

Cours : Sécurité des Systèmes Informatiques

**Groupe 7**

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

**Sujet : Le Piratage de Banco *de Chile***

Université de Technologie d'Haïti | **UINITECH**

Professeur : Blaise ARBOUET

# Plan de la présentation

1. Contexte de Banco de Chile
2. Chronologie de l'attaque
3. Nature et déroulement de l'attaque
4. Effets de l'incident
5. Enjeux de cybersécurité (Confidentialité, Intégrité, Disponibilité)
6. Vulnérabilités et risques
7. Réponses institutionnelles
8. Leçons stratégiques pour Haïti
9. Recommandations concrètes
10. Concepts vus en cours (ISO, IAAA, SIEM...)
11. Conclusion et ouverture
12. Références



## Banco de Chile : Un acteur majeur du secteur financier

- Fondée en 1893, l'une des plus anciennes banques d'Amérique latine
- Millions de clients, milliers d'employés, présence nationale étendue
- **Services** : comptes, prêts, investissements, services aux entreprises, e-banking
- **Rôle crucial** dans l'économie chilienne, impliquée dans les transactions nationales et internationales
- Une modernisation numérique rapide... mais aussi de nouveaux risques cyber



Une modernisation numérique rapide... mais aussi de nouveaux risques cyber



# Chronologie de l'attaque

Mai-Juin 2018

**24 mai 2018**

Panne détectée  
dans les agences et  
services téléphoniques



**28 mai 2018**

Identification d'un virus  
sur les postes de travail

**Début juin 2018**

Découverte de  
transactions suspectes  
dans SWIFT



**11 juin 2018**

Confirmation du vol de  
10 millions de dollars,  
transférés à Hong Kong



**11 juin 2018**

Confirmation du vol  
de 10 millions de dollars,  
transférés à Hong Kong

# Nature et déroulement de l'attaque

---

## Phase 1: Malware Wiper



- Affectation de 9 000 PCs et 500 serveurs
- Désorganisation volontairement provoquée chez les équipes IT
- Exploitation du chaos pour agir sans interruption

## Phase 2: Détournement via SWIFT

- Utilisation d'un SWIFT valide pour émettre une transaction
- Vol de 10 millions USD transférés vers des comptes en Asie
- Exploitation du chaos pour agir sans interruption

Une attaque planifiée, ciblée, discrète  
et techniquement avancée.

# Schéma du déroulement de l'attaque





# Effets de l'attaque



## Effets internes

- Paralysie de nombreux services informatiques
- Panne de 9 000 postes et 500 serveurs
- Interruption temporaire des opérations internes:
  - Comptabilité
  - Support client
  - Échanges interbancaires

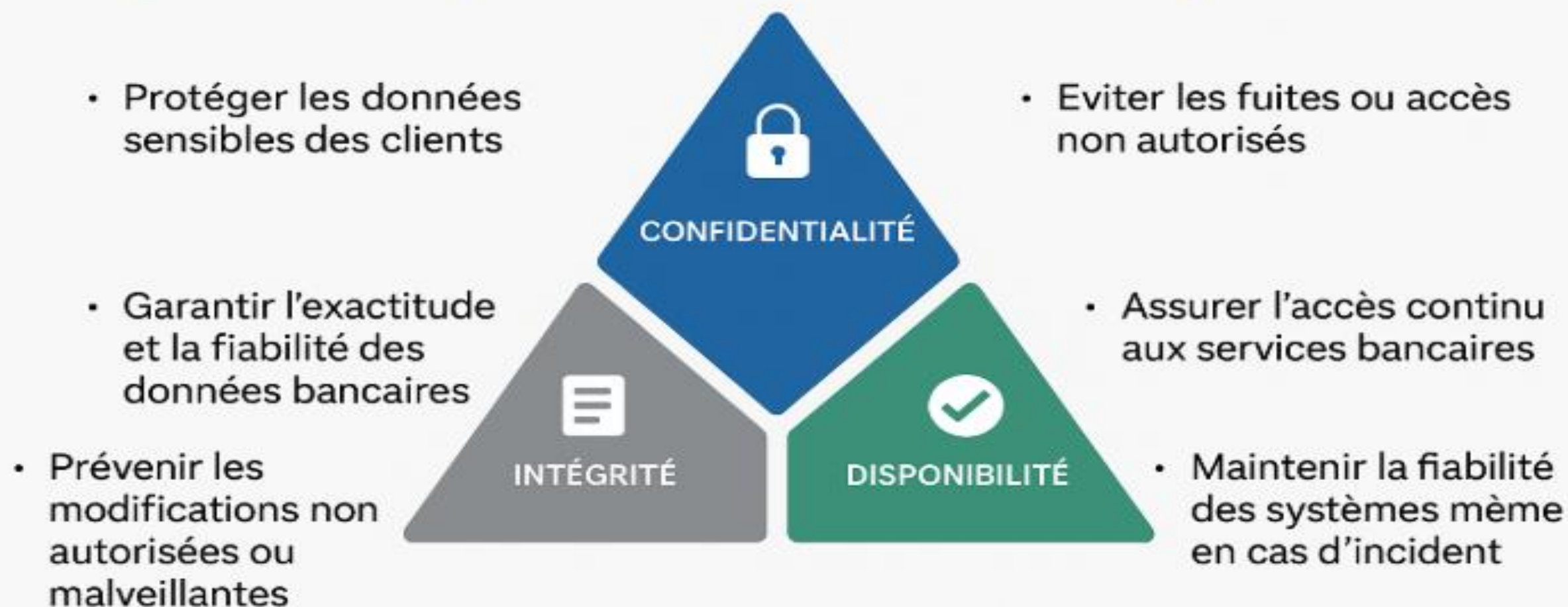


## Effets sur les clients

- Guichets automatiques (ATMs) hors service
- Plateformes en ligne inaccessibles (e-banking, virements)
- Augmentation des plaintes
- Perte de confiance des usagers et du grand public

▲ Une attaque visible, paralysante et fortement ressentie à tous les niveaux.


