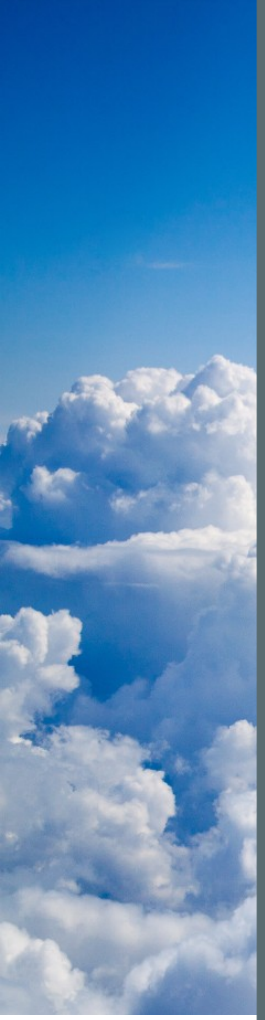


THIERRY MEYER
SÉCURITÉ INFORMATIQUE

Cours

La sécurité du cloud computing

V 1.0 – 02/2021 - https://www.tm-consultants.fr

Introduction

LA SÉCURITÉ DU CLOUD COMPUTING
Introduction

> Cloud computing (infrastructure dans les nuages, ou infonuagique) évolution majeure de l'informatique aujourd'hui :

- presque naturelle, et qu'il aurait été possible d'anticiper compte tenu des avancées des nouvelles technos et notamment :
  - Omniprésence d'internet.
  - Naissance de la virtualisation.
  - Conteneurisation
  - …

> A ce sujet avis sont mitigés :

- partisans mettent en avant les nombreux avantages (on verra plus loin)
  - mutualisation des ressources
  - réduction des coûts (quoique),
  - …
- détracteurs dont l'argument principal est centré autour des dangers pour la vie privée.

> Quoiqu'il en soit le cloud semble dessiner le futur de l'informatique.

- Usage de plus en plus courant de services en « mode cloud ».
- Mot à la mode.
- Constitution de groupes de travail et consortiums :
  - *http://www.cloud-council.org/ pour aider les clients,*
  - *http://www.cloudsecurityalliance.org* pour travailler sur les questions de sécurité,
  - …

> Mais chaque nouvelle avancée technologique présente des incertitudes, pour le cloud nombreuses :

- Quid du niveau réel de sécurité ?
- Conformité réglementaire (échanges au-delà des frontières géographiques, données personnelles)
- Quels responsabilités pour le prestataire ?
  → secnumcloud
- …
- bref de quoi faire

Les concepts du cloud computing

> Définitions, bénéfices et points d'attention :

- Définition donnée par le NIST : http://www.nist.gov/itl/cloud/ :

  Le Cloud computing est un modèle qui permet de façon simple et pratique de fournir à la demande un accès via le réseau à un pool de ressources informatiques partagées et paramétrables qui peuvent être rapidement provisionnées et réalisées avec un minimum d'effort de gestion ou d'interaction avec le fournisseur.

LA SÉCURITÉ DU CLOUD COMPUTING
Les concepts du cloud computing

> Comparaison avec / sans cloud :

- Avantages pour le client :
  - Simplification de la gestion informatique :
    - accès aux nouvelles ressources se fait de façon simple
      → interface web de gestion …
    - le client se concentre sur son coeur de métier
  - Avantages économiques pour le client :
    - Permet de modifier le rapport OPEX (Operating expenditure, dépense d'exploitation) / CAPEX (Capital expenditure, dépenses d'investissement)
      → cf article MISC n°80 p68
    - Permet de lisser les investissements tout au long de la croissance du projet
    - Permet de limiter les mauvais choix (plus simple de résilier un contrat que de se débarrasser d'un investissement.
  - Flexibilité :
    - permet de faire varier rapidement et simplement les ressources utilisées (absorption de pics de charge temporaire)
      → meilleure agilité business, simplifie la gestion de la croissance économique

> Comparaison avec / sans cloud :

- Avantages pour le fournisseur :
  - Optimisation des ressources :
    - Mutualisation possible entre plusieurs clients.
    - Lissage de ressources possible dans des zones géographiques.
  - Permet un suivi plus fin de la consommation des ressources par le client :

    → n'allouer que ce qui est nécessaire pour fournir à d'autres ce qui n'est pas utilisé.

