**1. Introduction**

Le 28 avril 2022, **Massy Stores**, l'une des plus grandes chaînes de supermarchés de Trinité-et-Tobago, a été victime d'une cyberattaque majeure. Cette attaque a entraîné la fermeture de ses 23 magasins à travers le pays, perturbant gravement ses opérations et affectant ses services de pharmacie, de transfert d'argent (Surepay et MoneyGram), ainsi que ses systèmes de paiement en magasin .

L'attaque a été attribuée au groupe de ransomware **Hive**, qui a utilisé une méthode d'attaque par **phishing ciblé** pour accéder aux systèmes internes de l'entreprise. Une fois à l'intérieur, les attaquants ont déployé un logiciel malveillant pour chiffrer les données et exfiltrer des informations sensibles. En octobre 2022, le groupe Hive a publié en ligne environ 87 550 dossiers et 704 047 fichiers d'entreprise, comprenant des informations personnelles sur les employés, des documents financiers internes, des copies de passeports de clients et des informations de transfert bancaire .

Cet incident souligne la vulnérabilité des entreprises de la région caraïbe face aux cybermenaces et met en évidence la nécessité d'une approche proactive en matière de cybersécurité. Le présent document vise à analyser cet incident en profondeur, à évaluer les risques associés et à proposer des recommandations pour renforcer la résilience des entreprises face aux cyberattaques.

**2. Sommaire Exécutif**

Le 28 avril 2022, **Massy Stores** a subi une cyberattaque majeure qui a paralysé ses opérations à Trinité-et-Tobago. L'attaque a été attribuée au groupe de ransomware **Hive**, qui a utilisé une méthode de phishing ciblé pour accéder aux systèmes internes de l'entreprise. Une fois à l'intérieur, les attaquants ont déployé un logiciel malveillant pour chiffrer les données et exfiltrer des informations sensibles.

En octobre 2022, le groupe Hive a publié en ligne environ 87 550 dossiers et 704 047 fichiers d'entreprise, comprenant des informations personnelles sur les employés, des documents financiers internes, des copies de passeports de clients et des informations de transfert bancaire. Cette fuite de données a été qualifiée de « plus grande fuite de données des Caraïbes à ce jour » .

L'impact de l'attaque a été considérable :

* **Perturbation des opérations** : Fermeture de tous les magasins pendant plusieurs jours, affectant les ventes et les services aux clients.
* **Exposition des données sensibles** : Fuite de données personnelles des employés et des clients, augmentant les risques de fraude et de vol d'identité.
* **Atteinte à la réputation** : Perte de confiance des clients et des partenaires commerciaux.

Les principales conclusions de l'analyse de l'incident sont les suivantes :

* **Vulnérabilités identifiées** : Manque de formation des employés sur les menaces de phishing, absence de sauvegardes hors ligne sécurisées, et absence de plan de réponse aux incidents bien défini.
* **Réponse initiale** : Suspension rapide des systèmes affectés et collaboration avec des experts externes pour résoudre la situation.
* **Leçons apprises** : Nécessité d'améliorer la cybersécurité à tous les niveaux de l'organisation, de renforcer la formation des employés et de mettre en place des mesures de protection des données plus robustes.

Les recommandations immédiates incluent :

* **Renforcement de la formation** : Sensibilisation accrue des employés aux menaces de phishing et aux bonnes pratiques en matière de cybersécurité.
* **Amélioration des sauvegardes** : Mise en place de sauvegardes régulières et sécurisées, y compris hors ligne.
* **Renforcement de la sécurité des systèmes** : Mise à jour régulière des systèmes et des logiciels pour corriger les vulnérabilités connues.
* **Développement d'un plan de réponse aux incidents** : Élaboration et test réguliers d'un plan de réponse aux incidents pour assurer une réaction rapide et efficace en cas de cyberattaque.

**3. Contexte (Portée)**

**3.1 Présentation de Massy Stores**

**Massy Stores** est une chaîne de supermarchés opérant principalement à Trinité-et-Tobago, avec des magasins également en Jamaïque, en Guyane, à Sainte-Lucie et à la Barbade. Elle fait partie du groupe **Massy Group**, un conglomérat régional diversifié opérant dans les secteurs de la distribution, de l'énergie, des services financiers et des technologies.

En Trinité-et-Tobago, Massy Stores est l'un des principaux détaillants alimentaires, avec 23 magasins à travers le pays. L'entreprise offre une large gamme de produits, y compris des produits alimentaires, des articles ménagers, des services de pharmacie et de transfert d'argent. Elle sert une clientèle diversifiée, allant des consommateurs individuels aux entreprises locales.

