Barracuda
Your journey, secured.

# Checklist de cyber-résilience

La checklist de cyber-résilience suivante s'appuie sur le cadre de cybersécurité de l'U.S. National Institute of Standards and Technologies (NIST).

| OBJECTIF | AXE STRATÉGIQUE POUR LES CHEFS D'ENTREPRISE – CE QUE VOUS DEVEZ SAVOIR | PROGRESSION |
|---|---|---|
| **PRÉPARATION** | **Organiser**<br>• Conformité réglementaire<br>Quelles sont vos obligations en matière de législation et de conformité dans chacun des marchés où vous opérez ?<br>• Implication et responsabilité de la direction<br>Qui, au sein de l'équipe de direction, doit être impliqué dans les décisions relatives à la cyber-résilience et aux risques ?<br>• La cyberassurance<br>De quel type d'assurance avez-vous besoin/dans quel type d'assurance êtes-vous prêt ou capable d'investir ? | ☐<br>☐<br>☐ |
| | **Identifier**<br>• Gestion des actifs<br>De quels actifs disposez-vous, où se trouvent-ils et qui y a accès ? Quels sont les éléments clés dont vous disposez pour assurer la continuité de vos activités et de vos opérations ?<br>• Gestion des risques et stratégie<br>Quels sont vos actifs les plus exposés ? Quels sont les risques auxquels ils sont confrontés ? Quel est l'impact potentiel d'une attaque en termes de dommages, de perturbations ou de pertes ? | ☐<br>☐ |
| **RÉSISTER** | **Protéger**<br>• Processus, politiques et technologies de sécurité<br>Comment protéger au mieux les biens, les infrastructures et les personnes dans la limite des ressources disponibles ?<br>• Formation de sensibilisation à la cybersécurité<br>Comment formez-vous et accompagnez-vous les employés ?<br>• Maintenance et contrôle : correctifs, etc.<br>Avez-vous mis en place les mesures de sécurité de base ? Application de correctifs, authentification robuste, contrôles d'accès (authentification multifactorielle/Zero Trust), etc. | ☐<br>☐<br>☐ |
| | **Détection**<br>• Technologies et procédés de détection<br>Vos systèmes de sécurité peuvent-ils détecter et bloquer les menaces nouvelles et émergentes ?<br>• Centre des opérations de sécurité<br>Votre surveillance de la sécurité est-elle fiable et continue ? Pouvez-vous superviser et gérer l'ensemble du parc informatique 24 heures sur 24, 7 jours sur 7 ? Disposez-vous des outils, des compétences et des effectifs nécessaires pour enquêter sur les signaux d'alerte et les anomalies ? | ☐<br>☐ |
| **AGIR** | **Atténuer**<br>• Planification et processus de réponse aux incidents<br>Disposez-vous d'un plan de réponse aux incidents couvrant l'ensemble de l'entreprise ? Est-il régulièrement testé et mis à jour ? Comment procédez-vous pour circonscrire et neutraliser les incidents ? Pendant combien de temps vos systèmes critiques peuvent-ils tenir en cas d'interruption ? Pouvez-vous revenir à des processus manuels si nécessaire ? Dans le cas où une interruption affecte vos clients, quel est le niveau de service contractuel ? Votre système est-il sur site ou dans le cloud ? (S'agit-il d'un service de sécurité (SaaS) fourni par une entreprise, d'un système d'entreprise, etc.) En termes de conformité réglementaire, qui devez-vous informer et quand ?<br>• Communications internes et externes<br>• Analyse et atténuation des incidents | ☐<br>☐<br>☐ |
| **RÉCUPÉRER** | **Restaurer**<br>• Planification de la reprise<br>Disposez-vous d'un plan de continuité des activités/un plan de reprise après sinistre ? Avez-vous mis en place une solution de « haute disponibilité » avec votre fournisseur de cloud ? Avez-vous besoin de l'assistance d'un tiers pour identifier et combler toutes les lacunes ?<br>• Communications internes et externes<br>• Améliorations<br>Quelles leçons avez-vous apprises ? Quelles mesures prenez-vous ou devez-vous prendre pour renforcer votre sécurité ? | ☐<br>☐<br>☐ |