Table des Matières

1. Introduction 1
2. Sommaire exécutif1
3. Contexte (portée)2
4. Enjeux de cybersécurité3
5. Classification des données4
6. Analyse de risque6
7. Recommandations (mesure de contrôles)10
8. Conclusion12

**Références 13**

1. **Introduction**

Dans un contexte numérique en constante évolution, les entreprises sont de plus en plus exposées à des cybermenaces sophistiquées. En avril 2022, le Groupe Massy, conglomérat régional, en a récemment fait les frais à travers une attaque par ransomware de grande ampleur. Cet incident a révélé de sérieuses vulnérabilités au sein de l'infrastructure informatique de l’organisation, mettant en évidence la nécessité impérieuse d’une stratégie de cybersécurité robuste et proactive.

Ce devoir vise à analyser en profondeur les circonstances de cette attaque, les impacts observés, ainsi que les failles ayant permis sa réalisation. Il propose une évaluation des risques encourus, une classification des données sensibles affectées, et une série de recommandations pour renforcer les défenses de l’entreprise. L’objectif principal est de dégager des enseignements concrets afin de prévenir de futures intrusions et d’assurer une continuité opérationnelle face aux menaces numériques croissantes.

1. **Sommaire exécutif**

L’attaque subie par le Groupe Massy illustre les défis auxquels sont confrontées les entreprises dans un paysage cyber de plus en plus hostile. L’incident a débuté par une campagne de phishing ciblée, suivie de l’exploitation de vulnérabilités techniques pour prendre le contrôle des systèmes. Les pirates ont ensuite procédé à un double chantage : chiffrement des données et menace de divulgation des informations volées.

Les conséquences ont été sévères : interruption des services pendant plusieurs jours, coûts de remédiation estimés entre 5 et 10 millions de dollars, et risque d’amendes pour non-conformité au RGPD. Plus grave encore, la confiance des clients et partenaires a été ébranlées, avec un impact durable sur la réputation de l’entreprise.

Les risques associés à cette attaque sont multiples : atteinte à la réputation, exposition juridique en lien avec la législation sur la protection des données, pertes économiques liées à la reprise d’activité et à la sécurisation des systèmes, ainsi qu’un risque direct pour les personnes concernées par les données compromises.

Ce document dresse un état des lieux de l’attaque en identifiant les failles d’accès qui ont permis d’évaluer l’ampleur des dommages et propose une série de recommandations stratégiques pour renforcer la capacité de continuité du Groupe Massy face aux menaces numériques. Il insiste également sur l’importance de mettre en place une culture de cybersécurité plus proactive à l’échelle de l’organisation.

1. **Contexte (portée)**

Le groupe Hive, à l’origine de cette attaque, est connu pour ses méthodes agressives de double extorsion.

Dans le cas présent, les enquêtes ont révélé que les pirates ont exploité une combinaison de facteurs : des employés trompés par des emails de phishing, des correctifs de sécurité non appliqués et un manque de segmentation réseau. Ces failles ont permis aux attaquants de se déplacer latéralement dans le système jusqu’à atteindre les données les plus sensibles.

Cette stratégie consiste à chiffrer les données de l’organisation ciblée tout en menaçant de divulguer les informations sensibles dérobées mettant ainsi la pression sur les victimes pour qu’elles cèdent à la demande de rançon. Selon certaines sources, le groupe de ransomware Hive aurait mis en ligne environ 87 550 dossiers et 704 047 fichiers d'entreprise, appartenant à Massy Stores Trinidad et Tobago. Le fait que ces données aient été publiées **suggère que Massy Stores n’a pas payé la rançon**, ce qui a conduit les pirates à publier les fichiers sur le dark web. Par la suite, la page web permettant de télécharger les fichiers avait été supprimée. Un expert de cybersécurité estime que cela pourrait signifier que Massy Stores a finalement payé la rançon, car les pirates auraient alors retiré la page de téléchargement des fichiers de l’entreprise. Cependant, le lien direct vers les fichiers sur le serveur restait accessible.

