UNIVERSITÉ DE TECHNOLOGIE D'HAÏTI

PROGRAMME TIC-HAÏTI-BRH

5/26/2025

DESS

Réalisation d'un avis de sécurité sur l'incident de cybersécurité de Banco de Chile

Realisation: EQUIPE 7

- John-Eder EXUME
- Egzael LABADY
- Lubens LUMA
- Renel SIDRENICE
- Wideline TAVIL

Sécurité des Systèmes Informatiques

Professeur: Blaise Arbouet

Table des matières

1. Sommaire exécutif

Ce document présente un avis de sécurité sur l'incident cybercriminel ayant visé la **Banco de Chile** en 2018, son est d'analyser les causes, les impacts et les vulnérabilités exploitées, puis de proposer des recommandations réalistes fondées sur les normes ISO et les enseignements du cours de **Sécurité des systèmes informatiques**.

D'abord, cette cyberattaque majeure subie par Banco de Chile en mai 2018 a entraîné une perte de 10 millions de dollars via le réseau SWIFT. En analysant les causes, les mécanismes d'attaque, les vulnérabilités exploitées, et les réponses institutionnelles, ce document met en lumière les risques systémiques posés par les cybermenaces dans le secteur financier. D'où l'étude s'appuie sur les principes de la sécurité des systèmes d'information (SSI) et les normes internationales (ISO/IEC 27001, SWIFT CSP), et propose donc des recommandations spécifiques adaptées à d'autres contextes, notamment celui des banques haïtiennes.

Cette étude vise également à sensibiliser les décideurs bancaires, notamment les responsables des systèmes d'information et les autorités de régulation sur l'importance d'une posture de cybersécurité proactive. Par conséquent, elle démontre que même une institution bien établie, comme Banco de Chile, peut être vulnérable sans une stratégie intégrée, alignée sur les bonnes pratiques mondiales.

2. Introduction

Le développement rapide des technologies de l'information et de la communication a révolutionné le secteur bancaire, permettant une automatisation accrue, un accès élargi aux services financiers, et une réduction des délais de traitement. Toutefois, cette transformation numérique a également accru la vulnérabilité des institutions face aux cyberattaques.

Le cas de Banco de Chile illustre donc parfaitement cette réalité. De ce fait, en mai 2018, cette banque, réputée pour sa stabilité et sa fiabilité, a été la cible d'une attaque complexe qui a utilisé un logiciel malveillant pour détourner des fonds à travers le réseau SWIFT. Plus qu'un simple incident technique, cette attaque a révélé des failles importantes dans les systèmes de sécurité, la gestion des accès et la capacité de réponse aux incidents.

L'étude de ce cas permet de mieux comprendre les nouvelles menaces qui pèsent sur les systèmes d'information bancaires et de proposer des actions concrètes pour y faire face.

3. Contexte

3.1. Présentation de Banco de Chile : histoire, taille, services, et importance économique

Banco de Chile est l'une des plus anciennes et grandes banques du pays. Fondée en 1893, elle est devenue un pilier du système bancaire chilien. La banque propose une gamme complète de services : comptes courants et d'épargne, crédits, investissements, services aux entreprises, gestion d'actifs, et services en ligne.

Avec des milliers d'employés et une base client dépassant plusieurs millions, Banco de Chile joue un rôle clé dans l'économie chilienne. De plus, ses systèmes informatiques doivent gérer un volume très élevé de transactions quotidiennes, ce qui nécessite une infrastructure à la fois performante et sécurisée.

Par ailleurs, la banque est aussi engagée dans l'innovation technologique, intégrant des technologies avancées comme le big data, l'intelligence artificielle pour la gestion des risques, et la biométrie pour l'authentification.

