UQAC

Université du Québec
à Chicoutimi

**Département d'informatique et de mathématique**

Cours : Éthique et informatique

Chargés de cours : Jean pierre Béland

Exercice d'intégration 6

**Cyberattaque**

**Comment relever le défi d'une cybersécurité efficace?**

Sujet du travail : Analyse de cas d'une cyberattaque

# THEME CHOISI : ATTAQUE DE KASEYA

MEMBRE DU GROUPE E :

THIERNO RASSID DIALLO

SARAN MADY KEITA

MAMADOU SANOUSSY BAH

SOMMAIRE :


- Introduction
- Éléments  du contexte de la cyberattaque
- Processus d’analyse d’impacte
- Gouvernance
- Conclusion
- Références

# Introduction

Les cyberattaques sont devenues un enjeu majeur pour les entreprises et les organisations à travers le monde. Elles se multiplient en fréquence et en sophistication, représentant une menace significative pour la sécurité des données, la continuité des activités et la confiance des utilisateurs. Parmi les incidents marquants des dernières années, l'attaque de Kaseya en juillet 2021 illustre parfaitement les risques liés aux vulnérabilités des infrastructures informatiques et leurs répercussions à grande échelle.

Kaseya est une entreprise américaine spécialisée dans les solutions de gestion informatique pour les fournisseurs de services managés (MSP). Elle propose des logiciels permettant aux entreprises de surveiller et de gérer leurs infrastructures IT à distance, ce qui en fait une cible de choix pour les cybercriminels cherchant à maximiser l'impact de leurs attaques. En exploitant une faille de sécurité dans le logiciel VSA de Kaseya, les attaquants ont déployé un ransomware qui s'est rapidement propagé à travers plusieurs clients de l'entreprise, affectant entre 800 et 1 500 entreprises à travers le monde.

Parmi les victimes, le secteur de la distribution a été particulièrement touché. En Suède, la chaîne de supermarchés **Coop** a dû fermer temporairement environ **800 magasins** en raison de l'indisponibilité de ses systèmes de caisses, ce qui a entraîné des pertes financières considérables et mis en évidence la dépendance critique des entreprises aux technologies informatiques.

Cette attaque s'est déroulée dans un contexte économique et politique marqué par une montée en puissance des cybermenaces à l'échelle mondiale. Les attaques par ransomware sont devenues particulièrement lucratives, avec des groupes cybercriminels organisés qui ciblent des infrastructures critiques et des entreprises de premier plan. En outre, la pandémie de COVID-19 a accéléré la transformation numérique des entreprises, augmentant leur dépendance aux systèmes informatiques et, par conséquent, leur vulnérabilité aux cyberattaques. L'incident Kaseya met ainsi en lumière l'importance d'une gouvernance efficace de la cybersécurité et la nécessité d'adopter des stratégies robustes pour prévenir et atténuer les menaces émergentes.

## Objectif du travail

Ce travail vise à analyser en détail l'attaque de Kaseya, en mettant en évidence son contexte, ses impacts et les mesures de gouvernance en cybersécurité qui auraient pu atténuer ses effets ou prévenir son occurrence. En appliquant un processus structuré d'analyse d'impacts, nous chercherons à comprendre comment une telle attaque a pu se produire et quelles leçons peuvent en être tirées pour renforcer la résilience des entreprises face aux menaces cybernétiques.

## Méthode d'analyse

L'analyse de cette cyberattaque suivra plusieurs étapes clés :

- **Contexte de l'attaque** : Présentation de Kaseya, de son rôle dans l'écosystème technologique et des vulnérabilités exploitées par les attaquants.
- **Déroulement de l'attaque** : Explication technique de la faille exploitée, du mode opératoire des cybercriminels et des mécanismes utilisés pour la propagation du ransomware.
- **Analyse des impacts** : Évaluation des conséquences économiques, organisationnelles et légales pour Kaseya et ses clients, y compris les pertes subies par les entreprises affectées, comme les supermarchés Coop.
- **Leçons et gouvernance** : Proposition de mesures de gouvernance et de stratégies de cybersécurité permettant de réduire les risques et d'améliorer la résilience des organisations face aux attaques de ce type.

