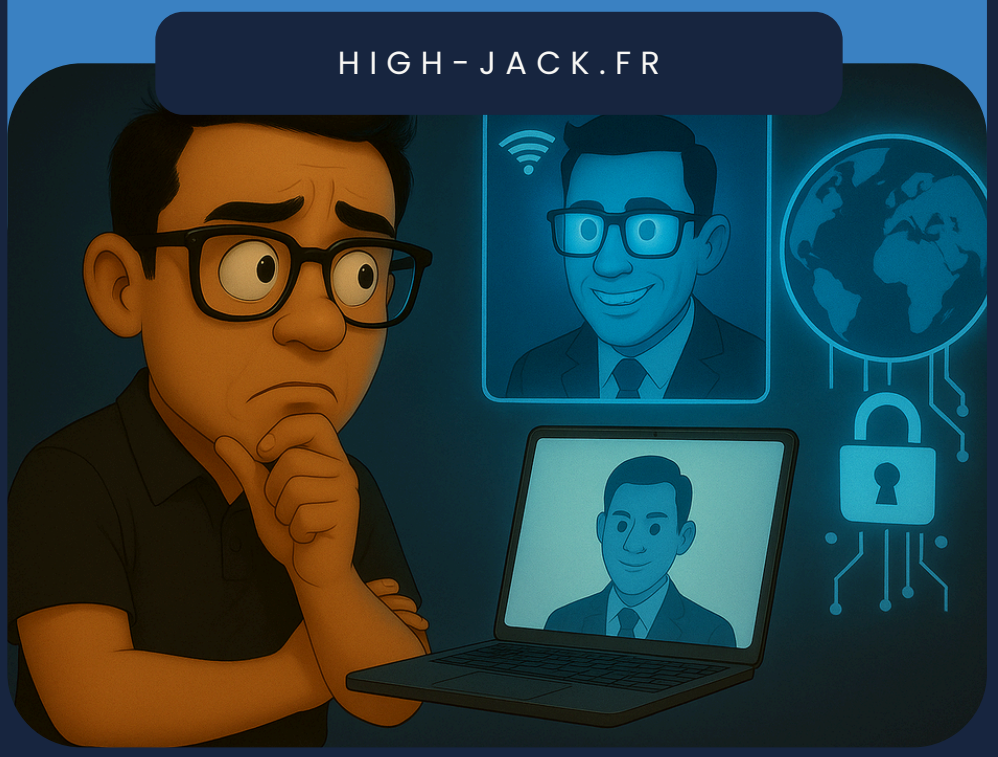
Téléchargez

notre guide offert !

CHECKLIST
CYBERSÉCURITÉ
2025

LES 10 POINTS CLÉS



HIGHJACK

Introduction

La cybersécurité n’est plus un sujet réservé aux équipes informatiques : elle concerne désormais directement les dirigeants, les DAF, les DSI et, plus largement, tous les métiers de l’entreprise.
Une attaque aujourd’hui ne touche pas seulement des machines : elle met en danger la réputation, les finances, la continuité d’activité et parfois même la confiance des clients et partenaires.

Cette checklist a été conçue pour donner une vision claire, humaine et accessible des **dix points critiques** sur lesquels chaque organisation doit se concentrer.
L’objectif n’est pas de créer de la peur, mais de permettre à chaque décideur de comprendre où se situent les **risques**, pourquoi ils existent, et quelles **actions simples** et réalistes peuvent être mises en place pour renforcer la **sécurité globale**.

Chez High Jack, nous défendons une approche pragmatique : **sécuriser les entreprises sans complexifier leur quotidien, en s’appuyant sur l’expérience terrain et un accompagnement pédagogique**.

1. Gestion des accès et identités (IAM)

Les comptes utilisateurs, les accès trop larges ou les mots de passe simples créent des portes d'entrée faciles pour les attaquants. Contrôler qui accède à quoi est la base de toute sécurité.

Enjeux :

- Réduire les risques d'intrusion.
- Protéger les données sensibles.
- Éviter qu'un compte oublié devienne la cause d'une attaque.

Objectifs :

- Imposer des mots de passe complexes.
- Activer la double authentification.
- Nettoyer les comptes tous les trimestres.

2. Sauvegardes chiffrées et testées

Une sauvegarde doit être isolée, protégée et testée régulièrement pour être réellement utile en cas d'incident.
Sans isolation, elle peut être chiffrée en même temps que le système lors d'une attaque. Sans test, elle peut s'avérer inutilisable au moment critique. Une bonne sauvegarde, c'est avant tout une capacité à redémarrer l'activité rapidement et sereinement.

Enjeux :

- Assurer la reprise rapide de l'activité.
- Protéger l'entreprise d'une perte totale des données.
- Éviter une paralysie longue et coûteuse.

Objectifs :

- Conserver une copie isolée.
- Tester deux fois par an.
- Chiffrer toutes les sauvegardes.

3. Mises à jour et correctifs

Les failles connues sont souvent les premières ciblées par les attaquants, car elles sont faciles à exploiter lorsque les systèmes ne sont pas à jour.
Réaliser les mises à jour permet de corriger ces vulnérabilités, de renforcer la stabilité des outils et de réduire considérablement les risques d'intrusion.

Enjeux :

- Empêcher les attaques opportunistes.
- Réduire la surface d'attaque.
- Maintenir un environnement sain.

Objectifs :

- Activer les mises à jour automatiques.
- Faire un audit semestriel.
- Remplacer les matériels obsolètes.

