Deloitte.

Digitalisierung – Cloud – Security

Ein großer Bogen in die Zukunft

Ellen Dankworth | it-sa 09.10.2019

it sa

Cloud setzt sich durch

Insbesondere Cloud Technologien stellen die Unternehmen vor neue Herausforderungen in Fragen der Informationssicherheit.

- über 200 Mrd. Geräte miteinander verbunden[1]
- 85% aller neu entwickelten Software bereits auf Cloud-Basis[2]
- Cloud als wichtigste Technologie für die Digitalisierung[3]
- Laut BMWi nutzen 43% der deutschen Unternehmen Cloud-Computing

Amazon Web Services: Tausende virtuelle Festplatten frei zugänglich im Netz

Ein Forscher fand tausendfach offen zugängliche Elastic Block Store-Volumes mit vertraulichen Daten im Netz, wo sie sich beliebig durchsuchen lassen.

Lesezeit: 2 Min. In Pocket speichern

Hacker kapern Tesla-Server zum Schürfen von Kryptowährung

Die Cloud-Umgebung des E-Autobauers Tesla wurde offenbar gehackt. Die Hacker hatten es aber nicht auf Unternehmens-Daten abgesehen, sondern benutzten die Rechenkapazität der Server für Crypto-Mining.

Lesezeit: 1 Min. In Pocket speichern 31

(Bild: Pixabay / CC0)

21.02.2018 11:27 Uhr

Von Oliver Bünte

Capital One: Hackerin prahlt mit Bank-Hack mit 100 Millionen Betroffenen

Das FBI hat eine Frau angeklagt, die damit geprahlt haben soll, eine Bank gehackt zu haben. Es gibt 100 Millionen Betroffene in den USA, 6 Millionen in Kanada.

Lesezeit: 2 Min. In Pocket speichern 148

Vorankündigung der Eröffnung eines Bank-Cafés im Vorjahr der nun gehackten Bank Capital One (Bild: Phillip Pessar CC BY 2.0)

30.07.2019 09:45 Uhr

Von Daniel AJ Sokolov

Cloud bietet Chancen und Herausforderungen zugleich

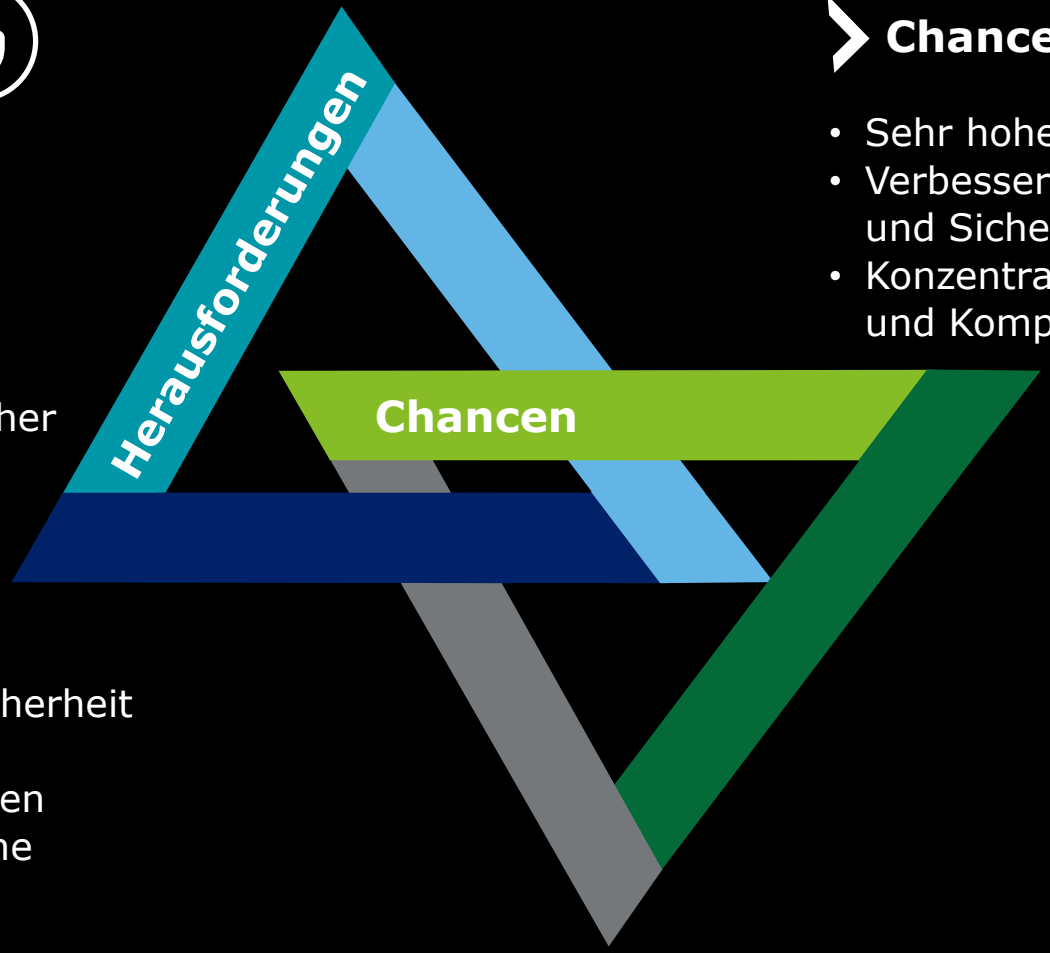
Die Nutzung von Cloud Technologien kann ein entscheidender Wettbewerbsvorteil sein, birgt gleichzeitig aber Herausforderungen für die Informationssicherheit.