Les pirates ont probablement utilisé une **faille humaine (phishing)** pour entrer dans le système de l’entreprise, puis exploité des **failles techniques** pour s’étendre, voler les données et finalement **déclencher le ransomware** qui a finalement chiffré les systèmes critiques. L’incident n’a été découvert et signalé qu’après cette dernière étape, révélant ainsi l’ampleur de la compromission. Plusieurs systèmes critiques ont été impactés par cette attaque, notamment les serveurs de données centraux, les systèmes de gestion des ressources humaines, les bases de données clients et les réseaux de communication internes.

1. **Enjeux de cybersécurité**

Le groupe Massy, conglomérat centenaire basé à Trinité-et-Tobago, est confronté à plusieurs enjeux stratégiques et opérationnels alors qu'il poursuit son expansion dans les Caraïbes, en Amérique latine et aux États-Unis. Voici un aperçu des principaux enjeux et priorités actuels du groupe :​

1. **Expansion internationale et diversification (pour numeration je propose 4.1 …)**

Massy vise une croissance organique et par acquisitions pour atteindre un chiffre d'affaires de plus de 4 milliards de dollars américains d'ici 2030. Le groupe se concentre sur trois secteurs clés : **le commerce** **de détail intégré**, **les produits gaziers** et **les moteurs et machines**. Des acquisitions majeures ont été réalisées, notamment Rowe’s IGA en Floride, Air Liquide à Trinité-et-Tobago et IGL en Jamaïque, pour un total de 244 millions de dollars américains.​

1. **Rentabilité et gestion des coûts**

Malgré une augmentation de 15 % du chiffre d'affaires pour les neuf mois se terminant en juin 2024, Massy a enregistré une baisse de 4 % de son bénéfice avant impôts par rapport à 2023. Cette baisse est attribuée à des coûts ponctuels, notamment des provisions pour créances douteuses, des investissements en gouvernance et des frais juridiques.​

1. **Cybersécurité et confiance des parties prenantes**

Conscient de l'importance cruciale de la confiance dans ses relations d'affaires, Massy a immédiatement renforcé ses contrôles de sécurité informatique et mis en place une stratégie de communication transparente avec ses clients, employés et partenaires. L'entreprise s’est engagée dans une démarche proactive pour restaurer et consolider la confiance : audits réguliers, sensibilisation des équipes, mise en conformité avec les meilleures pratiques de cybersécurité et renforcement de la gouvernance numérique. Ces efforts visent à garantir la résilience de ses systèmes tout en assurant à ses parties prenantes que la protection de leurs données et de leurs intérêts reste une priorité absolue.

1. **Résilience monétaire et gestion des devises**

Massy met l'accent sur la "résilience monétaire" pour protéger ses actionnaires contre les fluctuations des devises. L'expansion aux États-Unis, notamment avec l'acquisition de Rowe’s IGA, permet au groupe de générer des revenus en devises fortes, réduisant ainsi les risques liés aux marchés locaux

1. **Soutien à l'entrepreneuriat local**

Massy a lancé l'initiative "Nudge" pour soutenir les micro-entrepreneurs dans les Caraïbes. Ce programme offre formation, financement et opportunités de vente au détail, renforçant ainsi l'économie locale et la responsabilité sociale de l'entreprise

Massy navigue entre expansion internationale, défis financiers, renforcement de la cybersécurité et engagement communautaire pour assurer une croissance durable.

1. **Classification des données**

La classification des données est une démarche essentielle en cybersécurité, permettant d’identifier, de catégoriser et de protéger les informations selon leur sensibilité, leur valeur et les risques associés à leur divulgation ou altération. Cet outil de gouvernance est d’autant plus crucial lorsqu’une organisation, comme le Groupe Massy, fait face à une cyberattaque majeure ayant entraîné la fuite de plus de 17 Go de données sensibles en 2022.

