"T.I.S.P. Community Meeting 2021"

Berlin, 03.-04.11.2021

Verschlüsselung in Cloud, um Cloud und um Cloud herum

Inés Atug, HiSolutions AG

Cloud Computing

Cloud Computing ist ein Modell, das es erlaubt bei Bedarf, jederzeit und überall

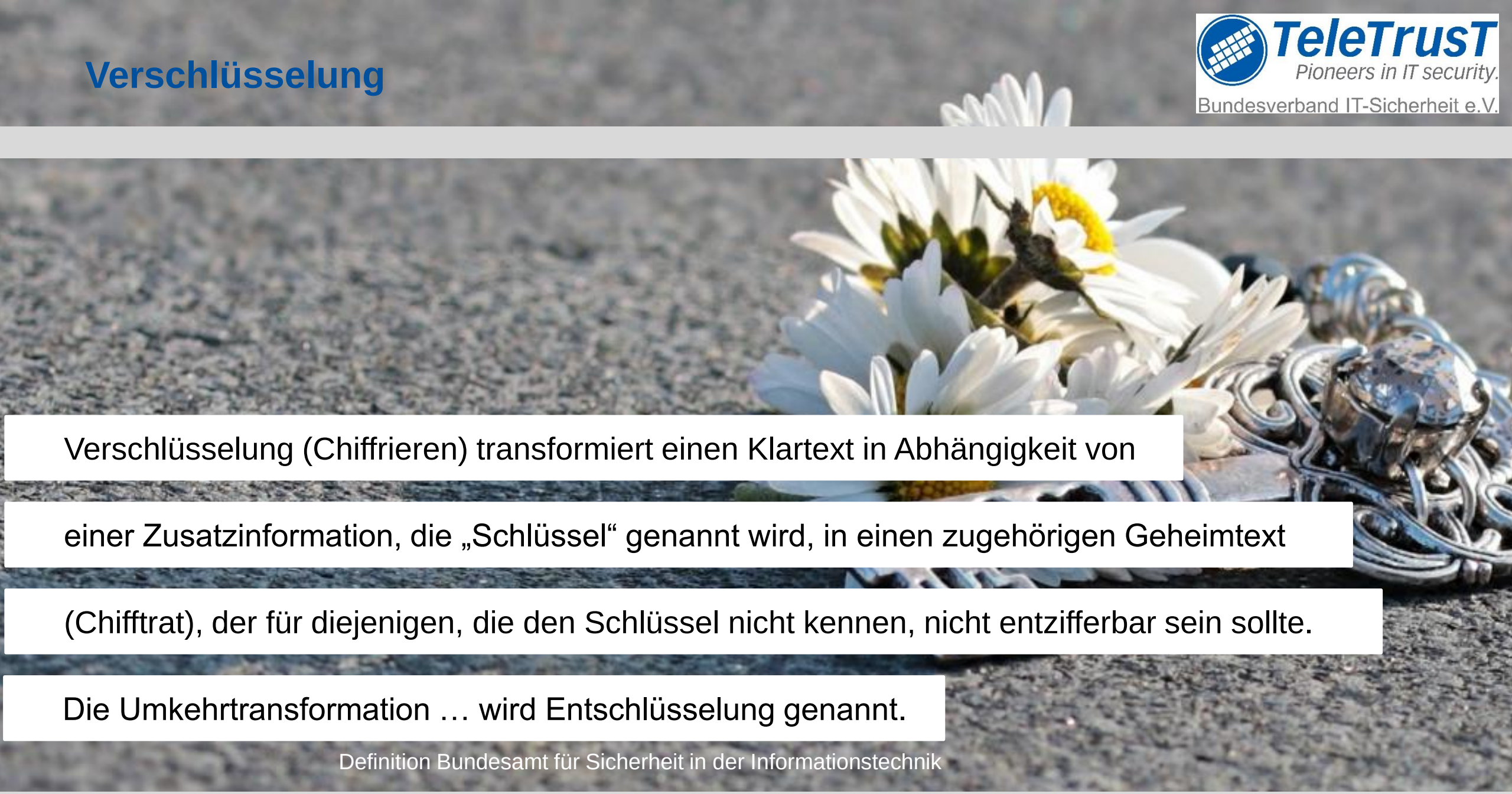
bequem über ein Netz auf einen geteilten Pool von konfigurierbaren Rechnerressourcen …

Zuzugreifen, die schnell und mit minimalem Managementaufwand oder geringer

Serverprovider-Interaktion zur Verfügung gestellt werden können.

