HACKMOSPHERE

Votre sécurité nous tient hackeur.

Rapport Exécutif - Pentest ExCorp

Synthèse Exécutive

Résultats du test de sécurité — Mars 2026

Agenda

Ce que nous avons fait

Un test de sécurité (« pentest ») reproduit les actions d'un attaquant réel pour identifier les failles d'ExCorp avant qu'elles ne soient exploitées. Cinq dimensions ont été testées entre le 9 et le 28 février 2026.

Application Web

Site & services exposés sur Internet

Infrastructure Interne

Réseau bureautique & Active Directory

Réseau Industriel (OT)

Production, automates, supervision

Sécurité Physique

Accès aux locaux, postes du lobby

Phishing

Sensibilisation des employés

Dates du test : 9 au 13 février 2026

Le verdict

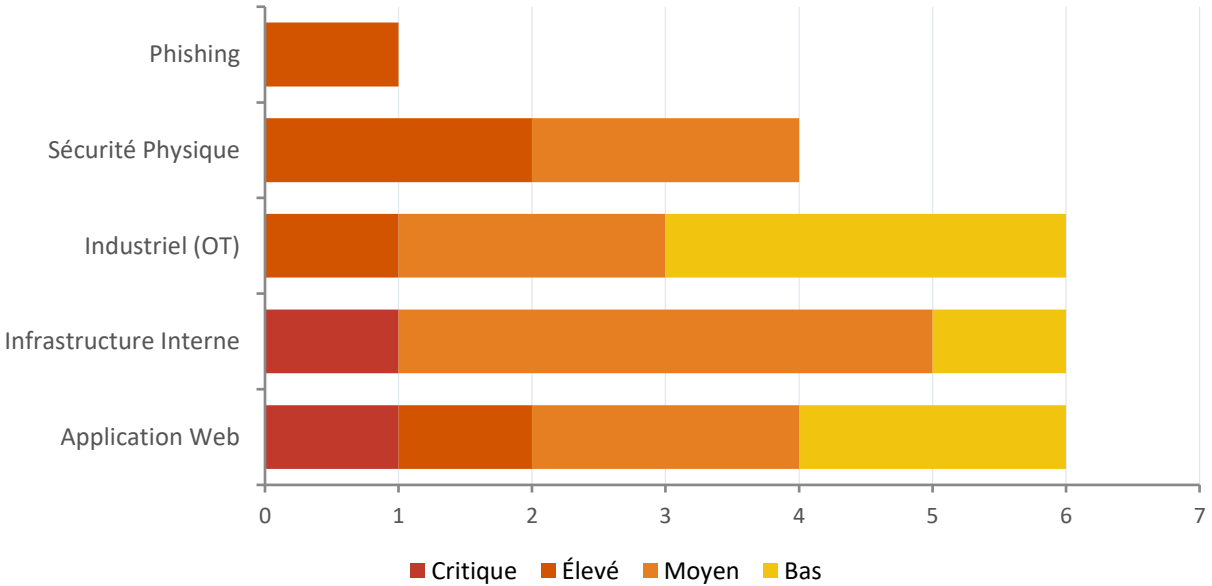
Niveau de risque global identifié

CRITIQUE

Avec une simple connexion Internet, un attaquant motivé aurait pu prendre le contrôle total de votre infrastructure Informatique et de votre réseau de production, en quelques jours.

Vue d'ensemble des vulnérabilités

Répartition des failles identifiées par domaine et par niveau de gravité.



Total identifié

Critique	2
Élevé	5
Moyen	10
Bas	6

Comment un attaquant aurait pu vous atteindre

Scénario d'attaque réaliste reconstitué à partir des failles identifiées.

1

Accès initial

Un cambrioleur trouve plusieurs « fenêtres ouvertes » : des serveurs vulnérables exposés sur Internet, un poste accessible dans le lobby, ou un employé piégé par un email frauduleux.