**3.2 Contexte géopolitique et cybercriminel dans les Caraïbes**

La région des Caraïbes a connu une augmentation significative des cyberattaques ces dernières années. En 2022, la région a enregistré 144 millions de tentatives de cyberattaques, avec une prévalence particulière des ransomwares . Cette tendance est alimentée par plusieurs facteurs :

* **Numérisation accrue** : Adoption rapide des technologies numériques par les entreprises et les gouvernements, créant de nouvelles surfaces d'attaque.
* **Manque de ressources en cybersécurité** : De nombreuses organisations manquent de personnel qualifié et de ressources pour mettre en œuvre des mesures de cybersécurité efficaces.
* **Lacunes législatives** : Absence de législations robustes en matière de protection des données et de lutte contre la cybercriminalité.

Les groupes de cybercriminels, tels que **Hive**, ciblent souvent des entreprises de taille moyenne, considérées comme des cibles vulnérables offrant un bon retour sur investissement. Ces groupes utilisent des techniques sophistiquées, telles que le phishing ciblé et les ransomwares-as-a-service, pour mener leurs attaques.

**3.3 Historique des incidents similaires**

Avant l'attaque contre Massy Stores, plusieurs autres entreprises de la région ont été victimes de cyberattaques notables :

* **TSTT (Telecommunications Services of Trinidad and Tobago)** : En octobre 2023, TSTT a subi une attaque par ransomware du groupe **RansomEXX**, entraînant l'exfiltration de 6 Go de données clients .
* **AeroPost** : En avril 2022, des informations de carte de crédit de clients d'AeroPost ont été compromises à la suite d'une cyberattaque.
* **Hôpital Corbeil-Essonnes (France)** : En août 2022, l'hôpital a été victime d'une cyberattaque, entraînant la fuite de données sensibles sur le dark web.

Ces incidents soulignent la vulnérabilité des entreprises, même dans les petites économies insulaires, face aux cybermenaces croissantes. L'attaque contre Massy Stores représente une escalade significative dans la sophistication des attaques dans la région des Caraïbes.

## 4. Enjeux de Cybersécurité

### 4.1 Vulnérabilités exploitées

L’attaque contre Massy Stores a exploité plusieurs vulnérabilités classiques mais critiques, révélant des lacunes dans la posture de cybersécurité de l’organisation :

* **Phishing ciblé** : Le vecteur initial de l’attaque a été un courriel de phishing sophistiqué, trompant un ou plusieurs employés pour obtenir un accès aux systèmes internes. Ce type d’attaque exploite la faiblesse humaine, soulignant l’importance d’une formation continue en cybersécurité.
* **Absence de sauvegardes sécurisées** : L’absence ou l’insuffisance de sauvegardes hors ligne sécurisées a empêché une restauration rapide des données. Cette lacune a amplifié la dépendance à la négociation avec les attaquants.
* **Défauts de gestion des correctifs (patchs)** : Une mauvaise gestion des mises à jour de sécurité a laissé des failles exploitables par le ransomware. L’application tardive ou incomplète des patchs critiques est souvent une porte d’entrée pour les cybercriminels.
* **Manque de segmentation réseau** : L’attaque a pu se propager rapidement à travers les systèmes, signe d’un réseau insuffisamment segmenté, facilitant la diffusion du malware.

### 4.2 Impacts opérationnels

L’impact sur les opérations a été immédiat et profond :

* **Fermeture de tous les magasins** : Les 23 magasins ont dû fermer temporairement, impactant directement les revenus et la chaîne d’approvisionnement.
* **Interruption des services annexes** : Les services de pharmacie et les systèmes de transfert d’argent ont été suspendus, affectant la clientèle et la réputation de l’entreprise.
* **Perte d’accès aux systèmes internes** : Les employés ont été privés d’accès à leurs outils de travail, ralentissant les opérations de gestion, de comptabilité et de logistique.

### 4.3 Conséquences légales et réputationnelles

* **Atteinte à la confiance des clients** : La fuite de données sensibles a compromis la confiance des consommateurs, particulièrement dans un secteur lié à l’alimentation et à la santé.
* **Responsabilité légale** : Selon les lois locales et régionales sur la protection des données (inspirées du GDPR), Massy Stores risque des sanctions pour manquement à la sécurité des données personnelles.
* **Risques financiers** : Outre le coût de la restauration et de l’intervention, l’entreprise fait face à des risques de poursuites judiciaires, de pénalités réglementaires et d’éventuelles pertes commerciales.

## 5. Classification des Données

### 5.1 Types de données compromises

Les données affectées par l’attaque comprennent :

* **Données personnelles des clients** : Noms, adresses, numéros de téléphone, copies de passeports, informations sur les cartes d’identité.
* **Données financières** : Informations relatives aux transactions financières, données de paiement, transferts d’argent (Surepay, MoneyGram).
* **Données des employés** : Informations personnelles et professionnelles, contrats de travail, documents administratifs.
* **Données opérationnelles** : Informations internes liées à la gestion des stocks, logistique, approvisionnement.

