Cloud Computing

Les défis de la cybersécurité pour la Suisse politique

Etat des lieux

Le cloud computing est un modèle permettant de fournir un accès réseau omniprésent, pratique et à la demande à un ensemble de ressources informatiques configurables (p.ex. réseaux, serveurs, stockage, applications et services) qui peuvent être rapidement déployées et partagées avec un minimum de charge administrative ou d'interaction avec les fournisseurs de services[1]. Ces prestations peuvent être plus ou moins réparties en trois catégories: Infrastructure as a Service (infrastructure en tant que service – IaaS), Platform as a Service (plate-forme en tant que service – PaaS) et Software as a Service (logiciel en tant que service – SaaS). Il est possible de créer des environnements cloud hybrides dans lesquels les organisations utilisent à la fois des ressources privées et publiques.

Le principal avantage du cloud est qu'il permet aux organisations,

1) d'utiliser et de payer les ressources informatiques en fonction de leurs besoins, en évitant les gros investissements de départ et en bénéficiant de coûts de fonctionnement variables,

2) d'accéder à une pile technologique continuellement affinée, améliorée et gérée de manière professionnelle, et ainsi de se concentrer sur l'expérience client, sur leur promesse de valeur/prestations et leurs applications (commerciales), de réduire le temps de mise sur le marché et de s'adapter rapidement à la demande, plutôt que de mettre en œuvre et d'exploiter à l'interne l'infrastructure technologique nécessaire,

3) de bénéficier d'économies d'échelle, car l'infrastructure cloud publique est partagée par de nombreux clients.

Recommandations

1. Le cloud computing est une tendance de fond qui va perdurer. Les lois et règlements qui impactent le traitement des données ou les modèles commerciaux (lois sur la protection des données, règlements sur les cyberrisques, etc.) devraient être fondés sur ce constat, en pesant soigneusement les opportunités et les risques pour l'économie et la société.
2. Les organisations comprennent les implications du cloud computing au-delà des aspects purement technologiques.
   - Elles sont conscientes des opportunités en termes de modèle économique et commercial, d'amélioration de l'innovation, de délai de commercialisation, etc.
   - Peser soigneusement les opportunités et les risques, comprendre les options d'atténuation des risques.
   - Une fois la migration vers le cloud terminée, elle sera basée sur une stratégie de cloud appropriée, abordée comme un projet de changement organisationnel (par opposition à une pure migration technologique) et garantira que les risques sont compris et efficacement atténués.

La tendance à la fourniture de ressources informatiques via le cloud computing présente certaines similitudes avec le passage de la production d'électricité dans les petites centrales électriques propres à l'achat d'électricité auprès de grandes centrales appartenant à des tiers. Les conséquences sont importantes.

[1] NIST - https://csrc.nist.gov/publications/detail/sp/800-145/final

Contrairement à la production d'électricité, le cloud computing est dominé dans le monde entier par quelques grands acteurs dont les prestations ne sont L'introduction de l'Elastic Compute Cloud par Amazon Web Services en 2006 a rendu le cloud computing public accessible à grande échelle. L'infrastructure mondiale du cloud est désormais dominée par Amazon, Google, Microsoft et Alibaba. La disponibilité de l'infrastructure de cloud computing a conduit à l'émergence de nombreuses offres de Software as a Service (p. ex. SalesForce, ServiceNow, Workday, etc.).

La Suisse n'a pas pris une position de leader dans l'introduction du cloud computing, notamment pour des raisons de conformité (y compris la protection des données) et de sécurité. Toutefois, la dynamique s'accélère, car les services de cloud computing ont mûri en termes de sécurité et de contrôles (tout comme la transparence qui y est associée) et de grands fournisseurs globaux de cloud computing (Google, Microsoft) ont ouvert des centres de données en Suisse.

Défis

Les principaux cyberrisques associés au cloud computing sont les suivants:

1. **Conformité** – traitement des données conformément aux lois, règlements et directives organisationnelles applicables parfois contradictoires, ambigus ou conçus en fonction d'une infrastructure technologique plus traditionnelle. La tendance générale est également à une réglementation accrue du traitement des données, qui restreint leur libre circulation en raison de préoccupations liées à la protection des données ou à des intérêts (de sécurité) nationaux. Il est à craindre que certaines lois et réglementations contenant des dispositions en vertu desquelles des entités gouvernementales (étrangères) peuvent accéder aux données d'une organisation via le fournisseur de prestations de cloud computing puissent être interprétées de manière large ou faire l'objet d'une utilisation abusive (p. ex. US Cloud Act[2] et Chinese Cyber Law[3]).
2. **Shadow IT** – les organisations ont souvent des difficultés à comprendre où et comment leurs données sont traitées. Cela est dû au fait que les unités **organisationnelles** utilisent souvent des infrastructures et des applications en nuage pour contourner les mécanismes de gouvernance établis et généralement appliqués par le département informatique d'une entreprise. Il en émerge une Shadow IT qui ne respecte pas la règlementation de l'entreprise et qui ne dispose probablement pas de contrôles de sécurité adéquats.
3. **Sécurité** – comme les fournisseurs de public cloud concentrent les données de nombreux clients sur leur infrastructure informatique, ils constituent une cible intéressante pour les cyberattaques. Ce problème est atténué dans une certaine mesure, car les grands fournisseurs de cloud computing disposent des ressources et de l'expertise nécessaires pour implémenter et utiliser ce qui se fait de mieux en matière de contrôle de la sécurité. Néanmoins, les organisations qui utilisent le cloud computing doivent posséder une connaissance approfondie des méthodes de contrôle et de surveillance de l'accès aux données traitées dans le nuage et de protection de la confidentialité et de l'intégrité de ces données. Cela inclut souvent le cryptage des données pendant la transmission et en mode veille. Toutefois, lors de leur traitement, les données ne sont généralement pas cryptées. Il est nécessaire d'évaluer et de gérer le risque inhérent de manière appropriée.
4. **Exploitation** – le passage au cloud computing doit aller de pair avec la transition vers des processus opérationnels plus agiles et – souvent – **automatisés**, pour le développement, le déploiement et la sécurisation de l'informatique. Les bénéfices retirés n'en seront que plus grands. Le passage au cloud computing est donc souvent associé à la mise en œuvre de nouveaux concepts tels que le (Sec)Dev