# Éléments  du contexte de la cyberattaque

1. **Cible (systèmes ou personnes affectées dans l'organisation)**

L'attaque de Kaseya a principalement visé son logiciel de gestion à distance, Kaseya VSA, utilisé par de nombreux fournisseurs de services managés (MSP). En compromettant ce logiciel, les attaquants ont pu toucher indirectement des centaines de petites et moyennes entreprises qui utilisaient les services des MSP infectés. Parmi les victimes figurent des entreprises de divers secteurs, notamment le commerce de détail, la finance, l'éducation et les services publics. Environ 1500 entreprises à travers le monde ont été affectées, entraînant des arrêts d'activité, des pertes financières et des perturbations dans les chaînes d'approvisionnement.

2. **Méthode et type d'attaque (techniques utilisées)**

L'attaque a été menée à l'aide d'un ransomware de type REvil (également connu sous le nom de Sodinokibi), qui a exploité une vulnérabilité zero-day dans Kaseya VSA. Les cybercriminels ont utilisé une attaque de type « supply chain attack » (attaque de la chaîne d'approvisionnement), une technique où un fournisseur de services ou un logiciel centralisé est compromis afin d'infecter de nombreux clients en aval. Une fois la faille exploitée, le ransomware a été déployé, chiffrant les fichiers des systèmes infectés et exigeant une rançon pour leur déchiffrement.

3. **Motivations de l'attaquant**

Les attaquants, identifiés comme étant affiliés au groupe REvil, avaient une motivation essentiellement financière. Le groupe REvil est connu pour mener des attaques par ransomware avec des demandes de rançon élevées. Dans le cas de Kaseya, ils ont exigé une rançon de 70 millions de dollars en échange d'une clé de déchiffrement permettant à toutes les entreprises affectées de récupérer leurs fichiers. Leur modèle économique repose sur le « ransomware-as-a-service » (RaaS), où des cybercriminels développent des ransomwares et les louent à d'autres acteurs malveillants qui mènent les attaques.

Cette attaque montre que les cybercriminels cherchent à maximiser leurs gains financiers en ciblant des infrastructures critiques et en exploitant des vulnérabilités dans des systèmes largement utilisés par de nombreuses entreprises.

# • Processus d'analyse d'impacte

1. **Analyse en trois étapes (La personne transformée)**
    a. **Avant l'attaque** : Kaseya était un fournisseur de solutions de gestion informatique fiable et reconnu, garantissant la sécurité et la performance des systèmes de ses clients.
    b. **Pendant l'attaque** : L'entreprise a subi une crise majeure, confrontée à une perte de contrôle sur ses systèmes, une propagation rapide du ransomware et une réaction en urgence pour limiter les dégâts.
    c. **Après l'attaque** : Des mesures de renforcement de la cybersécurité ont été mises en place, impliquant une refonte des protocoles de sécurité, une meilleure communication avec les clients et une collaboration accrue avec les autorités pour traquer les cybercriminels.
2. **Impact**

L’impact de l’attaque a été multiple : pertes financières considérables, atteinte à la réputation de Kaseya, interruption des opérations de nombreuses entreprises clientes, augmentation de la réglementation en cybersécurité et une prise de conscience généralisée de la vulnérabilité des services IT.

3. **Critères (enjeux E3LS)**
    a. **Économique** : Coûts liés à la gestion de crise, pertes de revenus, impact sur les clients et indemnisation des victimes.
    b. **Éthique** : Responsabilité de Kaseya envers ses clients, importance de la transparence dans la gestion de crise.
    c. **Légal** : Risques de poursuites judiciaires, mise en conformité avec de nouvelles réglementations.
    d. **Social** : Impact sur la confiance des clients, des partenaires et des investisseurs.
    e. **Technologique** : Amélioration des infrastructures de sécurité, mise à jour des protocoles de réponse aux incidents.
4. **Valeurs correspondantes**
    a. **Sécurité** : Mise en place de meilleures pratiques pour éviter de futures attaques.
    b. **Responsabilité** : Engagement envers les clients pour garantir un service sécurisé.
    c. **Transparence** : Communication ouverte sur l’incident et les mesures prises.
    d. **Résilience** : Renforcement des protocoles de cybersécurité et adaptation aux nouvelles menaces.