3.2. Présentation détaillée du secteur bancaire au Chili et son évolution numérique

Le secteur bancaire chilien occupe une place stratégique dans l'économie nationale. Depuis la fin des années 1990, il a connu une modernisation progressive et une intégration accrue des technologies numériques dans ses opérations. Cette transformation a été portée par une demande croissante des clients pour des services plus rapides, accessibles à distance, et sûrs, ainsi que par la concurrence accrue tant locale qu'internationale, et l'une des institutions financières majeures du pays est la Banco de Chile, fondé en 1893. Cette banque détient alors une part de marché importante, notamment dans les services bancaires aux particuliers, aux entreprises et aux grandes industries, ce qui explique l'adoption de solutions numériques ayant permis à la banque de proposer des services tels que la banque en ligne, les applications mobiles, et les systèmes de paiement électroniques.

Toutefois, cette digitalisation rapide a aussi exposé le système bancaire à de nouvelles formes de risques, ce qui entraine la fragilisation des systèmes informatiques, des réseaux de

communication, et des bases de données clients qui deviennent des cibles privilégiées pour les cybercriminels.

3.3. Spécificités du contexte chilien en matière de cybercriminalité

Le Chili est reconnu pour son système financier robuste et régulé, mais également vulnérable à certains types de cyberattaques. Les infrastructures bancaires sont souvent ciblées par des groupes organisés, certains liés à la cybercriminalité internationale, utilisant des attaques coordonnées et sophistiquées.

La législation chilienne a évolué pour inclure des normes de cybersécurité spécifiques pour les institutions financières, notamment sous la supervision de la Commission pour le Mercado Financiero (CMF). Cependant, en dépit de cela, des lacunes persistent dans la prévention proactive et dans la capacité de réaction rapide face aux incidents.

Du coup, les attaques informatiques en 2018, notamment contre Banco de Chile, ont mis en évidence les insuffisances de certains mécanismes de défense, obligeant une prise de conscience collective dans le secteur.

3.4. **Contexte précis de l'attaque 2018 : chronologie et premières réactions**

Date	Événement
24 mai 2018	Détection d'une panne affectant les services en agence et par téléphone
28 mai 2018	Identification d'un virus affectant les postes de travail
Début juin 2018	Découverte de transactions suspectes dans le système SWIFT
11 juin 2018	Confirmation du vol de 10 million de dollars vers Hong Kong

En mai 2018, Banco de Chile a subi une attaque informatique majeure. Les hackers ont réussi à pénétrer les systèmes internes via une faille dans la messagerie sécurisée, exploitant ainsi une vulnérabilité non corrigée. Du coup, Cette intrusion a conduit au transfert frauduleux de plus de 10 millions de dollars vers plusieurs comptes à l'étranger.

Plus de peur que de mal, la banque a détecté l'anomalie après plusieurs heures et a immédiatement activé son plan d'urgence, ce qui a rapidement fait suspendre toutes les opérations de manière temporairement, et au même moment les équipes de cybersécurité internes, aidées par des experts externes, ont commencé à analyser l'attaque et à colmater les brèches.

En outre, les autorités chiliennes ont également été alertées, et une enquête conjointe a été lancée, impliquant la police spécialisée en cybercriminalité, ainsi que des agences internationales.

Malheureusement, cette attaque a profondément choqué le marché et la clientèle, remettant en cause la confiance dans la capacité des banques chiliennes à protéger les actifs et les données sensibles.

4. Enjeux de cybersécurité

Les enjeux de cybersécurité dans le secteur bancaire représentent des aspects fondamentaux pour assurer la confiance, la résilience et la performance des institutions financières. Cette section vise à identifier les principales dimensions à sécuriser telles que la disponibilité des services, l'intégrité des données et la confidentialité des informations afin de mieux comprendre les impacts potentiels d'une faille de sécurité, et d'en déduire les exigences clés en matière de protection des systèmes d'information bancaires. Les enjeux de cybersécurité peuvent être analysés à travers le prisme du triangle CID (Confidentialité, Intégrité, Disponibilité) présenté en cours. Ce triangle forme donc la base de toute politique de sécurité de l'information, particulièrement dans les secteurs critiques comme celui de la finance.