Herausforderungen

- Zunehmender Kostendruck
- Zeitdruck durch immer schneller werdende Entwicklungs- und Innovationszeiten
- Bedarf nach hochqualifizierten Mitarbeitern
- Unsicherheiten bzgl. regulatorischer Anforderungen (z.B. DSGVO)

Unsicherheiten

- Ganzheitliche Informationssicherheit
- Awareness der Mitarbeiter
- Dezentrale Verantwortlichkeiten
- Vertragliche und regulatorische Fragestellungen



Chancen

- Sehr hohe Skalierbarkeit
- Verbesserung der Transparenz und Sicherheit
- Konzentration auf Kerngeschäft- und Kompetenzen

Zunehmende Vernetzung ändert die Bedrohungslage

Cyber-Sicherheit ist sowohl inhärenter Bestandteil als auch Voraussetzung für das erfolgreiche Gelingen von Digitalisierung.

Jedes Unternehmen, das online Geschäft treibt, ist potentiell Opfer von Cyberkriminalität

Kleine und mittelständische Unternehmen (KMU) besonders attraktiv für Angreifer

- Weniger Ressourcen
- Mangel an erforderlichem Know-how
- Wenig Erfahrung mit Cloud Technologien

steigende Anzahl von Cyber-Angriffen

Cyber-Sicherheit...

