Rapport d’Analyse Sécurité – Projet CovY Full Remote

- Version : 2
- Date : juillet 2025
- Classification : Interne – Ne pas diffuser
- Pilotage : Adel B : Directeur de CovY / Caulin L : Chef de la Sécurité (RSSI)

Contexte et périmètre

Entreprise : CovY – Plateforme e-commerce
Transition full remote imposée par la pandémie
Périmètre :
• Postes de travail distants (laptops, home-office)
• VPN, MFA, accès cloud (IaaS, PaaS, SaaS)
• Services cœur : site web, base de données, CRM, ERP, messagerie, collaboration
• Infrastructure cloud multi-AZ / multi-région
• Processus support : sauvegarde, PCA/PRA, sensibilisation, pentests

Méthodologie

– Référentiels : ISO 27001, RGPD, modèle 3-2-1, bonnes pratiques cloud (CIS, NIST)
– Inventaire des actifs et classification (Tier 1–4 via BIA)
– Scan automatique de vulnérabilités (Qualys, Nessus) et analyse manuelle
– Tests d'intrusion internes/externes (white box)
– Interviews RSSI, DSI, support IT, référents métiers
– Atelier de cartographie des processus critiques

Inventaire et évaluation des actifs critiques

Actifs Tier 1 (RTO ≤ 1 h / RPO ≤ 15 mn)
• Front-office e-shop (Web servers, API)
• Base de données produits et clients
• Services d'authentification (Azure AD – MFA)
• Solution de paiement (PCI DSS)
Actifs Tier 2 (RTO ≤ 4 h / RPO ≤ 1 h)
• Portails internes (RH, facturation)
• Messagerie et collaboration (Exchange Online / Teams)
Actifs Tier 3–4 (RTO ≤ 24 h)
• Archivage, logs, backups historiques

Menaces et vulnérabilités identifiées

C1. Postes distants mal protégés
• OS non mis à jour, antivirus absent ou périmé
• Wi-Fi domestique non chiffré ou partagé
C2. Accès cloud insuffisamment restreints
• Rôles AWS/Azure trop larges, absence de principe de moindre privilège
• MFA non systématique sur API et comptes à haut privilège
C3. Infrastructure réseau
• VPN mal segmenté, pas de micro-segmentation
• Exposition inutile de ports (RDP, SSH)
C4. Sauvegarde et PCA/PRA

• Processus 3-2-1 non adapté aux endpoints : pas de cache local sur chaque poste
• Scripts de restauration non testés en full remote
C5. Gouvernance et sensibilisation
• Taux de complétion de formation < 60 %
• Phishing tests non réguliers
C6. Conformité
• Absence de DPO formellement nommé
• Registre de traitements RGPD incomplet

Analyse des risques

Matrice risque (probabilité × impact) positionne :
• C2 (accès cloud) et C1 (endpoints) en zone rouge – risque élevé
• C3 (VPN) et C4 (sauvegarde) en zone orange – risque moyen
• C5/C6 en zone jaune – risque faible à moyen
Risques métier majeurs : perte de confiance client (fuite données PV), indisponibilité site > 1 h
Risques financiers : amendes RGPD, sanctions PCI DSS

Évaluation des contrôles existants

Points forts :
• VPN chiffré TLS, solution SaaS multi-AZ, plan #3-2-1 global
• PSSI en place couvrant 13 sections, plans de formation et PCA/PRA théoriques
Points faibles :
• Gestion des accès IAM non centralisée, absence de workflows d'approbation
• Sauvegardes endpoints non automatisées et non inventoriées dans un GRC
• Processus d'audit interne pas encore déployé en full remote

Recommandations et plan d'actions

8.1 Sécurisation des postes distants
• Déployer MDM/EDR sur tous les endpoints avec mises à jour automatiques
• Forcer chiffrement disque (BitLocker, FileVault) et Wi-Fi WPA3
8.2 Renforcement IAM & Cloud
• Mettre en place un PAM pour comptes privilégiés, limiter les droits par rôle
• Activer MFA sur toutes les consoles cloud et APIs sensibles
• Automatiser la rotation des clés et certificats avec un CA interne ou AWS KMS
8.3 Réseau et segmentation
• Segmenter le VPN en pools métiers, isolation micro-seg aussi sur cloud
• Fermer tous les ports non strictement nécessaires (just-in-time access)
8.4 Sauvegarde & PCA/PRA full remote
• Étendre l'architecture 3-2-1 « endpoint-cloud-cloud » ; chiffrer et inventoriariser via GRC
• Procédures de failover automatisées (IaC, Terraform/ARM, scripts déclenchés via pipeline CI/CD)
• Exercises trimestriels distants (tabletop) et annuels de bascule complète
8.5 Gouvernance, conformité, sensibilisation

• Nommer formellement un DPO, compléter le registre RGPD
• Mettre en place un audit interne ISO 27001 annuel avec check-lists Cloud et remote
• Lancer campagnes phishing trimestrielles et web-trainings obligatoires

8.6 Pentest et remédiation

• Planifier un test d’intrusion externe sur l’infra SaaS et IaaS every 6 months
• Documenter les failles, suivre la résolution dans un backlog ITSM et dashboard KPI/KRI

Suivi, indicateurs et amélioration continue

• KPIs : taux de correctifs, MTTD/MTTR, % de postes conformes, taux de clic phishing
• KRIs : vulnérabilités critiques non patchées, droits excessifs, incidents PCA déclenchés
• Comités trimestriels PCA/PRA et revue annuelle de la PSSI
• Mise à jour de la PSSI et du rapport d’analyse sous 30 jours après chaque exercice ou incident

Conclusion

Cet état des lieux démontre que CovY dispose d’une base solide (cloud multi-AZ, VPN, chiffrage) mais doit prioritairement durcir la protection des endpoints, standardiser la gestion des accès et renforcer ses processus de sauvegarde/PCA en full remote. La mise en œuvre rapide des recommandations et le suivi via indicateurs garantiront la résilience de la plateforme e-commerce et la conformité réglementaire.