

"TeleTrust-Konferenz 2021"

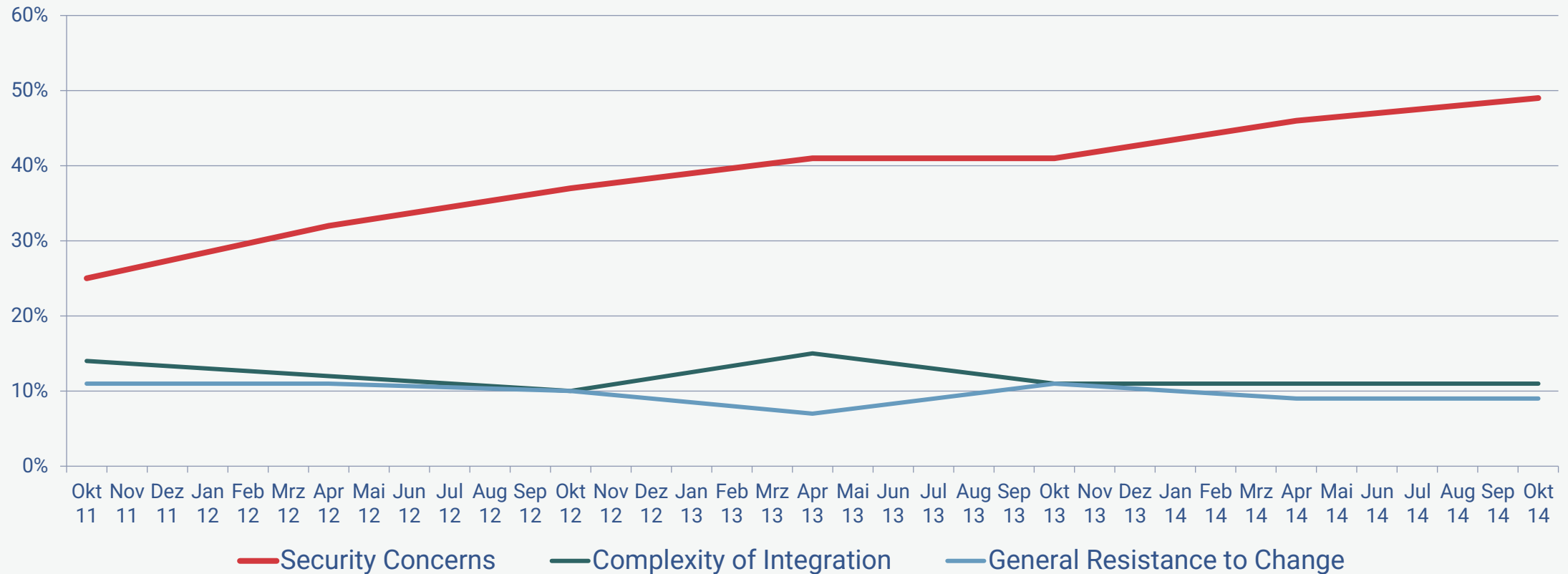
Berlin, 25.11.2021

Cloud Security Aktueller Stand der Technik"

Oliver Dehning

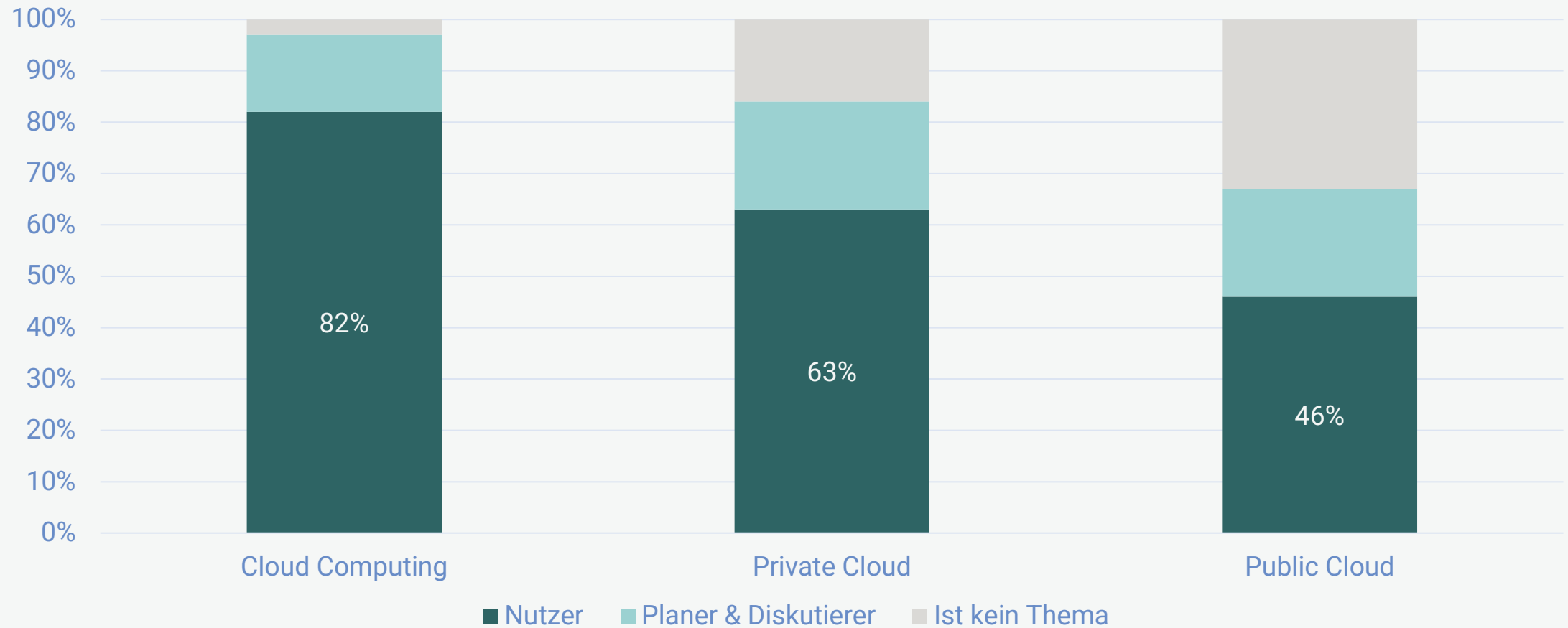
Reasons for not using the Cloud

Of those companies not currently using Cloud, what is the most important reason why?