...als inhärenter Bestandteil von Digitalisierung

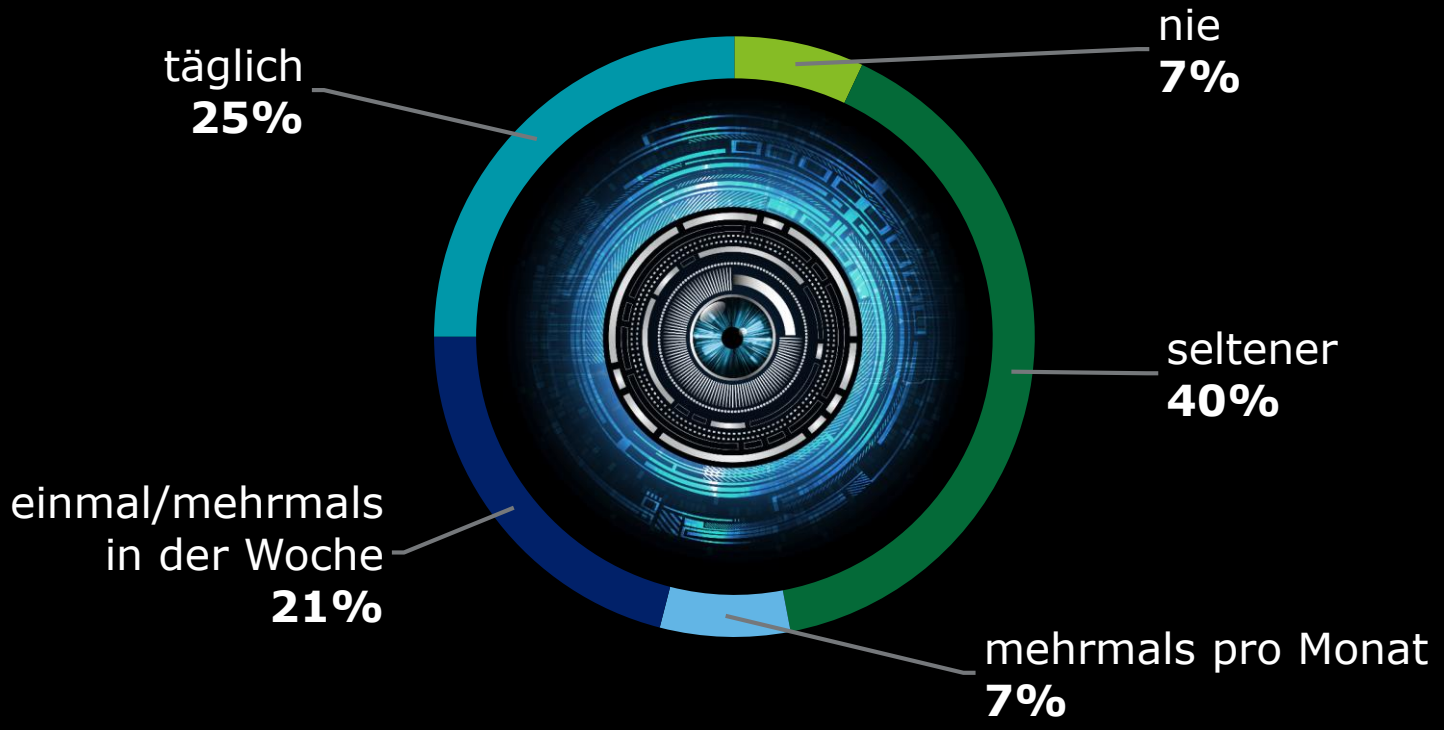
...als Voraussetzung für das erfolgreiche Gelingen von Digitalisierung

Bis 2022 könnten 95% der Cloud Sicherheitsmängel vom Anwender selbst verursacht werden (Gartner)

Aktuelle Lage der IT-Sicherheit in Deutschland

Service Provider werben mit den Vorteilen der Cloud – diesen stehen jedoch die Unsicherheiten der Kunden im Hinblick auf den Datenschutz gegenüber.

Wir haben gefragt: Wie häufig ist Ihr Unternehmen IT-Angriffen ausgesetzt, durch die Ihr Unternehmen ausspioniert oder geschädigt werden soll?