2

Pivot dans le réseau

Une fois à l'intérieur, l'attaquant se déplace de machine en machine en exploitant des mots de passe mal protégés et des configurations laxistes rendant les serveurs vulnérables.

3

Prise de contrôle totale

Il obtient les clés d'administration de tout le réseau ExCorp via Active Directory — et peut pivoter vers le réseau de production industrielle.

Risque industriel : depuis Internet, un attaquant peut atteindre les automates qui pilotent la production industrielle.

Ce que cela peut signifier

Cinq impacts business directs découlent des failles identifiées.

Paralysie opérationnelle

Un ransomware ou une prise de contrôle hostile peut stopper la production pendant plusieurs jours, voire semaines.

Espionnage industriel

Vol de données sensibles, savoir-faire, formules, plans de production via l'accès au réseau OT.

Perte de confiance clients

Une cyberattaque rendue publique entraîne une dégradation durable de l'image et de la confiance des partenaires.

Non-conformité réglementaire

Sanctions potentielles au titre du RGPD et de la directive NIS2, désormais applicable au secteur industriel.

Coût financier direct

Le coût moyen d'une cyberattaque sur un environnement industriel **est sans commune mesure avec celui de la remédiation**.

Les 5 points les plus critiques à retenir

1	Des systèmes accessibles depuis Internet permettaient une prise de contrôle à distance, sans authentification.	Critique
2	Le réseau industriel (production) était accessible depuis le réseau bureautique.	Critique
3	Les mots de passe d'administrateurs étaient récupérables en mémoire des postes.	Élevé
4	N'importe qui dans le bâtiment pouvait brancher un appareil et accéder au réseau interne.	Élevé
5	Aucun plan de réponse à incident ni de reprise d'activité n'existe en cas d'attaque.	Élevé

Le facteur humain : résultats du phishing

83 emails envoyés

98,8% des emails ouverts

22,9% ont cliqué sur le lien malveillant

15,7% ont fourni leurs identifiants

21% ont signalé l'email à la DSI

Traduit en termes business :

Sur 100 employés, 15 auraient donné les clés pour entrer dans l'entreprise.

Le facteur humain reste l'une des premières portes d'entrée d'une cyberattaque.

Ce que coûte réellement une cyberattaque

Repères de marché pour une PME industrielle en France / Europe.

500 K€

Coût moyen d'un ransomware

sur un environnement industriel

21 jours

Durée moyenne d'interruption

d'activité après une attaque

4 % CA

Sanction RGPD maximale

en cas de manquement avéré

Investir dans la remédiation aujourd'hui = éviter un coût 10× supérieur demain.

Le contexte réglementaire : NIS2

Qu'est-ce que NIS2 ?

Directive européenne entrée en application en France en 2024–2025.

Elle étend les obligations de cybersécurité à de très nombreux secteurs, dont l'industrie manufacturière.

ExCorp est très probablement concernée au titre des « entités importantes » ou « entités essentielles ».

Implications pour les dirigeants

Responsabilité **personnelle** des dirigeants en cas de manquement.

Obligation de notifier un incident sous 24 à 72 heures.

Audits de cybersécurité réguliers obligatoires.

Sanctions financières pouvant atteindre 2 % du chiffre d'affaires.

Cette slide est optionnelle et peut être retirée selon le contexte de la présentation.

Roadmap globale sur 12 mois

*Trois horizons temporels pour ramener le risque de **Critique** à **Faible**.*

COURT TERME
0 – 3 mois

Stopper l'hémorragie

- Mise à jour des systèmes exposés
- Isolation du réseau industriel
- Politique de mots de passe + LAPS
- Désactivation USB du lobby

MOYEN TERME
3 – 6 mois

Consolidation & durcissement

- Monitoring / SIEM
- Durcissement Active Directory
- Antivirus sur le réseau OT
- Sensibilisation des employés

