Kritische Sicht auf die Cloud

Herbert.Leitold@a-sit.at

IT-Forum der österreichischen Krankenhausträger
Graz, 17.-18. Oktober 2019

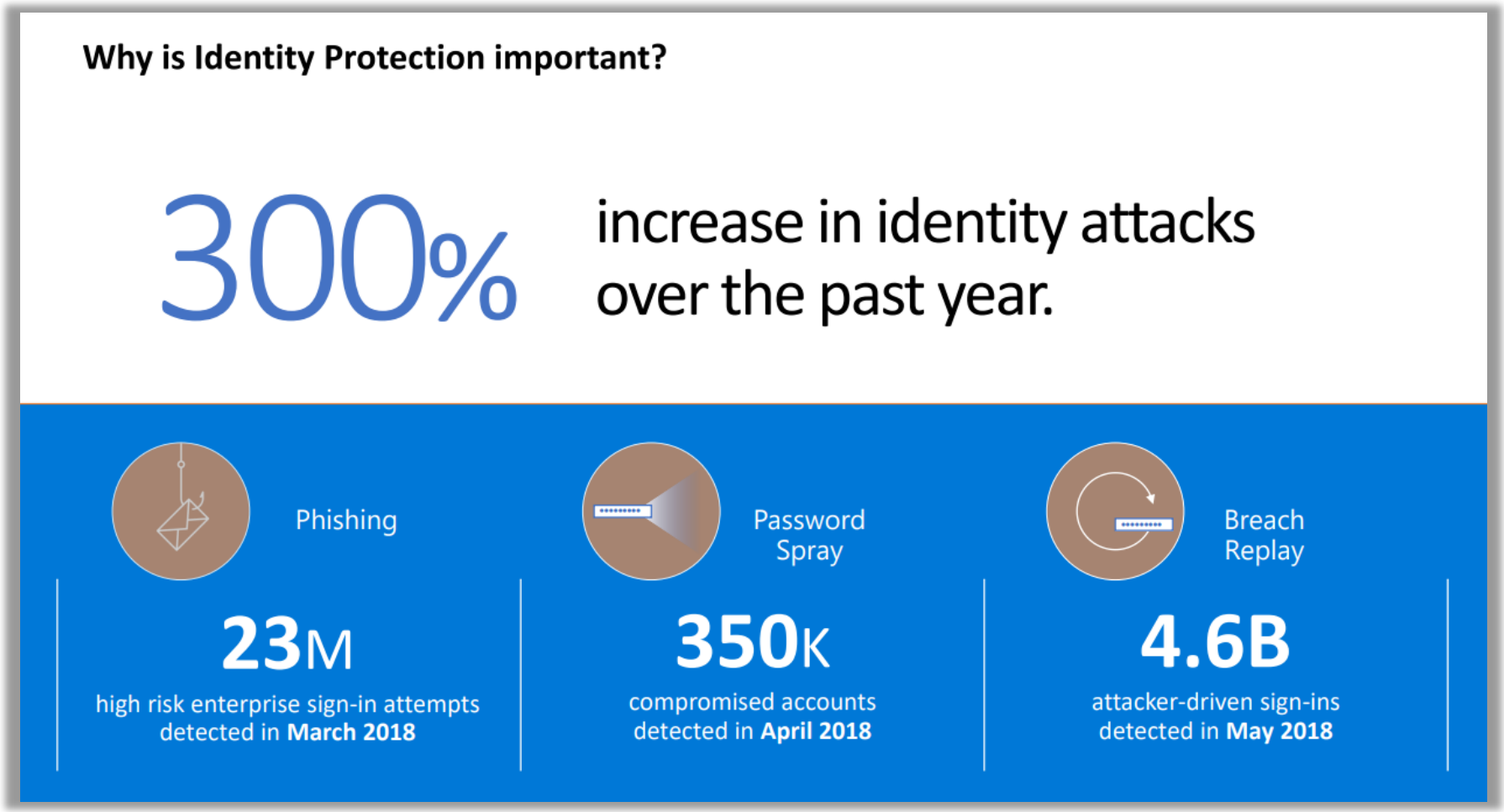
Inhalte

- Ausgewählte Sicherheitsfragen
- Zu betrachtende Bereiche
- Schlussfolgerungen

Inhalte

- Ausgewählte Sicherheitsfragen
  - ***Zahlen einiger Anbieter***
  - ***Was sind die Top-Bedrohungen?***
  - ***Problem geteilter Ressourcen?***
- Zu betrachtende Bereiche
- Schlussfolgerungen

