Que doit contenir un rapport de sécurisation du système informatique ?

Cybermalveillance.gouv.fr a réalisé des fiches de référence dont l'objectif est de clarifier les attendus minimaux dans le cadre d'une intervention en cybersécurité par un prestataire, notamment dans une démarche de labellisation ExpertCyber. Ces fiches ont été rédigées par le comité de labellisation, en collaboration avec l'ANSSI, Coter Numérique, Fédération EBEN et Numeum. Elles s'adressent à tous les prestataires informatiques, mais peuvent aussi intéresser les entreprises qui ont ou vont faire appel à un prestataire.

L'importance d'une maintenance continue

La fiche sur les essentiels d'un rapport de sécurisation indique, par exemple, que le résumé des objectifs de la sécurisation et son contexte (politique de sécurité, réglementation, mise à niveau…) doivent être rappelés en introduction du rapport. La synthèse doit être compréhensible par des personnes non expertes en sécurité des systèmes d'information. Les méthodes et démarches utilisées doivent être détaillées, de même que le niveau de sécurité actuel du client et le déroulé de l'intervention. La conclusion doit lister les risques résiduels après la sécurisation et les

recommandations les plus importantes, en insistant sur l’importance de la maintenance continue et des audits réguliers pour assurer une sécurité optimale.

Pour en savoir plus : www.cybermalveillance.gouv.fr