> Comparaison avec / sans cloud :

- Avantages en matière de sécurité :
  - Net apport pour le S.I. en matière de :
    - Résilience,
    - Résistance.
  - Voir interview de Hervé Schauer dans un des talk show du Haut Comité Français pour la Défense Civile (HCFDC) au cours du salon Milipol 2015 concernant le cloud : (https://www.youtube.com/watch?v=KKMbZWcl_s4)

Les modèles de déploiement du cloud computing

LA SÉCURITÉ DU CLOUD COMPUTING

Les modèles de déploiement du cloud computing

> Déploiement d'un cloud possible de différentes façons :

- Cloud public.
- Cloud communautaire.
- Cloud privé/cloud privé outsourcé.

> Cloud public :

- L'infra cloud est provisionnée et ouverte au publique. Le service est standard est fourni par internet (ex : Googledrive)
- L'infrastructure peut appartenir et/ou être gérée par :
  - une société privée,
  - une administration,
  - ou une organisation gouvernementale (ou une combinaison de tout ça).

> Cloud communautaire :

- L'infrastructure est mise à disposition d'une ou plusieurs organisations et uniquement à ses membres
  (cas de joint-venture : filiale commune à plusieurs entité et à durée de vie limitée. Pour les besoins d'un business à l'étranger par exemple)
- Partagent les mêmes métiers ou objectifs.
- l'infrastructure appartient et est gérée par :
  - une ou plusieurs des organisations membres,
  - ou un tiers (fournisseur),
  - ou la combinaison de tout ça.

> Cloud privé/cloud privé outsourcé

- L'infrastructure est provisionnée et mise à disposition d'une seule organisation (qui peut comprendre plusieurs entités utilisatrices (filiales, ...)
- L'infra appartient et est gérée par :
  - l'organisation en question,
  - ou un tiers de confiance,
  - ou une combinaison de tout ça.
- Elle est fournie par un réseau privé.

> Cloud hybride :

- Modèle qui regroupe au moins deux autres types de modèles, au sein d'un seul même mode de déploiement.
- Concept de « Cloudbursting » (un premier problème de sécurité.)
  - Voir http://blog.trendmicro.com/what-is-cloudbursting/
  - Signifie que l'on atteint les capacités limites de notre cloud et que l'on éclate (burst) le cloud vers un autre cloud pour bénéficier de ses ressources (load balancing)
  - Le cas typique de cloud hybride, est le cas d'un cloud privé couplé à un cloud publique vers lequel le client pourra « déborder » (burst) si ses ressources privées sont toutes épuisées.

> Intérêts de chacun des modèles :

Public	Communautaire	Privé/outsourcé
Paiement à l'usage (OPEX : Operating expenditure, dépense d'exploitation)	Amélioration de la collaboration entre partenaires	Optimisation des ressources
Time to market (temps qu'il faut à un produit de sa conception jusqu'à la fin de sa réalisation)	Partage et optimisation des coûts	Qualité de service
Simplicité		Facturation interne
Flexibilité		

> Un cloud à part, le Cloud gouvernemental ou Cloud souverain

- Nécessité pour un état de disposer d'un cloud dont il est à l'origine :
  - Pas de réelle définition sur la notion de Cloud gouvernemental mais l'ENISA note cependant les caractéristiques suivantes : *https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cloud-computing/governmental-cloud-security/good-practice-guide-for-securely-deploying-governmental-clouds*
  - un cloud qui fournit des services en accord avec la législation du Pays et de l'EU sur les thèmes de la sécurité, la confidentialité et la résilience.
  - un moyen sécurisé et de confiance sur lequel on peut fournir des services sous l'identité du gouvernement.
  - un modèle de déploiement pour construire et fournir des services aux agences d'état, au citoyens et aux entreprises.

Les modèles de services

LA SÉCURITÉ DU CLOUD COMPUTING

Les modèles de service du cloud computing

> Plusieurs modèles de services :

- SaaS : Software As a Service.
- PaaS : Plateform As a Service.
- IaaS : Infrastructure As a Service.
- FaaS : Function As a Service.

  … mais aussi XaaS (Anything as a Service)

- Botnet as a Service.
- Security as a Service.
- …

> SaaS : Software As a Service.

- Utilisation par le client d'applications « web » mises à disposition par le fournisseur (RH, achats, messagerie, …).
- l'application fonctionne sur une infrastructure cloud du fournisseur.
- L'utilisateur du service ne gère pas les fonctionnalités sous-jacentes à l'application, il ne fait que l'utiliser (ex : gmail, googledrive, …).

