RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en cybersécurité

LES ESSENTIELS d'un rapport de sécurisation

Dans le cadre d'une prestation de sécurisation d'un système d'information, le **rapport** remis au client constitue un **livrable essentiel**. Il matérialise la démarche engagée, les constats réalisés, les actions menées et les recommandations formulées pour renforcer la sécurité du système d'information.

Le présent document a pour objectif de préciser les attendus minimaux essentiels à tout **rapport de sécurisation** à remettre à l'issue de l'intervention, afin d'assurer une traçabilité claire des travaux effectués, une compréhension homogène des résultats par le client et une valorisation du professionnalisme du prestataire dans une logique de transparence et de confiance.

Les éléments listés ci-dessous seront notamment attendus dans le cadre d'une labellisation ExpertCyber.

01 INTRODUCTION

- **Objectifs du projet** : Résumé des objectifs de la sécurisation,
- **Contexte** de la sécurisation, raisons invoquées (politique de sécurité, réglementation, mise à niveau…),
- **Portée et limites** : détails sur les systèmes, réseaux et processus couverts.

02 SYNTHÈSE MANAGÉRIALE

Doit être compréhensible par des personnes non expertes en sécurité des systèmes d'information.

- **Contexte global** (objectifs, portée),
- **Résumé** des principaux risques identifiés et des mesures correctives mises en place,
- **Liste des recommandations** les plus importantes.

03 MÉTHODOLOGIE

Méthodes et démarches utilisées pour la sécurisation, parmi lesquelles :

- **Analyse des risques** (actifs critiques, menaces et vulnérabilités, risques),
- **Diagnostic** (matériels, configurations, accès…),
- **Tests de pénétration** (en boite noire, grise, blanche),
- **Outils et logiciels utilisés par le prestataire,**
- **Référentiels appliqués,**
- **Etc.**

04 ÉVALUATION DU NIVEAU DE SÉCURITÉ ACTUEL DU CLIENT

- **Mesures de sécurité en place** (physiques, réseaux, systèmes, applications, données, utilisateurs),
- **Résultats des tests et audits antérieurs**,
- **Résultats de l'analyse des risques.**

05 DÉROULÉ DE L'INTERVENTION

- **Périmètre et chronologie.**
- **Mesures correctives mises en place pour la sécurité,** par exemple :
  - des **réseaux** (pare-feu, VPN, segmentation du réseau…),
  - des **systèmes** (mises à jour, configurations, anti-virus…),
  - des **données** (sauvegardes, chiffrement, gestion des accès…),
  - des **applications** (sécurité des logiciels, gestion des correctifs…),
  - de la j**ournalisation,**
  - des **utilisateurs** (formation, sensibilisation, politiques de mot de passe…),
  - des **tests, audits effectués après sécurisation,**
  - **physique** (accès aux locaux, protection des équipements…),
- **Vulnérabilités restantes après sécurisation,**
- **Etc.**

06 RECETTE POST SÉCURISATION

- **Restitution des tests effectués** (méthodologie et résultats).

07 SYNTHÈSE GLOBALE

- **Recommandations avec priorisation** (physiques, réseaux, systèmes, données, applications, utilisateurs),
- **Plan d'actions** (actions à gains rapides, calendrier, responsable, budget…).

08 CONCLUSIONS

- **Liste des risques résiduels après la sécurisation,**
- **Liste des recommandations les plus importantes,** en insistant sur l'importance de la maintenance continue et des audits réguliers pour assurer une sécurité optimale.