451 Research, 2014

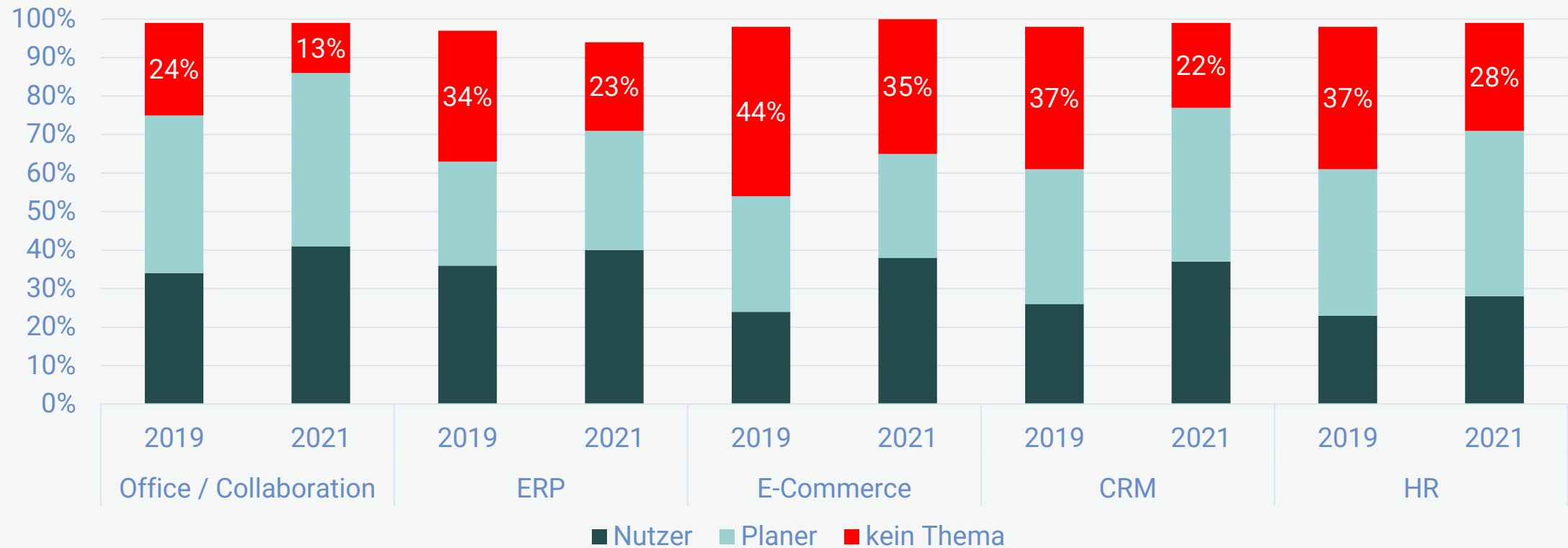
Cloud-Nutzung in Unternehmen in D



BITKOM / KPMG: Cloud-Monitor 2021

Corona treibt die Cloud-Nutzung voran

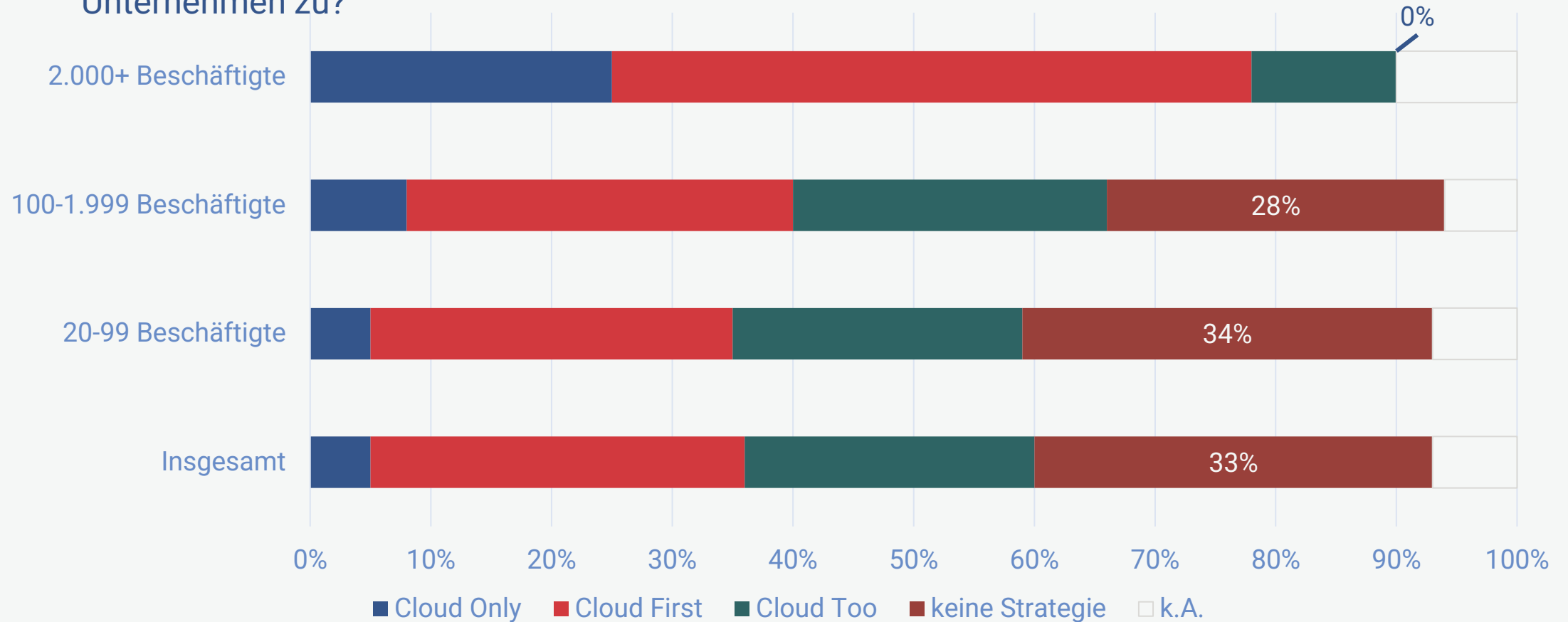
Welche der folgenden Anwendungen nutzt Ihr Unternehmen bereits aus der Public Cloud?



