Information Security Society Switzerland

# KMU Cloud Migration: gibt es Gründe die Cloud-Chancen nicht zu nutzen?

**27. August 2019, Arié Malz**

# Bedeutung der KMU für die Schweiz

- 99% aller Betriebe
- 67% aller Beschäftigen
- 90% Klein- und Mikrounterunter nehmen
- 60% der Wirtschaftsleistung

# KMU im Fokus der Cybergefahr?

## Gesamtbild?

## Was wissen wir?

## Jedes zweite Unternehmen bereits ein Opfer eines Cyberangriffs?

# Allgemeine Erkenntnisse

- Angriffe auf Verfügbarkeit (Ransomware) nehmen 2019 wieder zu
- Angriffe auf die Vertraulichkeit nehmen zu (Informationen, Berechtigungsnachweise / Credentials, Geistiges Eigentum)

# KMU Umfrage 2017: Ergebnisse der Umfrage (N=301)

- <10% hohes Risiko
- 15% fühlen sich schlecht geschützt
- 36% von erfolgreichen Attacken betroffen
- 80% haben Grundschutzmassnahmen umgesetzt (Malware-Schutz, Firewall, Patchmanagement, Backup)

- >50% ablehnend gegenüber Meldepflicht

# Wo stehen die KMU?

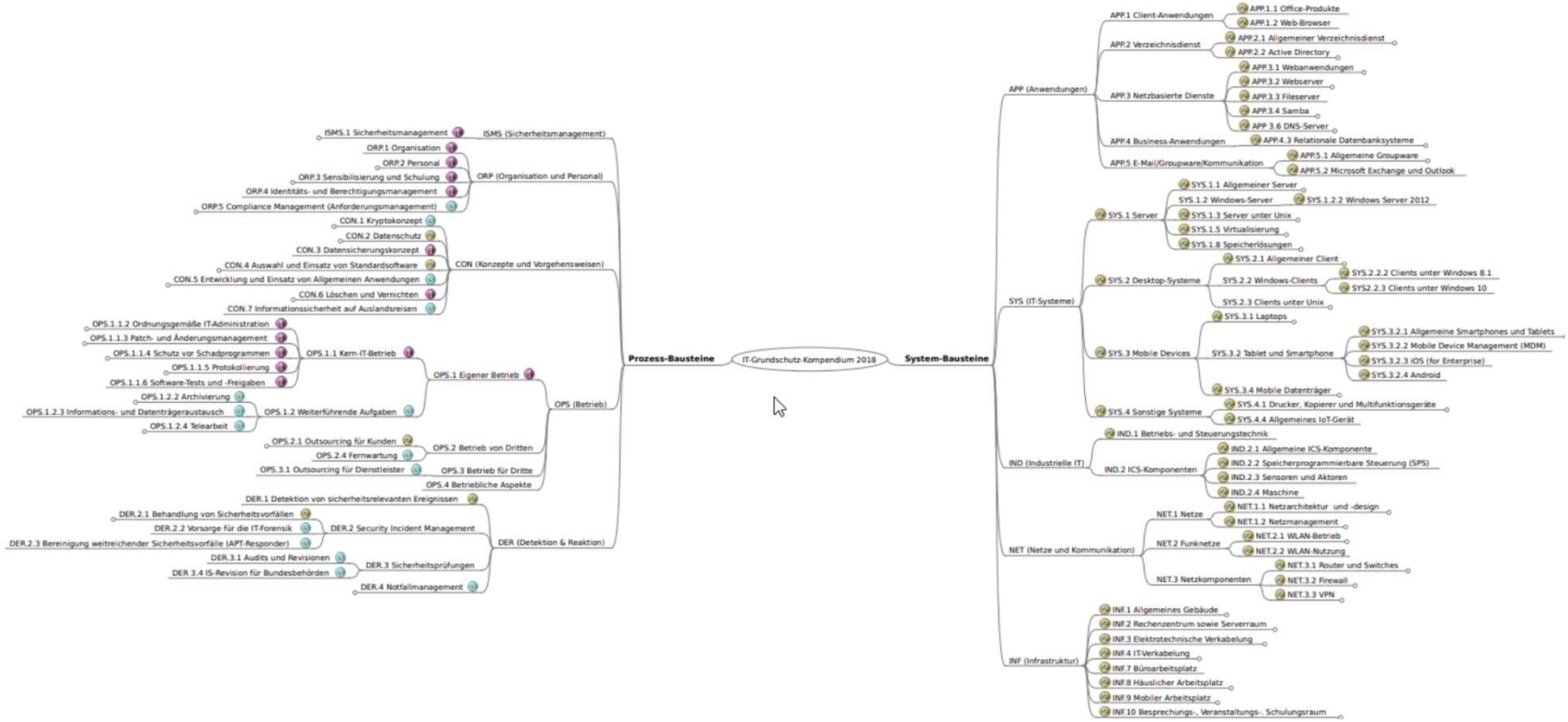
«Awareness ja, aber warum soll es gerade mich treffen?»

