Politique de sécurité des systèmes d'information, comment maintenir un certain niveau de sécurité ?

Qu’est-ce qu’une Politique de sécurité des systèmes d'information ?

« La PSSI reflète la vision stratégique de la direction d’une structure en matière de sécurité des systèmes d’information », selon l'**ANSSI**.

La PSSI est un véritable instrument de sensibilisation interne et externe. Les acteurs prennent conscience de leurs responsabilités au niveau sécurité.

PSSI : une approche globale avant tout

INFORSUD Technologies privilégie la méthode EBIOS Risk Manager, méthode recommandée par l'ANSSI. Elle permet aux organisations de réaliser une appréciation et un traitement des risques.

Cette approche méthodologique est organisée autour de différents thèmes prédéfinis :

- La sécurité liée à l’organisation,
- La sécurité physique et environnementale,
- La gestion des ressources humaines et des actifs,
- Les contrôles des accès logiques,
- La sécurité liée à l’exploitation,
- La sécurité des communications,
- Les relations avec les partenaires,
- La gestion des incidents de sécurité,
- La continuité de service.

Chaque collaborateur est soumis à un questionnaire pour évaluer ses connaissances en sécurité.

Le rapport de l’audit intègre les livrables suivants :

- Analyses des écarts par rapport à des précédents audits,
- Plan d’actions à mettre en place pour atteindre le niveau de sécurité fixé,
- Présentation et fichier de suivi avec les recommandations.

Comment réussir sa PSSI ?

L’approche PSSI a pour objectif d'évaluer le risque et proposer des mécanismes permettant de le réduire ou de l’accepter.

L’implication des postes clés est un impératif pour obtenir un résultat et insuffler un état d’esprit à tous les utilisateurs du système d’information.

Exemple

Un des exemples les plus concrets que peut intégrer une PSSI, reste la capacité à redémarrer une activité en cas de sinistre sur une plateforme informatique. Savoir limiter la quantité de données perdues grâce à une politique de sauvegarde permet de reprendre une activité plus rapidement. Il ne reste dans ce cas-là qu’à restituer les sauvegardes et ignorer la demande de rançon, en cas d’attaque de type Ransomware, autorisant l’accès aux données non-chiffrées.

Le conseil d’Inforsud Technologies

La stratégie de sécurité offre à l’organisation une démarche claire et cohérente à suivre par tous les acteurs.

Nos prestations visent à sécuriser votre Système d’Information, détecter les failles de sécurité, évaluer les risques et neutraliser préventivement les menaces.

Vous anticipez ainsi les comportements et usages à risque.

Pour plus d'informations, retrouvez-nous sur :
inforsud-technologies.com

INFORSUD TECHNOLOGIES
Solutions et impulsions pour l’avenir