Cloud Computing

Cybersecurity – Herausforderungen für die politische Schweiz

Stand der Dinge

Cloud Computing ist ein Modell, das einen allgegenwärtigen, bequemen und bedarfsgerechten Netzzugang zu einem gemeinsamen Pool konfigurierbarer Computing-Ressourcen ermöglicht (z. B. Netzwerke, Server, Speicher, Anwendungen und Dienste). Die Ressourcen können mit minimalem Verwaltungsaufwand oder mit minimaler Interaktion mit dem Dienstanbieter schnell bereitgestellt und freigegeben werden. Die zur Verfügung gestellten Dienste lassen sich grob in drei Kategorien einteilen: Infrastruktur-as-a-Service (IaaS), Plattform-as-a-Service (PaaS) und Software-as-a-Service (SaaS). Es sind auch hybride Cloud-Umgebungen möglich, in denen Organisationen sowohl private als auch öffentliche Ressourcen nutzen.

Der Hauptvorteil der Cloud besteht darin, dass sie Organisationen Folgendes ermöglicht:

1. Rechenressourcen nach Bedarf zu verbrauchen und zu bezahlen, wodurch grosse Vorabinvestitionen vermieden werden können und nur die variablen Betriebskosten anfallen.
2. Zugang zu einem ständig verfeinerten, verbesserten und professionell verwalteten Technologiepaket, der es Organisationen ermöglicht, sich auf das eigentliche Geschäftsmodell zu konzentrieren anstatt die zugrunde liegende Technologieinfrastruktur zu implementieren und zu betreiben.
3. von Grössenvorteilen zu profitieren, da die öffentliche Cloud-Infrastruktur von vielen Kunden gemeinsam genutzt wird.

Die Entwicklung hin zur Bereitstellung von Computing-Ressourcen über Cloud Computing weist einige Ähnlichkeiten mit dem Übergang von der Stromerzeugung in firmeneigenen kleinen Kraftwerken zum Verbrauch von Strom aus großen Kraftwerken in Fremdbesitz auf. Im Gegensatz zur Stromerzeugung wird Cloud Computing weltweit von einigen wenigen grossen Akteuren dominiert, und ihre Dienste sind nicht austauschbar. Dies hat wichtige Konsequenzen, wie wir weiter unten sehen werden.

Empfehlungen

1. Cloud Computing ist aus unserem Alltag nicht mehr wegzudenken. Gesetze und Vorschriften, die sich auf die Datenverarbeitung oder auf Betriebsmodelle auswirken (Datenschutzgesetze, Cyberrisikovorschriften usw.), sollten unter dieser Prämisse erfolgen, wobei Chancen und Risiken für Wirtschaft und Gesellschaft sorgfältig gegeneinander abzuwägen sind.
2. Organisationen müssen die Auswirkungen des Cloud Computing über die rein technologischen Aspekte hinaus verstehen.
   - Ein Verständnis für die Chancen des Cloud Computing entwickeln, in Bezug auf Geschäfts- und Betriebsmodelle, verbesserte Innovation, Produkteinführungszeit, usw.
   - Chancen und Risiken sorgfältig gegeneinander abwägen, Optionen zur Risikominderung verstehen.
   - Den Umzug in die Cloud basierend auf einer geeigneten Cloud-Strategie durchführen: Der Umzug sollte als organisatorisches Veränderungsprojekt behandelt werden (im Gegensatz zu einer reinen Technologiemigration) und es muss sichergestellt sein, dass die Risiken verstanden und wirksam gemindert werden.

Mit der Einführung der Elastic Compute Cloud durch Amazon Web Services wurde 2006 das öffentliche Cloud Computing in grossem Massstab breit verfügbar gemacht. In der Zwischenzeit wird die globale Cloud-Infrastruktur von Amazon, Google, Microsoft und Alibaba dominiert. Die Verfügbarkeit der Cloud-Computing-Infrastruktur hat zum Aufkommen zahlreicher Software-as-a-Service-Angebote geführt (z.B. SalesForce, ServiceNow, Workday, etc.).

Die Schweiz hat bei der Einführung von Cloud Computing nicht zuletzt aufgrund von Bedenken bezüglich Compliance (einschliesslich Privatsphäre) und Sicherheit keine Spitzenposition eingenommen. Es gibt jedoch eine zunehmende Dynamik, da Cloud-Dienste in Bezug auf Sicherheit und Kontrollen (und die damit verbundene Transparenz) gereift sind und grosse globale Cloud-Anbieter (Google, Microsoft) Cloud-Rechenzentren in der Schweiz eröffnet haben.

Herausforderungen

Die wichtigsten Cyber-Risiken im Zusammenhang mit Cloud Computing sind:

1. Compliance: Es ist nicht trivial, die Daten gemäss geltenden Gesetzen, Vorschriften und organisatorischen Richtlinien zu verarbeiten. Diese können widersprüchlich, mehrdeutig oder basierend auf einer traditionelleren technologischen Infrastruktur konzipiert worden sein. Darüber hinaus gibt es einen allgemeinen Trend zu einer verstärkten Regulierung der Datenverarbeitung, die den freien Datenfluss aufgrund von Datenschutzbedenken oder nationalen (Sicherheits-)Interessen einschränkt. Es gibt zudem Bedenken, dass gewisse Gesetze und Vorschriften Bestimmungen enthalten, die ausgeweitet bzw. missbraucht werden können und (ausländischen) staatlichen Stellen über den Cloud-Provider Zugang zu den Daten einer Organisation ermöglichen (z.B. US Cloud Act, chinesisches Cyber-Gesetz).
2. Schatten-IT: Organisationen haben oft Schwierigkeiten zu verstehen, wo und wie ihre Daten verarbeitet werden. Das liegt daran, dass Organisationseinheiten häufig Cloud-Infrastrukturen und -Anwendungen nutzen, um etablierte Governance-Mechanismen zu umgehen, die typischerweise von der IT-Funktion einer Organisation durchgesetzt werden. Daher wird eine Schatten-IT eingerichtet, die nicht den geltenden Unternehmensrichtlinien entspricht und möglicherweise nicht über angemessene Sicherheitskontrollen verfügt.
3. Sicherheit: Da öffentliche Cloud-Anbieter die Daten vieler Kunden auf ihre Recheninfrastruktur konzentrieren, sind sie ein attraktives Ziel für Cyberattacken. Dieses Problem wird bis zu einem gewissen Grad durch die Tatsache ausgeglichen, dass die großen Cloud-Anbieter über die Ressourcen und das Know-how verfügen, um Sicherheitskontrollen auf dem neuesten Stand der Technik zu implementieren und zu betreiben. Nichtsdestotrotz müssen Organisationen, die Cloud-Dienste in Anspruch nehmen, ein tiefes Verständnis dafür haben, wie der Zugang zu den in der Cloud verarbeiteten Daten kontrolliert und überwacht und die Vertraulichkeit und Integrität dieser Daten geschützt werden kann. Dazu gehört oft auch die Verschlüsselung von Daten während der Übertragung und im Ruhezustand. Während der Datenverarbeitung sind die Daten jedoch in der Regel unverschlüsselt. Das damit verbundene Risiko muss entsprechend bewertet und gehandhabt werden.
4. Betrieb: Um die erwarteten Vorteile nutzen zu können, muss der Umstieg auf Cloud Computing mit dem Übergang zu agileren und - häufig - automatisierten Betriebsprozessen zur Entwicklung, Bereitstellung und Sicherung der IT einhergehen. Der Umstieg auf die Cloud ist daher oft mit der Implementierung neuer Konzepte wie (Sec)DevOps verbunden, die erhebliche Veränderungen bezüglich Organisation und Verhalten erfordern.

5. Anpassung der Kontrollen: während die Verantwortlichkeit für die Daten bei dem Unternehmen verbleibt, das Cloud Computing-Dienste nutzt, müssen sich Unternehmen darauf verlassen, dass die Cloud-Anbieter einen wesentlichen Teil der Sicherheitskontrollen ordnungsgemäss durchführen. Daher ist es von entscheidender Bedeutung, dass die Kontrollrahmen des Verbrauchers und des Anbieters richtig aufeinander abgestimmt sind, die Wirksamkeit der Kontrollen überwacht wird und die Verantwortlichkeiten geklärt sind.

Auch wenn dies kein Cyberrisiko darstellt, soll hier auch die Herausforderung der Anbieterbindung – d.h. die Unmöglichkeit, den Cloud-Anbieter aus technischen oder anderen Gründen zu wechseln – erwähnt werden. In bestimmten Situationen kann der Wechsel weg von einem Anbieter die einzig mögliche Massnahme sein, um die oben diskutierten Cyberrisiken angemessen zu mindern. Der Trend zu Multi-Cloud-Lösungen, die von den grossen Cloud-Anbietern und anderen Technologiefirmen angeboten werden, trägt dazu bei, dieses Risiko abzuschwächen.

Handlungsbedarf

1. Gesetzgeber und regulierende Stellen sollen sich über die Grundlagen, Chancen und Risiken des Cloud Computing informieren, um eine intelligente Gesetzgebung und Regulierung zu ermöglichen.
   - Die SATW könnte Bildungsveranstaltungen mit Politikerinnen und Politikern sowie Regulierungsbehörden durchführen.
   - Die SATW könnte als Sounding Board fungieren und Feedback geben zu den Auswirkungen internationaler Regulierungen (z.B. US Cloud Act, Chinese Cyber Law) auf die Einführung von Cloud Computing in der Schweiz. Sie könnte auf diese Weise mögliche Reaktionen von Politikerinnen und Politikern sowie der Schweizer Regierung vorbereiten.
   - Die SATW könnte als Sounding Board fungieren und vor sowie während des Konsultationsprozesses für die bevorstehende Regulierung Feedback zum Verordnungsentwurf geben.
2. Die Forschung auf dem Gebiet der sicheren Datenverarbeitung (einschließlich homomorpher Verschlüsselung, Pseudonymisierung und anderer Konzepte) und die Entwicklung verwandter Produkte soll gefördert werden.
   - Die SATW könnte auf relevante Entscheidungs-/Bewertungsgremien, wie z.B. Schweizerischer Nationalfonds (SNF), Innosuisse, Jurys in Start-up-Wettbewerben, etc. Einfluss nehmen.

Referenzen

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

Cloud Act:

- https://en.wikipedia.org/wiki/CLOUD_Act
- https://www.gpo.gov/fdsys/pkg/BILLS-115hr1625enr/html/BILLS-115hr1625enr.htm

DevOps: https://en.wikipedia.org/wiki/DevOps

China Internet Security Law: https://en.wikipedia.org/wiki/China_Internet_Security_Law

Kontakt

Nicole Wettstein
Leiterin Schwerpunktprogramm Cybersecurity
+41 44 226 50 13

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

Impressum
Schweizerische Akademie der Technischen Wissenschaften SATW
Expertenbeiträge
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
Redaktion und Grafik
Beatrice Huber; Claude Naville, Adrian Sulzer, Nicole Wettstein

www.satw.ch
September 2020