> PaaS : Plateform As a Service.

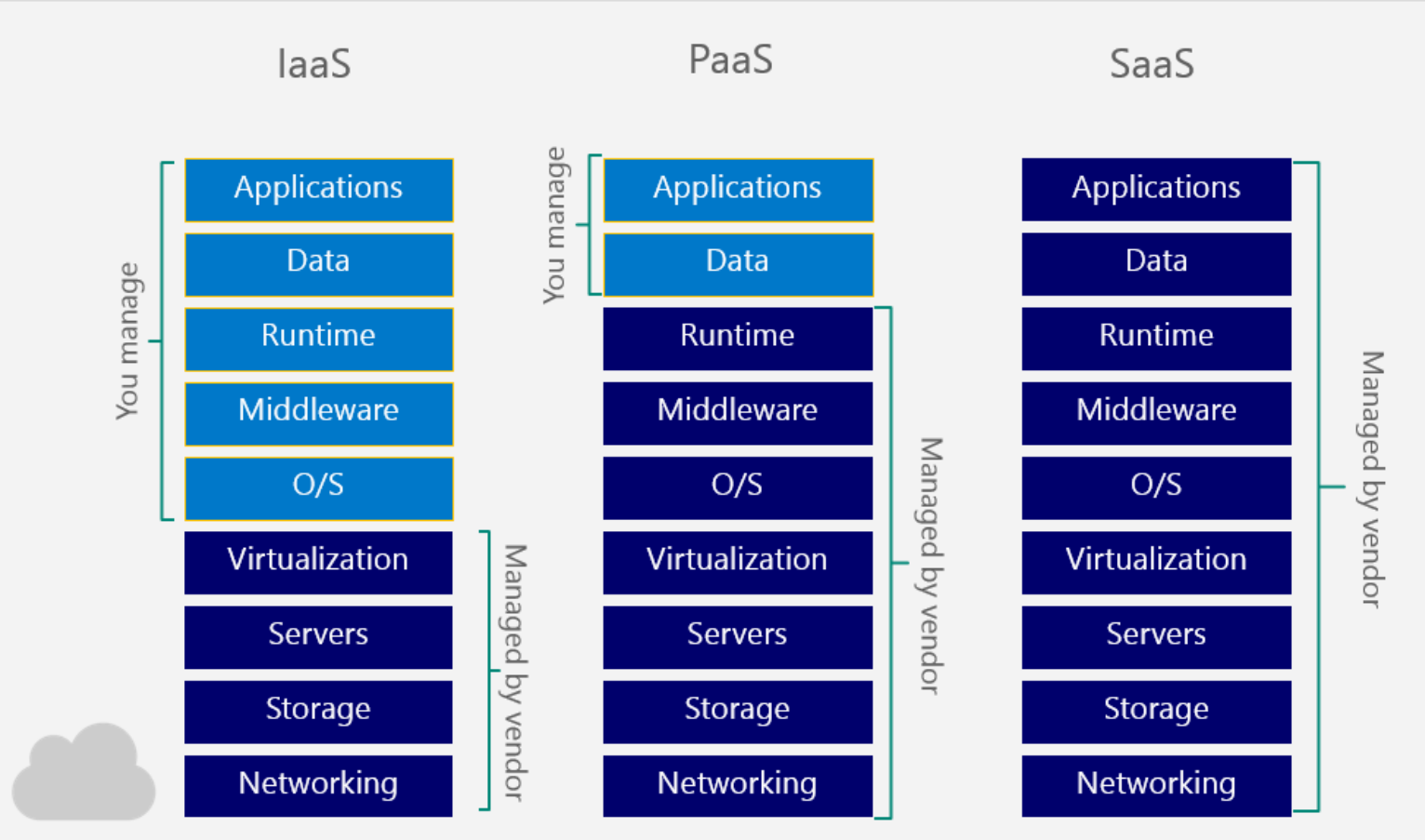
- Le fournisseur offre la possibilité au client de déployer ou créer ses propres applications en lui mettant à disposition les langages, librairies, services et outils nécessaires.
- Le client peut configurer son environnement de déploiement, mais n'a pas la main sur la partie sous-jacente (OS, serveur, rsx, matériel, …).

> IaaS : Infrastructure As a Service.