4. Sécurité des prestataires externes

Chaque prestataire qui dispose d'un accès à votre système représente un risque potentiel, même involontaire.
Un accès trop large, mal contrôlé ou laissé actif après la fin d'une mission peut devenir une porte d'entrée pour une attaque. Encadrer ces accès, c'est protéger l'entreprise sans freiner la collaboration.

Enjeux :

- Éviter une intrusion via un tiers.
- Protéger les zones sensibles.
- Maintenir un écosystème fiable.

Objectifs :

- Accorder des accès limités.
- Exiger des standards de sécurité.
- Supprimer les accès en fin de mission.

5. Segmentation du réseau

Un réseau non segmenté facilite la propagation d'une attaque, car une fois qu'un point d'entrée est compromis, l'attaquant peut se déplacer librement dans l'ensemble du système.
Segmenter le réseau permet de contenir l'incident, de protéger les zones sensibles et de limiter fortement l'impact potentiel sur l'entreprise.

Enjeux :

- Limiter les dégâts.
- Protéger les services critiques.
- Éviter la propagation interne.

Objectifs :

- Isoler les réseaux sensibles.
- Créer un réseau invité indépendant.
- Limiter les droits inutiles.

6. Sensibilisation des collaborateurs

Les erreurs humaines sont l'une des principales causes d'incidents, car un simple clic sur un lien malveillant ou un mot de passe trop simple peut suffire à compromettre l'entreprise.
Former et sensibiliser régulièrement les équipes permet de réduire drastiquement ces risques et de transformer chaque collaborateur en véritable acteur de la sécurité.

Enjeux :

- Réduire les risques liés au phishing.
- Développer une culture de vigilance.
- Impliquer l'ensemble des équipes.

Objectifs :

- Former une fois par an.
- Réaliser un test de phishing annuel.
- Diffuser un guide des bonnes pratiques.

7. Plan de réponse à incident

Improviser lors d’un incident augmente fortement les dégâts, car chaque minute perdue aggrave l’impact technique, organisationnel et financier.
Disposer d’un plan clair et testé permet de réagir vite, de limiter les interruptions d’activité et de garder la maîtrise de la situation, même sous pression.

Enjeux :

- Réduire les risques liés au phishing.
- Développer une culture de vigilance.
- Impliquer l’ensemble des équipes.

Objectifs :

- Réagir rapidement.
- Minimiser l’impact.
- Maintenir la confiance interne et externe.

8. Journalisation et monitoring

Sans surveillance, une attaque peut rester invisible pendant des jours ou des semaines, laissant le temps aux attaquants d'explorer le système, voler des données ou préparer un blocage complet.
Mettre en place un suivi régulier et des alertes permet de détecter rapidement les activités anormales et de réagir avant que la situation ne devienne critique.

Enjeux :

- Identifier les anomalies tôt.
- Réduire les attaques silencieuses.
- Faciliter les enquêtes.

Objectifs :

- Conserver 90 jours d'historique.
- Installer un outil de détection.
- Vérifier les alertes chaque semaine.

9. Sécurité des terminaux

Les postes de travail sont souvent la première cible, car ils concentrent les usages quotidiens : e-mails, navigation, mots de passe, documents sensibles.
Si un seul poste est compromis, l'attaque peut rapidement se propager à tout le système. Protéger chaque appareil, c'est protéger l'ensemble de l'entreprise.

Enjeux :

- Protéger les données.
- Empêcher les intrusions.
- Sécuriser la mobilité.

Objectifs :

- Chiffrer les appareils.
- Installer un EDR.
- Bloquer les appareils non conformes.

10 . Conformité (NIS2, DORA, ISO 27001)

Ces réglementations exigent une organisation structurée, car elles visent à garantir un niveau de sécurité suffisant face à l'augmentation des cybermenaces.
Elles obligent les entreprises à mieux documenter leurs pratiques, à renforcer leurs procédures et à prouver leur capacité à protéger les données et la continuité d'activité.

Enjeux :

- Répondre aux obligations légales.
- Renforcer la crédibilité.
- Mieux maîtriser les risques.

Objectifs :

- Documenter les processus.
- Réaliser un audit léger.
- Planifier une feuille de route de 12 à 24 mois.

Une démarche humaine, progressive et incarnée

Chez High Jack, l’approche humaine est portée par des profils expérimentés.

Cyrille ELSEN

Associé, DSI avec plus de 20 ans d’expérience dans la grande distribution et la gestion d’infrastructures critiques.

Alexis Mathieu

Administrateur réseaux et expert en cyber sécurité
Expert en analyse de risques, gestion de projets techniques et accompagnement opérationnel des PME et ETI.

CE QUE PROPOSE HIGH JACK :

Produits et Services :

- Accompagnement cybersécurité et gouvernance.
- Tests d’intrusion et audits techniques.
- Solutions de protection opérationnelle.
- Phishing
- DarkWeb

Formations courtes :

- Sensibilisation des salariés (Cybersécurité niveau 1 et 2)
- Référent Cybersécurité

Notre mission : protéger les organisations de façon simple, pragmatique et adaptée à leur réalité.

Notre vision :

SENSIBILISER - FORMER - AUDITER - ORGANISER - PROTÉGER

Téléchargez notre plaquette

Siège social : 74 rue du Docteur Lemoine, 51100 Reims
contact@high-jack.fr
03 10 45 40 01

HIGHJACK