Beispiel IDM: Microsoft



aus: Kim Cameron, Time to rebalance the web to benefit from user-centric security, ISSE'2018, Brüssel (11/2018)

Beispiel DDoS: Cloudflare

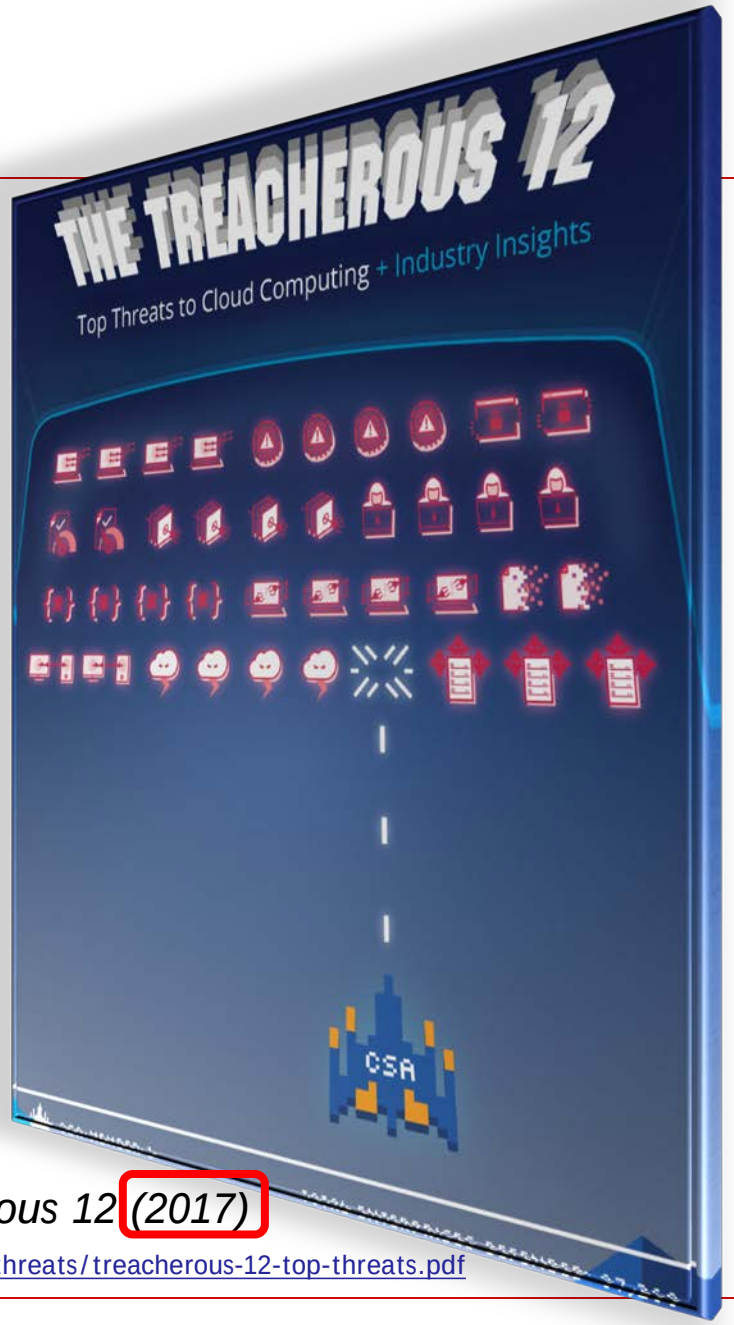
aus: 유지영, *Modern DDoS trends, AWS Summit Seoul (05/2019)*

Sind vorige Effekte Cloud-spezifisch?

- Die Zahlen sind „imposant und groß“, weil Anwendungen / Cloud „imposant und groß“
  - Beide Beispiele auch Alltag in Rechenzentren
  - Sowohl Cloud-Provider, als auch RZ-Betreiber sollten damit umgehen können
- Gibt es Cloud-spezifische Effekte?
  - Brechen der Isolation zwischen Tenants?
  - Aus gemeinsamer Nutzung von Elementen?

