Technischer Artikel

Sichere Oracle-Datenbanken in der Cloud

Stefan Oehrli
Solution Manager
31. Mai 2017

Datenschutz, Sicherheit und Cloud-Computing sind heiss diskutierte Themen mit vielen unterschiedlichen Meinungen und Standpunkten. Unabhängig vom jeweiligen Standpunkt wird in der Regel bei einfachen Standarddienstleistung eher eine Cloud basierte Lösung in Betracht gezogen. Doch wie sieht dies bei Datenbanken aus? Datenbanken enthalten häufig kritische oder teilweise sensitiven Daten. Lassen sich diese Datenbanken so ohne weiteres sicher in einer Cloud Umgebung betreiben? Welche Herausforderungen stellen sich bei Datenbanken in der Cloud? Welche Überlegungen gehören neben dem reinen Entscheid zugunsten von Feature und Optionen sonst noch dazu? In diesem Artikel werden diese Fragen diskutiert sowie weitere Aspekte von Cloud basierten Oracle Datenbanken aufgezeigt.

Unabhängig vom Speicherort sind Daten im Allgemeinen und Datenbanken im Speziellen unterschiedlichen Risiken ausgesetzt. Diebstahl, Verlust oder unerlaubte Manipulation der Daten können weitereichende Konsequenzen für ein Unternehmen und dessen Geschäft haben. Neben finanziellem Schaden, Image Verlust, strafrechtliche Folgen oder gar Existenzbedrohung stehen auch die Interessen der Mitarbeiter und Kunden im Zentrum. Zudem werden die Herausforderungen für die Umsetzung von Cloud Projekten mit der neuen europäischen Datenschutz-Grundverordnung (EU-DSGVO), welche ab Mai 2018 in Kraft tritt, nicht abnehmen. Nichtsdestotrotz bietet eine europaweite, einheitliche Datenschutzregelung Chancen, welche es zu nutzen gibt.

Ob On-Premises oder in der Cloud, Oracle Datenbanken funktionieren technisch im Prinzip in beiden Umgebungen gleich. Für den Betrieb einer Oracle Datenbank braucht es einen Server mit CPU, Memory und Speichersystem genauso wie Netzwerk- und weitere Infrastrukturkomponenten für die Interaktion respektive den Zugriff auf die Daten. Der wesentliche Unterschied bei Cloud basierten Datenbanken Systemen ist ihr Standort. Diese Datenbanken und die entsprechenden Server stehen eben nicht mehr „im Haus“, im Gegensatz zu On-Premises Systemen, wo die verschiedenen Infrastrukturkomponenten, die Standorte sowie die entsprechenden Administratoren bekannt sind. Obwohl man heutzutage in grösseren Unternehmen nicht mehr einfach im Rechenzentrum oder bei den Administratoren-Teams vorbeigehen kann, besteht doch eine definierte rechtliche Beziehung sowie eine Vertrauensbasis zwischen den Unternehmen und ihren Mitarbeitern. Sobald aber einzelne Dienste oder ganze Infrastrukturkomponenten durch externe IT Dienstleister betrieben werden, nimmt die Komplexität zu. Die rechtlichen Aspekte zwischen den beteiligten Partien werden mit Dienstleistungsverträgen festgehalten. Das bedeutet jedoch nicht zwangsläufig, dass ein Unternehmen allen Mitarbeitern eines Dienstleisters das gleiche Vertrauen entgegenbringt wie den eigenen Mitarbeitern.

Geht man einen Schritt weiter und betreibt Datenbanken komplett in einer Cloud, sind viele Faktoren nicht mehr transparent. Einmal kurz dem Datenbank- Administrator auf die Schulter klopfen oder beim Datenbankserver im Rechenzentrum vorbeigehen, ist nicht mehr möglich. Man gibt seine Daten respektive Datenbanken "aus der Hand", ohne dass man mit absoluter Sicherheit sagen kann, wo die Daten sind und wer effektiv alles darauf Zugriff hat. Für Unternehmen ergeben sich daraus konkrete Fragen, welche, im Gegensatz zu On-Premises Systemen, bei Cloud basierten Datenbanken zwingend zu klären sind.