BITKOM / KPMG: Cloud-Monitor 2021

Transformationsstrategien

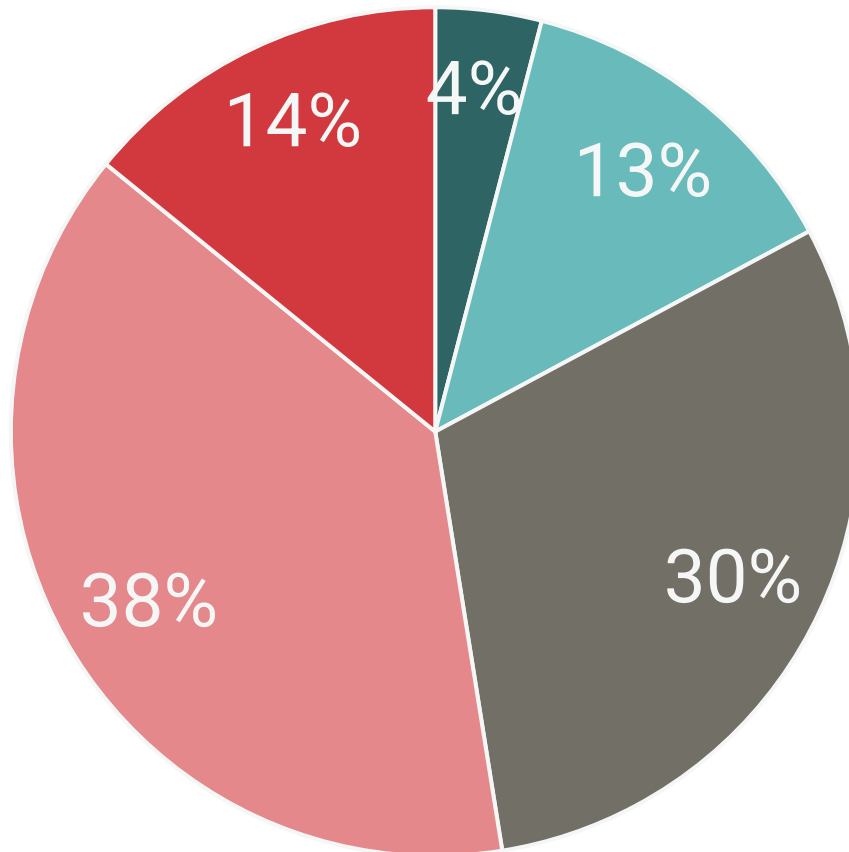
Welche der folgenden Strategien trifft am ehesten auf die Cloud-Transformation in Ihrem Unternehmen zu?



BITKOM / KPMG: Cloud-Monitor 2021

Risk of Cloud Security Breaches

Compared to traditional, on-prem IT environments, would you say the risk of security breaches in a public cloud environment is ...



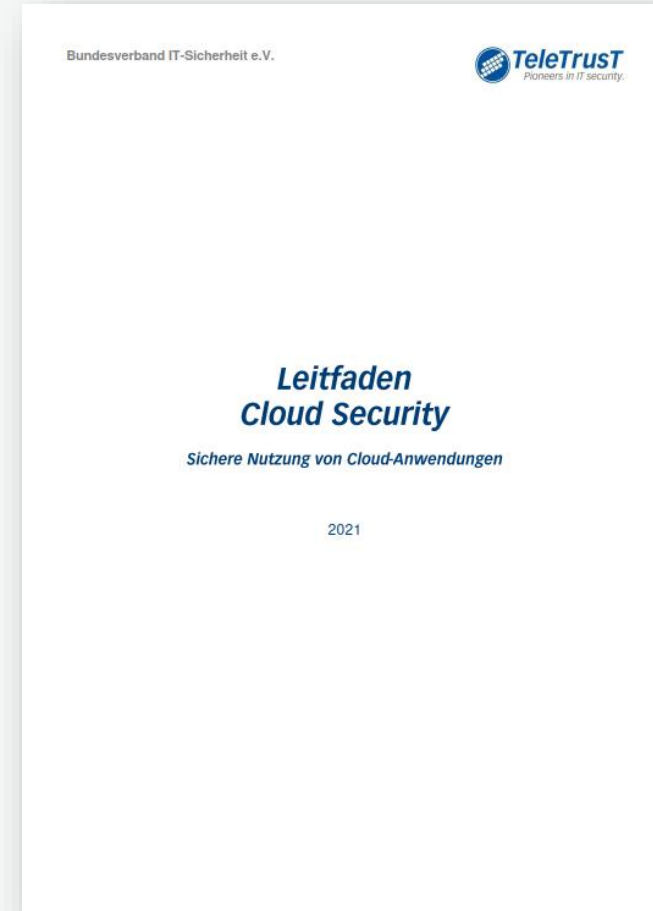
■ significantly lower ■ somewhat lower ■ about the same
■ somewhat higher ■ significantly higher

Source: Cybersecurity Insiders: 2020 Cloud Security Report

TeleTrust Leitfaden Cloud Security

Autoren:

- Karsten Bartels, HK2 Rechtsanwälte
- Dr. Yvonne Bernard - Hornetsecurity
- Stefan Cink, Net at Work
- Marion Demand, BSI
- Stefan Gora, securvo
- Peter Hansemann, ICN
- Dr. Hubert Jäger, Digital Trust Innovations
- Malte Kahrs, MTRIX
- Dr. Dennis-Kenji Kipker, Universität Bremen
- Alexander Kurz, eperi
- Tomasz Lawicki, m3 management consulting
- Anna Katharina Pfeiffer, esatus
- Dr. Ralf Rieken, Uniscon
- Peter Rost, secunet
- Yvonne Simon, eperi
- Andras Weiss, eco
- Oliver Dehning





Klassische Bedrohungen

- Hardware-Fehler
- Sicherheitslücken in der Software
- Konfigurationsfehler
- Sicherheitslücken beim Nutzer
- Malicious Insider
- Allgemeine Betriebsrisiken
- ...

Allgemeine Betriebsrisiken ...

- Brand in einem Rechenzentrum in Straßburg (Cloudprovider OVH)
- Ein RZ komplett abgebrannt, ein weiteres teilweise
- 12.000 Server für Private Cloud
- 15.000 direkt betroffene Kunden
- Ausfälle von mehr als 3,5 Mio. Websites und fast einer halben Million Domains.

Quellen: Reuters, funkschau, 2021

Millions of websites offline after fire at French cloud services firm

By Mathieu Rosemain, Raphael Satter

3 MIN READ



PARIS (Reuters) - A fire at a French cloud services firm has disrupted millions of websites, knocking out government agencies' portals, banks, shops, news websites and taking out a chunk of the .FR web space, according to internet monitors.