CSA: Die tückischen 12

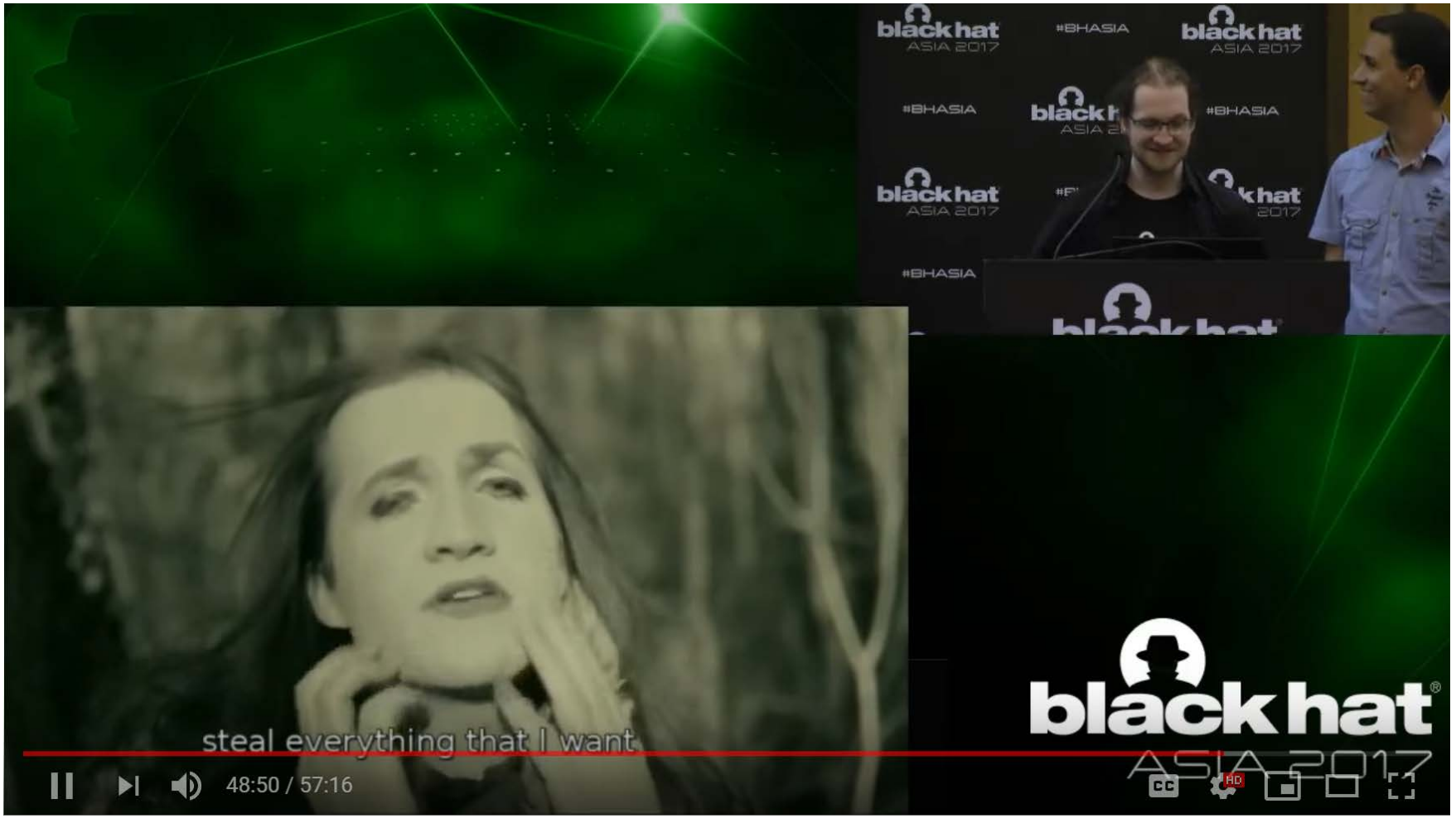
1. Data Breaches
2. Weak Identity, Credential & Access Mgmt.
3. Insecure APIs
4. System and Application Vulnerabilities
5. Account Hijacking
6. Malicious Insiders
7. Advanced Persistent Threats (APTs)
8. Data Loss
9. Insufficient Due Diligence
10. Abuse and Nefarious Use of Cloud Services
11. Denial of Service
12. Shared Technology Vulnerabilities



aus: Cloud Security Alliance, The Treacherous 12 (2017)

https://downloads.cloudsecurityalliance.org/assets/research/top-threats/treacherous-12-top-threats.pdf

