FICHE THEMATIQUE N°31

Numérique et Cybersécurité

Prise en compte du risque cyber et mesures de sécurité en place

Analyse des Risques

L'**identification des risques** est une première étape essentielle pour intégrer la cybersécurité dans l'analyse des risques de l'entreprise. Cela implique de repérer les menaces spécifiques qui peuvent affecter les activités critiques, telles que les **rançongiciels**, les **attaques de phishing** et les **vols de données**. Identifier ces menaces permet de cibler les points vulnérables et d'anticiper les actions de protection nécessaires.

L'**évaluation des risques** suit cette identification, en analysant la **probabilité** de survenue et l'**impact potentiel** de chaque menace. Cette évaluation aide à hiérarchiser les actions de sécurité en fonction des risques les plus pressants, garantissant ainsi une allocation optimale des ressources de protection et une meilleure résilience face aux cybermenaces.

Mise en Place des Mesures de Sécurité

La définition d'une **politique de continuité** prenant en compte les cyberrisques permet de garantir la capacité de l'entreprise à réagir efficacement et à se rétablir après un incident de cybersécurité. Cette politique vise à minimiser les interruptions d'activité, à protéger les données critiques et à maintenir les opérations essentielles en cas d'attaque.

Les **mesures préventives** sont un pilier central de cette politique. Cela inclut l'implémentation d'outils de sécurité comme des **pare-feu**, des **systèmes de détection d'intrusion**, des **antivirus**, ainsi que l'application régulière de **mises à jour de sécurité** pour protéger les systèmes contre les nouvelles menaces.

Les **contrôles d'accès** contribuent également à réduire les risques en restreignant l'accès aux systèmes critiques au seul personnel autorisé. L'utilisation de **mots de passe forts** et de l'**authentification multi-facteurs (MFA)** assure une protection accrue contre les accès non autorisés.

Enfin, des **sauvegardes régulières et vérifiées** des données critiques sont essentielles pour garantir que les informations vitales puissent être restaurées rapidement en cas de cyberincident. Assurer la fiabilité des sauvegardes est un gage de résilience, offrant une base solide pour la continuité des opérations dans un environnement numérique sécurisé.

Plan de Continuité et de Récupération

L'établissement d'un **Plan de Continuité d'Activité (PCA)** dédié aux cyberincidents est essentiel pour garantir que l'entreprise puisse réagir rapidement et maintenir ses opérations critiques en cas de cyberattaque. Ce PCA doit inclure des **stratégies de communication** pour informer les parties prenantes (employés, clients, partenaires) de manière transparente et coordonnée, tout en préservant la réputation de l'entreprise. En parallèle, des **procédures de restauration** doivent être définies pour permettre un retour rapide aux opérations normales après la neutralisation de la menace.

Le développement d'un **Plan de Reprise après Sinistre (DRP)** vient renforcer cette résilience en assurant une récupération rapide des systèmes et des données après un incident majeur. Ce DRP prévoit des actions spécifiques pour restaurer les infrastructures informatiques, les applications et les bases de données, en minimisant les pertes de données et les interruptions d'activité. Ensemble, le PCA et le DRP constituent une approche intégrée pour garantir la continuité des opérations et la protection des actifs essentiels de l'entreprise en cas de cyber incidents.