ceis

Janvier 2017

GUIDE PRATIQUE

ADOPTER LE CLOUD EN TOUTE SERENITE

David PATIN

En partenariat avec

BUSINESS DIGITAL SECURITY
Secure & Accelerate your business

ATiPiC AVOCAT

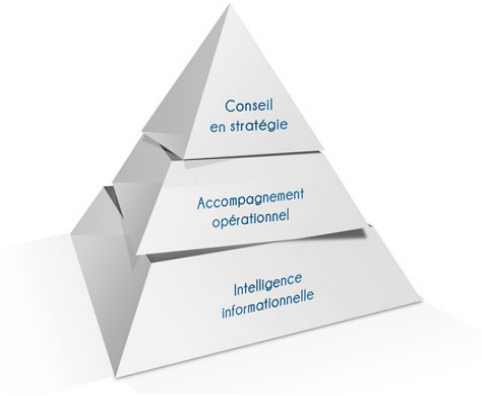
Les notes σtratégiques

L'INTELLIGENCE
DE LA DECISION

LES NOTES STRATEGIQUES

Guide pratique

CEIS est une société de conseil en stratégie et en management des risques. Notre vocation est d'assister nos clients dans leur développement en France et à l'international et de contribuer à la protection de leurs intérêts. Pour cela, nous associons systématiquement vision prospective et approche opérationnelle, maîtrise des informations utiles à la décision et accompagnement dans l'action.



Ce guide pratique a été écrit en collaboration avec Business Digital Security et ATIPIC Avocat

- Business Digital Security est un cabinet de conseil en stratégie intervenant dans les domaines de la cybersécurité, du numérique, et plus largement des technologies de l'information.
- ATIPIC Avocat est une société d'avocat dédiée au droit lié aux nouvelles technologies dans toutes ses composantes (Technologies, Informations, Propriété Intellectuelle, Commerce).

Synthèse

L'adoption du Cloud est désormais inéluctable. A l'heure où un grand nombre de fournisseurs Cloud poussent, parfois de manière agressive, leurs services sur le marché, il peut paraître décourageant pour une organisation, voire illusoire, de s'engager dans une démarche complète de maîtrise des risques. Ces derniers ne sont encore que peu ou pas assimilés par des lignes métiers qui ne perçoivent de ces solutions Cloud que les avantages tant vantés, et pourtant : à partir du 25 mai 2018, avec l'entrée en vigueur du Règlement général européen sur la protection des données (RGPD ou GDPR en anglais), les sociétés n'ayant pas mis en place les garde-fous nécessaires risqueront une amende s'élevant jusqu'à 4% du chiffre d'affaires mondial.

La première leçon, c'est qu'il n'est pas encore trop tard pour adopter de bonnes pratiques et se prémunir de ces risques. La seconde leçon, c'est qu'il n'est nul besoin de « réinventer le nuage ». La plupart des entreprises, soumises à une pression réglementaire grandissante et prenant conscience des nouvelles menaces qui les entourent, disposent déjà de nombreuses politiques, protocoles, fonctions et organes de gouvernance qui devront être repensés en fonction de la valeur de leurs actifs les plus précieux à protéger en priorité.

Afin de réussir vos projets Cloud, que ceux-ci constituent une transformation à l'échelle de l'entreprise ou un simple virage, nous avons identifié au cours de nos missions cinq grandes pratiques à prendre en considération.

CEIS, de par son expérience dans ce domaine, propose dans ce guide pratique quelques règles pragmatiques à mettre en place pour adopter le Cloud « en toute sérénité ». Ce guide fait suite au livre blanc rédigé en 2015, et s'adresse aux DSI, RSSI et à tout acteur impliqué dans la transformation digitale de son organisation.

Maîtriser votre environnement externe

Objectifs

→ Anticiper et gérer les facteurs de risques externes associés au Cloud, « ne pas confondre vitesse et précipitation »

En quoi cela consiste

→ Identifier et comprendre les origines et les sources des menaces cyber par la mise en place d'une démarche de « threat intelligence »
→ Surveiller en continu l'environnement réglementaire de votre organisation afin de préparer par exemple l'entrée en vigueur de nouvelles réglementations

Quels écueils à éviter

→ Croire que la menace liée au Cloud n'est pas spécifique
→ Se concentrer uniquement sur la nature de la menace technique (malware, …) et non sa source ou son origine (cyber criminels, concurrents, hacktivistes, …)
→ Croire de manière erronée que l'adoption du Cloud « libère » l'entreprise de ses responsabilités sur les données
→ Attendre que la réglementation GDPR soit applicable pour exiger de ses fournisseurs Cloud leur mise en conformité, en prenant le risque de voir tomber des sanctions

Adopter une approche business qui « parle » au business

Objectifs

→ Faciliter l'adoption du Cloud et l'intégrer dans sa stratégie d'organisation, et optimiser économiquement l'adoption sécurisée du Cloud

En quoi cela consiste

→ Accompagner les lignes métiers dans l'identification et la protection de leurs « Joyaux de la Couronne », actifs informationnels qui représentent le plus de valeur, qui seront hébergés par le fournisseur Cloud
→ Apprécier les coûts, les risques et les bénéfices de l'ensemble des projets Cloud présentant des « Joyaux de la Couronne »
→ Tester la démarche de priorisation sur un projet Cloud métier, et présenter les résultats au top management
→ Positionner la DSI comme intégrateur et fournisseur de Clouds publics et privés, qui propose une offre de services adaptée aux besoins de vos lignes métiers

