NumSpot
Cloud. Européen. Citoyen.

Le partenaire cloud souverain et de confiance des secteurs stratégiques et sensibles

Garantir les plus hauts standards de sécurité pour assurer la protection de leurs données et celles des citoyens.

Sécurité et confidentialité dans le cloud souverain : Pratiques essentielles

Résumé

- Choisissez un fournisseur de cloud souverain fiable, respectant les réglementations et normes de sécurité en vigueur.
- Formez les personnels aux bonnes pratiques de sécurité et de protection des données.
- Mettez en place des mécanismes de contrôle d'accès stricts.

La gestion de la donnée est primordiale dans la stratégie de toutes les entreprises, notamment pour les **données à caractère personnel**, pour lesquelles il est indispensable d'être en accord avec le **Règlement Général de Protection des Données** (RGPD).
En ceci, **le choix d'un cloud souverain** peut s'avérer particulièrement judicieux.

Qu'est-ce qu'un cloud souverain ?

Un **cloud souverain** est un service d'hébergement et de traitement des données proposé par une **entreprise de droit français**. Cette entreprise doit être **présente physiquement sur le territoire français** et appliquer les **lois et normes françaises** relatives aux traitements des données. Le cloud souverain permet de garantir que les données stockées ne sont pas sous le coup de **lois extraterritoriales** et que le prestataire respecte le **Règlement Général de Protection des Données** (RGPD).

10 règles essentielles

La sécurité et la protection des données dans le cloud souverain sont d'une importance capitale pour garantir la confidentialité, l'intégrité et disponibilité des informations sensibles.
Voici donc les meilleures pratiques à suivre :

1 Choisir un fournisseur de cloud souverain fiable

Optez pour un fournisseur qui a une réputation solide en matière de sécurité et de protection des données et qui respecte les réglementations et les normes de sécurité en vigueur dans votre pays.

2 Chiffrer vos données sensibles

Avant de les stocker dans le cloud souverain, chiffrez toutes les données sensibles à l'aide de techniques de chiffrement robustes. Ainsi, même compromises, vos données restent illisibles sans la clé de chiffrement appropriée.

3 Contrôler l'accès aux données

Mettez en place des mécanismes de contrôle d'accès stricts pour vos données dans le cloud souverain, avec des mesures d'authentification forte, telles que des mots de passe complexes, des jetons d'accès ou des certificats numériques, pour limiter l'accès aux seules personnes autorisées.

4 Effectuer des sauvegardes régulières

Assurez-vous de sauvegarder régulièrement vos données dans le cloud souverain : en cas de défaillance technique ou de perte de données, vous pourrez restaurer les informations à partir des sauvegardes.

5 Surveiller et auditer les activités

Utilisez des outils de surveillance et de journalisation pour suivre les activités dans le cloud souverain : cela vous permettra de détecter rapidement toute activité suspecte ou toute violation de sécurité.

6 Mettre à jour régulièrement vos systèmes

Assurez-vous que les systèmes et les logiciels utilisés dans le cloud souverain sont régulièrement mis à jour avec les derniers correctifs de sécurité pour combler les failles de sécurité connues et réduire les risques d'exploitation.

7 Sensibiliser votre personnel

Formez votre personnel aux bonnes pratiques de sécurité et de protection des données. Ils doivent comprendre les risques associés au cloud souverain et savoir comment prendre des mesures appropriées pour les atténuer.

8 Effectuer des évaluations de sécurité régulières

Réalisez des audits de sécurité réguliers pour évaluer l'efficacité des mesures de sécurité mises en place dans le cloud souverain : ceci vous permettra d'identifier les éventuelles vulnérabilités et de prendre des mesures correctives.

9 Respecter les réglementations en matière de protection des données

Assurez-vous de respecter toutes les réglementations en vigueur, comme le **Règlement général sur la protection des données** (RGPD) en Europe. Veillez à ce que vos pratiques de sécurité dans le cloud souverain soient conformes aux exigences légales.

10 Planifiez une stratégie de gestion des incidents

Élaborez un plan d'intervention en cas d'incident de sécurité dans le cloud souverain, qui vous aidera à réagir rapidement et efficacement en cas de violation de sécurité ou de perte de données.

À vous de choisir

En suivant ces meilleures pratiques, vous pouvez renforcer la sécurité et la protection des données dans le cloud souverain, et ainsi réduire les risques de compromission ou de perte d'informations sensibles.

À propos de NumSpot

NumSpot est un acteur du cloud souverain et de confiance. Né de la volonté de 4 entreprises françaises de premier plan des secteurs public et privé (Banque des Territoires, Docaposte, Dassault Systèmes et Bouygues Télécom), NumSpot propose une offre de cloud indépendant, souverain et robuste adossé au IaaS d'OUTSCALE qualifié SecNumCloud. NumSpot est un cloud réversible et transparent, basé principalement sur l'open source et des solutions européennes. L'offre NumSpot s'adresse prioritairement aux secteurs confrontés à une forte sensibilité des données (secteur public, santé, services financiers et assurance, OIV et OSE) en France et en Europe, et à la recherche d'une solution souveraine et de confiance en accord avec les règlementations RGPD et européennes. NumSpot fait ainsi le choix d'œuvrer pour l'intérêt général en proposant un véritable pacte de confiance entre un fournisseur de cloud, ses clients et les citoyens européens.

Suivez-nous @NumSpot @NumSpotCloud