UNIVERSITÉ DE TECHNOLOGIE D'HAÏTI

SECURITE DES SYSTEMES INFORMATIQUES

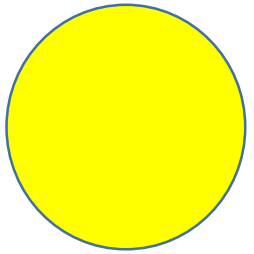
SSI1024 – SESSION HIVER 2025

L'attaque contre le gouvernement du Costa-Rica (2022) par le groupe Conti - paralysie de services publics, demande de rançon, médiatisée

Présenté à : Blaise ARBOUET

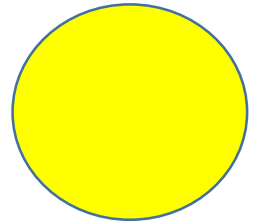
Membres de l’Equipe

- ✓Christna ETIENNE
- ✓Jean-Robert JACQUES
- ✓John Rolklef DECLAMA
- ✓Niskens SANON
- ✓Paul Denis COQUILLON



Plan

- Introduction
- Sommaire
- Contexte
- Enjeux de cybersécurité
- Classification des données
- Analyse de risques
- Recommandations
- Conclusion
- Bibliographie



Introduction

À l’ère numérique, les systèmes informatiques sont devenus indispensables au fonctionnement des États, des entreprises et des services essentiels. Mais cette dépendance croissante s'accompagne de risques majeurs : les cyberattaques.

Les cyberattaques désignent des actions malveillantes menées à travers des réseaux ou des systèmes numériques. Elles peuvent provoquer le vol de données, la perturbation de services ou même la paralysie d'infrastructures critiques
.
Parmi elles, les rançongiciels (ou ransomwares) sont particulièrement redoutables : ils chiffrent les données et exigent une rançon pour les restituer.

Face à ces menaces, la cybersécurité s’impose comme un domaine stratégique. Elle vise à garantir la **confidentialité**, l’**intégrité** et la **disponibilité** des systèmes d’information, tout en protégeant la vie privée des utilisateurs.

Sommaire

En avril 2022, le gouvernement du **Costa Rica** a été victime d’une attaque massive menée par le groupe de ransomware **Conti**.

Conséquences immédiates :

Paralysie de plus de **30 ministères** et services publics.

Blocage de services vitaux : impôts, salaires, sécurité sociale, commerce extérieur.

Vol, chiffrement et fuite de **plus de 600 Go** de données sensibles.

Rançon exigée : **10 millions USD** (non payée).

Contexte

En avril 2022, le gouvernement du Costa Rica a subi une cyberattaque majeure menée par le groupe de ransomware Conti. Cette attaque a paralysé plusieurs ministères et services publics, entraînant une grave crise administrative.

En refusant de payer la rançon exigée, l'État a dû faire face à la publication de données sensibles. Cet incident met en évidence la vulnérabilité des infrastructures publiques face aux cybermenaces et souligne l'importance de renforcer la cybersécurité au sein des institutions gouvernementales.

Enjeux de cybersécurité

L’attaque contre le Costa Rica a mis en évidence la fragilité des systèmes gouvernementaux face aux cybermenaces, affectant les trois piliers de la cybersécurité : Confidentialité, Intégrité, Disponibilité (CID).

- **Confidentialité** : Fuite massive de données fiscales, personnelles et médicales ; publication sur le dark web ; atteinte à la vie privée des citoyens.
- **Disponibilité** : Blocage des services essentiels (impôts, salaires, sécurité sociale) ; retour temporaire à des procédures manuelles ; ralentissement administratif.
- **Intégrité** : Fichiers chiffrés ou corrompus ; données altérées ou incomplètes ; difficulté à vérifier l’exactitude des bases.