4.1. Disponibilité des services

La continuité des services bancaires est un pilier fondamental de la confiance client. Lors de l'incident, certaines opérations ont été suspendues temporairement, ce qui aurait pu engendrer une panique financière si la situation s'était prolongée. Une telle indisponibilité peut provoquer une ruée vers les guichets, une désorganisation interne et des pertes économiques majeures.

4.2. Intégrité des données

Dans un système bancaire, la précision des données est essentielle. Toute altération malveillante ou accidentelle des soldes, des historiques de transaction ou des écritures comptables peut entraîner des erreurs de facturation, des pertes financières, voire des fraudes à grande échelle. L'incident de 2018 a rappelé que même un détournement limité de fonds, s'il passe inaperçu, peut avoir des implications juridiques et opérationnelles graves.

4.3. Confidentialité

Les banques détiennent des volumes importants de données personnelles et financières sensibles. Une violation de la confidentialité par exemple via un logiciel malveillant ou une faille exploitée à distance –expose l'institution à des poursuites, à des sanctions réglementaires, mais surtout à une perte de confiance de la clientèle. Dans le cas de Banco de Chile, bien que les données des clients n'aient pas été directement exposées selon les déclarations officielles, l'incident a suscité des inquiétudes justifiées sur la robustesse des mesures de protection des informations.

5. Les objectifs du travail

5.1. Objectifs généraux

L'objectif principal de cette étude est de réaliser une analyse approfondie du piratage informatique subi par Banco de Chile en 2018. Il s'agit de comprendre comment cette attaque a été possible, d'identifier les vulnérabilités exploitées, d'évaluer les impacts tant financiers qu'opérationnels, et de proposer des mesures correctives et préventives adaptées au contexte bancaire chilien et international.

Ce travail vise à apporter une compréhension claire des mécanismes de l'attaque pour sensibiliser les institutions financières, les régulateurs, ainsi que les chercheurs en cybersécurité, sur l'importance cruciale de la sécurité informatique dans le secteur bancaire.

5.2. Objectifs spécifiques

5.2.1. Analyse technique des vulnérabilités

Une partie essentielle de l'étude consiste à décortiquer techniquement les failles dans les systèmes de Banco de Chile qui ont permis l'intrusion.

5.2.2. Étude des méthodes d'attaque

Comprendre les méthodes, outils et tactiques utilisés par les cybercriminels est crucial pour anticiper et se prémunir contre des attaques similaires.

5.2.3. Évaluation des impacts

Evaluer les répercussions globales de l'attaque sur Banco de Chile : coûts financiers directs et indirects, interruptions de services, impact sur la confiance des clients, et conséquences légales et réglementaires.

5.2.4. Recommandations stratégiques et opérationnelles

À partir des résultats de l'analyse, proposer des recommandations précises pour renforcer la cybersécurité.

5.2.5. Proposition d'un plan d'action

Proposer un plan d'action adapté aux banques des pays en développement, notamment en Haïti.

6. Méthodologie pour atteindre les objectifs

6.1. Revue documentaire

La méthodologie repose sur l'analyse de sources diverses : rapports d'enquête, articles spécialisés, publications institutionnelles (Banque centrale du Chili, CERT), et normes de cybersécurité reconnues (ISO/IEC 27001, ISO 27005, SWIFT CSP).

6.2. Étude de cas

Banco de Chile est utilisée comme cas central. Son analyse permet une exploration détaillée des défaillances, des réponses et des leçons à tirer.

6.3. Approche EMR

L'approche EMR signifie généralement Événement – Mécanisme – Résultat, et c'est une méthode utilisée pour analyser un incident ou une attaque (notamment en cybersécurité, en gestion des risques ou en environnement) de manière structurée. Cette approche permet de cartographier les menaces, les vulnérabilités, et d'évaluer les risques associés à chaque actif critique.

6.4. Classification des données

Les données détenues par Banco de Chile sont classifiées comme suit :

- **Niveau 1 : Critique** — données SWIFT, identifiants de connexion, codes d'accès internes.
- **Niveau 2 : Sensible** — données clients, historiques de transaction, numéros de comptes.
- **Niveau 3 : Interne** — documentation interne, politiques de sécurité, notes de service.