Definition Bundesamt für Sicherheit in der Informationstechnik

Verschlüsselung



Verschlüsselung (Chiffrieren) transformiert einen Klartext in Abhängigkeit von

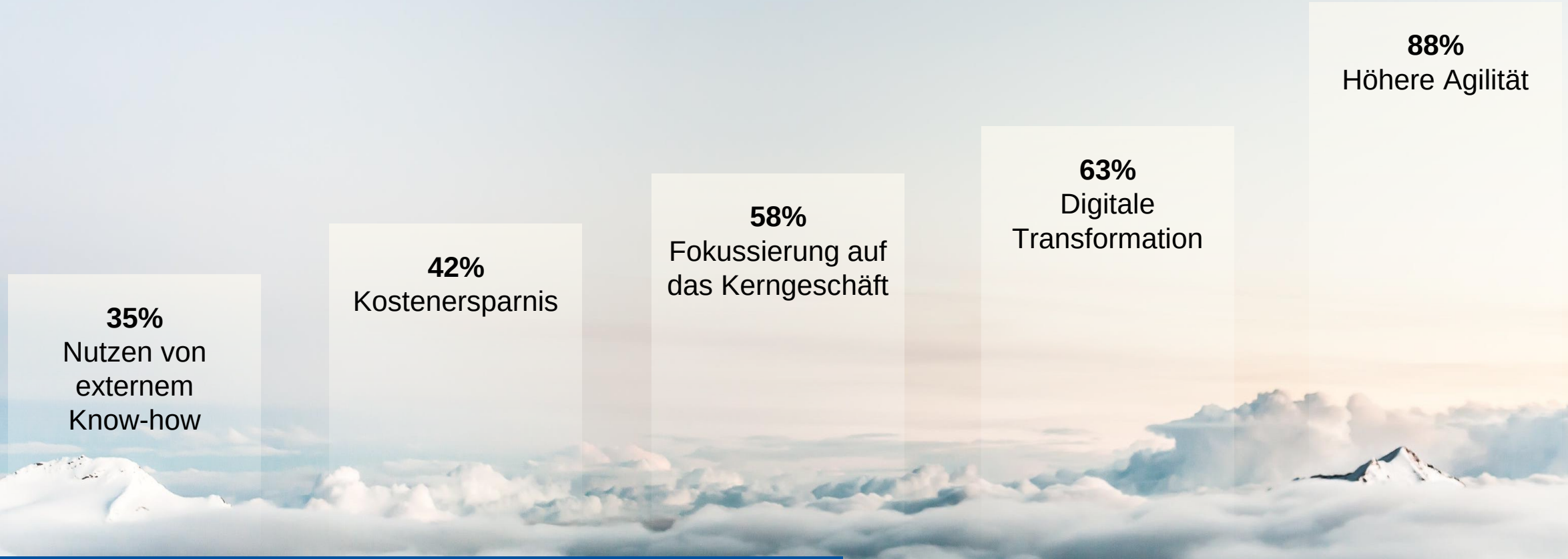
einer Zusatzinformation, die „Schlüssel“ genannt wird, in einen zugehörigen Geheimtext

(Chifftrat), der für diejenigen, die den Schlüssel nicht kennen, nicht entzifferbar sein sollte.

Die Umkehrtransformation … wird Entschlüsselung genannt.

Definition Bundesamt für Sicherheit in der Informationstechnik

Viele Wege führen in die Cloud



Cloud Computing Marktbarometer Deutschland 2020

BITKOM Cloud-Monitor 2020

51%

Speichern vertrauliche Daten in der Public Cloud, wie z.B. Kundendaten, personenbezogene Daten

Wer kann alles unberechtigt auf die Cloud zugreifen?

Hacker

Organisiertes Verbrechen, andere Cloud-Kunden, ….