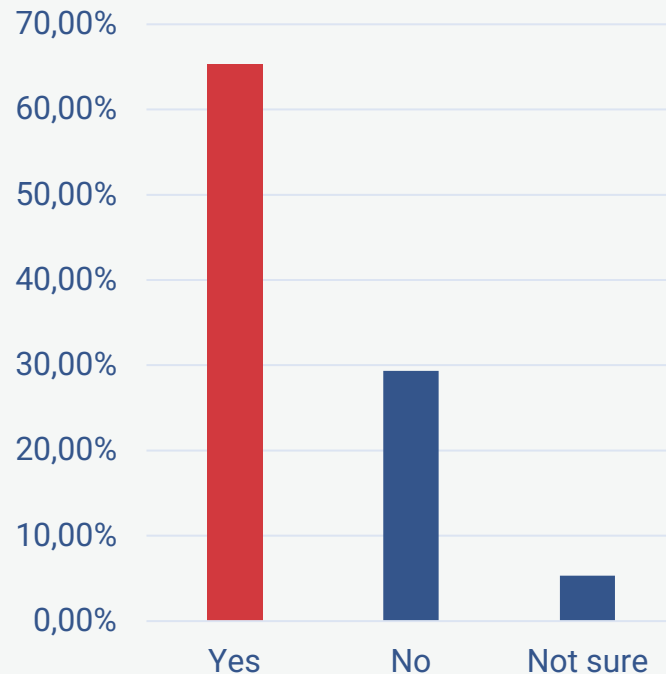
Cloud-spezifische Herausforderungen

- Auflösung des Perimeter
 - Tatsächlicher Ort der Daten nur schwer kontrollierbar
 - Inkonsistente Sicherheitsmechanismen
 - Große Angriffsfläche
- Management Interfaces offen zum Internet
- Mehr-Mandanten-Systeme
 - Datentrennung, Isolationsfehler
- Loss of Governance, Kontrollverlust
 - Datenlöschung nur schwer kontrollierbar
 - Nachvollziehbarkeit von Verarbeitungswegen
 - Leistungsverweigerung des Anbieters
- Massierung von Daten
 - Cloud-Services sind ein attraktives Angriffsziel
- Compliance-Risiken, Datenschutz
- Vendor Lock-In

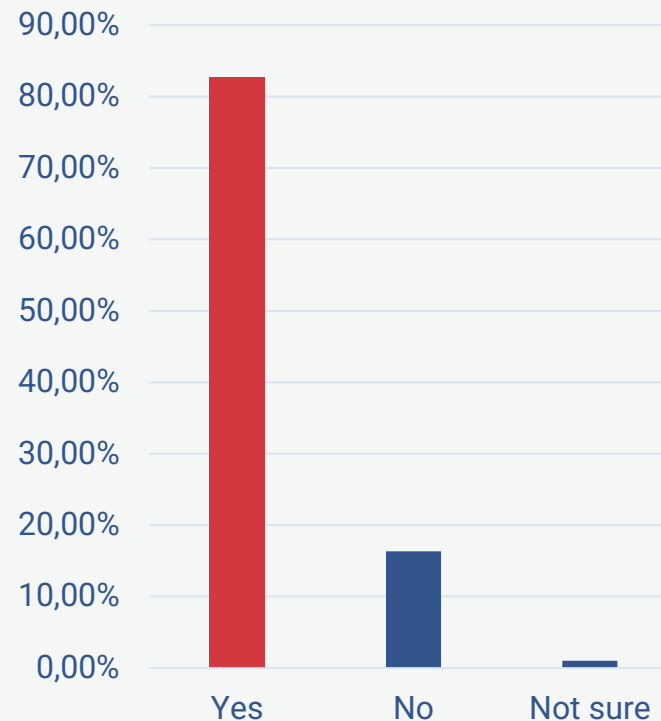


Privileged Cloud Credentials are the new Key to the Kingdom

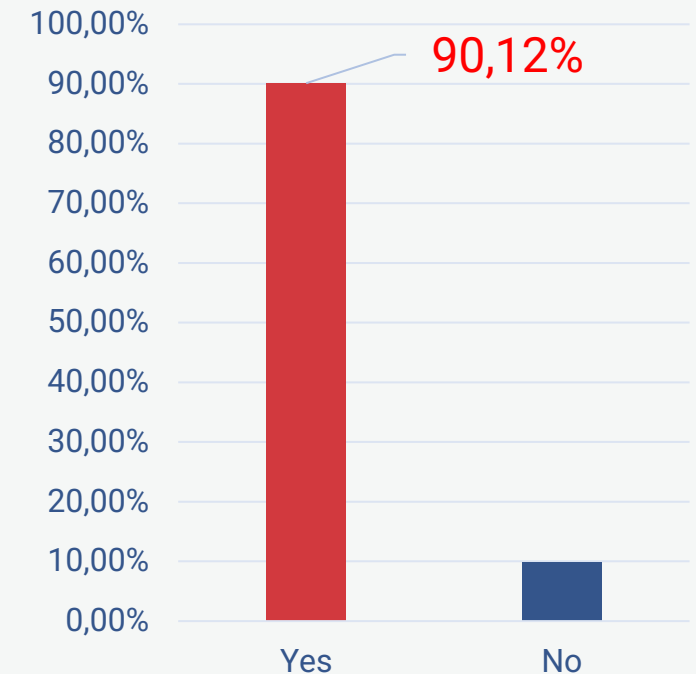
In the last year, have you identified any attempted cyberattacks on your cloud environment?



If yes, were any of the attacks successful in compromising your cloud environment?

