Changing the game!

# Cloud-Services

Nutzung von Cloud-Services in B2B / B2C Szenarien
insbesondere für unternehmens-kritische Applikationen und Daten.

## 1. Ausgangssituation

Die Cloud vereinfacht die Speicherung und den Zugriff auf Daten enorm und ist nicht mehr aufzuhalten. Allerdings halten Sicherheitsbedenken viele Firmen von der Nutzung der Cloud ab.

## 2. Aktuelle Problemfelder

### a. Zugriff auf Dateninhalte durch die Cloud-Anbieter

Neben der sicheren Übertragung der Daten in/aus der Cloud, stellt hier insbesondere der Zugriff auf Daten durch die Administratoren des Cloud-Anbieters ein großes Problem dar. Auf Dateiebene gäbe es die Möglichkeit zum Aufbau eines eigenen Schlüssel-Servers und Verschlüsselung der Daten BEVOR sie in die Cloud geladen werden, was aber wieder eigene Infrastruktur voraussetzt (bei einem gehosteten Schlüsselserver könnten sich ja wieder dessen Administratoren ggf. Zugriff auf die Schlüssel - und damit auch die Daten beschaffen). Aufgrund dieser Problematik können Cloud-Provider aktuell nicht wirklich garantieren, dass Ihre Mitarbeiter kei- nen Zugriff auf die Kundendaten erhalten, auch wenn sie es über organisatorische Ansätze versuchen zu lösen.

### b. Schutz gegen Missbrauch der Daten bei der Verarbeitung

Noch schwieriger ist der Schutz von Daten bei (erlaubter) Datenverarbeitung durch Dritte. Da aktuelle Technologien nicht in geschützter Form (z.B. Verschlüsselt) verarbeiten werden können, muss vor einer Verarbeitung immer der Schutz entfernt werden (z.B. durch Entschlüsselung). Was danach mit den Daten passiert, liegt in der Hand des Bearbeiters - somit existiert kein wirksamer Schutz gegen den Missbrauch.

### c. Public Cloud wird zur Private Cloud

Die Public-Cloud bei den großen Anbietern ist die effizienteste und physisch sicherste Möglichkeit der Cloud (große Rechenzentren, optimierte Prozesse, eine Vielzahl von Administratoren beispielsweise). Keine Firma kann in einem eigenen Rechenzentrum da mithalten - selbst große Player haben da Probleme. Das Problem ist allerdings, dass die Kontrollmöglichkeiten und insbesondere das Vertrauen bei den (amerikanischen) Anbietern eher gering ist. Auch rechtliche Einschränkungen bzw. Verpflichtungen (z.B. Patriot Act) in den USA verbieten eigentlich die Ablage und Nutzung der Public Cloud für sensible Daten.

### d. Key Management

In sehr großen Anwendungen mit sehr vielen Geräten, und/oder vielen wechselnden Benutzern funktioniert das klassische Key-Management nicht, da zu häufig neu ver- bzw. entschlüsselt werden muss. Im IoT Bereich kommt das Problem hinzu, dass die Schlüssen nur schwer oder gar nicht verändert werden können, was das Key- Management weiter verkompliziert.

### e. Deduplizierung (speicheroptimierte Datenablage) nur mit unverschlüsselten Daten möglich

Aktuell werden Daten insb. im B2C Umfeld von den Cloudanbietern nicht bereits am Client (Mobiltelefon, Laptop, Applikation) verschlüsselt sondern erst nach Übertragung zum Cloud-Server optimiert und verschlüsselt gespeichert. Die dadurch resultierenden Speicherplatzeinsparungen werden nicht an die Verbraucher weitergereicht sondern „Funden“ die Marketingkosten wie z.b. „Die ersten 2 GByte an Speicher sind kostenfrei“. Werden die Verbraucherdaten jedoch bereits am Client verschlüsselt so können die serverseitigen Optimierungsmethoden nicht angewendet werden, da verschlüsselte Daten eindeutig sind und nicht mehr komprimiert oder dedupliziert werden. Die Client-seitiges Verschlüsselung würde das Geschäftsmodell der Cloud-Anbieter zumindest im B2C-Umfeld torpedieren, u. a. durch Kostenexplosion der Speicherkosten bzw. durch Erhöhung der Lizenzgebühren was die Abwanderung vieler Verbraucher zur Konkurrenz mit sich ziehen würde.

Changing the game!

## 3. Lösungsansätze mit NVD – Non-visible-data Technologie

Die von SECLOUS entwickelte Lösung geht hier komplett neue Wege. Durch Umwandlung in das NVD-Format (binäre Blöcke) werden Daten bereits bei ihrer Entstehung sozusagen mit ihrer eigenen DNA verschlüsselt bzw. geschützt. Und dies autonom, durchgehend von Beginn der Datenerzeugung über die gesamte Lebensdauer der Daten.

