satw

Cloud Computing

Cybersecurity – challenges for political Switzerland

State of the art

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

[1] These services are broadly divided into three categories: Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS). Hybrid cloud environments are possible where organizations use both, *private* and *public* resources.

The main benefit of the cloud is that it enables organizations to

1. consume and pay for computing resources on demand, hence avoiding large upfront investments and benefit from variable operational costs,
2. get access to a constantly refined, enhanced and professionally managed technology stack which enables organizations to focus on customer experience, their value propositions/services and (business) applications, improve time to market and rapidly scale with demand as opposed to implementing and operating the underlying technology infrastructure,
3. benefit from economies of scale as the public cloud infrastructure is shared among many clients.

Hence, the evolution towards provisioning computing resources via cloud computing bears some similarities to the move from electric power generation in company-owned small power stations to consuming electric power from large third-party owned power plants. In contrast to electric power, cloud computing is globally dominated by a few major players and their services are not fungible. This has important consequences as we will see further below.

With the introduction of the Elastic Compute Cloud by Amazon Web Services, public cloud computing at scale has been made broadly available in 2006. In the meantime, the global cloud infrastructure is dominated by Amazon, Google, Microsoft and Alibaba.

Recommendations

1. Cloud computing is here to stay. Legislation and regulations with an impact on data processing or on operating models (data privacy laws, cyber risk regulations, etc.) should be done under this premise, carefully balancing opportunity and risk for economy and society.
2. Organizations must understand the impact of cloud computing beyond the pure technological aspects.
   - Get an understanding of opportunities regarding business and operating model, improved innovation and time to market, etc.
   - Carefully balance opportunities with risks, understand risk mitigation options.
   - Once moving to the cloud, do it based on a proper cloud strategy, treat it as an organizational change project (as opposed to a pure technology migration) and make sure risks are understood and effectively mitigated.

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

The availability of cloud computing infrastructure has led to the advent of numerous Software as a Service offerings (e.g. SalesForce, ServiceNow, Workday, etc.).

Switzerland has not been a front runner in cloud adoption, not the least due to compliance (including privacy) and security concerns. However, there is increasing momentum as cloud services have matured in terms of security and controls (and related transparency), and major global cloud providers (Google, Microsoft) have opened cloud data centres in Switzerland.

Challenges

The major cyber risks related to cloud computing are:

1. **Compliance** – processing data according to applicable laws, regulations and organizational policies, which can be contradicting, ambiguous or designed with a more traditional technology infrastructure in mind. In addition, there is general trend towards increased regulation of data processing limiting the free flow of data due to privacy concerns or national (security) interests. There are some concerns that certain laws and regulations containing provisions under which (foreign) government entities may get access to an organization's data via the cloud provider can be stretched or misused (e.g. US Cloud Act[2], Chinese Cyber Law[3]).
2. **Shadow IT** – organizations often struggle to understand where and how their data is processed. This is because organizational units frequently use cloud infrastructure and applications to circumvent established governance mechanisms which are typically enforced by an organization's IT function. Therefore, a *shadow* IT is established that is not compliant applicable company policies and might lack appropriate security controls.
3. **Security** – as public cloud providers concentrate the data of many customers on their computing infrastructure, they are an attractive target for cyberattacks. This issue is offset to a certain degree by the fact that major cloud providers have the resources and know-how to implement and operate state-of-the-art security controls. Nevertheless, organizations consuming cloud services must have a deep understanding on how to control and monitor access to data processed in the cloud, and to protect the confidentiality and integrity of such data. Often this includes encryption of data in transit and at rest. During computing, however, data is typically unencrypted. The related risk must be assessed and managed accordingly.
4. **Operations** – to reap the expected benefits, moving to cloud computing must be accompanied by transitioning to more agile and – often – automated operational processes to develop, deploy and secure IT. Hence, the move to the cloud often entails the implementation of new concepts like (Sec)DevOps[4], which require major organizational and behavioural change.
5. **Alignment of controls** – while accountability for the data remains with the organization consuming cloud computing services, organizations must rely on the cloud providers to properly operate a significant portion of the security controls. It is therefore critical that the control frameworks of the consumer and the provider are properly aligned, controls effectiveness is monitored and responsibilities are clarified.

While not a cyber risk, the challenge of **vendor lock-in** – i.e. not being able to change cloud providers for technical or other reasons – shall be mentioned here as well because in certain situations transitioning away from a provider might be the only action possible to adequately mitigate the cyber risks discussed above. The trend towards multicloud solutions offered by the major cloud providers and other technology firms help mitigate this risk.

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

Need for action

1. Legislators and regulators to educate themselves on the foundations, opportunities and risks of cloud computing to enable smart legislation and regulation
   - SATW to run educational sessions with politicians and regulators
   - SATW to act as a sounding board/provide feedback with regards to the impact of international regulation (e.g. US Cloud Act2, Chinese Cyber Law3) on the adoption of cloud computing in Switzerland, and on the potential response to such regulation by politicians and the Swiss government
   - SATW to act as a sounding board/provide feedback on draft regulation before and during the consultation process for upcoming regulation
2. Foster research on secure computing (incl. homomorphic encryption, pseudonymization, and other concepts) and development of related products
   - SATW to influence relevant decision/assessment bodies, such as Swiss National Science Foundation (SNSF), Innosuisse, juries in start-up competitions, etc.

References

- 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
Head of priority programme Cybersecurity
+41 44 226 50 13

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

Impressum
Swiss Academy of Engineering Sciences SATW
Expert contributions
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, Board of Directors and Advisor | 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
Editing and graphics
Beatrice Huber, Claude Naville, Adrian Sulzer, Nicole Wettstein

www.satw.ch
September 2020