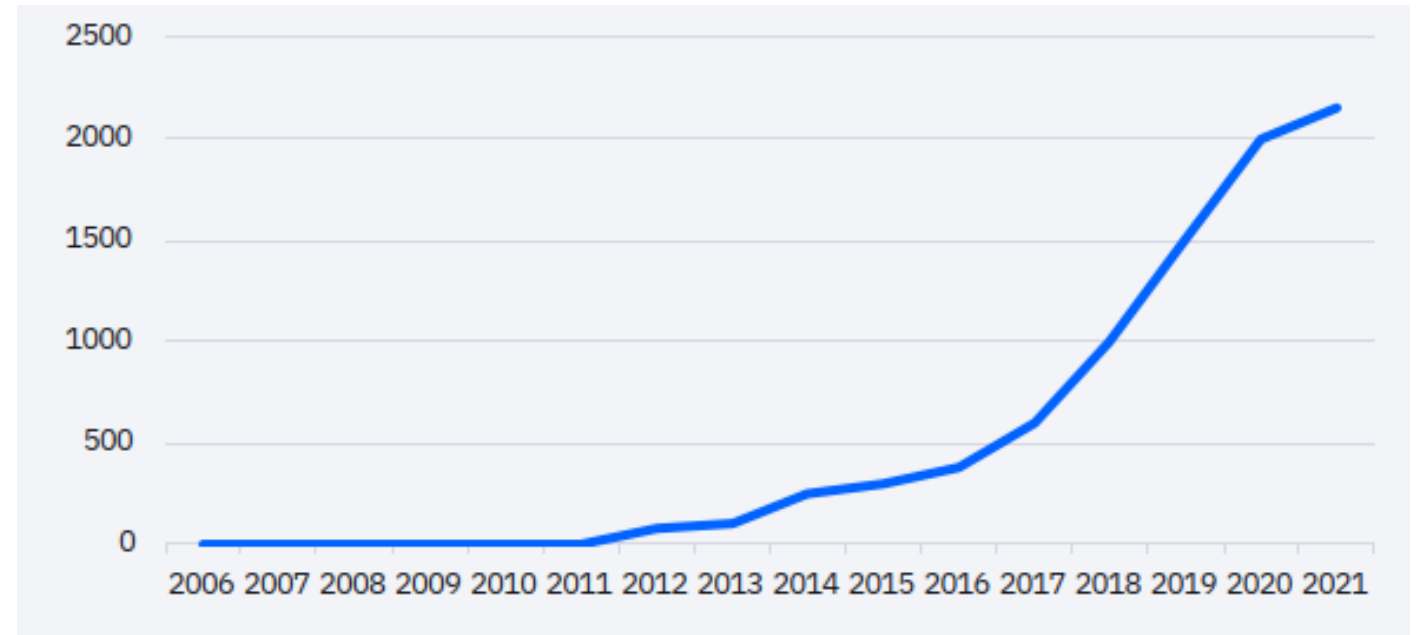


If yes, did compromised administrative credentials play a role in the attempted cyberattack?



Source: Centrify, 2021

Number of cloud vulnerabilities tracked by X- Force



2021 IBM Security X-Force Cloud Threat Landscape Report

Cloud Hacks

Dropbox, 2012 / 2016:

- Nutzerdaten von mehr als 68 Mio. Accounts veröffentlicht
- Der Einbruch war seit 2012 bekannt, aber erst 2016 wurde das wirkliche Ausmaß öffentlich

LinkedIn 2016:

- Diebstahl von 167 Mio. Benutzernamen und Passwörtern

Solarwinds, 2020:

- Angreifer schleusten Malware-Code Update-Binärdateien ein.
- 18 tausend Kunden zogen automatisiert Updates mit Trojanern, die Backdoors in ihren Systemen öffneten.

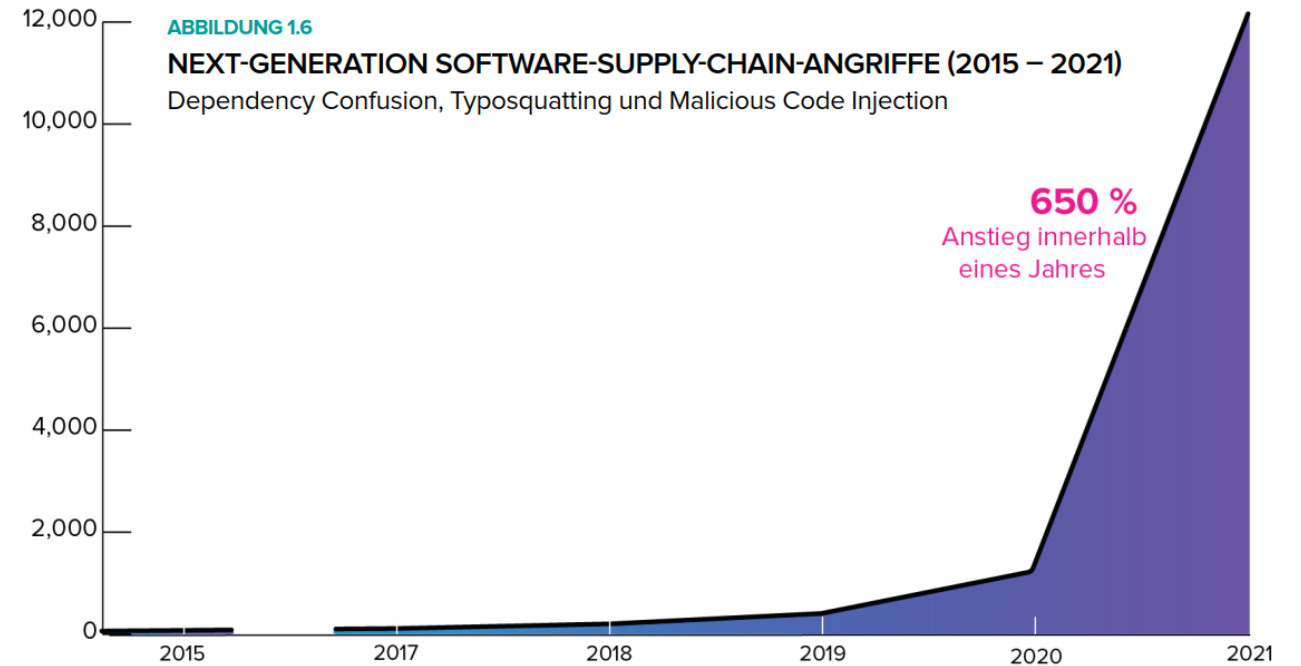
Kaseya, 2021:

- Ransomware wurde über einen Zero-Day-Exploit in eine Plattform für Remote Monitoring und Management eingeschleust, die von MSPs genutzt wird.
- 1500 Kunden dieser MSPs waren betroffen.