Insider

Cloud-Kunde, Mitarbeiter des Cloud-Provider, …

Staatliche Zugriffe

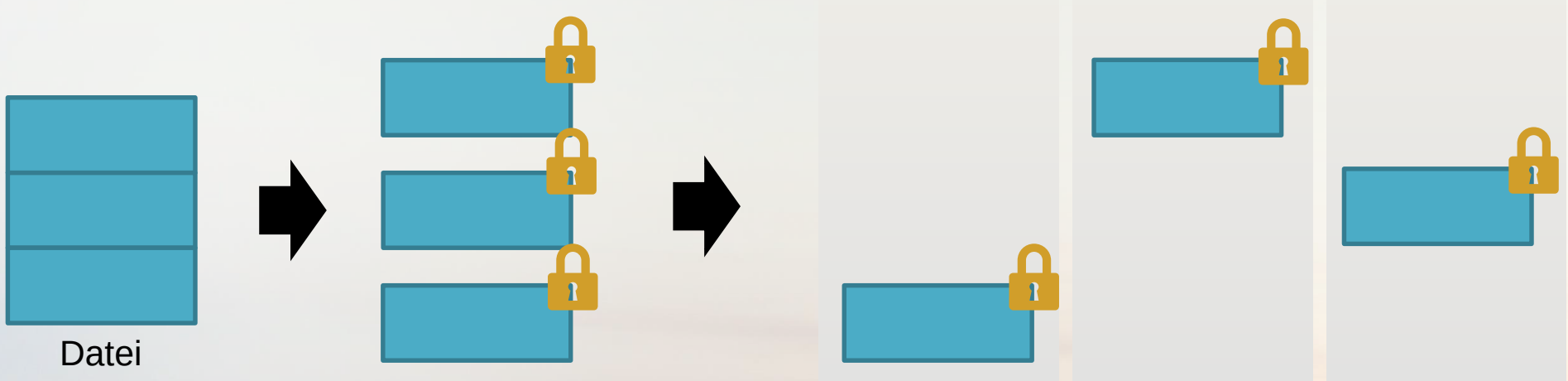
Spionage, Geheimdienste, …

Der Cloud-Provider verschlüsselt …

Festplatten (HD, SSD)	Datenbanken	Daten	Kommunikation
Schlüssel pro Festplatte	Schlüssel pro Instanz, Kunde, Datenbank möglich	Schlüssel pro Kunde möglich	Schlüssel pro Kunde / Session möglich
z.B. dm-crypto, BitLocker	z.B. TDE, Proxy/Wrapper	Siehe nächste Folie	z.B. TLS, IPSec

In allen Fällen erfolgt das Schlüsselmanagement durch den Cloud-Provider!

