Sécurité du Cloud

Accroissement des cybermenaces à l'ère du Cloud

L'avènement du Cloud a révolutionné la manière dont les entreprises gèrent leurs données et leurs activités métiers. Cependant, cette transition a également introduit des risques de sécurité. Par conséquent, bien que le Cloud offre des avantages, il est impératif de tenir compte des risques qu'il introduit et d'appliquer les mesures nécessaires pour assurer une protection efficace des données.

Principaux risques de sécurité introduits par le Cloud

- **Accès non autorisé :** Les services Cloud peuvent être vulnérables à des accès non autorisés en raison de lacunes dans la gestion des identités, l'utilisation de mots de passe faibles, et des attaques de phishing, etc.
- **Fuite de données :** Les données stockées dans le cloud peuvent être exposées en raison de failles de sécurité, de configurations incorrectes ou de mauvaises pratiques de gestion des données, entraînant ainsi des fuites d'informations sensibles.
- **Manque de visibilité et de contrôle :** La migration vers le cloud peut entraîner un manque de visibilité et de contrôle sur les données et les systèmes, rendant difficiles la détection et la réponse aux menaces.
- **Interruption de service :** Les interruptions de service dans le cloud peuvent perturber les opérations métiers en raison d'attaques DDoS, de pannes de réseau, ou de défaillances de serveur.
- **Dépendance à un tiers et conformité réglementaire :** L'utilisation du cloud crée une dépendance à des tiers pour la sécurité des données et soulève des préoccupations de conformité réglementaire et de souveraineté.

Mesures d'atténuation des risques liés au Cloud

Pour atténuer les risques liés à l'adoption du Cloud, il est impératif de mettre en œuvre certaines pratiques clés :

- **Gestion des identités et des accès :** Implémenter une authentification multifacteur (MFA) pour les comptes sensibles, limiter l'accès aux données en assignant des permissions strictement nécessaires, et réaliser des examens réguliers des comptes et des autorisations.
- **Chiffrement des données :** Utiliser le chiffrement pour sécuriser les données sensibles tant au repos qu'en transit.
- **Surveillance et contrôle :** Utiliser des outils de surveillance et de gestion des performances pour maintenir une visibilité sur l'activité des systèmes et des données et adopter des solutions de gestion de configurations pour assurer le contrôle et la conformité des paramètres de sécurité.
- **Haute disponibilité et résilience :** Utiliser des services cloud distribués sur plusieurs régions géographiques pour réduire l'impact des pannes régionales ou des catastrophes naturelles.
- **Contractualisation sécurisée :** Faire appel à un fournisseur qualifié SecNumCloud et certifié HDS, et s'assurer de la clarté et du respect des exigences de sécurité énoncées dans les contrats.

Ressources pertinentes mises à disposition

- Des recommandations de la **CNIL** concernant la sécurité des données dans le Cloud [PDF]
- Des bonnes pratiques dans le cadre de la sécurité du Cloud, diffusé sur la plateforme **France Num** [Site web]
- Un inventaire des fournisseurs Cloud, qualifiés SecNumCloud sur le site de l'**ANSSI** [Site web]