Beispiel: Cache als verdeckter Kanal

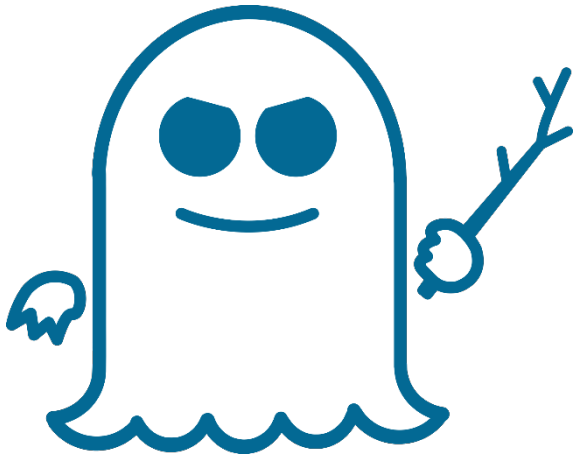


aus: Manuel Weber, Michael Schwarz, Hello from the other side, SSH over robust cache covert channels in the Cloud, Blackhat Asia 2017

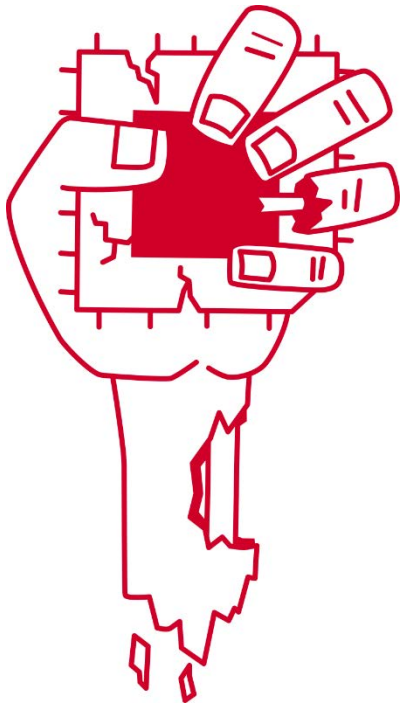
https://www.youtube.com/watch?v=6bCdFmehMSY&list=PLH15HpR5qRsWx4qw9ZIgmisHOcKG4ZcRS&index=8&t=3083s

Beispiel: Transiente Instruktionen

Meltdown
out-of-order processing



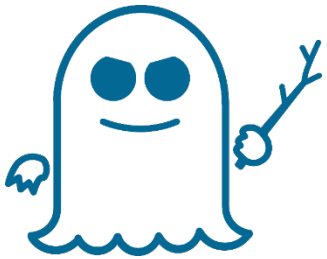
Spectre
speculative execution



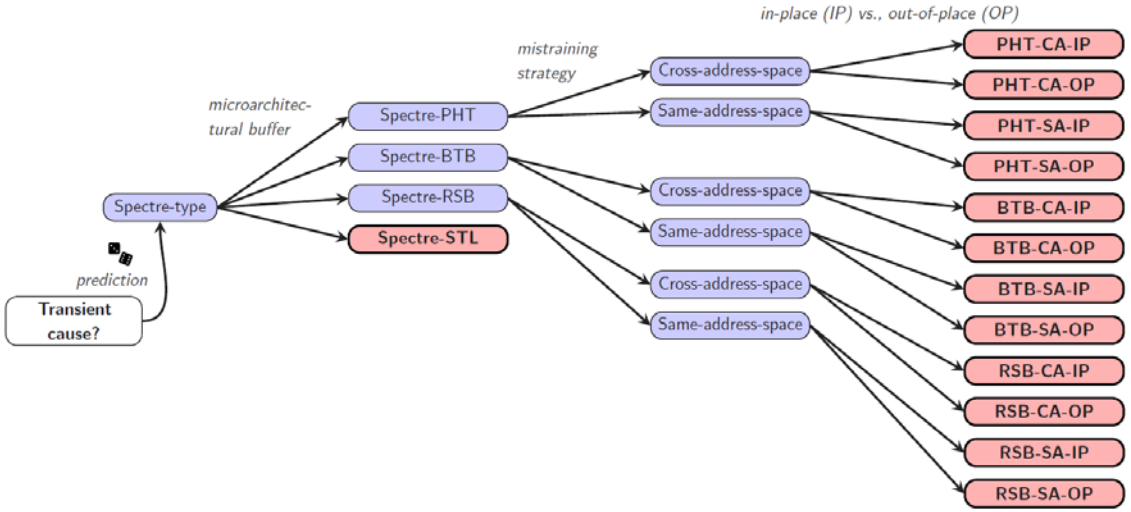
Zombieload
read fill buffers

u.a. von Daniel Gruß, Moritz Lipp und Michael Schwarz (2018)