7. La Portée de l'étude

7.1. Délimitations géographiques, temporelles et organisationnelles

L'étude se concentre exclusivement sur l'attaque informatique dont a été victime Banco de Chile en mai 2018. Géographiquement, l'analyse concerne le territoire chilien, où les infrastructures bancaires concernées sont situées, ainsi que les juridictions internationales impliquées dans les transferts frauduleux.

Sur le plan temporel, la recherche couvre la période allant de quelques mois avant l'attaque, afin de comprendre le contexte et les préparatifs des hackers, jusqu'à plusieurs mois après, pour évaluer les réponses, réparations et impacts durables.

Organisationnellement, l'étude cible Banco de Chile en tant qu'entité, en examinant ses infrastructures internes, ses politiques de sécurité, ses ressources humaines dédiées à la cybersécurité, ainsi que ses interactions avec les régulateurs et partenaires externes.

7.2. Technologies et systèmes couverts

L'analyse porte sur plusieurs couches technologiques utilisées par Banco de Chile :

- **Infrastructure réseau** : configuration des pare-feux, routeurs, segmentation des réseaux internes et externes.
- **Systèmes d'information bancaires** : logiciels de gestion des comptes, plateformes de paiement, systèmes de messagerie interne.
- **Protocoles de sécurité** : systèmes d'authentification, chiffrement des données, gestion des accès utilisateurs.
- **Systèmes de détection et de réponse aux incidents** : logiciels antivirus, systèmes de détection d'intrusions (IDS/IPS), surveillance des logs.
- **Gestion des vulnérabilités** : procédures de mises à jour, correctifs de sécurité, audits internes.

7.3. Limites et exclusions de l'étude

Cette étude ne couvre pas :

- Les attaques sur d'autres institutions financières chiliennes ou internationales, sauf dans une perspective comparative limitée.
- Les aspects légaux détaillés des poursuites contre les auteurs de l'attaque, qui relèvent du domaine judiciaire.
- Les aspects financiers internes profonds de Banco de Chile, non rendus publics, hormis les données accessibles via rapports officiels ou médias.
- Les aspects techniques liés aux infrastructures hors du périmètre bancaire, comme les systèmes gouvernementaux ou réseaux tiers non directement impliqués.

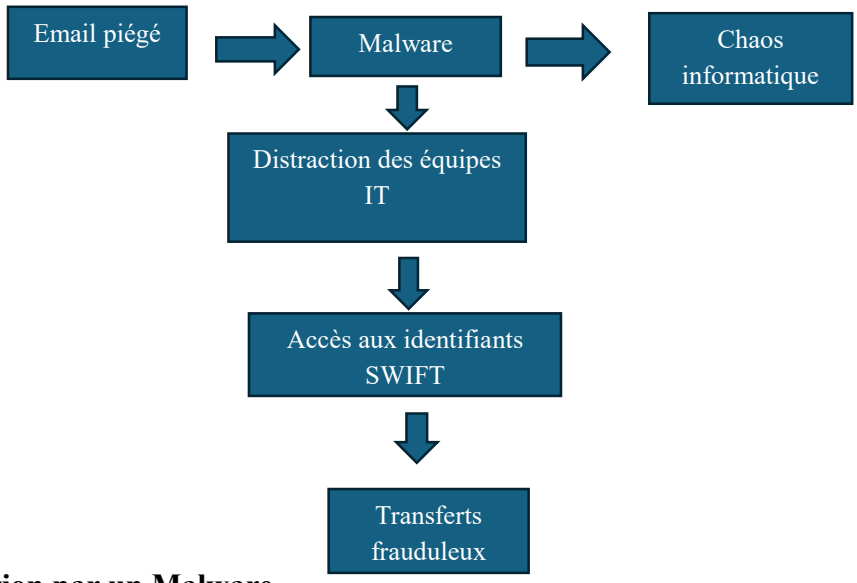
8. Nature de l'attaque

Le 24 mai 2018, Banco de Chile subit une cyberattaque initialement perçue comme un simple dysfonctionnement. En réalité, les systèmes de la banque étaient infectés par un malware qui a perturbé plus de 9 000 postes de travail et 500 serveurs. Cette attaque a ensuite été exploitée pour détourner des fonds vers des comptes étrangers en Asie.