Verschlüsselung von verteilten Daten

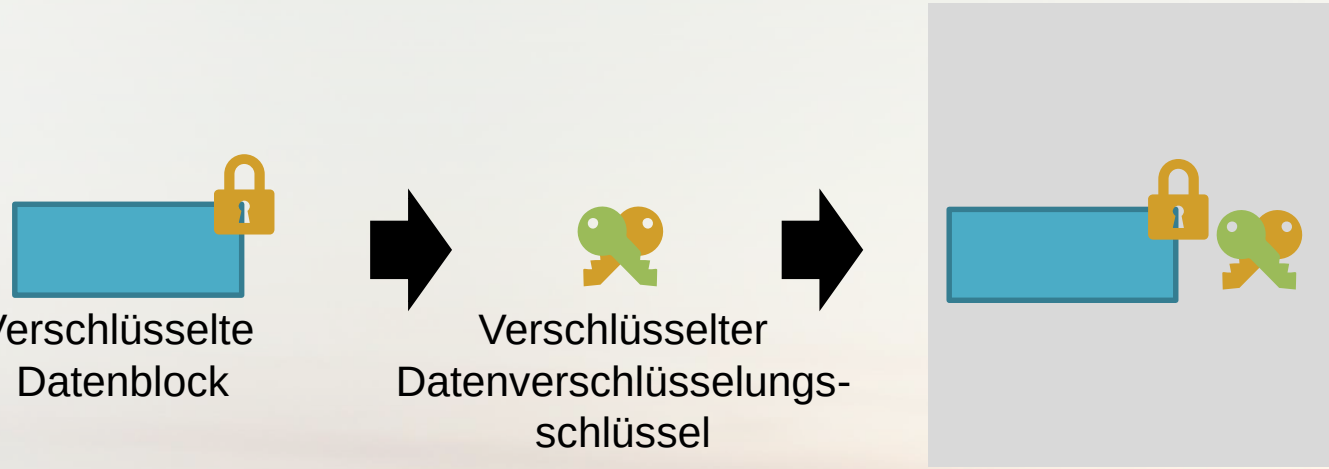


Der Cloud-Provider verwaltet die Schlüssel …

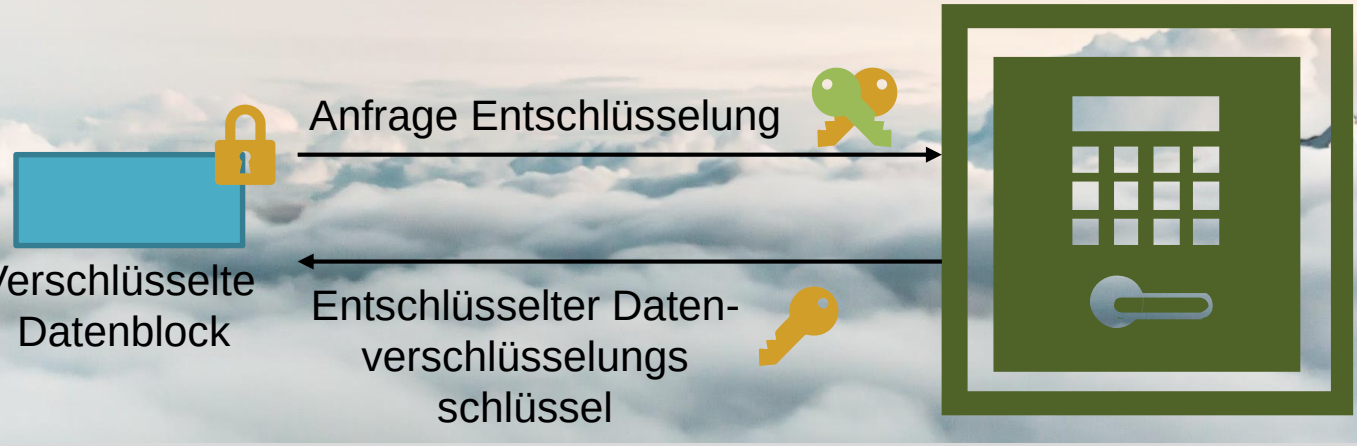
- Häufig erfolgt die Schlüsselverwaltung in einem Softwaretresor und der Kunde kann die Nutzung von Hardware Security Modulen (HSMs) hinzubuchen.
- Softwaretresore sollten Schlüsselmanagement-Funktionalitäten mitbringen, wie z.B. das automatische rotieren von Schlüsseln / Zertifikaten
- Die Softwaretresore sollten eine Ebene für die Konfiguration haben, auf die nur Benutzerkonten zugreifen dürfen und eine Datenebene über die die Schlüssel angefordert werden können. Hier sollte dann nur die Anwendung darauf zugreifen dürfen.
- Die HSMs sollten nach FIPS 140-2 Level 2 oder 3 zertifiziert sein.

Schlüsselmanagement bei Dateiverschlüsselung

Schutz des Datenverschlüsselungs-schlüssels



Entschlüsselung des Datenverschlüsselungs-schlüssels



Löschung von Kundendatenbanken in Azure

Bis zu 5 Min.