Dazu gehören:

- Welche Daten sind schützenswert, personenbezogen oder sensitiv?
- Sind davon ganze Datenbanken oder nur einzelne Datensätze/Tabellen betroffen?
- Welche Risiken / Angriffsvektoren bestehen für eine bestimmte Datenbank?
- Welcher Schaden kann Entstehen (direkte Geschäftsschädigung, Imageverlust, ...)
- Wie können diese Risiken durch technische Massnahmen verringert werden?
- Stimmt neben dem Preis, den Services und den vertraglichen Rahmenbedingungen auch das Vertrauen zu dem Cloud Anbieter?

Speziell der letzte genannte Punkt spielt eine nicht zu vernachlässigende Rolle bei der Wahl eines geeigneten Cloud Anbieters.

Angriffsvektoren

Bei On-Premises Datenbanken werden die Angriffsvektoren häufig vernachlässigt oder spielen nur eine untergeordnete Rolle. Aussagen wie "ist ja nur intern", "brauchen wir nicht", "da sehen nur die Administratoren alles" etc. sind in diesem Zusammenhang nicht selten. Oft wird die Verantwortung für die Sicherheit auf andere Systeme wie Firewalls, Gateways und Proxys verschoben. Jedoch wäre es naiv anzunehmen, dass dies ausreiche. Bei komplexen IT Architekturen, wie wir sie heute vorfinden, kann man sich nicht auf einzelne Systeme verlassen. Zudem kommen die Gefahren nicht zwingend immer von ausserhalb, sondern häufig auch aus den eigenen Reihen.

Die **Fehler! Verweisquelle konnte nicht gefunden werden.** zeigt schematisch das Umfeld einer Datenbank und mögliche Angriffsvektoren. Ein Hacker kann von aussen versuchen in Systeme einzudringen und Daten abzuziehen. Doch wie angemerkt, geschieht dies häufig direkt innerhalb eines Unternehmens. Es gab in der Vergangenheit immer wieder bekannte Vorfälle, wo einzelne Datensätze oder ganze Datensammlungen durch Mitarbeiter abgezogen und weitergegeben wurden. Bei Cloud basierten Datenbanken kommen dafür nicht nur die Mitarbeiter eines Unternehmens in Frage, sondern eben auch die Mitarbeiter und Administratoren der beteiligten Dienstleister und Cloud Anbieter.

Damit sollen aber nicht alle Administratoren unter Generalverdacht gestellt, sondern vielmehr die Risiken, Herausforderungen aber auch Chancen im Datenbankumfeld angesprochen werden. Bei Datenbanken spricht man üblicherweise von den folgende Top 10 Gefahren, die es zu bewältigen gilt:

1. Exzessive und nicht benötigte Userberechtigungen
2. Missbrauch von Rechten
3. Input Injection / SQL Injection
4. Malware
5. Schwaches Audit
6. Offenlegung / Zugang zum Speichermedium
7. Schwachstellen und Fehlkonfiguration
8. Nicht überwachte sensitive Daten
9. Denial of Service
10. Unzureichendes Sicherheitsfachwissen