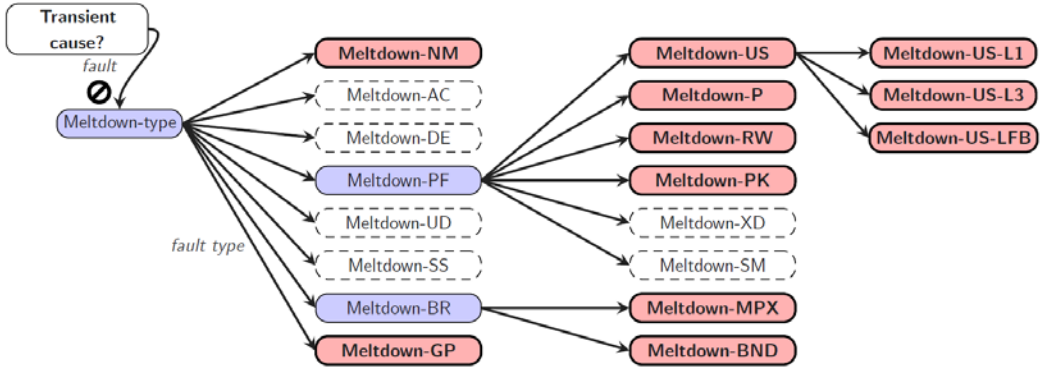
Basis weiterer Bedrohungen



Spectre-Varianten



Meltdown-Varianten



aus: Canella et.al., A Systematic Evaluation of Transient Execution Attacks and Defenses, 28th USENIX Security Symposium, CA, 2019

.. und Gegenmaßnahmen

Defense Evaluation	Penalty	Benchmark
KAISER/KPTI	0–2.6 %	System call rates
Retpoline	5–10 %	Real-world workload servers
Site Isolation	10–13 %	Memory overhead
InvisiSpec	22 %	SPEC
SafeSpec	-3 %	SPEC on MARSSx86
DAWG	1–15 %	PARSEC , GAPBS
SLH	29–36.4 %	Google microbenchmark suite
YSNB	60 %	Phoenix
IBRS	20–30 %	Sysbench 1.0.11
STIBP	30–50 %	Rodinia OpenMP, DaCapo
Serialization	62–74.8 %	Google microbenchmark suite
SSBD/SSBB	2–8 %	SYSmark 2018, SPEC integer
L1TF Mitigations	-3–31 %	SPEC

aus: Canella et.al., A Systematic Evaluation of Transient Execution Attacks and Defenses, 28th USENIX Security Symposium, CA, 2019

Inhalte

- Ausgewählte Sicherheitsfragen
- Zu betrachtende Bereiche
  - **Ausgewähltes zu rechtlichen, organisatorischen, wirtschaftl. und technischen Aspekten**
- Schlussfolgerungen

Kategorien nach BLSG AG Cloud

- Anleihen an BLSG Positionspapier

aus: BLSG AG Infrastruktur & Interoperabilität
https://www.ref.gv.at/Cloud-Computing.3451.0.html

Rechtliche Aspekte

- Datenschutz
  - z.B. Speicherort, Betroffenenrechte
- Vertragsrecht
- Vergaberecht
  - z.B. Standardverträge, Ausschreibungen
- Strafprozessrecht

Rechtlich: (anekdotisch) Standard-AGB

Árt. 57.10. **Erlaubte Nutzung; Sicherheitskritische Systeme.** Ihre Nutzung der Lumberyard-Materialien muss der AWS Acceptable Use Policy entsprechen. Die Lumberyard-Materialien sind nicht bestimmt für die Nutzung in Verbindung mit lebenswichtigen oder sicherheitskritischen Systemen wie die Nutzung für den Betrieb von medizinischen Anlagen, automatisierten Transport-Systemen, autonomen Fahrzeugen, Flugverkehrskontrolle, nuklearen Einrichtungen, bemannten Raumfahrzeugen oder die militärische Nutzung im Gefechtseinsatz.