Datenbank-transaktionen gelöscht

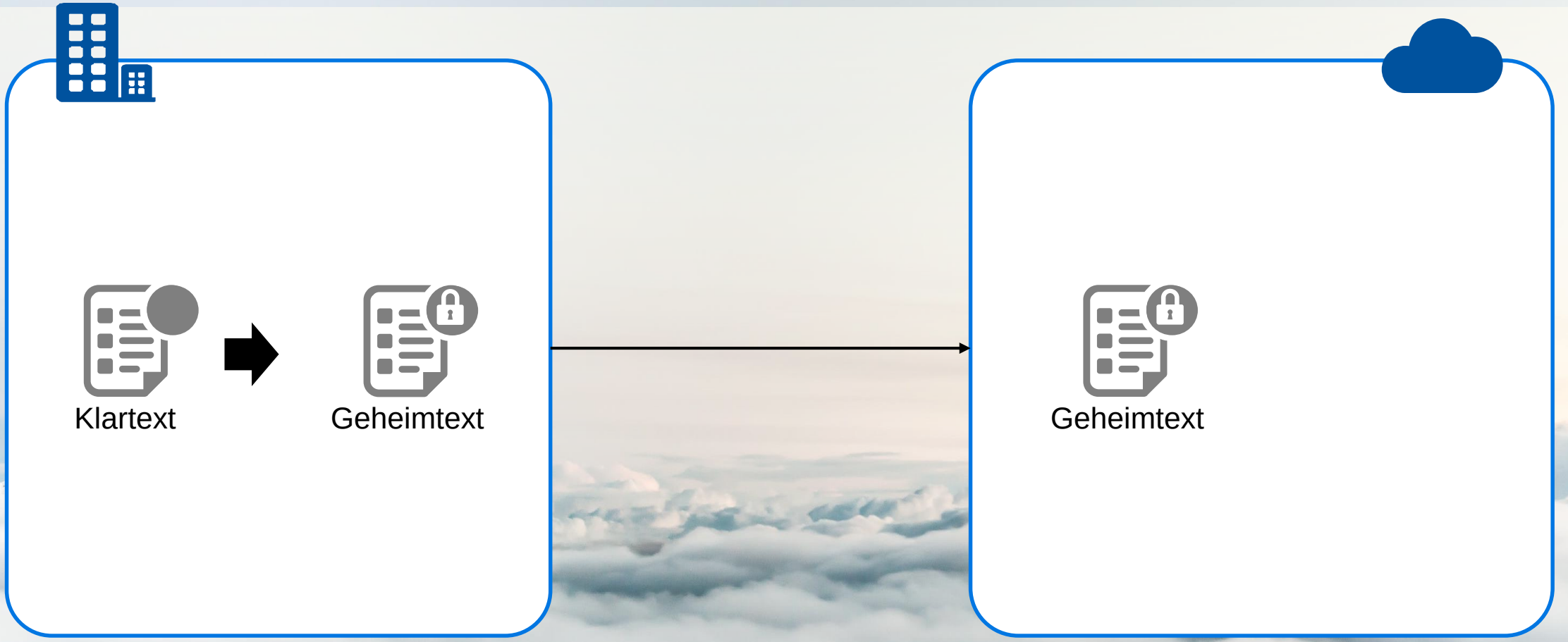
TDE

Cloud-Kunde mit TDE und eigenem Schlüssel waren betroffen

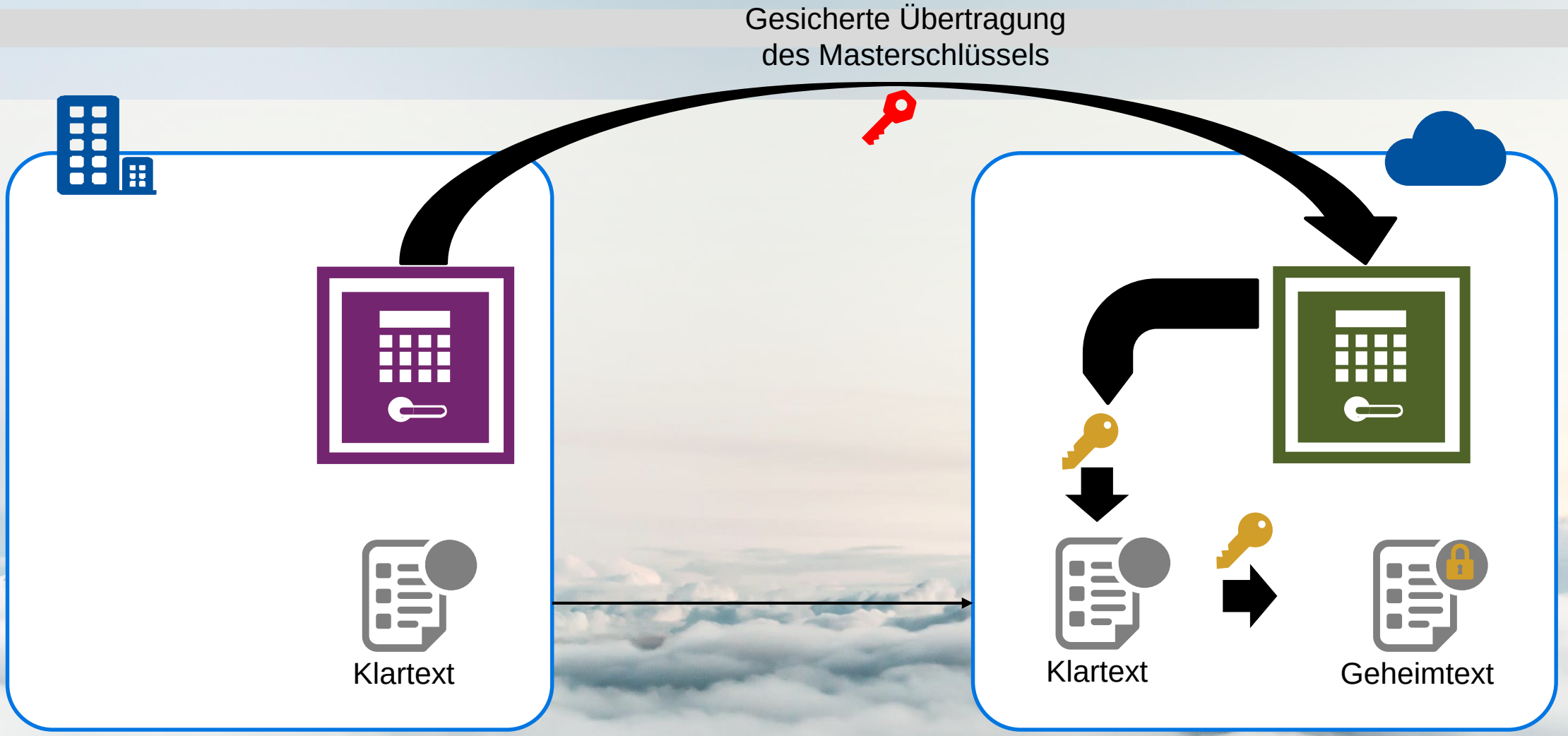
2 Monate

Freie Nutzung der Datenbanken für 2 Monate

Hold Your Own Key



Bring Your Own Key



Blick in die Zukunft: Quantencomputer

- Der Quanteninformatiker und Mitbegründer des Instituts für Quantum Computing an der Universität Waterloo, Michele Mosca, schätzt die Wahrscheinlichkeit auf 1:2, dass bis **zum Jahre 2031** ein Quantencomputer entwickelt wird, der **heutige kryptografische Verfahren brechen** kann.

- Dies betrifft insbesondere die asymmetrische Verschlüsselung deren Algorithmen auf schwerlösbaren mathematischen Problem basieren.

- Doch auch symmetrische Verschlüsselung kann von einem Quantencomputer betroffen sein, derzeit geht man von einer Verdopplung der Schlüssellänge aus, die notwendig ist, um weiterhin symmetrische Algorithmen, wie z.B. AES einzusetzen.

Aufgrund dieser Entwicklung haben sich zwei Forschungsgebiete herausgebildet: Quantenkryptografie und Post-Quantum-Kryptografie

Quantenkryptografie – Schlüssel im Licht

- In diesem Bereich werden Schlüsselaustauschmechanismen entwickelt, die auf der Polarisation eines Photons basieren.
- Die Photonen können verschiedenartig polarisiert sein: horizontal oder vertikal, rechtsdiagonal oder linksdiagonal.
- Für die Photonen gibt es eine Art Filter (Polarisatoren),der Photonen mit der gleichen Polarisierung hindurch lässt, mit der falschen Polarisierung allerdings blockiert.
- Der Schlüssel, den ein Sender einem Empfänger sendet, ist also dementsprechend ein Strom aus Photonen, der zufälligerweise polarisiert sind. Es wird ein One-Time Pad ausgehandelt.
- Die Sicherheit beruht auf quantenmechanischen Effekten: Eine Messung würde den Zustand eines Teilchens verändern, was bedeutet, der Sender und der Empfänger würden sofort mitbekommen, falls jemand ihre Kommunikation belauschen würde.