Vergleich 2013 → 2018

Täglich bis mehrmals pro Woche

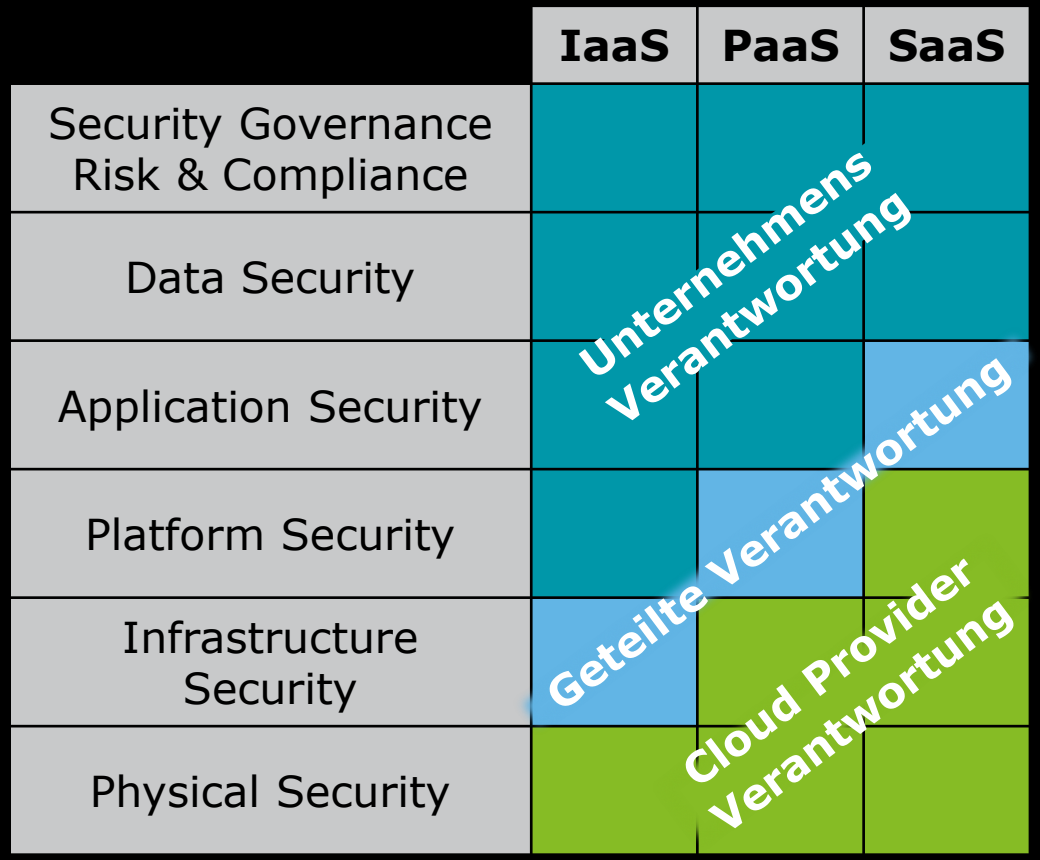
46%
2018

25%
2013

Wahrgenommene Häufigkeit von IT-Angriffen auf Unternehmen in Deutschland, Deloitte: „Cyber Security Report 2018" unter: https://www.deloitte.com/de/de/pages/risk/articles/cyber-security-report.html

Unterschiedliche Service-Modelle implizieren veränderte Verantwortlichkeiten

Das Shared Responsibility Model verdeutlicht die geteilte Verantwortung für Sicherheit – die abschließende unternehmerische Verantwortung verbleibt beim Kunden.



z. B. Sicherheits-anforderungen

z. B. Verschlüsselung von Daten

z. B. Patchen von Applikationen

z. B. Berechtigungs-konzepte

z. B. Netzwerk-konfiguration

z. B. Data Center Security

Security IN the Cloud
Der Kunde ist verantwortlich für die Sicherheit **in** der Cloud

Security OF the Cloud
Der Cloud Service Provider ist verant-wortlich für die Sicherheit der Cloud

Die abschließende Verantwortung für Datensicherheit verbleibt grundsätzlich beim Kunden!

Shared Security Model; *Certified Cloud Security Professional, Official (ISC)² Student Guide 3rd Edition, Page 411.*

Wie die Informationssicherheit bei Public Cloud Service Providern nachweisen?

Effektive Schutzmaßnahmen und zugleich eine wirtschaftliche Gestaltung der Cloud Services sichern die Konkurrenzfähigkeit von KMU.

Hürden bei der Sicher-stellung von Informations-sicherheit bei Public CSP

- Komplexe internationale Verträge
- Mangelnde Transparenz über Schutzmaßnahmen
- Unklares Zusammenspiel zwischen Provider und Kunde
- Limitierte Verhandlungsmöglichkeiten

Audit Reports als Nachweis über Schutzmaßnahmen

- System and Organization Controls 2 (SOC 2) Type 2
- ISO 27001 Code of Practice für Informationssicherheit
- BSI Cloud Computing Compliance Controls Catalogue (C5)

- **Effektiven Schutz gewährleisten**
- **Cloud Services wirtschaftlich gestalten**

Konkurrenzfähigkeit der KMU sichern

Beispiele zu inhaltlichen Herausforderungen der verschiedenen Servicemodelle

Abhängig vom Servicemodell entstehen unterschiedliche Fragestellungen zur Informationssicherheit.