# • Gouvernance

La gouvernance est un élément clé pour comprendre comment les entreprises réagissent et se protègent face aux cyberattaques. Pour le cas de Kaseya, une approche de gouvernance adéquate permettrait non seulement de répondre à l'attaque mais aussi de prévenir de futures intrusions. Il existe plusieurs types de gouvernance, chacun ayant une influence distincte sur la gestion de la crise. Nous allons explorer trois types de gouvernance qui s'appliquent au cas de l'attaque de Kaseya.

**1. Gouvernance juridique**

La gouvernance juridique en matière de cybersécurité repose sur des lois et des régulations nationales et internationales. Lors de l’attaque de Kaseya, plusieurs implications juridiques ont surgi :

- **Respect des lois sur la protection des données** :

  L'attaque a compromis de nombreuses données sensibles, affectant potentiellement des milliers d'entreprises et leurs clients. Kaseya, en tant que fournisseur de services informatiques, était tenu de respecter des normes légales strictes concernant la protection de ces informations. En Europe, le RGPD exige des entreprises qu'elles signalent les violations de données dans un délai de 72 heures, sous peine de lourdes amendes. Aux États-Unis, des lois comme le CCPA (California Consumer Privacy Act) imposent des obligations similaires pour les entreprises opérant en Californie.

- **Obligations de notification et de transparence** :

Sur le plan juridique, une entreprise victime d'une cyberattaque doit fournir une notification rapide et transparente aux parties affectées, ce qui était le cas avec Kaseya. Le respect de cette obligation légale est essentiel pour limiter les conséquences juridiques à long terme.

- **Sanctions et responsabilités** :

Si Kaseya avait failli à remplir ses obligations juridiques en matière de cybersécurité (par exemple, en n'appliquant pas des mesures de sécurité appropriées), elle pourrait être exposée à des actions en justice. En fonction de la législation applicable, les autorités pourraient également enquêter sur la négligence dans la gestion de la sécurité des systèmes.

**2. Gouvernance déontologique**

La gouvernance déontologique se réfère aux normes et aux pratiques éthiques qui régissent le comportement des professionnels dans le domaine de la cybersécurité. Cela inclut :

- **Respect des standards de la profession** :

Les professionnels de la cybersécurité sont guidés par des principes déontologiques tels que l'intégrité, la confidentialité et la responsabilité. Dans le cadre de l’attaque de Kaseya, la manière dont les employés et les consultants de l'entreprise ont géré l’incident est cruciale. Une réponse appropriée impliquerait non seulement une résolution rapide du problème, mais aussi une communication claire et honnête avec les parties prenantes.

- **Réaction à l'incident** :

Les professionnels de la cybersécurité chez Kaseya étaient responsables de la mise en place de mécanismes de défense pour prévenir une telle attaque et d'une réponse rapide lorsque l'attaque a eu lieu. La gouvernance déontologique inclut des critères tels que la rapidité d'intervention, la rigueur dans la gestion de la crise, et le respect des meilleures pratiques en matière de sécurité informatique.

- **Transparence et confiance** :

En plus de la gestion technique, la transparence vis-à-vis des clients est une composante clé de la gouvernance déontologique. Kaseya devait s'assurer que les informations relatives à l'attaque et aux mesures de récupération soient partagées avec les victimes de l'attaque dans les plus brefs délais.