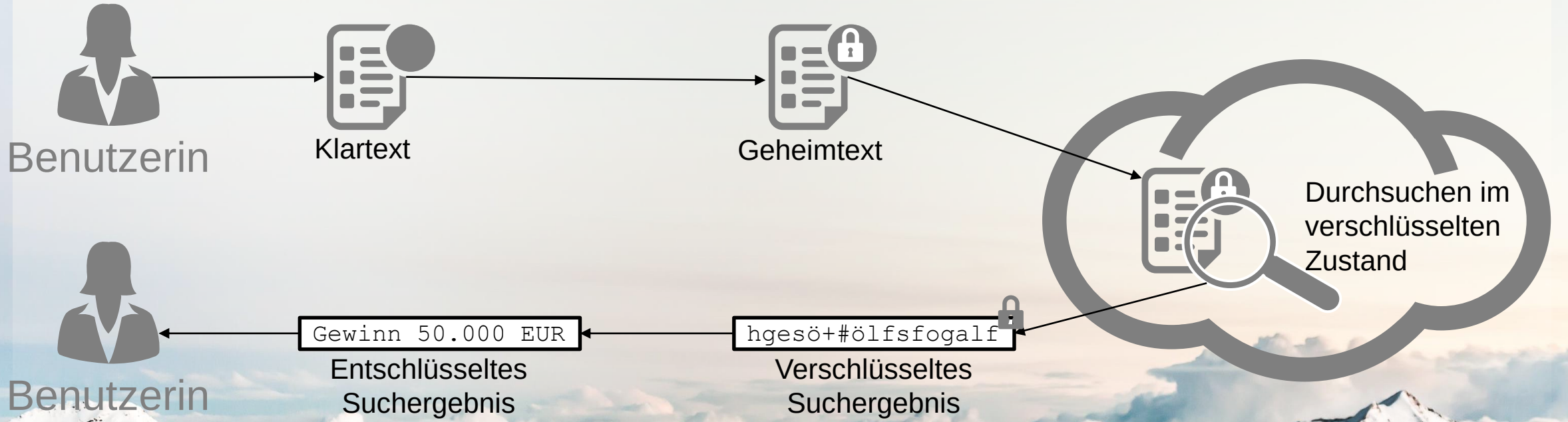
Stellt eine Alternative für asymmetrische Methoden dar, die häufig für den Schlüsselaustausch verwendet werden.

Post-Quantum Kryptografie – Die Probleme der Gitter

- Seit 2016 läuft ein Wettbewerb beim NIST für einen kryptografischen Algorithmus, der Quantencomputern wiederstehen kann.
- Inzwischen sind von ursprünglich 69 Algorithmen noch 15 Algorithmen im Rennen.
- Die Aussichtreichsten Algorithmen beruhen auf Problemen mit mathematischen Gittern
- Post-quantum Verschlüsselungsalgorithmen müssen im Gegensatz zur Quantenkryptografie nicht zwingend durch einen Quantenrechner umgesetzt werden, sondern können auch auf Verfahren mit klassischer Hardware basieren.

Der oder die Algorithmen der Post-Quantum Kryptografie sollen asymmetrische Verschlüsselungsverfahren in der Zukunft ersetzen.

Blick in die Zukunft: Homomorphe Verschlüsselung



Die ungewollte Verschlüsselung in der Cloud

- Gründe für Ransomware in der Cloud
  - Neue Umgebung, unbekannt Sicherheitsmaßnahmen
  - Alte Software mit Schwachstellen
  - Mitarbeiter kennen die neuen Risiken der Cloud nicht
- Mit z.B. Cerber gibt es einen Ransomware-as-a-Service (RaaS), der auf Office 365 abzielt. Über eine E-Mail mit einem infizierten Microsoft Office-Dokument bekommt die Ransomware einen Fuß ins Netzwerk und verschlüsselt dann im Hintergrund Dateien. Dies kann auch in der Cloud gespeicherte Dateien betreffen.

Zusammenfassend lässt sich sagen …

- Derjenige der Zugriff auf den kryptografischen Schlüssel hat, der hat auch die Möglichkeit auf die verschlüsselten Daten zuzugreifen.
- Verschlüsselung allein reicht zur Absicherung von Daten in der Cloud nicht aus. Ebenfalls entscheidend sind Identitäts- und Berechtigungsmanagement, vertragliche Vereinbarungen mit dem Cloud-Provider usw.
- Die Verschlüsselung ist ein wichtiger Bestandteil der Cloudsicherheit und so sind auch Themen der Zukunft mit zu betrachten, da diese schneller kommen können als wir ahnen.

Ob eine Verschlüsselung alle Sicherheitsrisiken ausreichend mitigiert, muss individuelle geprüft und entschieden werden!

Vielen Dank für Ihre Aufmerksamkeit!

Inés Atug
MSc Applied IT-Security
BSc (hons) Mathematics
Senior Expert – HiSolutions AG

Vortragstitel
Verschlüsselung in Cloud, um Cloud und um Cloud herum

Berufliche Mission
Durch Sicherheitsmaßnahmen die Vorteile der Digitalisierung nutzbar machen!

Zitat aus der Kryptografie
„Kryptographie wird normalerweise umgangen und nicht durchdrungen."

- Adi Shamir