**a.** Da durch NVD die Daten für unbefugte „unsichtbar" sind, können Provider beweisen, dass sie keinen Zugriff auf die Daten erhalten können. Dies könnte insbesondere für neue Player auf dem Markt von Interesse sein, schützt aber auch vor möglichen Strafen in regulierten Märkten oder durch die Gesetzgebung, z.B. durch die ab Mai 2018 neu definierten Vorgaben hinsichtlich des Schutzes von personenbezogenen Daten (GDPR)

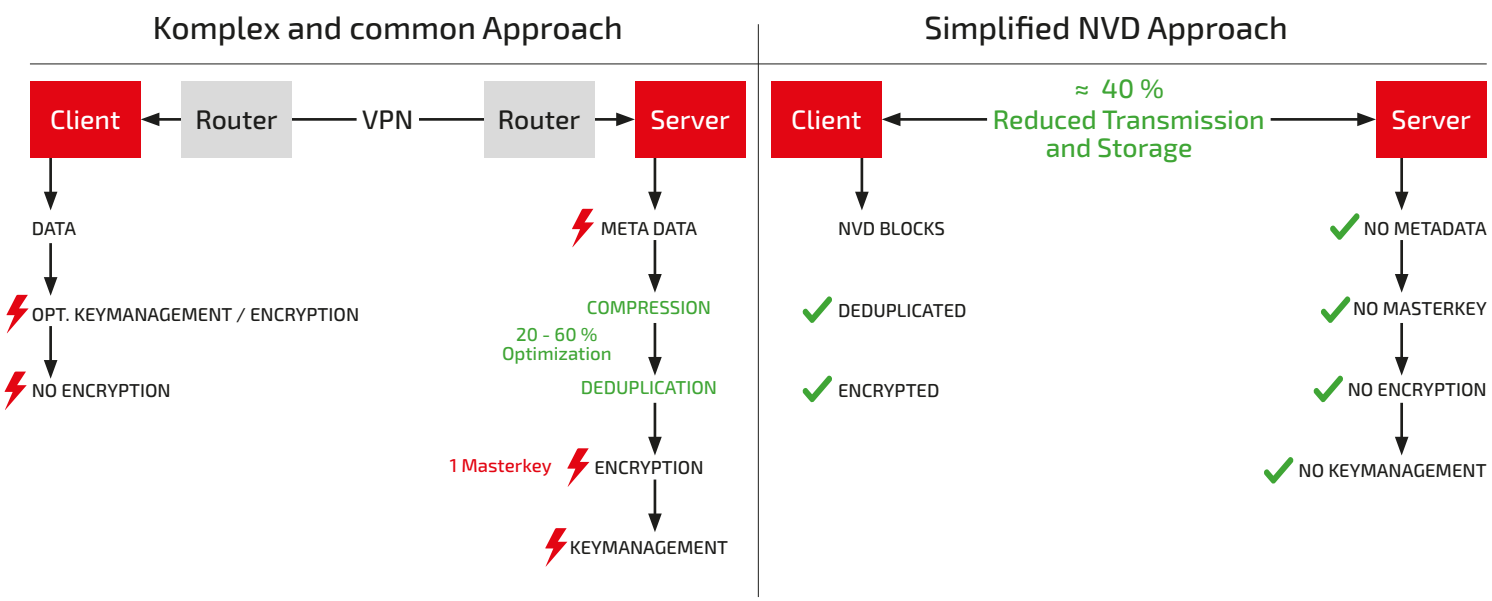
**b.** Bei einer komplett auf NVD ausgelegte Applikation (d.h. Lesen und Schreiben von Daten nur im NVD Format und unter Nutzung der NVD Zugriffsverfahren) benötigt ein Bearbeiter keine explizite Entschlüsselung der Daten, denn im Rahmen des Zugriffs würde der Bearbeitungsschritt Teil der Freigabe sein. Ebenso hätte der Bearbeiter keine Möglichkeit die Daten elektronisch weiterzugeben, da hier wieder der „NVD-only" Schutz greift. Angriffsmöglichkeiten durch Abfotografieren oder Abschrei- ben bestehen zwar weiterhin, können allerdings durch weitere Schutzmaßnahmen deutlich einfacher abgesichert werden.

**c.** Unsere Positionierung ist hier einzigartig - wir verbinden alle Vorteile der Public Cloud (Flexibilität, Effizienz und Kosten) mit dem bestmöglichen Schutz der Daten (-inhalte). Es ist völlig unerheblich wo NVD-Daten gespeichert werden. Sie sind gleich sicher – egal ob in einer Public- oder einer Private Cloud. Signifikante Infrastrukturkosteneinsparungen erhöhen die Margen erheblich bzw. schaffen Wettbewerbsvorteile durch Weitergabe der Kosteneinsparungen an die Kunden.