- le fournisseur met à disposition du client, de la puissance de calcul du stockage, du réseau, et tous les autres composants fondamentaux dont a besoin le client pour faire tourner ses applications (y compris le système d'exploitation)
- le client n'a pas le contrôle sur la couche basse de l'infrastructure.

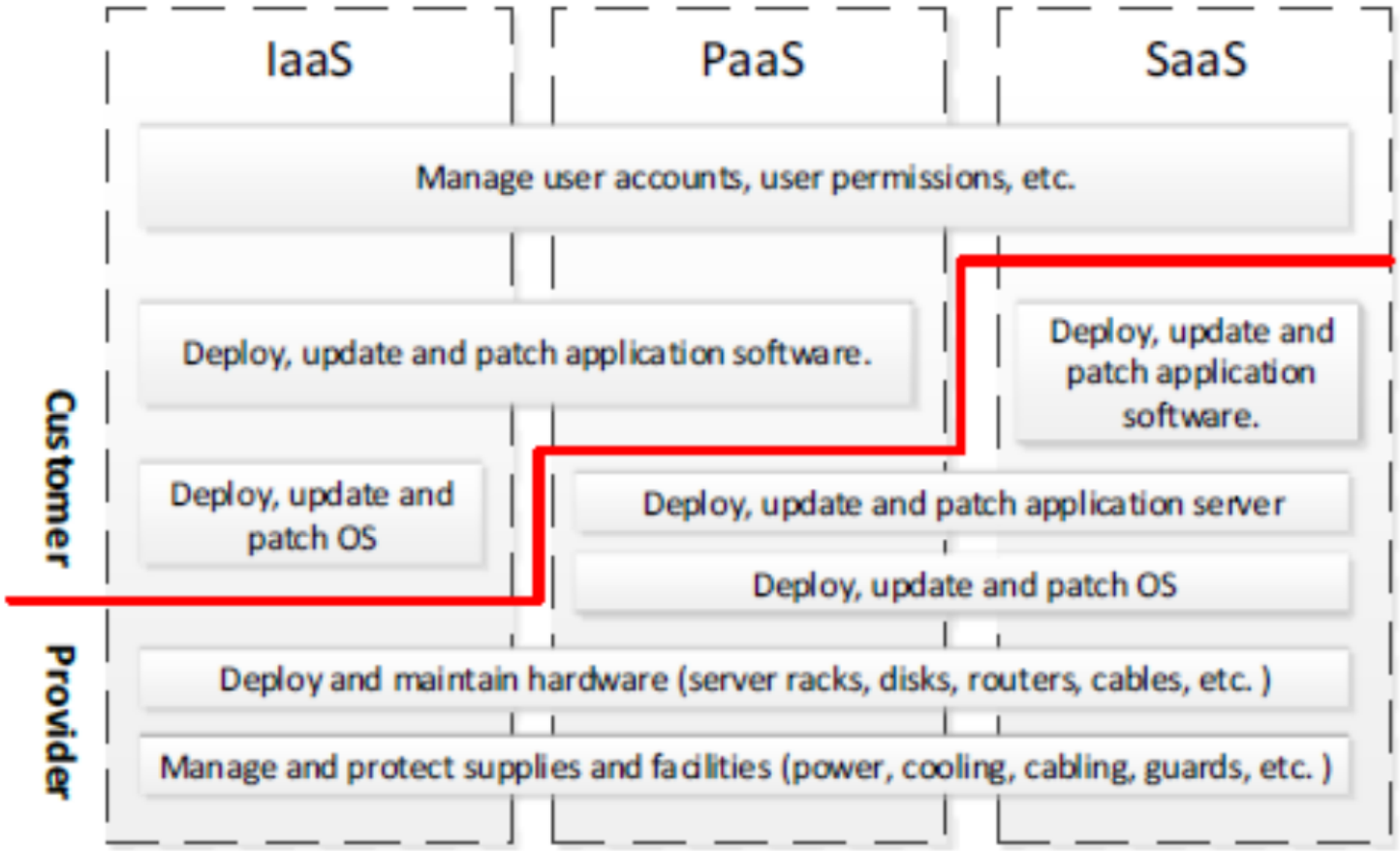
LA SÉCURITÉ DU CLOUD COMPUTING
Les modèles de service du cloud computing

> Quelles responsabilités ?