Cloud & Software Supply Chain

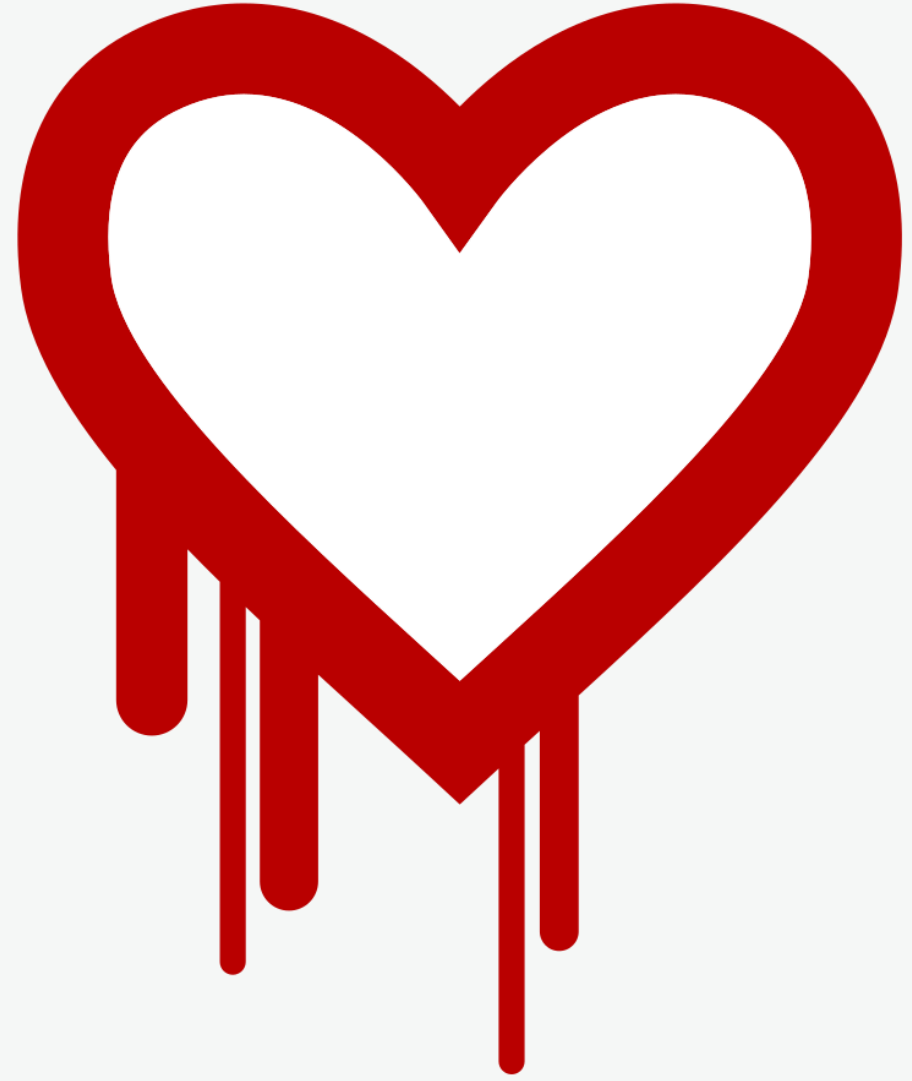
- Identity & Access Management
- Application Software
- Software Libraries
- Microservices
- Container Services
- Operating Systems
- Virtualization Layer
- Computer Hardware

11/30/2021



Heartbleed Bug

- Programmierfehler in älteren Versionen von OpenSSL
- Entdeckt und behoben im Frühjahr 2014
- Ermöglichte das Auslesen von Zugangsdaten und Serverzertifikaten





Cloud (in)security?

Cloud Computing macht Sicherheit günstiger und besser

“ ... put simply, all kinds of security measures are cheaper when implemented on a larger scale. Therefore the same amount of investment in security buys better protection.”

“... the ability of the cloud provider to dynamically reallocate resources for filtering, traffic shaping, authentication, encryption, etc, to defensive measures (e.g. against DDoS attacks) has obvious advantages for resilience.”

ENISA: Cloud Computing Security Risk Assessment; 2009

Cloud Computing verbessert die Sicherheit



Mehrere Rechenzentren



Robuster RZ-Betrieb



Massiv redundante Systeme



Erprobte fail-over Mechanismen



Physischer Zugangsschutz



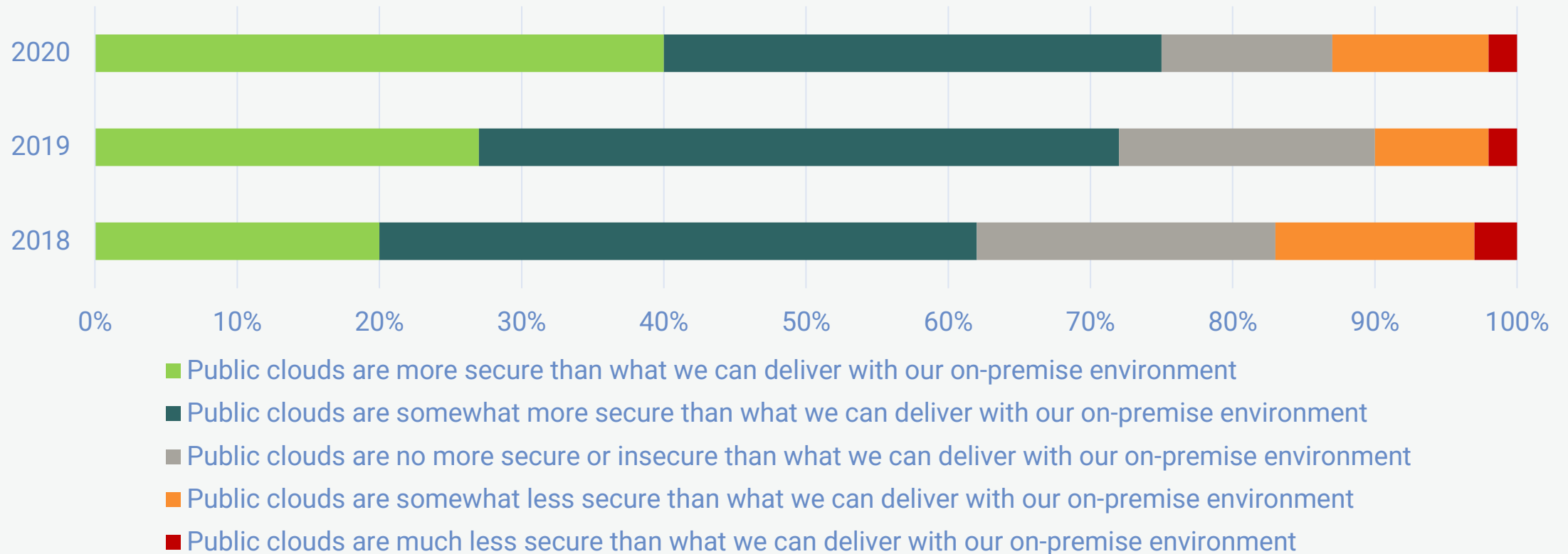
Effektives und effizientes Management von Updates und Einstellungen



24/7 Überwachung, ggf. Alarmierung, Eskalation
...