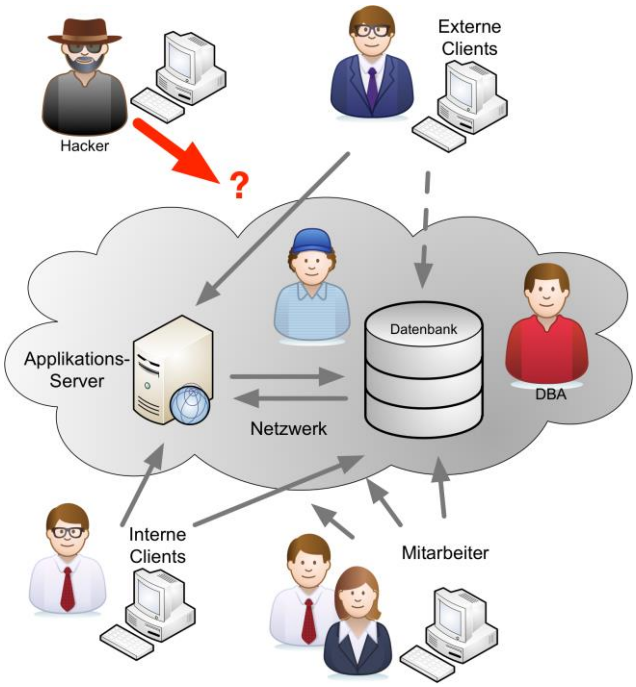

Abbildung 1 Angriffsvektoren

Viele der oben aufgeführten Gefahren lassen sich bereits mit wenigen, einfachen Massnahmen reduzieren. Bei anderen, wie z.B. dem Zugang zum Speichermedium, braucht es umfassendere Massnahmen, welche zwangsläufig auch zu höheren Kosten führen. Im Grundsatz treffen diese Gefahren sowohl bei On-Premises Systemen wie auch bei Cloud basierten Systemen zu. Es braucht daher zwingend ein geeignetes Sicherheitskonzept, welches beide Arten von Datenbank Umgebungen berücksichtigt.

Nicht alle Systeme respektive Daten sind aber gleich kritisch. Aus diesem Grund ist es nicht sinnvoll, alle Datenbanken gleich umfassend zu schützen. Mit einer Risikoanalyse können die Gefahren und Risiken für ein bestimmtes Umfeld festgelegt werden. Dazu gehört, dass der Dateneigentümer respektive Applikationsverantwortliche die Sensitivität seiner Daten kennt und definiert. Im Anschluss sind die Daten zu klassifizieren und einer entsprechenden Schutzklasse zuzuweisen. Für die unterschiedlichen Schutzklassen können anschliessend verschiedene administrative sowie technische Massnahmen für den Schutz der Daten definiert werden. Sinnvollerweise werden nicht zu viele unterschiedliche Schutzklassen gewählt. Für Datenbanken bieten sich folgende vier Schutzklassen an:

- **Öffentlich**: Daten sind im Internet oder an anderen Stellen öffentlich verfügbar – dürfen dort aber sicherlich nicht manipuliert werden
- **Intern**: Daten dürfen von allen Mitarbeitern gesehen werden
- **Vertraulich**: Daten dürfen nur von einem definierten Kreis von Mitarbeitern gesehen werden
- **Geheim**: Daten stehen nur einem kleinen Kreis von Mitarbeitern zur Verfügung. Wenn diese Daten verloren gehen, ist die Existenz einer Unternehmung gefährdet

Können On-Premises noch Datenbanken aller Sicherheitsklassen betrieben werden, gibt es bei Cloud basierten Datenbanken zwangsläufig gewisse Einschränkungen. So werden als *geheim* klassifizierte Systeme wohl primär lokal betrieben. In der Regel sind in einem Unternehmen der Grossteil der Datenbanken *intern* oder *vertraulich* klassifiziert. Dementsprechend ist Potential vorhanden, Datenbanken mit einer Cloud basierten Lösung zu betreiben.

Wieviel Sicherheit im Einzelnen für jede Schutzklasse benötigt wird, hängt immer stark von den effektiven Daten sowie allfälligen Compliance Auflagen ab. Im Folgenden werden verschiedene Massnahmen besprochen.

Identity und Access Management

Unabhängig davon, was für Massnahmen zur Verbesserung der Datensicherheit getroffen werden, spielt die Authentifizierung und Autorisierung eine zentrale Rolle. Arbeiten die Benutzer mit unzureichend starken Passwörtern oder haben zu viele zu hohe Rechte, bringen weitere Massnahmen wie die Verschlüsselung nur bedingt etwas. Neben einer System- und Datenbank-"Härtung" braucht es eine gute Basis. D.h. eine sichere Grundkonfiguration der Datenbank basierend auf Best Practice sowie ein geeignetes Benutzer- und Rollenkonzept.

Identity und Access Management (IAM) geht aber einen Schritt weiter. Der Fokus liegt nicht primär bei einer einzelnen Datenbank, sondern deckt mehrere Aspekte und Systeme ab. Mit *Oracle Enterprise User Security* und *Oracle Unified Directory* lassen sich Benutzer und Rollen zentral in einem Verzeichnis verwalten und somit in mehreren Datenbanken und Systemen benutzen. Durch die Integration in ein unternehmensweites IAM wird sichergestellt, dass die Sicherheit erhöht werden kann. Zudem ergeben sich Chancen, einheitliche und unternehmensweite Workflows zu implementieren.