Diese Beschränkung ist jedoch nicht anwendbar **im Falle des Auftretens einer weit verbreiteten Virusinfektion** (entsprechend der Festlegung des United States Centers for Disease Control oder Nachfolgeorganisationen), die durch Bisse oder Stiche oder durch den Kontakt mit Körperflüssigkeiten übertragen wird, die die **Wiederbelebung von Leichen zur Folge hat, die dann versuchen, lebendiges menschliches Fleisch, Blut, Hirn- oder Nervengewebe zu verzehren, und die voraussichtlich zum Untergang der entwickelten Zivilisation führen wird**

aus: AWS Service Terms (Version 26.6.2019)
https://d1.awsstatic.com/legal/awsserviceterms/AWS%20Service%20Terms%20-%20German%20Translation.pdf

Organisatorisches

- Standardisierung der IT
  - Potentiell organisatorische Vorteile
- Strukturelle Abhängigkeiten
  - Aber MultiStack / Multi-Cloud Lösungen
- Kostenvergleiche
  - Schwierig, wenn interne Kosten nicht bekannt

Wirtschaftliches

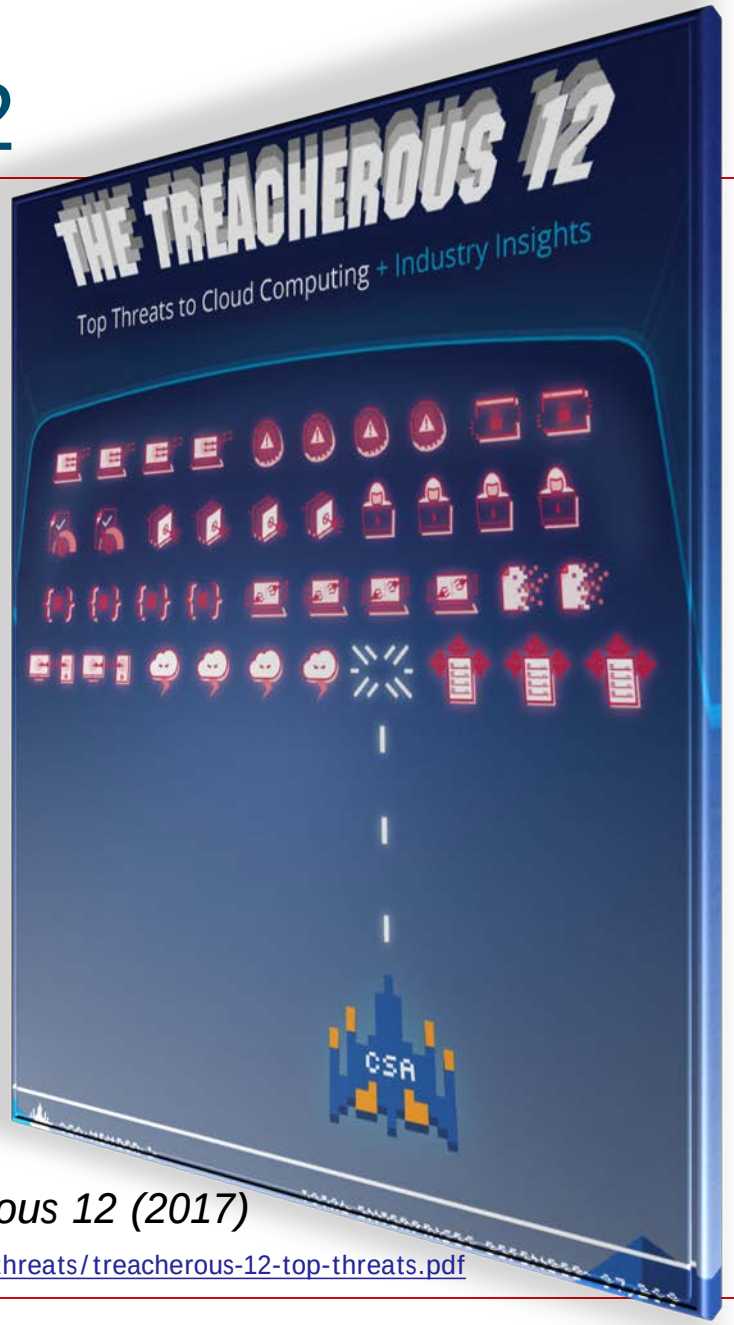
- Standardisierte Dienste
  - Typisch günstiger in hoher Qualität
- Komplexe Services und Anpassungen
  - Im öffentlichen Sektor oft notwendig
  - Skaleneffekte nicht immer klar
- Private Clouds
  - Massive Skalierung nicht immer gegeben