9. Déroulement de l'Attaque

L'incident de sécurité subi par Banco de Chile en mai 2018 est un exemple emblématique d'attaque multi-phasée, associant une infection massive par malware et un détournement financier sophistiqué via le réseau interbancaire SWIFT. Ce qui semblait au départ n'être qu'un acte de sabotage informatique s'est révélé être une opération de cybercriminalité financière à grande échelle. Cette section retrace les étapes techniques et stratégiques du déroulement de l'attaque.

Schéma de l'attaque en plusieurs phases



9.1. Infection par un Malware

L'attaque a débuté par l'introduction d'un **malware de type wiper** dans les systèmes internes de la banque. Ce type de logiciel malveillant est conçu pour effacer ou corrompre des données, afin de masquer d'autres activités malveillantes. Voici les principales caractéristiques de cette première phase :

- **Propagation rapide** : Le malware a infecté plus de **9 000 postes de travail** et environ **500 serveurs** au sein du réseau interne de Banco de Chile. Il s'est propagé à travers les segments réseau via des partages de fichiers non sécurisés et des vulnérabilités dans les configurations système.
- **Perturbation intentionnelle** : L'objectif n'était pas uniquement de nuire, mais surtout de détourner l'attention des équipes informatiques de la banque. En créant un chaos numérique, les cybercriminels ont occupé les ressources internes avec la résolution de pannes informatiques massives.
- **Système de détection contourné** : Le malware utilisé semblait être personnalisé, échappant ainsi aux outils antivirus et aux mécanismes de détection comportementale. Cela laisse penser qu'il s'agissait d'une attaque ciblée et planifiée bien à l'avance, probablement menée par un groupe disposant de compétences avancées.

Cette première phase a paralysé l'environnement numérique de la banque, donnant ainsi aux attaquants un accès prolongé sans interruption à d'autres systèmes plus sensibles, notamment ceux liés aux paiements internationaux.

9.2. Détournement de Fonds via SWIFT

Profitant du désordre informatique causé par le malware, les attaquants sont passés à la deuxième phase de leur opération : **le vol de fonds via le réseau SWIFT (Society for Worldwide Interbank Financial Telecommunication)**.

- **Détournement ciblé** : Alors que les équipes techniques étaient mobilisées sur les pannes internes, les cybercriminels ont réussi à initier une série de **transactions frauduleuses**, totalisant environ 10 millions de dollars. Ces transferts ont été effectués depuis les comptes institutionnels de la banque.
- **Utilisation du système SWIFT** : Le réseau SWIFT est censé être l'un des plus sûrs au monde. Cependant, une fois qu'un attaquant obtient les identifiants valides et l'accès à un poste authentifié, il peut émettre des ordres de transfert tout à fait légitimes d'apparence. C'est exactement ce que les attaquants ont fait.
- **Destinations des fonds** : L'argent volé a été transféré vers plusieurs comptes bancaires en Asie**,** notamment à Hong Kong, mais également dans d'autres juridictions offshores. Cela a immédiatement soulevé des soupçons quant à l'implication de groupes cybercriminels internationaux organisés, potentiellement liés à des réseaux connus pour opérer depuis l'Asie du Sud-Est.

Ce détournement a été planifié pour coïncider avec la confusion maximale au sein de la banque, ce qui démontre un haut degré de coordination, d'anticipation et de connaissance des processus bancaires internes.

9.3. Effets de l'Attaque

Les conséquences de cette attaque ont été multiples, tant sur le plan opérationnel qu'économique :

9.3.1. Paralysie des systèmes

La propagation du malware a entraîné la paralysie partielle ou totale des systèmes informatiques de la banque pendant plusieurs jours. De nombreuses opérations internes ne pouvaient plus être exécutées normalement, y compris les processus comptables, les outils de support client, et les plateformes d'échange de données.

