Audit Cybersécurité
E-Commerce Express

Présentation finale - INF1753

Groupe 2

November 28, 2025

Contexte

L'entreprise **E-Commerce Express**, spécialisée dans la vente d'articles de sport, fait face à des défis critiques en matière de cybersécurité.

E-Commerce Express connaît une croissance rapide accompagnée d'une forte augmentation de données personnelles :

- données d'identification;
- données financières;
- données comportementales.

Une tentative de cyberattaque a mis en lumière des failles importantes.

Objectifs de l'audit

1. Évaluer la sécurité informatique et la gestion des données.
2. Identifier les risques techniques, humains et organisationnels.
3. Vérifier la conformité réglementaire.
4. Proposer un plan d'action réaliste.
5. Établir une feuille de route.

Diagnostic de la situation

ACTIFS INFORMATIONNNELS CRITIQUES

- **Infrastructures technologiques** : serveurs, bases de données, réseau interne.
- **Données sensibles** : identifiants, paiements, historiques d'achats.
- **Utilisateurs et accès** : employés, clients, partenaires.

Risques techniques

- Vulnérabilités logicielles.
- Risques DDoS, malware, ransomware.
- Mauvaise gestion du chiffrement.
- Absence de mises à jour structurées.

Risques humains et organisationnels

Humains :

- erreurs de manipulation;
- phishing;
- mots de passe faibles.

Organisationnels :

- absence de politiques;
- gouvernance faible;
- non-conformité légale.

Conformité aux lois

LPRPDE (fédéral) :

- consentement des clients;
- sécurité proportionnelle;
- notification obligatoire en cas d'atteinte.

Loi 25 (Québec) :

- responsable de la protection des données;
- EFVP;
- transparence accrue.

Obligations en cas d'incident

- Détection, documentation, tenue d'un registre.
- Notification des autorités et des clients.
- Preuve de mesures raisonnables préexistantes.

Dilemmes éthiques

- Surveillance des employés.
- Gestion des accès (moindre privilège).
- Collecte et profilage des données clients.

Mesures préventives et correctives

Sécurité technique (priorité critique)

- Renforcement du chiffrement (HTTPS + TLS 1.3).
- MFA pour employés + option clients.
- Patch management automatisé.
- Système SIEM.
- Pseudonymisation.
- Segmentation réseau.
- Tests de pénétration.
- Sauvegardes 3-2-1.

Mesures préventives et correctives

Politiques internes (priorité élevée)

- Politique de sécurité de l'information.
- Politique de confidentialité.
- Politique de gestion des incidents.
- Gestion des accès (RBAC).
- Politique de conservation des données.
- Classification des données.

Mesures préventives et correctives

Organisation (priorité élevée)

- Recrutement d'un RSSI.
- Désignation d'un responsable de la protection des données.
- Coordination IT — juridique — direction.

Plan de sensibilisation du personnel

- Programme de formation
- Campagnes de sensibilisation continue
- Mesure de l'efficacité

Echéancier du plan d'action (Phase 1)

Tâche / Activité	Mois 1	Mois 2	Mois 3	Mois 4	Mois 5	Mois 6
URGENT (Semaines 1-6)						
Chiffrement HTTPS	■					
MFA Employés	■	■				
Politique Securité	■	■				
Nomination RPD	■					
PRIORITAIRE (Mois 1-3)						
Recrutement RSSI	■	■	■			
SIEM (Monitoring		■	■			
Formation initiale		■	■			
Patch Management		■	■			
Sauvegardes 3-2-1	■	■				
IMPORTANT (Mois 2-6)						
Segmentation réseau			■	■	■	
Tests Pénétration				■	■	
Politiques internes		■	■			
EFVP initiale			■	■		
Assurance cyber		■	■			
Campagnes Sensib.			■	■	■	■
Audit Conformité					■	■

Echéancier du plan d'action

- **Phase 2:** Consolidation (6-12 mois);
- **Phase 3:** Amelioration continue (12-24 mois).

Conclusion

L'audit d'E-Commerce Express a révélé des vulnérabilités majeures en cybersécurité, gouvernance des données et conformité légale, mises en évidence par une tentative de cyberattaque récente. Ces failles affectent la protection des données sensibles et la confiance des clients. Un projet global de cybersécurité est proposé pour renforcer la résilience de l'entreprise, protéger les données personnelles et, au-delà de la simple correction post-attaque, servir de stratégie pour une croissance durable et l'instauration d'une culture de sécurité robuste dans le contexte numérique actuel.