Software-as-a-Service

Datenkritikalität

- Wie kritisch sind die Daten, die in der Cloud verarbeitet werden sollen?
- Welche Regularien gelten?
- Welche Anforderungen habe ich an den Schutz der Daten?

Regularien

- Wo ist der Sitz des Anbieters?
- Verpflichtet er sich zur Einhaltung relevanter Regularien?
- Wo ist der Speicherort der Daten?

Nachweise

- Welche Audit Reports stellt der Provider bereit?
- Sind weitere Audit-Rechte vertraglich geregelt?

Infrastruktur-as-a-Service

Architektur

- Wie soll eine Trennung und Zonierung erfolgen?
- Wie wird diese technisch umgesetzt und überwacht?

Berechtigungsmanagement

- Welche technischen Zugriffsmöglichkeiten sollen bestehen?
- Wie sieht das Rollen- und Rechtekonzept aus?

Monitoring

- Wie wird die Einhaltung von Vorgaben überwacht?
- Wie werden Schwachstellen erkannt?

Plattform-as-a-Service

Schlüsselmanagement

- Wer hat die Hoheit über Master Keys?
- Wie ist das Lebenszyklus Management?
- Wo und wie werden Schlüssel gespeichert?

Development & Deployment

- Welche Images werden genutzt?
- Wie erfolgt die Kontrolle vor Deployments?

Schrittweise Umsetzung von Cloud Security

Wie Cloud Security schrittweise ganzheitlich auch in kleinen und mittelständischen Unternehmen eingeführt werden kann.

Transparenz schaffen

- Welche Cloud-Services werden genutzt?
- Welche Daten sind heute schon in der Cloud?
- Wie kritisch sind diese Daten?

Anforderungen prüfen

- Welche Anforderungen existieren an den Schutz von Daten, z. B. aus Kriterien-katalogen wie BSI C5 oder ISO 27001

Risiken analysieren

- Welche Risiken ergeben sich durch die Cloud Nutzung?
- Wie können diese reduziert werden?

Zielbild festlegen

- Welche Provider erfüllen die Sicherheits-anforderungen?
- Welche Anwen-dungsbereiche sind geeignet für Cloud?

SaaS - Fokus auf **Überwachung** von Sicherheitsmaßnahmen

IaaS und **PaaS -** Fokus auf **Umsetzung** von Sicherheitsanforderungen

Regelmäßige „Awareness-Trainings"

Kontinuierliches Security Monitoring

Deloitte.

Ellen Dankworth
Senior Manager

Deloitte GmbH
Kurfürstendamm 23
10719 Berlin
Deutschland

Phone: +49 (0) 30 25468 5517
Mobile: +49 (0) 151 5800 3188
edankworth@deloitte.de

www.deloitte.com/de

Vielen Dank.

Quellen und Bildnachweise

[1,2,3] Deloitte: „Was kann die Cloud wirklich?“, unter: https://www.deloitte.com/de/de/pages/technology/articles/Cloud.html

[3] Abbildung [1] Heise Artikel „Amazon Web Services: Tausende virtuelle Festplatten frei zugänglich im Netz“, unter: https://www.heise.de/security/meldung/Amazon-Web-Services-Tausende-virtuelle-Festplatten-frei-zugaenglich-im-Netz-4493402.html

[4] Abbildung [2] Heise Artikel „Hacker kapern Tesla Server zum Schürfen von Kryptowährung“, unter: https://www.heise.de/newsticker/meldung/Hacker-kapern-Tesla-Server-zum-Schuerfen-von-Kryptowaehrung-3974117.html

[5] Abbildung [3] Heise Artikel „Hackerin prahlt mit Bank Hack mit 100 Millionen Betroffenen“, unter: https://www.heise.de/newsticker/meldung/Hackerin-prahlt-mit-Bank-Hack-mit-100-Millionen-Betroffenen-4483011.html

Deloitte.