9.3.2. Perturbations des services bancaires

Les conséquences sur les clients ont été immédiates :

- **Guichets automatiques** : Plusieurs distributeurs de billets (ATMs) sont tombés en panne ou ont présenté des dysfonctionnements.
- **Services en ligne** : Les plateformes numériques comme la consultation de compte, les virements en ligne ou la gestion des cartes ont été temporairement indisponibles, générant une insatisfaction et de nombreuses plaintes.

10. Réponse institutionnelle à l'incident:

Face à cette crise sans précédent, Banco de Chile a déployé un plan de réponse aux incidents comprenant :

- L'isolement de certaines parties du réseau pour éviter la propagation du malware.
- Le recours à des équipes de cybersécurité externes pour appuyer les efforts internes.
- L'émission de communiqués de crise pour informer le public et rassurer les clients.
- Le renforcement temporaire des équipes opérationnelles, notamment dans les agences physiques, pour compenser l'indisponibilité des services numériques.

11. Leçons et Impact

L’attaque subie par Banco de Chile en mai 2018 a provoqué une onde de choc dans tout le secteur bancaire, bien au-delà des frontières chiliennes. Ce type d’incident, par son ampleur et sa sophistication, a mis en lumière les vulnérabilités systémiques des institutions financières face aux menaces cybernétiques.

11.1. Un signal d’alarme pour la région

L’événement a été interprété comme un sérieux avertissement pour les banques chiliennes, mais aussi pour l’ensemble des institutions financières d’Amérique latine. Il a donc mis en évidence le fait que les cybermenaces ne sont pas théoriques : elles sont effectivement réelles, concrètes, coûteuses, et peuvent frapper même les établissements considérés comme stables ou technologiquement avancés.

De nombreuses banques ont reconnu qu'elles étaient insuffisamment préparées à des attaques complexes ciblant non seulement les systèmes externes, mais surtout les infrastructures critiques internes, qui sont souvent moins surveillées.

11.2. Renforcement des mesures de cybersécurité

En réaction directe à cette attaque, plusieurs institutions ont entrepris de :

- **Réviser leurs plans de continuité d’activité et de réponse aux incidents**, pour pouvoir faire face rapidement à des crises similaires.
- **Investir dans des technologies de détection avancée**, notamment l’analyse comportementale, l’intelligence artificielle et la surveillance en temps réel.
- **Former davantage leur personnel** aux risques cyber, car l'ingénierie sociale (comme le phishing) reste l’un des vecteurs d’attaque les plus efficaces.
- **Renforcer la collaboration régionale**, par le biais de partages d’information sur les menaces (Threat Intelligence Sharing) entre banques, autorités monétaires et CERTs (Computer Emergency Response Teams).

12 Leçons stratégiques et enseignements pour Haïti

12.1 Leçons tirées de l'attaque contre Banco de Chile

L'attaque contre Banco de Chile démontre qu'une cyberattaque bien orchestrée peut contourner les protections classiques d'une institution bancaire. Paradoxalement, le réseau SWIFT n'a pas été piraté directement, mais les attaquants ont compromis l'environnement informatique local pour émettre des ordres valides. Cette attaque souligne l'importance de: contrôler les accès à privilèges, renforcer la journalisation, mettre en œuvre une authentification forte, cloisonner les postes sensibles et disposer de mécanismes de détection en temps réel (comme les SIEM). Même une infrastructure mondiale comme SWIFT peut être détournée si la sécurité de chaque banque n'est pas assurée.

12.2 Pourquoi ce cas est pertinent pour Haïti

Le choix de ce cas n'est pas anodin : il existe des parallèles entre le système bancaire chilien et celui d'Haïti. Le réseau SWIFT est aussi utilisé en Haïti par les banques pour :

- Les transferts de la diaspora,
- Les opérations commerciales à l'international,
- Les paiements d'organisations internationales.