Classification des données

Type de données	Exemples concrets	Confidentialité	Intégrité	Disponibilité	Type d'impact en cas de compromission
Données fiscales	-Déclarations de TVA -Dossiers d'impôt -Registres d'entreprises	Secret	Élevé	Élevé	Paralysie économique, perte de revenus, chaos administratif
Données personnelles	-Numéros d'identification -Adresses, numéros de téléphone -Infos médicales	Sensible / Privé	Modéré	Modéré	Vol d'identité, atteinte à la vie privée
Données RH	-Salaires -Contrats -Évaluations, congés -Données personnelles des agents publics	Confidentiel	Modéré	Modéré	Tension sociale, violation de la vie privée du personnel
Courriels internes	-Échanges entre ministères -Documents non publiés -Prises de décision	Confidentiel	Faible	Faible	Perte de crédibilité, possible manipulation externe
Documents publics	-Communiqués officiels -Rapports déjà disponibles sur les sites web	Public	Faible	Faible	Information déjà accessible légalement

Analyse de risques

Identification des actifs

Actif impacté	Exemple/Description	Sensibilité	Commentaire synthétique
Données fiscales	Déclarations, identifiants, historiques de paiement	5	Données critiques pour l'État et les citoyens
Données personnelles	Noms, adresses, numéros d'identification, salaires	5	Risque élevé d'usurpation et d'atteinte à la vie privée
Données administratives	Contrats, audits, communications internes	4	Impacts réputationnels et organisationnels
Données sociales	Dossiers de sécurité sociale, allocations, retraites	5	Risque de préjudice social et de blocage d'aides
Systèmes informatiques	Serveurs, applications, bases de données	5	Interruption de service, pertes économiques
Portails gouvernementaux	Sites web, plateformes de services en ligne	5	Indisponibilité majeure pour les citoyens

Identification des menaces et vulnérabilités

Menace / Vulnérabilité	Description / Exemple	Impact	Probabilité	Commentaire synthétique
Spear phishing	Courriels ciblés pour voler des identifiants	5	5	Accès initial confirmé
Failles logicielles non corrigées	Absence de patchs sur serveurs/applications	5	5	Mouvement latéral facilité
Segmentation réseau insuffisante	Réseaux plats, accès étendu	5	4	Propagation rapide du malware
Détection tardive des intrusions	Absence de SIEM, logs non surveillés	5	4	Exfiltration massive de données
Absence de plan de réponse	Procédures non testées, manque de formation	4	3	Retard de réaction

Recommandations (mesures de contrôles)

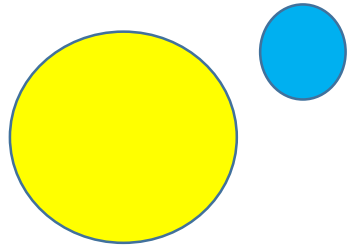
Pour prévenir et atténuer les cyberattaques comme celle subie par le Costa Rica, il est essentiel d'agir à plusieurs niveaux :

- **Réponse immédiate** : Isoler les systèmes infectés, enquêter sur l'attaque, informer les autorités et le public.

- **Renforcement à court terme (0-3 mois)** : Mettre à jour les systèmes, renforcer l'authentification, former le personnel et surveiller les activités suspectes.

- **Améliorations à moyen terme (3-12 mois)** : Segmenter le réseau, utiliser des outils de sécurité avancés, mieux gérer les accès, classifier les données.

- **Transformation à long terme (12 mois et plus)** : Adopter une gouvernance de cybersécurité (normes ISO), automatiser les contrôles, instaurer une culture de sécurité et adapter les stratégies aux nouvelles menaces.



Conclusion

L’attaque de 2022 contre le gouvernement du Costa Rica a montré les conséquences graves des cyberattaques sur les infrastructures critiques et les services publics. Elle souligne l’urgence de renforcer la résilience numérique et d’adopter une approche proactive pour protéger les systèmes essentiels.

Ce cas illustre aussi la montée du crime organisé numérique capable de déstabiliser des États entiers. Enfin, il met en avant l’importance cruciale de la prévention, de la préparation et de la coopération internationale en cybersécurité face à l’augmentation des menaces contre les infrastructures étatiques.