**Principes et objectifs de la classification des données**

La classification vise à:

* Définir des catégories de sensibilité (ex. : publique, interne, confidentielle, critique) pour chaque type de donnée.
* Déterminer qui peut accéder à quelles données et sous quelles conditions.
* Appliquer des mesures de sécurité adaptées (chiffrement, contrôle d’accès, surveillance, audits).
* Répondre efficacement aux exigences réglementaires (RGPD, Data Protection Act, PCI DSS, Loi 25, etc...) et faciliter la gestion des incidents.
* Limiter l’impact d’une fuite en circonscrivant l’exposition des données les plus sensibles.

**Application au cas Massy : typologie et niveaux de classification**

Suite à l’attaque du ransomware Hive, les données compromises chez Massy incluaient :

* Données personnelles : noms, adresses, numéros fiscaux, copies de passeports, signatures.
* Données financières : informations bancaires, relevés, audits internes.
* Données RH : salaires, contrats de travail.
* Données professionnelles : contrats commerciaux, listes de clients et partenaires.

**Ces données sont classées selon leur criticité :**

* **Niveau 1 – Critique :** Données bancaires, numéros fiscaux, documents d’identité (chiffrement fort, accès très restreint).
* **Niveau 2 – Sensible :** Salaires, contrats, listes de clients (authentification forte, segmentation réseau).
* **Niveau 3 – Interne :** Données techniques, logs (contrôles d’accès, anonymisation).

**Processus et meilleures pratiques**

Un schéma de classification efficace repose sur :

* L’identification et la cartographie de toutes les données existantes.
* L’évaluation de la sensibilité et de l’impact potentiel en cas de compromission.
* L’étiquetage systématique des données selon leur niveau de confidentialité.
* La restriction des accès selon les rôles et la nécessité professionnelle.
* L’utilisation de technologies de protection (chiffrement, IAM, détection d’intrusion).
* La formation continue du personnel à la gestion et à la sécurité des données sensibles.
* La tenue d’audits réguliers et la mise à jour périodique des politiques de classification.

**Gestion des incidents et conformité**

En cas de violation, il est impératif de :

* Isoler les systèmes compromis et contenir la brèche.
* Évaluer rapidement l’ampleur de l’incident et notifier les autorités compétentes (CNIL, dans les 72h si risque pour les personnes).
* Informer les personnes concernées pour limiter les conséquences.
* Tenir un registre des incidents et adapter la classification selon les leçons tirées.

1. **Analyse de risque**

**6.1 Méthodologie utilisée**

Cette analyse de risque repose sur une approche combinée alignée sur :

* **ISO/IEC 27005:2018**, fournissant une structure pour l’identification, l’évaluation et le traitement des risques liés à l'information.
* **EBIOS Risk Manager**, pour une appréciation systémique du risque selon le contexte métier.
* **NIST SP 800-30**, pour la méthodologie de calcul des niveaux de probabilité et d'impact.

Les étapes suivies sont :

1. **Définir le contexte** : comprendre l’environnement technique et organisationnel du Groupe Massy.
2. **Identifier les actifs** : systèmes critiques, bases de données, informations personnelles et financières.
3. **Identifier les menaces et vulnérabilités**.
4. **Évaluer la vraisemblance et l’impact**.
5. **Déterminer la criticité**.
6. **Proposer des mesures de traitement du risque**.

Chaque risque est évalué selon :

* **Probabilité** (faible, moyenne, élevée)
* **Impact** (faible, moyen, élevé, critique)
* **Niveau de criticité** (mineur, modéré, élevé, critique)

**6.2 Identification des actifs**

|  |  |  |  |
| --- | --- | --- | --- |
| **Actif** | **Description** | **Sensibilité** | **Priorité** |
| Bases de données clients | Informations personnelles et financières | Critique | 1 |
| Systèmes de ressources humaines | Données salariés (paye, contrats) | Critique | 2 |
| Réseaux internes | Communications stratégiques | Élevée | 3 |
| Systèmes de gestion financière | États financiers, audits | Critique | 1 |
| Systèmes de sauvegarde | Copies de données sensibles | Critique | 1 |