**3. Gouvernance éthique**

La gouvernance éthique, aussi connue sous le terme de gouvernance dialogique, se concentre sur l'engagement envers des principes moraux universels. Elle se base sur la responsabilité collective et sur le dialogue entre les parties prenantes pour instaurer une culture de sécurité partagée et respectueuse. Cela inclut :

- **Responsabilité sociétale des entreprises (RSE)** :

Une entreprise telle que Kaseya a la responsabilité de protéger non seulement ses données internes mais aussi celles de ses clients et partenaires. Une gouvernance éthique implique que l'entreprise prenne des mesures préventives pour minimiser le risque d'attaques, tout en mettant en œuvre des solutions pour limiter les dégâts une fois l'attaque survenue. La prise en charge des conséquences pour les victimes et l'engagement à restaurer la confiance sont des éléments cruciaux ici.

- **Pratiques proactives et éducation** :

Une gouvernance éthique recommande également une approche proactive en matière de cybersécurité. Kaseya aurait dû investir dans des formations de sensibilisation et des audits réguliers de sécurité pour ses employés et ses clients afin de prévenir de futures cyberattaques. En outre, l'éthique implique que l'entreprise adopte des solutions qui respectent les droits des utilisateurs tout en mettant en place des mécanismes de défense robustes.

- **Collaboration avec la communauté** :

Au-delà de la simple gestion de la crise, une gouvernance éthique encourage la collaboration avec des experts externes, des organismes de réglementation et d'autres entreprises pour renforcer les standards de cybersécurité dans le secteur. En cas de cyberattaque, il est également essentiel d'adopter une attitude ouverte au dialogue, ce qui aidera à renforcer la confiance à long terme entre l'entreprise et ses parties prenantes (clients, régulateurs, actionnaires, etc.).

# Conclusion

**Retour sur l'analyse globale**

L'attaque de Kaseya met en lumière les défis considérables auxquels sont confrontées les entreprises face à des cybermenaces de plus en plus sophistiquées et globales. En analysant cet incident, il apparaît clairement que la cybersécurité n'est pas une simple question technique mais un enjeu stratégique qui doit être géré à plusieurs niveaux. La gouvernance juridique, déontologique et éthique joue un rôle central dans la manière dont une organisation gère une crise de cybersécurité.

L'incident de Kaseya a révélé non seulement des vulnérabilités techniques mais aussi des failles dans la gestion de la sécurité à l'échelle organisationnelle, particulièrement en ce qui concerne les pratiques de gouvernance. Il a mis en évidence la nécessité d'une coordination étroite entre les équipes techniques, les responsables de la conformité, et les décideurs au sein de l'entreprise. L'attaque a également montré l'importance de la résilience des systèmes informatiques et des processus de réponse aux incidents, et de la mise en place de stratégies de prévention plus robustes.

Enfin, l'attaque de Kaseya a soulevé une question cruciale : à quel point les entreprises sont-elles préparées à une cyberattaque ? La gestion de la crise doit aller bien au-delà de la simple réaction technique, en intégrant des dimensions de gouvernance, de responsabilité sociale et de transparence vis-à-vis des parties prenantes.

**Les leçons tirées de cette analyse**

À travers l'analyse de l'attaque de Kaseya, plusieurs leçons essentielles peuvent être tirées :