LONG TERME
6 – 12 mois

Maturité & résilience

- Plan de Reprise d'Activité (PRA)
- Procédure de réponse à incident
- Architecture OT (modèle Purdue)
- Audits annuels & sécurité tiers

Plan d'action prioritaire — Court terme

0 – 3 MOIS

☐	Mettre à jour tous les systèmes exposés sur Internet	DSI
☐	Isoler le réseau industriel du réseau bureautique	DSI / OT
☐	Déployer une politique de mots de passe forte + LAPS	DSI
☐	Désactiver les ports USB sur les postes accessibles au public	DSI
☐	Implémenter le contrôle d'accès au réseau (NAC)	DSI
☐	Lancer une campagne de sensibilisation phishing immédiate	DSI / RH

Plan d'action — Moyen terme

3 – 6 MOIS

☐	Déploiement LAPS complet + modèle de tiering des administrateurs	DSI
☐	Mise en place d'un monitoring / SIEM (IT et OT)	DSI / CISO
☐	Durcissement des configurations RDP, MSSQL et Active Directory	DSI
☐	Audit et nettoyage des comptes administrateurs	DSI / CISO
☐	Déploiement d'antivirus sur le réseau OT	DSI / OT
☐	Formation cybersécurité (escape game, e-learning)	RH / CISO

Plan d'action — Long terme

6 – 12 MOIS

☐	Rédaction et test d'un Plan de Reprise d'Activité (PRA)	DG / CISO
☐	Rédaction d'une procédure de réponse à incidents	CISO
☐	Programme d'audits réguliers (pentest annuel)	CISO
☐	Activation DMARC et durcissement anti-spam	DSI
☐	Révision de l'architecture OT selon le modèle Purdue	DSI / OT
☐	Vérification des politiques de sécurité des prestataires	CISO / Achats

Estimation budgétaire indicative

Chantier	Horizon	Effort estimé	Priorité
Mise à jour des systèmes & isolation OT	0–3 mois	**20 – 40 k€**	**Critique**
Politique de mots de passe & LAPS, NAC	0–3 mois	**15 – 30 k€**	**Critique**
Monitoring / SIEM + durcissement AD	3–6 mois	**40 – 80 k€**	**Élevée**
Antivirus OT & sensibilisation employés	3–6 mois	**15 – 30 k€**	**Élevée**
PRA, procédure incidents & audits annuels	6–12 mois	**25 – 50 k€**	**Moyenne**
Architecture OT (Purdue) & sécurité tiers	6–12 mois	**30 – 60 k€**	**Moyenne**
TOTAL — fourchette indicative	**12 mois**	**145 – 290 k€**	—

Investir aujourd'hui pour éviter un coût 10× supérieur demain.

Ces estimations sont indicatives. Un chiffrage précis sera réalisé lors de la phase de remédiation.

Nos recommandations clés

Cinq messages que le COMEX doit retenir et porter en interne.

1. Le niveau de risque actuel est Critique : il appelle une **décision rapide**.
2. Isoler le réseau de production est la priorité absolue à 3 mois.
3. Le facteur humain est aussi critique que la technique : sensibiliser, tester, recommencer.
4. Sans plan de reprise d'activité, une cyberattaque met directement en péril ExCorp.
5. Investir maintenant coûte 10× moins qu'une attaque réussie.

Prochaines étapes

Actions concrètes attendues du COMEX et de la DSI sur les 60 prochains jours.

Délai	Action	Pilote
J + 15	Validation du plan de remédiation par le COMEX	**COMEX**
J + 30	Kick-off des chantiers d'urgence (mise à jour, isolation OT)	**DSI / CISO**
J + 30	Nomination d'un sponsor cybersécurité au COMEX	**DG**
J + 45	Lancement de la campagne de sensibilisation phishing	**DSI / RH**
J + 60	Premier point d'avancement & ajustement budgétaire	**COMEX / CISO**

H A C K M O S P H E R E

Votre sécurité nous tient hackeur.

https://www.hackmosphere.fr