Haïti est donc exposée aux mêmes types de risques, bien que les attaques y soient souvent moins médiatisées.

12.3 Vulnérabilités spécifiques au contexte haïtien

Les banques haïtiennes font face à des défis concrets : des budgets cybersécurité limités, un niveau de formation technique inégal, une supervision fragmentée entre la BRH, les banques commerciales et les prestataires IT, des infrastructures souvent vieillissantes et un accès limité à des outils avancés comme les pare-feux nouvelle génération ou les SIEM.
Cela crée un terrain favorable à des intrusions ciblées, via des malwares ou des erreurs de configuration.

12.4 Recommandations réalistes pour Haïti

Face à ces défis, plusieurs actions simples mais efficaces peuvent être mises en œuvre

- Segmenter les postes de travail critiques (notamment ceux liés à SWIFT),
- Mettre en place une double validation manuelle pour toute opération financière sensible,
- Sensibiliser les employés aux risques de phishing et d'ingénierie sociale,
- Implémenter une authentification forte (MFA) sur les accès critiques,
- Mettre en place des journaux d'audit activés et vérifiés régulièrement,
- Adopter progressivement les normes ISO/IEC 27001 et 27005 via des projets pilotes réalistes.

Ces recommandations visent à établir une stratégie de cybersécurité réaliste, évolutive et adaptée aux contraintes locales, pour renforcer la confiance dans le système financier haïtien.

13. Analyse de risque

13.1. Menaces

- Déploiement d'un malware destructeur
- Phishing ciblé contre des employés
- Accès non autorisé à des privilèges d'administration

13.2. Vulnérabilités

- Faible segmentation réseau
- Défaut de supervision des comptes à privilèges
- Surveillance inadéquate des activités SWIFT

13.3. Risques

- Détournement de fonds
- Indisponibilité temporaire des services
- Fuite d'informations confidentielles
- Atteinte à la réputation

Actif critique	Menace	Vulnérabilité	Probabilité	Impact	Niveau de risque
Système SWIFT	Détournement de fonds	Faible segmentation, accès non contrôlé	Élevée	Critique	Élevé
Données clients	Fuite d'informations	Absence de journalisation ou de SIEM	Moyenne	Élevé	Moyen à élevé
Poste de travail internes	Infection par malware	Mauvaise hygiène logicielle	Élevée	Élevé	Élevé

13.4. Évaluation

Les risques sont classés selon leur gravité et leur probabilité. L'attaque de 2018 est un exemple de risque élevé ayant un impact critique sur l'activité.

Cette démarche d'évaluation suit les recommandations de la norme ISO/IEC 27005, étudiée en classe, qui structure l'analyse de risque autour des actifs, menaces, vulnérabilités, impacts et probabilités.

14. Recommandations (mesures de contrôle)

Les recommandations sont classées selon les trois types de mesures présentés en cours :
Techniques: liées à la technologie (firewalls, IDS/IPS, etc.) ;
Organisationnelles : gouvernance, procédures, SOC, PCA/PRA ;
Humaines : formation, sensibilisation, culture de sécurité.

En gros, on a donc les mesures :

14.1. Techniques

- Implémentation de pare-feux nouvelle génération et de systèmes de détection d'intrusion (IDS/IPS).
- Séparation stricte des environnements critiques (segmentation réseau).
- Authentification multifactorielle sur tous les accès sensibles.

Sur cet aspect technique, on a :

Modèle IAAA (Identification, Authentification, Autorisation, Audit)

La gestion des accès dans Banco de Chile aurait gagné à être structurée autour du modèle IAAA (Identification, Authentification, Autorisation, Audit), étudié en classe. Ce cadre assure que seuls les utilisateurs dûment identifiés et autorisés accèdent aux ressources sensibles, que leurs actions soient tracées, et qu'un audit post-incident soit possible. Cette approche renforce considérablement la sécurité des environnements critiques comme les interfaces SWIFT.

