impression I informatique I télécom I dématérialisation

premium

Plus d'une corde à son arc

CONSEIL 3 : SENSIBILISER VOTRE PERSONNEL

La cybersécurité ne repose pas uniquement sur des outils techniques : le facteur humain demeure le maillon le plus vulnérable. Un collaborateur mal informé peut, sans le savoir, compromettre l'ensemble du système d'information de l'entreprise.

Nous vous encourageons fortement à la sensibilisation et à la documentation de vos personnels sur les sujets des risques informatiques et de la protection des données. Cette politique de sensibilisation peut revêtir différentes formes de communication interne, notamment par le biais de newsletters dans les boîtes mail professionnelles, de notices d'information affichées dans l'entreprise, ou encore de sessions de formation dispensées dans ou hors de l'entreprise. De plus, votre charte informatique doit être un vecteur de sensibilisation (et de contrainte), en ce qu'elle recense les droits et devoirs de vos salariés en matière de sécurité informatique.

Il est donc essentiel de mettre en place une politique de sensibilisation régulière et adaptée à tous les niveaux de l'organisation. **Cette démarche peut inclure :**

1) Des **formations courtes et ciblées** (phishing, gestion des mots de passe, usage des réseaux publics, etc.)

2) Des **simulations d'attaques** pour tester les réflexes de sécurité

3) La diffusion de supports pédagogiques simples et accessibles

4) L'instauration de **référents cybersécurité** internes

En cultivant une culture de la vigilance, l'entreprise réduit significativement les risques liés aux erreurs humaines et renforce la résilience de ses systèmes face aux menaces numériques.