«Ich habe kein IT Risiko: das macht mein Provider seit Jahren – ich kenne ihn persönlich…»

«IT-Security ist zu teuer, inhouse Wissen habe ich nicht»

«IT-Sec.? Kein Problem: ich habe einen Virenscanner

# IT-Grundschutz-Kompendium 2018 | 1. Edition




Die Ziffern (1) bis (3) kennzeichnen die vorgeschlagene Bearbeitungsreihenfolge der Bausteine:

- R1: Diese Bausteine sollten vorrangig umgesetzt werden, da sie die Grundlage für einen effektiven Sicherheitsprozess bilden.
- R2: Diese Bausteine sollten als nächstes umgesetzt werden, da sie in wesentlichen Teilen des Informationsverbundes für nachhaltige Sicherheit erforderlich sind.
- R3: Diese Bausteine werden zur Erreichung des angestrebten Sicherheitsniveaus ebenfalls benötigt und müssen umgesetzt werden, es wird aber empfohlen, diese erst nach den anderen Bausteinen zu betrachten.

**Stand: Oktober 2017**

# Lösung: Outsourcing, Cloud, Managed Services

## SaaS/Managed Services?

## PaaS?

## IaaS?

# Herausforderung: Geteilte IT-Verantwortung

| Verantwortung | lokal | IaaS | PaaS | SaaS |
|---|---|---|---|---|
| Datenverantwortung (Sorgfalt, Rechenschaft) | | | | |
| Endpoint-Sicherheit | | | | |
| IAM: Kontrolle und Sicherheit | | | | |
| Kontrolle Anwendungslevel | | | | |
| Netzwerkontrolle | | | | |
| Host Infrastrukture | | | | |
| Physische Sicherheit | | | | |

+++ Flexibilität ---

Coud Benützer

Coud Provider

# …gibt es einen Grund Nicht in die Cloud zu gehen?

# Welche Gründe sprechen dafür, nicht in die Cloud zu gehen?

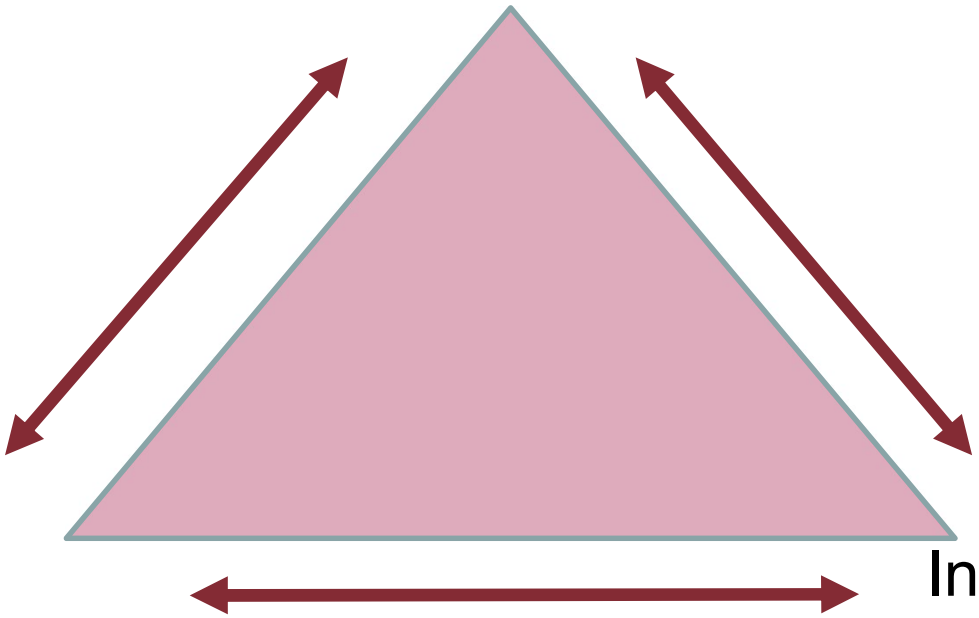
- **regulatorische Bestimmungen**
- **Vertragliche Gründe**
- Synchronisation der Stammdaten über verschiedene Applikationen hinweg
- **Hohe Verfügbarkeit: z.B. OT**
- **Lock-In Risiko**
- Kompatibilität des Change Management mit dem Cloud Provider
- Customizing, zu teuer oder unmöglich
- Sicherheit des Providers? Erlaubt er eine Überprüfung (vuln.-Scan, Pentests?)