**6.3 Identification des menaces et vulnérabilités**

|  |  |  |
| --- | --- | --- |
| **Menace** | **Vulnérabilités exploitées** | **Mode d’attaque** |
| Ransomware (Hive) | Failles humaines (phishing), correctifs non appliqués | Double extorsion |
| Exfiltration de données | Manque de segmentation réseau | Mouvement latéral post-compromission |
| Déni de service (opérationnel) | Dépendance excessive aux systèmes IT | Chiffrement des serveurs |
| Perte de réputation | Publication de données sur dark web | Fuite publique d’informations |
| Sanctions juridiques | Non-conformité RGPD/loi locale | Retard ou absence de notification |

**6.4 Évaluation des risques**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Risque** | **Probabilité** | **Impact** | **Criticité** | **Justification** |
| Exfiltration massive de données | Élevée | Critique | Critique | Plus de 17 Go exfiltrés, données sensibles exposées. |
| Interruption des services critiques | Moyenne | Critique | Élevée | Serveurs encryptés, paralysant la continuité. |
| Dégradation de la réputation | Élevée | Élevé | Élevée | Perte de confiance du public, impact durable. |
| Sanctions réglementaires | Moyenne | Élevé | Élevée | Exposition à amendes RGPD/Data Protection Act. |
| Paiement de rançon | Élevée | Critique | Critique | Groupe Hive connu pour pressions sévères. |

**6.5 Matrice de risques (ISO 27005/NIST adaptée)**

|  |  |  |  |
| --- | --- | --- | --- |
| **Impact \ Probabilité** | **Faible** | **Moyenne** | **Élevée** |
| **Critique** | Élevé | Élevé | **Critique** |
| **Élevé** | Modéré | Élevé | **Élevé** |
| **Moyen** | Mineur | Modéré | Élevé |
| **Faible** | Mineur | Mineur | Modéré |

**Note** : L’analyse place l’exfiltration, l’interruption opérationnelle et la demande de rançon dans la zone de criticité maximale (Critique).

**6.6 Analyse quantitative des impacts**

Basée sur les coûts estimés (ordre de grandeur pour une attaque de cette ampleur dans une entreprise de taille intermédiaire selon IBM Cost of a Data Breach Report 2023) :

* **Coûts de remédiation** : 1,5 à 3 millions USD (forensic, restauration, renforcement).
* **Perte d’activité** : 2 à 5 millions USD (selon durée de paralysie).
* **Amendes légales** : jusqu'à 4 % du chiffre d’affaires annuel (selon RGPD).
* **Impact réputationnel** : non chiffrable précisément, mais effet sur valorisation boursière et perte de part de marché possible (5-10 %).

**6.7 Synthèse**

* **Risque global** : Critique
* **Priorité d’action** : Immédiate
* **Axes de traitement** :
  + Prévention des attaques initiales (renforcement du MFA, patch management strict),
  + Surveillance renforcée (EDR/SOC),
  + Plan de réponse à incident testé et documenté,
  + Sensibilisation et formation continue.

**Références Normatives utilisées**

* ISO/IEC 27005:2018 - Information security risk management.
* ISO/IEC 27001:2022 - Information security management systems.
* NIST SP 800-30 Rev.1 - Guide for Conducting Risk Assessments.
* ANSSI - EBIOS Risk Manager - Méthode d’analyse de risque.
* IBM Security - Cost of a Data Breach Report 2023.
* ENISA - Threat Landscape 2024.

1. **Recommandations (mesure de contrôles)**

À la suite de la cyberattaque majeure par ransomware ayant affecté le Groupe Massy, un ensemble de mesures techniques, organisationnelles et stratégiques a été mis en œuvre afin de contenir l’incident, restaurer la sécurité opérationnelle et renforcer la résilience à long terme.