### 5.2 Niveau de sensibilité et cadre réglementaire

* **Protection des données personnelles** : Trinité-et-Tobago a adopté en 2011 la **Data Protection Act**, qui impose des obligations aux entreprises pour protéger les données personnelles et garantir leur confidentialité, intégrité et disponibilité.
* **Normes internationales** : Bien que non obligatoire, le cadre européen GDPR sert de référence pour la gestion des données sensibles et impose un haut niveau de protection. L’incident de Massy Stores montre que ces normes ne sont pas toujours respectées, exposant les données à un risque élevé.
* **Impact** : Les données compromises sont considérées comme hautement sensibles, notamment les informations financières et personnelles, ce qui accroît les risques de fraude, d’usurpation d’identité et de pertes économiques.

## 6. Analyse de Risque

### 6.1 Méthodologie utilisée

Pour cette analyse, nous avons utilisé une approche hybride combinant les référentiels **ISO 27005** et **NIST Cybersecurity Framework (CSF)**, permettant d’évaluer à la fois les risques liés à la sécurité de l’information et la résilience opérationnelle.

### 6.2 Évaluation des risques

| **Risque** | **Probabilité** | **Impact** | **Niveau de risque** |
| --- | --- | --- | --- |
| Phishing ciblé | Élevée | Critique | Très élevé |
| Absence de sauvegardes sûres | Moyenne | Critique | Élevé |
| Propagation rapide du malware | Élevée | Important | Élevé |
| Fuite de données personnelles | Moyenne | Critique | Élevé |
| Perte de confiance client | Moyenne | Important | Élevé |
| Sanctions légales | Faible | Important | Moyen |

### 6.3 Scénarios de menaces

* **Réattaque** : Sans renforcement des mesures, Massy Stores risque une nouvelle attaque, potentiellement plus dévastatrice.
* **Fuite massive de données** : L’exploitation ou la vente des données volées peut causer des dommages financiers et réputationnels à long terme.
* **Impact sur les partenaires** : Les fournisseurs et partenaires pourraient aussi être affectés, amplifiant la portée des risques.

## 7. Recommandations (Mesures de Contrôle)

### 7.1 Mesures immédiates

* **Restauration à partir de sauvegardes hors ligne** : Assurer la récupération rapide des systèmes en isolant les sauvegardes de toute connexion réseau.
* **Investigation forensique** : Collaborer avec des experts pour identifier précisément la souche du ransomware, comprendre la méthode d’intrusion et évaluer l’étendue de la compromission.
* **Communication transparente** : Informer les clients, employés et autorités réglementaires de manière claire et rapide pour maintenir la confiance.

### 7.2 Mesures à moyen terme

* **Formation et sensibilisation** : Mettre en place des programmes réguliers de formation au phishing et aux bonnes pratiques de cybersécurité pour tous les employés.
* **Mise en place d’un SOC (Security Operations Center)** : Développer une équipe dédiée à la surveillance, détection et réponse aux incidents de cybersécurité en temps réel.
* **Amélioration de la gestion des correctifs** : Instaurer une politique stricte de mise à jour et de patching pour réduire la surface d’attaque.

### 7.3 Mesures à long terme

* **Adoption d’un cadre de cybersécurité reconnu** : Intégrer les normes ISO 27001 ou NIST CSF pour structurer et améliorer continuellement la sécurité.
* **Segmentation réseau et contrôle des accès** : Réduire la propagation des attaques en limitant les accès aux systèmes sensibles.
* **Tests d’intrusion réguliers** : Effectuer des audits et tests de pénétration pour identifier les vulnérabilités avant que les attaquants ne le fassent.
* **Plan de continuité et de réponse aux incidents** : Établir et tester un plan pour garantir la résilience des opérations face à de futures attaques.

## 8. Conclusion

L’attaque par ransomware contre Massy Stores illustre la gravité des cybermenaces auxquelles sont confrontées les entreprises des Caraïbes, même celles opérant dans des secteurs essentiels comme la distribution alimentaire. Cet incident met en lumière des failles critiques dans la gestion de la cybersécurité, notamment la vulnérabilité humaine face aux attaques de phishing, le manque de sauvegardes sécurisées, et une préparation insuffisante face à une attaque de grande ampleur.

La conséquence directe de cette attaque a été une perturbation majeure des opérations, une fuite massive de données sensibles et une atteinte significative à la réputation de l’entreprise. Ces impacts soulignent à quel point la cybersécurité doit être intégrée au cœur de la stratégie d’entreprise.

Pour prévenir la répétition de tels incidents, Massy Stores, et plus largement les entreprises de la région, doivent adopter une approche proactive et holistique en cybersécurité. Cela inclut non seulement la mise en place de technologies avancées, mais aussi la formation des employés, la gouvernance des risques et la collaboration avec les autorités.

La résilience numérique est désormais un impératif stratégique. L’exemple de Massy Stores devrait servir de signal d’alarme pour toutes les entreprises caribéennes, les incitant à renforcer leurs défenses, à anticiper les menaces et à protéger les données de leurs clients et collaborateurs. Seule une vigilance constante et des investissements continus permettront de réduire l’impact des cyberattaques dans cette région dynamique mais vulnérable.