Source : https://learnwithshahriar.files.wordpress.com/2014/10/saas-vs-paas-vs-iaas.png

> Quelles responsabilités ?



Source : Enisa

Cloud computing et sécurité

LA SÉCURITÉ DU CLOUD COMPUTING
Les préoccupations des clients

> Comme pour tout service externalisé le client (doit) se pose(r) des questions ...

- Comment vais-je être en mesure de sécuriser mes données dans un environnement que je ne maîtrise pas en totalité ? (sous-traitance)
- Ai-je des garanties de disponibilité ? (Services en ligne)
- Le Cloud me permet-il de rester conforme avec mes exigences règlementaires ? (perte de gouvernance, « dépérimétrisation » physique et géographique)
- Est-il possible d'inclure le cloud dans ma gestion de la sécurité ? Est-ce que je dispose des ressources en interne pour permettre cela ? (nouveaux risques, nouvelles technologies, ...)
- ...

LA SÉCURITÉ DU CLOUD COMPUTING
Les principaux risques

> Les risques liés à l'usage du Cloud :

- Perte de gouvernance et enfermement,
- Nouvelle façon de travailler,
- Nouvelles technologies.

> Perte de gouvernance et enfermement,

- Introduction d'un (nouveau) tiers dans la gestion du S.I. :

  Cf. ISO/CEI 27002:2013(F) – Chap. 15 Relation avec les fournisseurs

- Perte de la maîtrise de l'environnement (tout ou partie)
- Perte de visibilité et du contrôle sur une partie de l'informatique du S.I.
- Impacts sur les rôles du DSI et du RSSI

LA SÉCURITÉ DU CLOUD COMPUTING
Les principaux risques

> Nouvelle façon de travailler :

- Nouveaux usages donc nouvelles règles de sécurité.
- Accès à partir d'environnements dont la sécurité n'est pas (ou mal) maîtrisée :
  - postes personnels,
  - smartphones,
  - postes itinérants ou en télétravail en environnement non sûrs
    Voir ISO/CEI 27002:2013(F) – Chap. 6.2 Appareils mobiles et télétravail
- Confusion possible entre environnements et exposition de l'environnement de test.

LA SÉCURITÉ DU CLOUD COMPUTING
Les principaux risques

> Nouvelles technologies :

- Du point de vue du fournisseur de services :
  - nouvelles technologies, nécessité de former le personnel (Haute disponibilité, virtualisation, conteneurisation, SAML, XACML, ...)
  - Parfois peu de retours sur les aspects sécurité (conteneurisation, …)
- Complexité de gérer des environnements mutualisés ainsi que la répartition des ressources
  → risques de défaut de cloisonnement.
- Difficile de correctement gérer le réutilisation des ressources avec comme contrainte la confidentialité des données déjà présente sur le supports (mémoire vive, disques, ...)
  → effacement fiable avant usage.

LA SÉCURITÉ DU CLOUD COMPUTING
Les principaux risques

> Nouvelles technologies - du point de vue du fournisseur de services :

- nouvelles technologies, nécessité de former le personnel *(Haute disponibilité, virtualisation, conteneurisation, SAML, XACML, ...)*
- Parfois peu de retours sur les aspects sécurité (conteneurisation, …)
- Complexité de gérer des environnements mutualisés ainsi que la répartition des ressources
  → risques de défaut de cloisonnement.
- Difficile de correctement gérer le réutilisation des ressources avec comme contrainte la confidentialité des données déjà présente sur le supports (mémoire vive, disques, ...)
  → effacement fiable avant usage.

LA SÉCURITÉ DU CLOUD COMPUTING
Les principaux risques

> Nouvelles technologies - du point de vue du client :

- Exposition du service et/ou api sur le web :
  - Vulnérabilité logicielle
- Exposition de l'interface de gestion :
  - Compromission,
  - Usurpation d'identité.
- Risque d'atteinte à la disponibilité :
  - → Forte dépendance envers la connexion internet
- Problématique de la sécurité des données externalisées:
  - Dispersion de données stockées,
  - Réutilisation de la mémoire, et des périphériques de stockage
  - Accès indirect aux données
    → critique en cas d'incident, ou de désaccord avec le prestataire.

