MINISTÈRE DE L'INTÉRIEUR
Liberté
Égalité
Fraternité

LA LETTRE CYBER en Région Grand Est

Gendarmerie nationale

GENDARMERIE

NOTRE ENGAGEMENT, VOTRE SÉCURITÉ

N°05/2025

LA THEMATIQUE DU MOIS:
Les Services Cloud, pourquoi et comment choisir ?

INTRODUCTION

Le cloud est devenu au fil des années un élément indispensable pour étendre nos capacités de stockage, que ce soit à titre professionnel ou encore personnel. Il s'est également imposé comme un service incontournable pour les entreprises pour y stocker des applications permettant de fournir des services en ligne à leurs utilisateurs, partenaires ou clients.
S'il s'agit d'une avancée importante, il convient de s'assurer tout de même de la sécurité des données que nous confions à ces clouds. Nous allons voir qu'il existe plusieurs types de clouds en fonction de nos besoins. Nous allons également vous donner quelques axes de réflexion pour vous aider à choisir.

LES TYPES DE CLOUD

IAAS = location d'une infrastructure existante (serveurs, stockage, réseau, machines virtuelles). La gestion est totalement à la charge du client. Responsabilité **++**
Il en existe deux types : privé ou public. En **privé** l'infrastructure est dédiée au client. En **public**, l'infrastructure est mutualisée avec d'autres. (Microsoft Azure, Google Compute Engine)

PAAS = location d'une plateforme complète pour développer et déployer des applications. Ici la gestion de l'infrastructure (système - serveurs) n'est plus à la charge du client mais à celle du fournisseur cloud. (Google App Engine, Heroku, Microsoft Azure App services...)

SAAS = Utilisation directe d'une application en ligne prête à l'emploi. Ici le client n'est responsable que des données qu'il met en ligne. (Gmail, Google Drive, Microsoft 365, Dropbox...)

LES TYPES DE DONNEES

- Les données de **référence** : Données utiles au fonctionnement de l'entreprise : clients, employés, produits, fournisseurs, etc...
- Les données **personnelles** : Données d'informations, d'identités etc. soumises au RGPD (Règlement Général sur la Protection des données)
- Les données **confidentielles** : Données relatives au savoir faire, à la propriété intellectuelle, aux secrets de fabrication etc...

Selon la sensibilité de la donnée, les moyens (financiers ou humains), la confiance accordée au prestataire cloud peuvent varier...**et donc comment choisir son cloud ? Et pour quel usage ?**

Comment (bien) choisir son service cloud ?

Il n'est pas possible de donner une réponse générique à cette question : cela dépend de vos besoins, de vos moyens, de vos attentes, de la sensibilité de vos actions et de vos données etc... Mais nous pouvons cependant vous communiquer quelques points sur lesquels être attentif au cours de votre réflexion.

- Il faut d'abord bien intégrer que votre responsabilité est totale à l'égard de ce que vous mettez dans le cloud, indépendamment de ce qui est y déjà mis à disposition par le service support.
- fiabilité du service: lors de la signature du contrat, faites attention à ce qui vous est proposé comme les capacités d'innovation, d'accompagnement en cas de sinistre, de réaction en cas d'incidents ou encore les modalités de mises à jour, etc..
- pour vous aider, l'ANSSI publie le référentiel **SecNumCloud**, référentiel d'exigence applicables aux prestataires de service cloud. https://cyber.gouv.fr/actualites/lanssi-actualise-le-referentiel-secnumcloud
- **attention au lieu de stockage des données**. Si celui-ci se trouve en Europe, elles sont protégées et encadrées par le RGPD. En revanche, si celui-ci se trouve aux États-Unis ou une entité dépendante de ceux-ci, vos données sont soumises au Patriot Act (qui autorise les autorités américaines à accéder à vos informations dans le cadre d'investigations) et au Cloud Act (qui permet aux fournisseurs d'exploiter librement vos données).

Comment se protéger sur un cloud?

La protection sur le cloud ne diffère pas beaucoup, voire pas du tout, de l'hygiène à adopter sur un appareil physique.

- Il est tout d'abord primordial de choisir un **mot de passe robuste et de le changer régulièrement.**
- Privilégier au minimum **une double authentification**, c'est-à-dire un mot de passe associé à une deuxième preuve de votre identité numérique (code généré par une application d'authentification, code envoyé par SMS, ou encore authentification biométrique enregistrée sur votre téléphone).
- Enfin, un cloud ne vous garantira jamais la conservation de vos données, il y a toujours des risques. **Il faut donc avoir une sauvegarde en ligne ou physique** et pour les entreprises, **établir un PRA (Plan de Reprise d'Activité)** dans tous les cas.

CONCLUSION

Les services cloud doivent être choisis en fonction de vos besoins et de vos moyens, en toute connaissance de cause. Il faut savoir avant la signature du contrat ce que deviennent vos données et qui y a accès. Il faudra aussi anticiper une défaillance du système, qui est toujours possible.
En définitive, il ne faut jamais se reposer aveuglément sur un prestataire de services cloud. Vous devez pouvoir contrôler son activité afin de rester maître de vos données.

+ D'INFOS

ANJ AUTORITÉ NATIONALE DES JEUX

Grand Est Cybersécurité — CENTRE D'ASSISTANCE DE PROXIMITÉ — 0 970 512 525

CYBER MALVEILLANCE .GOUV.FR

PHAROS — PLATEFORME D'HARMONISATION, D'ANALYSE, DE RECOUPEMENT ET D'ORIENTATION DES SIGNALEMENTS

e-Enfance 3018

CNIL. PROTÉGER les données personnelles ACCOMPAGNER l'innovation PRÉSERVER les libertés individuelles

ANSSI Agence nationale de la sécurité des systèmes d'information

Région de gendarmerie du Grand Est
LA LETTRE CYBER en région Grand Est

Directeur de la publication: GCA F.GUILLAUME
Responsable éditorial: COL L. GRAU
Rédacteur: ADJ M.KNOBLOCH

Si vous souhaitez recevoir cette lettre, envoyez un mail à :
Laurent.grau@gendarmerie.interieur.gouv.fr
Mathieu.knobloch@gendarmerie.interieur.gouv.fr

Suivez l'actualité de la gendarmerie: