Dipl. Ing. Uwe Irmer

Cloud Security Grundlagen

„Erfolg ist, von Fehler zu Fehler zu stolpern, ohne den Verlust an Enthusiasmus“
Uwe Irmer, Juni 2018

Inhaltsverzeichnis

Vorwort

Die Cloud Technologie scheint der Business Treiber der letzten Jahre zu sein. Entsprechend mehreren Studien suchen international Konzerne sowie kleine und mittlere Unternehmen KMU ihre Informationstechnologie in die Cloud zu verlagern.

Die Erwartungshaltungen sind hoch und kurz zusammengefasst:
Niedrige Kosten für die Nutzung der Informationstechnologie, flexible Nutzung und Fakturierung, technologisch stets auf dem aktuellsten Stand, hohe Verfügbarkeit, hohe Agilität, keine Bindung eigener Ressourcen, keine Verantwortung für Betrieb und Wartung.

Eine verlockende Idee.

Aber wie ist es mit der Einhaltung der Governance, der Verantwortung gegenüber der Information Sicherheit und dem Datenschutz? Wie wird die Cloud Technologie compliant in das Unternehmen integriert, welche Verantwortung hat das Management, wie sind Prozesse anzupassen, welche Auswirkungen entstehen für das Unternehmen, was sind die Risiken?
Und wie schützt sich das Unternehmen vor Datendiebstahl, Manipulation, Zerstörung und allenfalls Spionage?

Diese Fragen legt die Buchserie „Cloud Security“ offen und zeigt Lösungen auf.

Das vorliegende Buch „Cloud Security Grundlagen“ ist Teil 1 der Serie „Cloud Security“. In diesem werden die grundlegenden prozessoralen Massnahmen beschrieben und Ausblicke auf die technischen Massnahmen beschrieben.

Teil 2 der Serie ist das Buch „Cloud Security Best Practice“. In ihm werden Massnahmen zur prozessoralen Umsetzung und vertieft technische Massnahmen beschrieben.

Warum die Aufteilung in zwei Bücher?

Die Cloud Technologie hat Innovationszyklen von etwa 6 Wochen. In diesem Zeitraum ändern sich technologische Eigenschaften, Fähigkeiten der Services und Prozesse.

Während der eine Teil, die Governance, Compliance und Anpassung der Unternehmen Prozesse einen geringeren Innovationszyklus erfährt, ist der zweite Teil, die Technologie und die Anpassung der Prozesse, sehr agil.

Appenzell im Juni 2018

MniConsult GmbH
Uwe Irmer
Dipl. Ing. Univ.
Dipl. Wirtschaftsingenieur

KAPITEL EINS

Abkürzungen

Abkürzung	Erlläuterung
COSO	Committee of Sponsoring Organizations of the Treadway Commission
CPU	Central Processing Unit
CRM	Customer Relationship Management
DNS	Domain name service
ERM	Enterprise Risk Management
GPS	Global Positioning System
IAM	Identity an Access Management
IKS	Internes Kontroll System
IoT	Internet of Things
ISMS	Information Sicherheit Management System
IT	Informationstechnologie
KI	Künstliche Intelligenz
KMU	Kleine und mittlere Untermehmen
LDAP	Lightweigt Directory Access Protocol
NIST	National Institute of Standards and Technology
SLA	Service Level Agreement
SMS	Short Message Service
SQL	Structured query language
SSL	Secure socket layer
VPN	Virtuelles privates Netzwerk
WAF	Web Application Firewall

WLAN	Wireless Local Area Network

Abbildungsverzeichnis

Abbildung 17, Bewertung der Cloud Architekture

Definitionen

Fussnoten

Fussnote Nummer	Gegenstand
1	Dropbox
2	Edward Snowden
3	Salesforce
4	Docker
5	Kubernetes
6	Mesosphere

KAPITEL ZWEI

Einstieg in die Cloud Technologie

Die Cloud Technologie übt eine schier faszinierende Magie auf Personen und Unternehmen aus, sodass der Eindruck entsteht, es müssten dringend alle Daten und Anwendungen in die Cloud verlagert werden um ja nicht den Anschluss zu verpassen. Viele Services wie Dropbox[1] oder die vielen freien Webmail Angebote sind schnell auf den Smartphones, Tablets und PC installiert und sofort einsetzbar.

Den grossen Start um Unternehmen in die Cloud zu bringen vollzog Microsoft, als es mit Office 365 im Juni 2011 live ging. Gerade viele Kleine und mittlere Unternehmen KMU in der Schweiz drängten seinerzeit auf das Angebot von Office 365 und verlagerten ihre IT in die Cloud Technologie. Zu verlockend war die Tatsache, keine eigenen Server mehr betreiben zu müssen, ein Office Paket zu haben das immer aktuell ist, ein email Server, der nicht mehr gewartet werden muss und schliesslich Speicher und Dokumentenablage inklusive Backup. Endlich konnte die eigene IT Infrastruktur aus dem Unternehmen verbannt werden.

Einen Rückschlag erlitt die Euphorie im Jahr 2013, als Edward Snowden[2], ein ehemaliger CIA Mitarbeiter, NSA Agent und Whistleblower, mit seinen Enthüllungen über die weltweiten Überwachungs- und Spionageaktivitäten, überwiegend der US Amerikanischen und Britischen Geheimdienste, die NSA Affäre auslöste. Damit erfuhren

Privatpersonen als auch Unternehmen, dass Zugriff auf die Daten in der Cloud besteht, dass Kommunikation abgehört wird, dass emails und Telefonate mitgeschnitten werden und von den Geheimdiensten gesammelt werden. Gerade in der Schweiz war seinerzeit das Vertrauen in Cloud Services nicht mehr gegeben, sogar das Vertrauen gegenüber Unternehmen wie Microsoft.

Mittlerweile im Jahr 2018 ist unstrittig, dass Unternehmen die Cloud Technologie nutzen und in den nächsten Jahren verstärkt Services aus der Cloud nutzen werden.

Ebenso unstrittig ist aber, gerade mit den Erkenntnissen der Snowden Enthüllungen, dass die Cloud Technologie prozesstechnisch und regelkonform in das Unternehmen integriert werden muss. Gesetze und Regularien müssen eingehalten werden und das Unternehmen muss seine Schutzbedürfnisse auch in der Cloud Technologie erfüllen.

Was dies im Einzelnen bedeutet, worüber sich das Unternehmen Gedanken machen muss und welche Anpassungen nötig sind, dies wird in den nachfolgenden Kapiteln erörtert.

Das Buch startet mit einer Einführung in die Cloud Technologie. Hier werden zentrale Begriffe definiert, es wird die Cloud Technologie beschrieben, vorhandene Lösungen, Architekturen und Objekte, die in der Cloud Technologie zur Verfügung stehen. Es werden Studien analysiert, die die Bedürfnisse der Unternehmen betreffend der Cloud Technologie darstellen. Daraus ergeben sich die Anpassungen in den einzelnen Domänen eines Unternehmens, um die Cloud Technologie sicher einsetzen zu können.