[2] https://www.gpo.gov/fdsys/pkg/BILLS-115hr1625enr/html/BILLS-115hr1625enr.htm
[3] https://en.wikipedia.org/wiki/China_Internet_Security_Law

Ops[4] qui nécessite d'importants changements organisationnels et comportementaux.

5. Ajuster les contrôles – bien que la responsabilité des données incombe toujours à l'entreprise qui utilise les services de cloud computing, les entreprises doivent se fier aux fournisseurs de cloud computing pour mettre correctement en œuvre une part importante des contrôles de sécurité. Il est donc essentiel de coordonner convenablement les cadres de contrôle des utilisateurs et des fournisseurs, de surveiller de près l'efficacité des contrôles et de clarifier les responsabilités.

Bien qu'il n'y ait pas de cyberrisque, il est important de mentionner ici le défi du Vendor lock-in (enfermement propriétaire) – c'est-à-dire l'impossibilité de changer de fournisseur pour des raisons techniques ou autres – car dans certaines situations, le changement de fournisseur peut être la seule mesure possible pour atténuer de manière adéquate les cyberrisques évoqués plus haut. La tendance aux solutions multicloud proposées par les principaux fournisseurs de cloud et d'autres entreprises technologiques contribue à atténuer ce risque.

Nécessité d'agir

1. Les législateurs et les régulateurs doivent s'informer sur les principes fondamentaux, les opportunités et les risques du cloud computing afin de permettre une législation et une réglementation intelligentes.
   - La SATW devrait organiser des séances de formation avec les politiciens et les régulateurs.
   - La SATW devrait faire office de caisse de résonance et donner un feed-back sur l'impact des réglementations internationales (p. ex. US Cloud Act et Chinese Cyber Law) sur l'introduction du cloud computing en Suisse et sur la réaction possible des politiciens et du gouvernement suisse à ces réglementations.
   - La SATW devrait faire office de caisse de résonance et fournir un feed-back avant et pendant les processus de consultation sur le futur règlement.

2. Promotion de la recherche dans le domaine du traitement sécurisé des données (y compris le cryptage homomorphe, la pseudonymisation et d'autres concepts) et développement de produits connexes
   - La SATW doit influencer les organes de décision/d'évaluation compétents, tels que le Fonds national suisse (FNS), Innosuisse, les jurys des concours de création de start-up, etc.

[4] https://en.wikipedia.org/wiki/DevOps

Références

- NIST: https://csrc.nist.gov/publications/detail/sp/800-145/final
- Cloud Act: https://en.wikipedia.org/wiki/CLOUD_Act
- DevOps: https://en.wikipedia.org/wiki/DevOps

China Internet Security Law: https://en.wikipedia.org/wiki/China_Internet_Security_Law
https://www.gpo.gov/fdsys/pkg/BILLS-115hr1625enr/html/BILLS-115hr1625enr.htm

Contact

Nicole Wettstein
Responsable du programme prioritaire Cybersécurité
+41 44 226 50 13

https://www.satw.ch/cybersecurity-defis

Impressum
Académie suisse des sciences techniques SATW
Contributions d'experts
Karl Aberer, EPFL | Umberto Annino, InfoGuard | Alain Beuchat, Banque Lombard Odier & Cie SA | Matthias Bossardt, KPMG | Adolf Doerig, Doerig & Partner | Stefan Frei, ETH Zürich | Roger Halbheer, Microsoft | Pascal Lamia, MELANI | Martin Leuthold, Switch | Hannes Lubich, Verwaltungsrat und Berater | Adrian Perrig, ETH Zürich | Raphael Reischuk, Zühlke Engineering AG | Riccardo Sibilia, VBS | Bernhard Tellenbach, ZHAW | Daniel Walther, Swatch Group Services | Andreas Wespi, IBM Research Lab
Rédaction et graphisme
Beatrice Huber; Claude Naville, Adrian Sulzer, Nicole Wettstein

Les opinions exprimées ici sont celles des membres du conseil consultatif sur la cybersécurité de la SATW et ne reflètent pas nécessairement la position officielle de SATW et de ses membres.

www.satw.ch
Septembre 2020