Quels écueils à éviter

→ Réaliser des analyses de risques sur tous les projets, sans priorisation
→ Ne se focaliser que sur les risques de sécurité informatique
→ Croire que l'adoption et l'encadrement du Cloud est « l'affaire de la DSI »

Considérer votre fournisseur Cloud comme un partenaire

Objectifs

→ Développer la transparence entre votre organisation et votre fournisseur, et instaurer une relation de confiance

En quoi cela consiste

→ Comprendre l'offre de vos fournisseurs, leurs mesures de sécurité et leurs limites
→ Identifier la chaîne des sous-traitants de votre fournisseur Cloud
→ Elaborer des questionnaires avec des points-clé à la fois sur la société et les solutions proposées lors du sourcing
→ Demander les résultats des derniers tests d'intrusion à votre fournisseur
→ Réaliser des audits de sécurité uniquement sur certains fournisseurs et dans des cas précis

Quels écueils à éviter

→ Envoyer des questionnaires de 300 questions, inutiles et inadaptées
→ Ne pas tenir compte de la stratégie de sécurité de l'information dans la proposition de valeur du fournisseur Cloud
→ Demander au fournisseur la mise en œuvre de mesures de sécurité disproportionnées au regard de ses ressources financières et humaines
→ Lancer des audits ou des tests d'intrusions sur des fournisseurs Cloud de type Tier1 matures en termes de sécurité de l'information

Encadrer les usages du Cloud

Objectifs

→ Accélérer l'adoption sans prise de risques inconsidérée et répondre aux exigences de multiples régulateurs

En quoi cela consiste

→ Donner une réponse rapide et réaliste aux différentes lignes métiers afin d'éviter les frustrations, les annonces trop précoces et l'effet de fatigue
→ Définir et mettre en place une approche risques pluri disciplinaire (Achats, Juridique, RSSI, DPO, Risques, Conformité)
→ Mettre en place une gouvernance dédiée au Cloud et représentative de l'ensemble des parties prenantes
→ Elaborer un référentiel commun et communiqué

Quels écueils à éviter

→ Travailler en silo, sans comprendre que la réussite d'un projet Cloud passe par l'adhésion de l'ensemble des parties prenantes et éventuellement par la refonte des processus
→ Acheter des solutions Cloud avec un niveau de sécurité soit trop fort soit trop faible

Libérer l'innovation liée au Cloud

Objectifs

→ Créer de la valeur, dégager de nouvelles sources de revenus, accélérer votre développement

En quoi cela consiste

→ Identifier les usages Cloud propres à votre organisation
→ Adapter votre stratégie de sécurité de l'information à la catégorie du fournisseur
→ Utiliser des référentiels et standards reconnus sur le marché (ISO 27017, Cloud Confidence, référentiel SecNumCloud de l'ANSSI …)
→ Co construire un plan de développement de sécurité entre votre organisation et le fournisseur pour ne pas écarter les start-ups innovantes
→ Classifier et, quand cela le nécessite (« Joyaux de la Couronne »), chiffrer les données « à la source » avant dépôt dans le Cloud. Pour cela, garder la maîtrise de vos clefs cryptographiques

Quels écueils à éviter

→ Appeler tout système informatique un « Cloud »
→ Avoir des exigences de sécurité non adaptées aux start-ups
→ Elaborer un Plan d'Assurance Sécurité générique et non adapté à votre fournisseur Cloud
→ Demander à vos fournisseurs Cloud de chiffrer l'ensemble des données

Cumulus, une offre unique de conseil dédiée au Cloud

Notre expertise en matière de Due Diligence & Management des Risques d'une part, et de Conseil en Cybersécurité d'autre part, nous permet, avec nos partenaires, de proposer à nos clients une approche transverse et globale liée aux prestations Cloud, regroupant :

- Risque juridique, induit par les contrats & CGV,
- Risque commercial, lié intrinsèquement à vos prestataires,
- Risque IT, en particulier au niveau sécurité.

Nous proposons un service personnalisé, adapté au niveau de maturité de votre organisation, et à votre « appétit » en termes d'adoption progressive de solutions Cloud.

Quelle que soit votre maturité, notre service inclut nativement une analyse stratégique, sécuritaire et juridique de vos fournisseurs et solutions Cloud stratégiques, grâce à des prestations de due diligence et de veille.

Pour plus de détails sur l'offre Cumulus :

Vincent RIOU | Directeur Business Development | CEIS
vriou@ceis.eu
Tél : +33 (0)6 07 34 09 14

ceis

PUBLICATIONS RECENTES

A télécharger sur ***www.ceis.eu***

Les futurs missiles de croisière hypersoniques, des game-changers ? Mai 2016

L'influence du Dark Web sur la démocratisation du Malware-As-A-Service Décembre 2015

Impact de la numérisation sur l'exercice du commandement Décembre 2015

Les objets connectés et la Défense Décembre 2015

Le SIA Lab - Retour sur 2 ans d'activité Juin 2015 (English version available)

Les programmes SIOC en Europe Mars 2015 (English version available)

Société Anonyme au capital de 150 510 €
SIRET : 414 881 821 00022 - APE : 741 G
Tour Montparnasse – 33, avenue du Maine
BP 36 – 75 755 - Paris Cedex 15
Tél. : 01 45 55 00 20 - Fax : 01 45 55 00 60