**d.** Mit NVD entfällt das Key Management, bzw. ist es integraler Teil des Zugriffsverfahren. Neben der massiv reduzierten Komplexität durch den Entfall des Key Management ist aber insbesondere der Entfall der dauerhaften Speicherung der Schlüssel ein massiver Sicherheitsgewinn - denn Angreifer können schlicht die Schlüssel nicht stehlen (aktuell werden die sog. Key- Vaults bestehender Lösungen immer häufiger das Ziel von Angriffen).

**e.** Non-visible-Data ist von Anfang bis Ende des Lebenszyklus des Datums verschlüsselt. Der Schutz resp. die Verschlüsselung ist in die Daten integriert und erfolgt autonom dort wo die Daten entstehen (Client, Applikationsserver). Trotz Verschlüsselung können diese Datenblöcke (ohne Metadateninformationen) dedupliziert werden und zwar ganz entscheidend bereits am Client sodass bereits die Datenübertragung zum Cloud-Server signifikant (zw. 30 und 50 %) reduziert werden kann. Keine andere Technologie kann dies mit verschlüsselten Daten erzielen (unzählige Versuche homomorphistischer Verschlüsselung bei gleichzeitiger akzeptabler Performance zu implementieren sind alle gescheitert). Kommt NVD als Standardwerkzeug in den Cloudsystemen zum Einsatz so ergeben sich für diese Anbieter unzählige Vorteile gegenüber der Nutzung heutiger Technologien. Angefangen von dem Kosteneinsparpotential (40 %) bis hin zum Imagegewinn des Anbieters (Vertrauensgewinn durch die verschlüsselte Übertragung der Verbraucherdaten). Durch diesen entscheidenden Wettbewerbsvorteil wird der Cloud-Anbieter sich gegenüber der Konkurrenz differenzieren, und mit sehr hoher Wahrscheinlichkeit auch Kunden „abwerben" bzw. Neukunden gewinnen können.

## 4. Architekturvergleich



Changing the game!

## 5. Bewertung der Anwendungsszenarien

Die nachfolgende Bewertung der Lösungsansätze konzentriert sich im Wesentlichen auf

**a.** Die Lösungsumsetzung hinsichtlich Komplexität, Wahrscheinlichkeit der Umsetzung, den erforderlichen Erweiterungen der NVD Technologie sowie dem Umsetzungsaufwand

**b.** Der Betrachtung hinsichtlich quantitativer Vorteile (Umsatzsteigerung bzw. Kosteneinsparung) sowie qualitativer Vorteile (Imagegewinn, Compliance) sowie einer abschließenden Risikobetrachtung

**c.** Aus unserer Sicht besonders geeignete Zielkunden und Segmente

## a. Quantitative und qualitative Bewertung

| Lösungsansatz | Quantitative Vorteile | | Qualtitative Vorteile | | Kundensegment | Zielkunden |
|---|---|---|---|---|---|---|
| | Umsatzsteigerung | Kostenreduktion | Imagegewinn | Konformität | | |
| a) Anonyme Speicherung der Daten in der Cloud | **Hoch** | Niedrig | **Hoch** | **Hoch** | Cloudanbieter | AWS, Microsoft, Telekom IBM |
| b) "NVD-only" Funktionalität | Niedrig | Medium | Medium | **Hoch** | | |
| c) Public Cloud wird zur Private Cloud | **Hoch** | n. a. | **Hoch** | **Hoch** | | |
| d) Entfall des Key Managements | Medium | **Hoch** | Medium | n. a. | | |
| e) Deduplizierung mit verschlüselten Daten | Medium | **Hoch** | n. a. | n. a. | | |

## b. Umsetzungsbetrachtung

| Lösungsansatz | Umsetzung | | |
|---|---|---|---|
| | Komplexität | Erweiterungen | Aufwand |
| a) + e) Anonyme Speicherung der Daten in der Cloud | Niedrig | Plattformerweiterung (IOS, Unix, Mobile) | Gering |
| b) "NVD-only" Funktionalität | Niedrig | | Hoch |
| c) Public Cloud wird zur Private Cloud | Medium | Plattformerweiterung (IOS, Unix, Mobile) | Medium |
| d) Entfall des Key Managements | Medium | Plattformerweiterung (IOS, Unix, Mobile) | Medium |

Changing the game!

## c. Risikobetrachtung

### Strengths

- NVD is fully in line with existing compliance requirements (GDPR)
- Refinement of existing and new products and services through „secure through NVD"
- Additional image improvement due to „we take your privacy requirements serious"

### Weaknesses

- Lack of references due to brand new technology

**SWOT**

### Opportunities

- Explore new digital businesses, e.g. secure Data brokerage Services
- First Mover in new businesses will take the big pice of the cake
- Re-gain competitive advantages

### Treats

- Brand new technology may cause resistance within the Market and Organisation