# Enjeux de cybersécurité: le triangle CID



*Ces trois piliers sont indispensables pour maintenir la confiance et la résilience des systèmes bancaires.*




# Vulnérabilités et risques

 **Risque** = Menace × Vulnérabilité × Impact

Exemples tirés de l'incident :

Menace	Vulnérabilité	Risque
Cybercriminels (APT)	Absence de segmentation réseau	Accès non autorisé à SWIFT via postes internes
Email piégé (phishing)	Mauvaise sensibilisation des utilisateurs	Infection initiale du réseau via malware wiper
Transactions SWIFT	Faible séparation des privilèges / pas d'audit	Vol de 10M USD sans détection immédiate

 Des vulnérabilités techniques et humaines ont facilité la matérialisation du risque.

# Réponses institutionnelles



## Mesures techniques immédiates:

- Isolement de segments réseau infectés
- Blocage d'accès à distance
- Désactivation temporaire du service SWIFT



## Communication:

- Déclaration publique le 11 juin 2018
- Assurance donnée aux clients sur la non-affectation des comptes
- Coordination avec les autorités chiliennes et la banque centrale



## Actions organisationnelles:

- Activation d'un plan de continuité d'activité (PCA)
- Renforcement de l'équipe cybersécurité
- Lancement d'un audit complet des systèmes

# Leçons stratégiques pour Haïti

 Principaux enseignements de l'attaque de Banco de Chile :

- |   |  |
|---|--|
| <p>① <b>Renforcer la gestion des accès</b><br/>Implémenter le modèle IAAA<br/>Séparation stricte des droits<br/>(rôles, services, privilèges)</p>   | <p>② <b>Structurer la réponse</b><br/>Élaborer un Plan de Continuité<br/>(PCA) et un Plan de réponse<br/>aux incidents</p>   |
| <p> <b>Former les utilisateurs</b><br/>Sensibilisation au <i>phishing</i><br/>Réduction des erreurs humaines</p> | <p> <b>Structurer la réponse</b><br/>Élaborer un Plan de Continuité<br/>(PCA) et un Plan de réponse<br/>aux incidents</p> |

Haïti peut progresser malgré ses contraintes, avec une approche ciblée, réaliste et stratégique de la cybersécurité.



# Recommandations concrètes



## Techniques

- Segmenter le réseau (SWIFT, interne, DMZ...)
- Installer un SIEM open-source (ex: Wazuh)
- Activer la journalisation des logs critiques



## Organisationnelles

- Mettre en place un PCA/PRA
- Définir une politique claire de gestion des accès
- Mettre en place un plan de réponse aux incidents



## Humaines

- Sensibiliser contre le phishing
- Simuler des attaques pour tester l'équipe
- Former tous les nouveaux employés

✓ Des mesures *simples, efficaces et realistes* pour renforcer la cybersécurité sans exploser le budget.

# Concepts vus en cours

## Normes et cadres de référence

- **ISO 27001**: Système de management de la sécurité de l'information (SI)
- **ISO 27005**: Analyse et gestion des risques
- **PCA / PRA**: Continuité et reprise d'activité

## Modèles de contrôle des accès

- **IAAA**: Identification, Authentification, Autorisation, Audit
- **RBAC / MAC**: Contrôle des accès basé sur les rôles ou les règles

## Outils et technologies

- **SIEM**: Système de gestion des événements de sécurité (ex : Wazuh)
- **Journalisation & audit**: tracabilité des actions critiques
- **Segmentation réseau**: cloisonnement des flux sensibles

*Tous ces concepts ont été mobilisés pour structurer l'analyse, la réponse et les recommandations proposées.*

# Conclusion et Ouverture

## Conclusion

- L'attaque contre Banco de Chile révèle la fragilité des systèmes bancaires connectés.
- Elle démontre la nécessité :
  - d'une gestion rigoureuse des accès
  - d'une préparation structurée
  - d'une cohérence entre technologie, organisation et formation

## Ouverture

Et si demain, une banque haïtienne était ciblée ?

La question n'est plus si, mais quand.

Il est urgent de se préparer avec des moyens ciblés et une stratégie adaptée.

 **La cybersécurité ne se décrète pas : elle se construit, couche par couche, action après action.**



# Références

## **Normes et cadres de sécurité :**

- ISO/IEC 27001 – Système de management de la sécurité de l'information
- ISO/IEC 27005 – Gestion des risques liés à la sécurité de l'information

## **Notions du cours SSI1024 :**

- Modèle IAAA (Identification, Authentification, Autorisation, Audit)
- Concepts clés : SIEM, PCA, PRA, RBAC, journalisation, analyse de risque
- Supports internes du cours (séances, documents, exercices)

## **Sources documentaires :**

- Banco de Chile – Rapport officiel, 2018
- ThreatPost – Banco de Chile Confirms SWIFT Attack, \$10M Stolen, juin 2018
- BleepingComputer – Malware Attack Disables ATMs in Chile, 2018
- Comparitech – Cyber Attacks in Latin America, 2022