LA SÉCURITÉ DU CLOUD COMPUTING

Les principaux risques réparties par modèles de déploiement et service

Risque élevé
Risque moyen
Risque faible

Risques	Modèle de déploiement			Modèle de service		
	Public	Communautaire	Privé	SaaS	PaaS	IaaS
Perte de gouvernance et enfermement						
Incident dans la relation avec le fournisseur						
Perte de maîtriise et de visibilité de l'environnement						
Accès à partir d'environnements dont la sécurité n'est pas (ou mal) maîtrisée						
Exposition de l'environnement de test						
Exposition du service sur le web						
Compromission de l'interface de gestion						
Usurpation d'identité						
Perte de disponibilité						
Stockage réparti des données						
Réutilisation des données						
Accès indirect aux données						
Technologies nouvelles						
Service réparti dans différents pays						
Complexité de gestion des ressources						
Evolution de l'environnement partagé						
Défaut de cloisonnement						

Basculer dans le cloud en toute sécurité

> Migration/souscription, gestion de projet incluant la sécurité :

- Toujours la même approche classique
  - SMSI ISO27001 plus que jamais important.
  - Mener une appréciation des risques (ISO27005, EBIOS RM, …)
    - Prendre en compte (comme toujours) le référentiel réglementaire (OIV, RGS v2, RGPD, …)
    - Penser à inclure l'évaluation des services de sécurité du fournisseur.
    - Si existante, amender la PSSI avec les nouveaux risques liés au Cloud.

> Migration/souscription, l'importance de la contractualisation

- Les points de vigilance communs :
  - Comité de suivi sécurité : nécessaire de pouvoir suivre la sécurité y compris pour les services hébergés.
  - Processus de transmission des données
  - Obligations du client et du prestataire
  - Gestion des données personnelles et les nouvelles obligations issues du RGPD
  - Obligations générales de sécurité (PSSI)
  - Confidentialité

LA SÉCURITÉ DU CLOUD COMPUTING
Basculer dans le cloud en toute sécurité

> Migration/souscription, l'importance de la contractualisation

- Les points de vigilance propre à un projet cloud :
  - Accord de niveau de service attendu
  - Développements applicatifs
  - Possibilité de commanditer des audits de sécurité sur les périmètres :
    - Opérationnels,
    - Organisationnels.
  - Réversibilité
  - Résiliation
  - Effacement des données

> Les questions que l'on peut légitimement se poser avant de contractualiser ...

- Concernant les ressources partagées :
  - Quels mécanismes de cloisonnement entre compartiments ?
  - Quel nettoyage avant ré-utilisation ?
  - Quelle politique et quelles règles de sécurité applicables ?
  - Comment imputer les actions à leurs auteurs ?

LA SÉCURITÉ DU CLOUD COMPUTING
Basculer dans le cloud en toute sécurité

> Les questions que l'on peut légitimement se poser avant de contractualiser ...

- Flexibilité/Allocation dynamique :
  - Quelles limites géographiques et donc quelles réglementations applicables ?
  - Quels moyens disponibles pour assurer la disponibilité des ressources ?
- Provisioning automatisé :
  - Qui garde le contrôle ?
  - Quel workflow d'approbation ?
  - Quel engagement et quel support de la part du fournisseur ?

LA SÉCURITÉ DU CLOUD COMPUTING
Basculer dans le cloud en toute sécurité

> Les questions que l'on peut légitimement se poser avant de contractualiser ...

- Accès en ligne :
  - Quelles garanties de protection de la plate-forme qui est exposée ?
  - Quels moyens de surveillance et de réaction ?
- Usage mesuré/Paiement à l'usage :
  - La sécurité est-elle incluse dans le prix ou optionnelle ?
  - Comment contrôler la facture ?

LA SÉCURITÉ DU CLOUD COMPUTING
Basculer dans le cloud en toute sécurité

> Le choix du prestataire :

- Privilégier des prestataires :
  - sur le même territoire que le votre,
  - disposant de certifications (ISO27001, …) ou d'une qualification (ANSSI).
- Qualification de prestataire :
  - Secnumcloud
    - Cf référentiel d'exigences de l'ANSSI *https://www.ssi.gouv.fr/administration/qualifications/prestataires-de-services-de-confiance-qualifies/referentiels-exigences/#anchor5*
    - nolimitsecu : *https://www.nolimitsecu.fr/secnumcloud/*

Merci pour votre attention !

> Des questions ?

Thierry MEYER Consultants, est un cabinet de conseil, audit, et expertise technique spécialisé en sécurité des systèmes d'information depuis sa création en 2005.

contact@tm-consultants.fr
@Th1tux