**1. Réponse immédiate et containment**

* Isolement et sécurisation des systèmes compromis : Les systèmes infectés ont été immédiatement isolés du réseau afin de limiter la propagation du malware et protéger les actifs critiques.
* Activation des plans de continuité : Des environnements alternatifs ont été mobilisés pour assurer la continuité minimale des fonctions essentielles.
* Mobilisation d’une cellule de crise : Une équipe spécialisée en cybersécurité a été constituée pour piloter l’investigation, coordonner la remédiation et assurer la communication avec les parties prenantes.
* Communication transparente : Les clients, partenaires, employés et autorités ont été informés de la situation conformément aux obligations réglementaires, afin de maintenir la confiance et la conformité.
* Surveillance renforcée : Une supervision accrue des systèmes a été instaurée pour détecter toute activité suspecte résiduelle ou tentative d’attaque secondaire.
* Réinitialisation des identifiants : Par précaution, l’ensemble des mots de passe et des accès utilisateurs a été réinitialisé pour prévenir toute exploitation ultérieure des données d’authentification compromises.

**2. Renforcement à court terme (0-3 mois)**

* Déploiement d’outils avancés de détection et de réponse (EDR) : Mise en place de solutions permettant une visibilité accrue sur les menaces et une réaction rapide aux incidents.
* Généralisation de l’authentification multifacteur (MFA) : Renforcement des contrôles d’accès aux ressources sensibles par l’activation systématique de la MFA.
* Audit des droits d’accès : Revue exhaustive des privilèges pour appliquer strictement le principe du moindre privilège et réduire la surface d’attaque.
* Formation d’urgence du personnel : Sensibilisation renforcée des collaborateurs aux risques
* cyber, notamment au phishing et aux bonnes pratiques de sécurité.
* Renforcement des sauvegardes : Vérification, test et sécurisation des procédures de sauvegarde et de restauration pour garantir la résilience en cas de nouvelle attaque.
* Journalisation systématique : Mise en place d’une journalisation exhaustive et centralisée des accès et activités sur les systèmes critiques, indispensable pour l’investigation et la remédiation.

**3. Améliorations structurelles à moyen terme (3-12 mois)**

* Segmentation réseau avancée : Compartimentage du réseau pour limiter les mouvements latéraux des attaquants et isoler les systèmes critiques.
* Mise en place ou externalisation d’un SOC : Surveillance proactive et continue assurée par un Centre Opérationnel de Sécurité interne ou externalisé.
* Programme de sensibilisation continue : Mise en œuvre d’un plan de formation récurrent pour maintenir un niveau élevé de vigilance au sein des équipes.
* Tests d’intrusion et exercices de crise : Organisation régulière de simulations d’attaque et de tests d’intrusion pour évaluer la résilience de l’organisation et améliorer les procédures de réponse.
* Chiffrement des données : Déploiement de solutions de chiffrement pour garantir la
* confidentialité des données sensibles, tant au repos qu’en transit.

**4. Transformation à long terme (au-delà de 12 mois)**

* Adoption du modèle Zero Trust : Passage à une architecture de sécurité fondée sur la vérification systématique de chaque accès, remplaçant les modèles périmétriques traditionnels.
* Intégration de l’intelligence artificielle et de la machine learning : Utilisation de technologies avancées pour une détection plus rapide et plus intelligente des comportements anormaux et des menaces émergentes.
* Stratégie globale de résilience cyber : Élaboration d’un plan intégrant les dimensions
* techniques, organisationnelles, juridiques et de communication de crise.
* Partenariats sectoriels : Collaboration avec des réseaux de partage d’informations sur les menaces pour anticiper les attaques et renforcer la veille cyber.
* Gouvernance renforcée : Création d’un comité de gouvernance cybersécurité au niveau exécutif, garantissant l’intégration des enjeux cyber dans la stratégie globale du Groupe Massy.

1. **Conclusion**

**Références**

<https://www.caribbean-council.org/massy-rocked-by-one-of-the-caribbeans-largest-ever-data-breach-dumps/>

<https://www.guardian.co.tt/news/massy-stores-investigates-cyber-attack-information-leak-6.2.1560033.09a6c52664>

<https://massygroup.com/about-us/security/>

<https://www.youtube.com/watch?v=C0PmaBY-g24&ab_channel=makeITsimpleTT>