ou vol d'informations personnelles)
* **Perte de productivité** et de fonctionnement interne
* **Coûts élevés** pour la remise en état des systèmes et des infrastructures informatiques
* **Atteinte à l’image** et à la crédibilité de l’institution
* **Pression psychologique** sur les agents et les usagers (stress, inquiétudes, méfiance)

### ****3. Mesures préventives et réactions immédiates****

#### ✅ **Mesures préventives :**

* Mise en place de **pare-feux, antivirus, et solutions de détection d’intrusion**
* **Sensibilisation et formation du personnel** aux risques cyber
* Politique stricte de **gestion des mots de passe** et des accès
* Réalisation régulière de **sauvegardes sécurisées**
* Élaboration d’un **plan de continuité d’activité (PCA)** et d’un **plan de reprise informatique (PRI)**

#### 🚨 **Réactions immédiates :**

* **Coupure des systèmes** pour limiter la propagation (comme l’a fait la Guadeloupe)
* **Notification aux autorités compétentes** (CNIL, ANSSI…)
* Enquête technique pour **identifier la faille** et évaluer les dégâts
* Communication claire avec les usagers et les partenaires
* Mise en place d’un plan de **remédiation et restauration progressive**

### ****4. Niveau de sensibilité des données traitées par une collectivité territoriale****

Les données traitées par une collectivité sont généralement **confidentielles**, parfois **secrètes**, selon leur nature. Elles peuvent inclure :

* Informations personnelles des citoyens (état civil, santé, situation sociale)
* Données RH (salaires, contrats, données bancaires du personnel)
* Données financières de l’administration
* Dossiers d’appels d’offres, contrats publics

La fuite ou la compromission de ces données peut entraîner des **violations de la vie privée**, des **fraudes**, et nuire gravement au **fonctionnement des services publics**.