Technisches

- Standards und Normen
- Sicherheit
  - Schutzziele
  - Herkömmliches wie Vertraulichkeit, Integrität, Authentizität, Verfügbarkeit
  - vgl. Cloud Security Alliance Top-12 Threats
- Zertifizierungen als Qualitätsmerkmal

Wieder: CSA tückische 12

1. Data Breaches
2. Weak Identity, Credential & Access Mgmt.
3. Insecure APIs
4. System and Application Vulnerabilities
5. Account Hijacking
6. Malicious Insiders
7. Advanced Persistent Threats (APTs)
8. Data Loss
9. Insufficient Due Diligence
10. Abuse and Nefarious Use of Cloud Services
11. Denial of Service
12. Shared Technology Vulnerabilities



aus: Cloud Security Alliance, The Treacherous 12 (2017)

https://downloads.cloudsecurityalliance.org/assets/research/top-threats/treacherous-12-top-threats.pdf

Empfehlung zu Weiterführendem

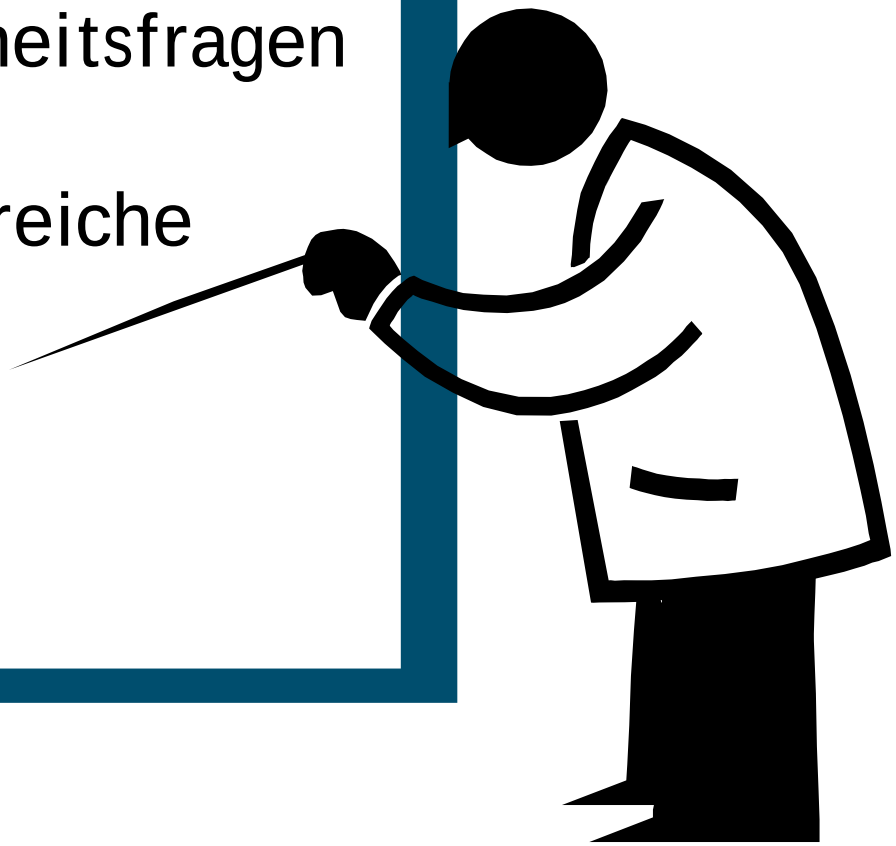
- Cloud Computing Kompass
  - Umfassender Überblick zu Standards im Umfeld Cloud-Computing

Cloud-Computing Kompass (2018)

https://www.onlinesicherheit.gv.at/service/technologie-trends/Cloud-Computing-Kompass.pdf

Inhalte

- Ausgewählte Sicherheitsfragen
- Zu betrachtende Bereiche
- Schlussfolgerungen



Schlussfolgerungen

- Cloud ist in allen IT-Bereichen angekommen
- Public Cloud Services verfügen auch über gute Security-Maßnahmen und -Teams
- Schwachstellen können natürlich trotzdem vorkommen und sind zu bedenken

Danke für Ihre Aufmerksamkeit!

Herbert.Leitold@a-sit.at

IT-Forum der österreichischen Krankenhausträger
Graz, 17.-18. Oktober 2019