SIEM et surveillance des journaux

La mise en place d'un SIEM (Security Information and Event Management) aurait permis de centraliser les journaux système et d'analyser en temps réel les activités suspectes. Comme vu en séance 10, ces outils détectent les anomalies, déclenchent des alertes automatiques et facilitent les enquêtes post-incident. Cela aurait potentiellement permis une détection plus rapide des transferts frauduleux via SWIFT.

En conclusion, l'attaque ayant ciblé des comptes privilégiés liés au réseau SWIFT démontre une faiblesse dans la gestion des accès critiques et une application rigoureuse du modèle IAAA (Identification, Authentification, Autorisation, Audit) aurait permis de mieux contrôler, tracer et restreindre l'usage des comptes à haut privilège.

14.2. Organisationnelles

- Élaboration et test régulier d'un PCA/PRA.
- Mise en place d'une équipe SOC (Security Operations Center) 24/7.
- Application du principe de moindre privilège dans la gestion des comptes.

Modèles de contrôle d'accès : MAC / DAC / RBAC

L'application du modèle RBAC (Role-Based Access Control) permettrait une gestion plus fine des droits d'accès selon les fonctions, limitant ainsi le risque d'abus. De plus, dans les environnements bancaires très sensibles, des contrôles de type MAC (Mandatory Access Control) peuvent aussi être utilisés pour verrouiller l'accès à certaines ressources critiques. Ces modèles, abordés en séance 9, contribuent à une posture de sécurité renforcée.

Ainsi, une bonne gestion des identités et des accès (GIA) est essentielle pour toute institution bancaire et l'intégration des modèles IAAA et RBAC, combinée à une journalisation systématique, permet de limiter les abus internes, détecter les activités suspectes et réagir rapidement en cas d'incident.

Ces recommandations répondent donc aux exigences de la norme ISO/IEC 27001 – Annexe A, également abordée en séance 3, qui fournit un cadre structuré pour la mise en œuvre des politiques de sécurité de l'information.

14.3. Humaines

- Formation continue en cybersécurité pour tous les employés.
- Sensibilisation renforcée aux techniques de phishing et d'ingénierie sociale.
- Intégration de la cybersécurité dans la culture d'entreprise.

Typologie des mesures de sécurité : préventive, détective, corrective, dissuasive

Ces recommandations s'inscrivent dans la typologie étudiée en séance 5 :

Préventives : MFA, segmentation réseau, principe du moindre privilège
Détectives : journaux d'audit, SIEM, surveillance comportementale
Correctives : procédures de réponse aux incidents, restauration système
Dissuasives : politiques internes strictes et sanctions prévues

L'association équilibrée de ces catégories renforce la résilience du système bancaire.

15. Conclusion

L'attaque subie par Banco de Chile en 2018 illustre les multiples failles pouvant exister même dans les institutions les plus avancées technologiquement. L'analyse de cet incident a permis d'appliquer les fondements théoriques vus dans le cours , notamment les principes de gestion des risques (ISO 27005), la sécurité du réseau SWIFT, la classification des mesures (préventives, détectives, correctives), et la gouvernance des accès selon le modèle IAAA.

Elle a également révélé l'importance d'une approche intégrée de la cybersécurité, combinant technologies (SIEM, MFA, segmentation), processus organisationnels (SOC, plans de continuité), et sensibilisation des ressources humaines. Ces éléments doivent être harmonisés pour répondre efficacement aux menaces modernes, en particulier celles de type multi-phasé comme l'attaque étudiée.

Enfin, cette étude rappelle que les banques haïtiennes doivent s'approprier ces enseignements en fonction de leurs contraintes réelles, en priorisant des actions simples, ciblées et efficaces.

16. Références

- Banco de Chile Cyberattack Report, 2018
- ISO/IEC 27001:2013
- ISO/IEC 27005
- SWIFT Customer Security Programme (CSP)
- Kaspersky Security Report on Lazarus Group
- NIST Cybersecurity Framework
- Wired, ZDNet, LeMagIT
- CERT-Chile, Banque centrale du Chili