# Drei Herausforderungen in der KMU-Welt

- Fehlende Business-IT-Risikoüberlegungen
- Cloud-Lösung= IT-Sicherheit = «Aus den Augen aus dem Sinn?»
- Bedenken und Ängste der KMU

# Business-IT-Security Alignment

Life-Cycle der Anwendungen



IT-Sicherheitsüberlegungen

Investitionsrisiken der Migration; u.a. Flexibilität, Customizing

# Aus den Augen aus dem Sinn?
# Aufgaben des Users:

- Regulatorische Auflagen
- Vertragliche Auflagen
- Keine Schatten-IT
- Keine Dark-Data
- Endpoint-Security
- Verschlüsselung der Daten
- Data Loss Prevention
- IA-Security Management (CASB, 2FA)
- **IT-Security-Organisation**
- Management dee SLA (Incident, legal compliance)

# Bedenken und Ängste der User

«Cloud?  Das ist nicht sicher, mein Server ist besser!»
«Ich habe alte Applikationen, die rühr ich nicht an!»
«Ich habe Kundendaten, die dürfen nicht in die Cloud!»
«Migration und Umstellung zu teuer und ich weiss nicht wie….»

# Fazit

## Wie bringe ich die KMU in die Cloud?

## Awareness: Cloud bringt auch Sicherheit-, Rechenschafts- und Sorgfaltspflichten

# Fragen?

# Inputs?

# Kritik?

# Beispiel: IAM

**Stufe Basic**:

- Sichere und verschiedene Passwörter für verschiedene Systeme (Applikationen wie ERP, CRM)
- Pro Endgerät ein Passwort
- Keine Passwortspeicherung auf gemeinsam genutzten System
- **Einschränkung von Admin.-Accounts auf IT-Verantwortliche**

# Beispiel: IAM

**Stufe Basic Plus**:

- Personalisieren sie alle Accounts
- System der geringsten Privilegien für alle Service-Accounts
- Managen sie permanent Zugriffsrechte und Benutzerkonten
- Kontrollsystem: verschiedene Passwörter für verschiedene Systeme
- Verschlüsselte Aufbewahrung von Admin.-Passwörtern

# Beispiel: IAM

**Stufe Risikobasiert**:

- Kontrolle über alle Logdaten
- 2FA (Zweifaktor-Authentisierung) implementiert
- Passwortzuteilung Rollen und nicht MA-basiert organisiert
- Single Sign On (integrierte IAM-Lösung)

# Grundlagen Netzwerksicherheit

| Bereich | Gefahr | Massnahmen |
|---|---|---|
| Protection | Exploit (Verwundbarkeit) | IPS, IDS, web application firewall (Disarm),**Sandboxing** |
| Protection | Payload (Schädlicher Code der Malware) | Virenscanner, IPS, IDS **Deep Pocket Inspection Sandboxing** |
| Detection | Daten-Kommunikation in & out Botnet; «No Callback» | Firewall, URL Filter DNS Filter **Traffic Anomaly Detection** |

# Beispiel: Netzwerksicherheit

**Stufe Basic Plus**:

- Netzwerksegregation oder Netzwerk-Outsourcing
- Logische Trennung von Bereichen mit OT (cyberphysische Geräte)
- Least Access & und Visibilität mit Internet
- UTM
- Firewall least outbound policy z.B. Drucker…
- Web Application Firewall

# Beispiel: Netzwerksicherheit

**Stufe Risikobasiert**:

- Traffic Control
- Traffic Anomaly Detection
- Benutzen Sie ein Tool um auch im Gästenetz die Authentifizierung zu ermöglichen

# Lessons learned

- Interne Umsetzung dieses KMU-Grundschutzes kostenintensiv
- IT-Grundschutz nicht skalierbar; Aufwand bleibt
- Ressourcen (mind. 1 IT-Sec.-Experte oft nicht vorhanden)
- Lösung: Cloud und Managed Services

# ‚sondern warum Sie nicht in die Cloud sollten

# Faktoren gegen Outsourcing und Cloud (SaaS) Lösungen

- regulatorische Bestimmungen, die eine Datenspeicherung und -Bearbeitung innerhalb eines spezifischen Rechtssystems verbieten
- vertragliche oder regulatorische Gründe gegen ein Outsourcing
- Vertraglich geregelte Möglichkeit, die Daten zu einem anderen Anbieter oder in-house zu verschieben (Lock-in Risiko)
- Technische und ökonomisch tragbare Lösung gegen Lock-in Risiken
- Notwendiges Customizing zu teuer, langwierig oder unmöglich
- Zu grosses Risiko, alte Systeme abzulösen
- der Provider erlaubt keine Verwundbarkeitstests oder Pentest

# Ist der Cloud-Provider sicher?

- Klären Sie Ihre Sicherheitsbedürfnisse und ob er diese erfüllen kann.
- Klären Sie, ob er diesen IKT-Grundschutz erfüllt
- SLA betr.
  - Legal Compliance
  - Security Management
  - Incident Management
  - Remote-Zugänge
  - Sicherheitsstandards
- **Verbindliche Zertifizierung für IT und IT-Sec. Provider**