Perceived Cloud Security

Perceived Security of Public Cloud



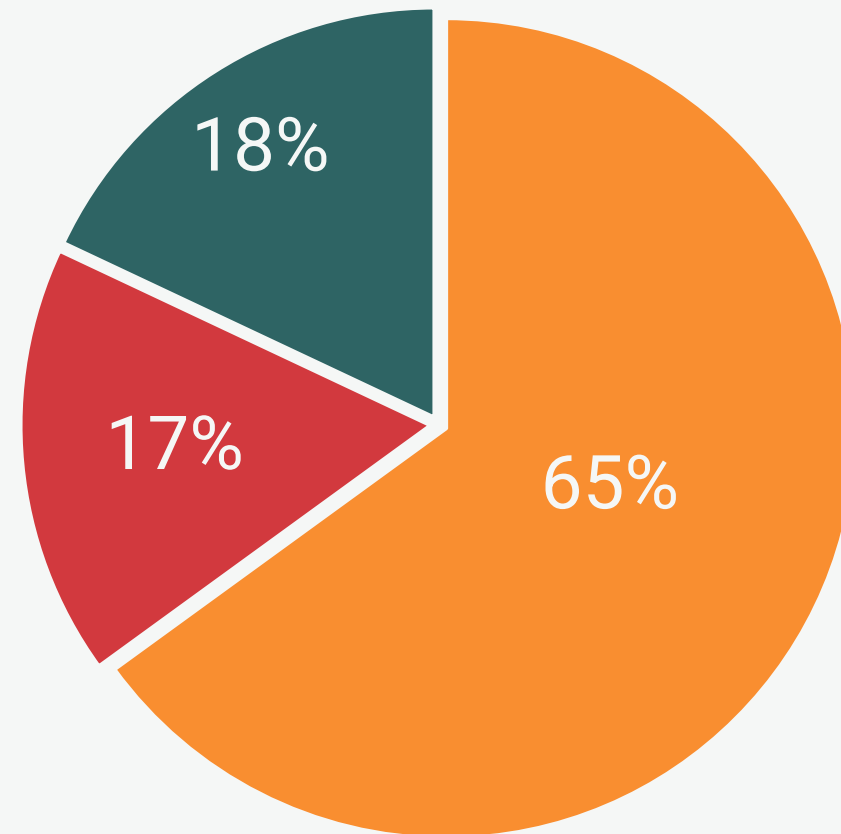
Oracle Cloud Threat Report 2020

Cloud Security Shared Responsibility Model

TeleTrust Studie Cloud Security, 2021

		On-prem	IaaS	PaaS	SaaS
Überwiegend vom Nutzer zu verantworten	Client- und Endgeräteschutz				
	Geschäftsspezifische Daten				
	Benutzerkonten und Berechtigungen				
	Geschäftsspezifische Anwendungen				
	Identitäts- und Zugangsmechanismen				
Vom Anbieter oder vom Nutzer zu verantworten	Entwicklungs- und Laufzeitumgebung				
	virtuelles Netzwerk				
	Betriebssysteme				
	Virtuelle Server				
Vom Anbieter zu verantworten	Virtuelle Umgebung				
	Physisches Netzwerk				
	Physische Server und Speicher				

How well do your traditional network security tools work in cloud environments?



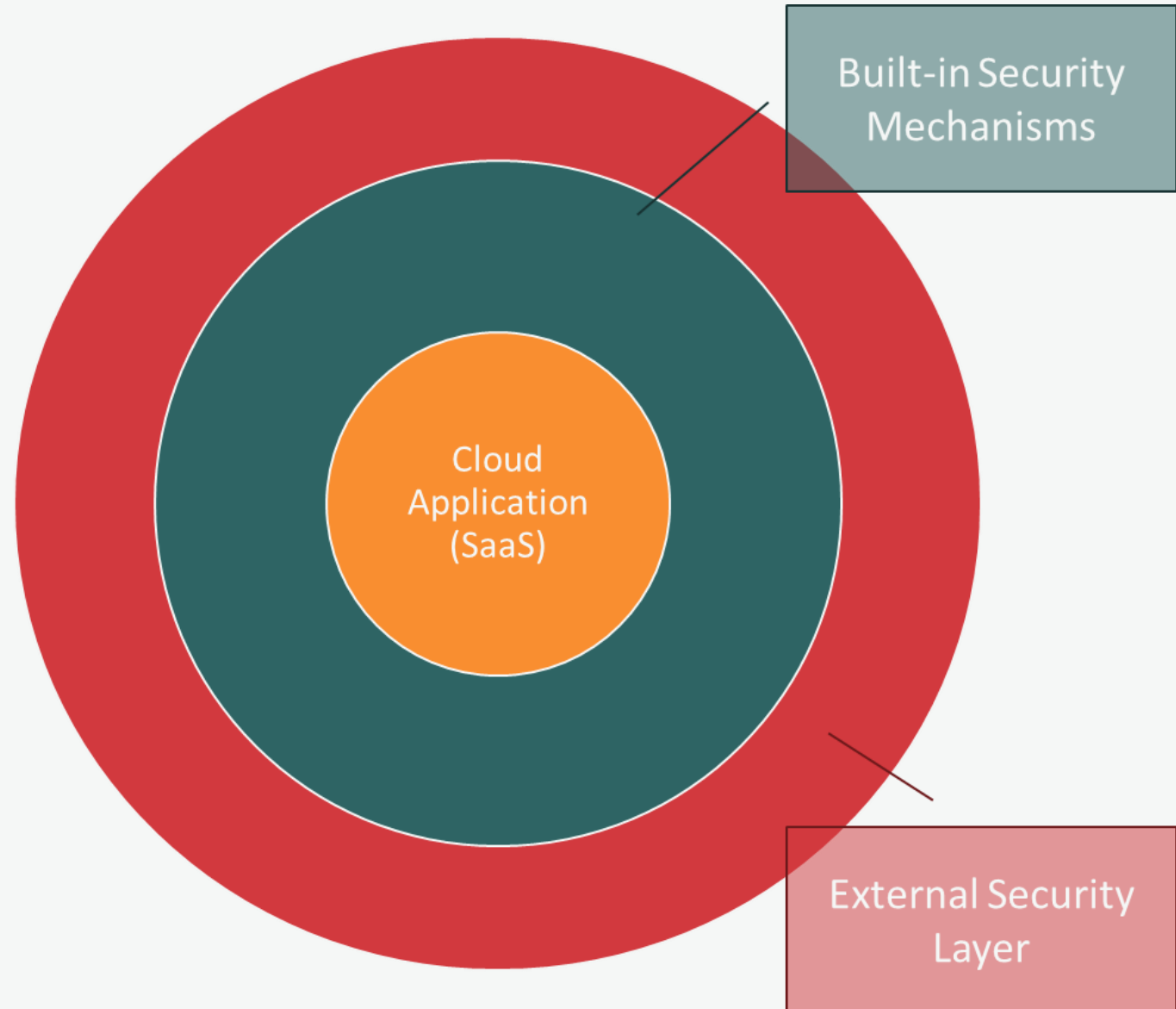
- Limited functionality
- Our traditional network security tools don't work in the cloud
- All capabilities work in the cloud