- **Prévention et anticipation** : Une approche préventive est bien plus efficace qu'une gestion réactive. En investissant dans des solutions de sécurité robustes, telles que la segmentation des réseaux, les systèmes de détection d'intrusion, et des programmes de formation pour les employés, les entreprises peuvent se protéger contre de nombreuses attaques. L'attaque de Kaseya a montré que les entreprises doivent être prêtes à gérer non seulement les menaces existantes, mais aussi celles qui sont en train d'émerger.
- **Réactivité et communication** : En cas de cyberattaque, la réactivité est essentielle. La rapidité avec laquelle Kaseya a répondu à l'incident, en informant ses clients et en mettant en place des mécanismes de réponse, a été un facteur clé dans la gestion de la crise. Toutefois, une meilleure communication en temps réel avec les parties prenantes aurait pu réduire l'impact de l'attaque. Les entreprises doivent préparer des plans de communication d'urgence pour minimiser l'incertitude.
- **La gouvernance à plusieurs niveaux** : L'attaque a mis en évidence l'importance d'une gouvernance claire et cohérente à tous les niveaux de l'entreprise. La gouvernance juridique, déontologique et éthique doit être intégrée dans la stratégie globale de cybersécurité de l'entreprise. L'application des lois sur la protection des données et les codes de conduite professionnels est fondamentale, tout comme l'engagement éthique de l'entreprise à protéger ses utilisateurs.
- **Collaboration internationale et réglementation** : L'attaque de Kaseya a illustré la nécessité d'une collaboration internationale pour faire face aux cybermenaces. Les attaques d'envergure mondiale, comme celle de Kaseya, touchent non seulement l'entreprise ciblée mais aussi de nombreux autres acteurs dans des pays différents. La coopération entre entreprises, gouvernements et régulateurs est cruciale pour renforcer les capacités de défense contre les cybercriminels.

**Quelques pistes pour alimenter la réflexion**

1. **Êtes-vous confiant dans votre capacité à promouvoir la cybersécurité dans une entreprise ?** Cette question invite les professionnels de la cybersécurité à évaluer non seulement leur capacité à réagir techniquement à une attaque, mais aussi à instaurer une culture de la sécurité dans l'entreprise. Promouvoir la cybersécurité nécessite de la vigilance continue, de la formation régulière et la mise en place de politiques internes adaptées. En tant que futur professionnel, êtes-vous préparé à transmettre ces valeurs et à plaider pour des investissements dans la cybersécurité ?
2. **Comment les entreprises peuvent-elles équilibrer le besoin de sécurité avec le respect de la vie privée des utilisateurs ?** L'équilibre entre la sécurité et la vie

privée est l'un des défis les plus complexes de la cybersécurité. La mise en œuvre de technologies de sécurité, telles que le chiffrement ou la surveillance des réseaux, peut potentiellement empiéter sur la vie privée des utilisateurs. Il est donc nécessaire de trouver des solutions qui permettent de renforcer la sécurité tout en respectant les droits des utilisateurs. Comment garantir cette balance tout en respectant les principes éthiques et légaux en matière de protection des données ?

3. **Quel rôle les gouvernements devraient-ils jouer dans la réglementation de la cybersécurité au niveau international ?** La cybersécurité est un problème mondial qui dépasse les frontières nationales. Les gouvernements doivent jouer un rôle clé dans la définition de régulations harmonisées pour la cybersécurité, et s'assurer que les entreprises respectent des normes minimales en matière de sécurité des données. Par exemple, le développement de normes internationales pour les pratiques de cybersécurité et la coopération transnationale dans la lutte contre la cybercriminalité seraient des mesures importantes. De plus, une législation uniforme pour les violations de données et les exigences de notification pourrait renforcer la réponse mondiale face aux cyberattaques.
4. **Quels défis les entreprises doivent-elles relever pour rester compétitives tout en garantissant la cybersécurité ?** Alors que les cyberattaques deviennent de plus en plus fréquentes et sophistiquées, les entreprises doivent trouver un équilibre entre la nécessité d'innovation et la mise en place de mesures de cybersécurité. Comment les entreprises peuvent-elles intégrer des solutions de sécurité dans leurs processus sans freiner l'innovation ? Il devient impératif que la cybersécurité devienne une partie intégrante de la stratégie de développement de chaque entreprise, et non un simple ajout à la fin du processus.

# Références


www.ih2ef.gouv.fr

www.cairn.info

www.fao.org

www.dalloz-actualite.fr

https://www.lesechos.fr/tech-medias/hightech/kaseya-ce-que-lon-sait-de-la-cyberattaque-geante-qui-a-paralyse-des-centaines-dentreprises-1330321

Cyberattaque contre Kaseya VSA, explications | Stormshield

Cyberattaque | Kaseya a de la difficulté à redémarrer ses serveurs en toute sécurité | La Presse