Cybersecurity Insiders: 2020 Cloud Security Report

Cloud Security Layers

External Security Layer:

- Cloud VPN
- Cloud Firewall
- Cloud Access Security Broker
- Cloud Encryption Broker
- Cloud Email Gateway
- Cloud Security Posture Management
- Identity Provider
- Cloud Backup

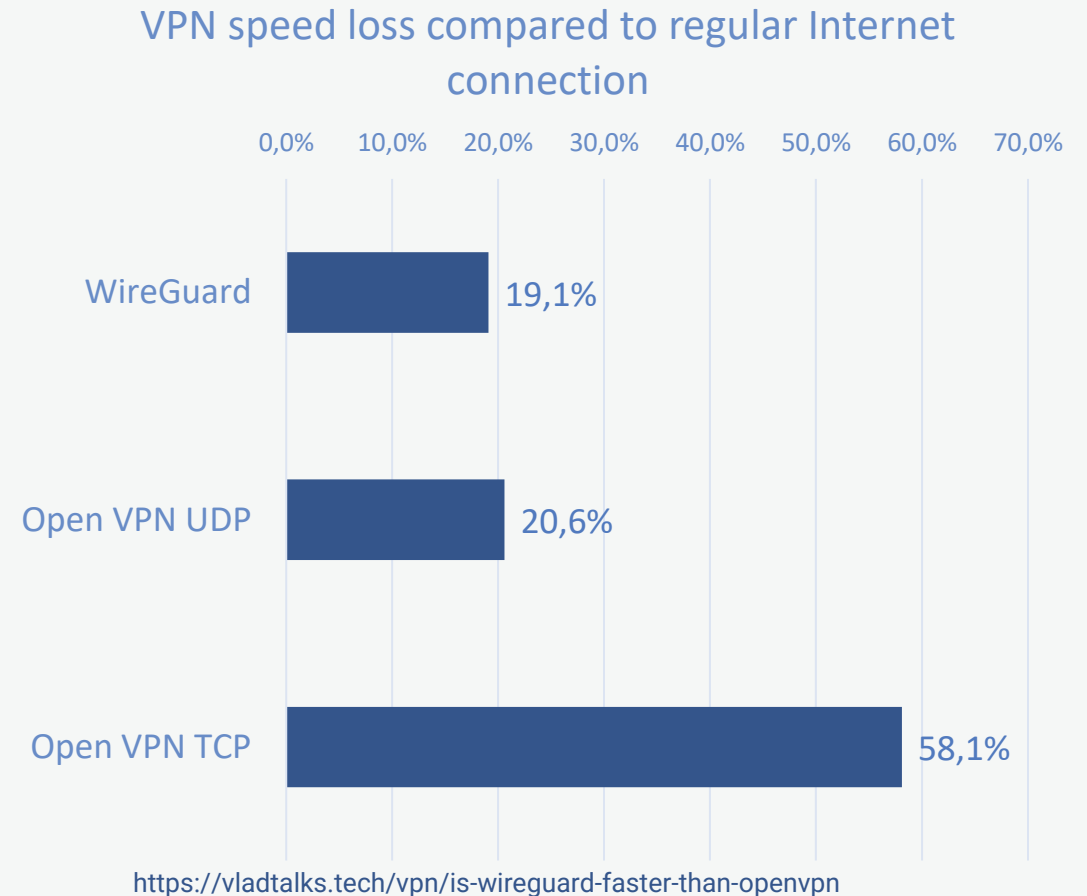


Backup und Notfallplanung

- Höhere Verfügbarkeit durch Redundanz und Replikation
- Geschriebenes Backup Konzept auch für Daten und Anwendungen in der Cloud
- Sicherung in der Cloud
- Geo-Redundanz
- Verschlüsselung (Sicherung der Schlüssel!)
- Sicherung gegen Totalausfall des Providers

Cloud VPN

- Vorteile gegenüber herkömmlichen VPN:
 - Breitbandige Anbindung
 - Entlastung der Internet-Anbindung des eigenen Standorts, insbesondere bei mobiler Nutzung von Cloud Services
 - Z.T. Einbindung externer Cloud Services in das eigene Netz möglich
 - Betrieb durch Cloud Provider
- Nachteile gegenüber herkömmlichen VPN:
 - Cloud Provider kann die übermittelten Daten einsehen
- Meist angebotene Varianten:
 - IPSec
 - Open VPN
 - WireGuard



Verschlüsselung in der Cloud

- Transportverschlüsselung (Data in transit)
- Verschlüsselung gespeicherter Daten (Data at rest)
- Und dazwischen?
- Schlüsselmanagement
 - Wo ist der Schlüssel gespeichert?
 - Wer hat Zugriff auf den Schlüssel?



Confidential Computing

- Schutz vor unbefugten Zugriffen interner Angreifer und privilegierter Benutzer
- Bereitstellung einer gesicherten und vertrauenswürdigen Verarbeitungsumgebung (Trusted Execution Environment, TEE)
- Daten werden erst innerhalb der TEE entschlüsselt und vor dem Verlassen der TEE wieder verschlüsselt



Weitere Informationen

- TeleTrust Leitfaden Cloud Security
 - <https://www.teletrust.de/publikationen/broschueren/cloud-security/>
- TeleTrust Handreichung Stand der Technik
 - <https://www.stand-der-technik-security.de/startseite/>



Kontakt

Oliver Dehning

- odehyning@odehning.de
- Twitter: @odehning
- LinkedIn:
[linkedin.com/in/odehning/](https://www.linkedin.com/in/odehning/)