Verschlüsselung und Key Management

Auch wenn die Benutzer und Rechteverwaltung korrekt gelöst und entsprechend umgesetzt wurde, besteht die Gefahr, dass Unbefugte direkten Zugriff auf die Daten erhalten. Sei dies auf dem Transportweg vom Client zur Datenbank oder direkt auf dem Datenbank- oder Storage Server. Dementsprechend gilt es, die kritischen Daten mit Verschlüsselung entsprechend zu schützen.

Oracle erlaubt ohne zusätzliche Kosten den Schutz des Transports („data in motion“) mit der nativen Netzwerk- oder SSL/TLS Verschlüsslung. Beide Verfahren erlauben auf einfache Weise das Verschlüsseln der Netzwerk-Pakete auf dem Weg vom und zum DB Server. Im Gegensatz zu SSL/TLS ist die native Netzwerkverschlüsselung einfacher zu konfigurieren und schneller ausgerollt. Wogegen bei SSL/TLS zusätzlich eine Integritätsprüfung gemacht wird und bei Bedarf die Client Authentifizierung sichergestellt wird. Letzteres bedingt aber eine entsprechende Public-Key-Infrastruktur im Unternehmen.

Bei Cloud basierten Lösungen ist zudem die Verschlüsselung der Daten am Speicherort ein wesentliches Kriterium („data on rest“). Oracle bietet mit *Oracle Advanced Security* die entsprechende Option. Mit *Transparent Data Encryption* (TDE) lassen sich einzelne Spalten sowie ganze Tablespaces verschlüsseln. Seit Oracle 12c Release 2 geht dies auch für die ganze Datenbank inklusive SYSTEM und SYSAUX Tablespaces. TDE benötigt für die Verschlüsselung jeweils einen Master Key, welcher in einem lokalen Software Keystore bzw. Wallet abgelegt ist. Wir der Software Keystore bei Cloud Datenbanken ebenfalls in der Cloud abgelegt, liegt der Schlüssel für die verschlüsselten Daten direkt bei den Daten. Dies gilt es durch eine On-Premises Key Verwaltung zu vermeiden. Entweder durch ein Hardware Security Modul (HSM) oder mit *Oracle Key Vault*.

Unglücklicherweise schützt TDE nur vor Zugriffen von "aussen", d.h. wenn jemand direkt auf Datafiles, Backup's etc. zugreift. Hat ein Administrator Zugriff via SQL Plus, kann er die Daten mit hohen Systemprivilegien lesen. Um dies einzuschränken, braucht es im Oracle Umfeld zwingend ein *Oracle Database Vault*. Damit wird die Trennung der Verantwortlichkeit forciert und Systemprivilegien eingeschränkt.

Datenbank Audit und Security Monitoring

Der aktive Schutz der Datenbank ist ein Teil. Ein weiterer Punkt ist die Überwachung respektive das Auditing der Oracle Datenbank. Beim Auditing geht es in erster Linie darum festzustellen, ob jemand unerlaubt auf Daten zugreift oder diese manipuliert. Zudem wird die Nachvollziehbarkeit sichergestellt. Mit Unified Auditing und Audit Policies lassen sich entsprechende Regeln zur Überwachung von DDL und DML Statements definieren. Mit Fine Grained Auditing (FGA) bietet Oracle zudem die Funktionalität, Audit Events feingranular zu definieren. Z.B. soll eine Abfrage nur auditiert werden, wenn jemand die Salär Spalte abfragt, in welcher das Salär höher als 10'000.- pro Monat ist. Andere Abfragen generieren keinen Audit Eintrag.

Unified Auditing, Fine Grained Auditing, etc. protokolieren die Audit Events grundsätzlich immer in einem lokalen Audit Trail. Damit die Audit Events zentral verwaltet und entsprechend ausgewertet können, bietet Oracle mit *Oracle Audit Fault and Database Firewall* ein dediziertes Produkt. Damit werden alle Audit und Firewall Events in einem zentralen Repository abgelegt. Zudem wird so das Risiko minimiert, dass Audit Events auf dem Datenbankserver manipuliert werden. Zusätzlich erlaubt ein zentraler Audit Vault Server neben der Auswertung auch die Definition von Alarmen zum aktiven Monitoring bei kritischen Verstössen.

Maximum Data Security Architektur

Werden alle möglichen Oracle Security Features und Optionen zusammen eingesetzt, lässt sich, wie in Abbildung 2 aufgezeigt, eine Maximum Data Security Architektur aufbauen.

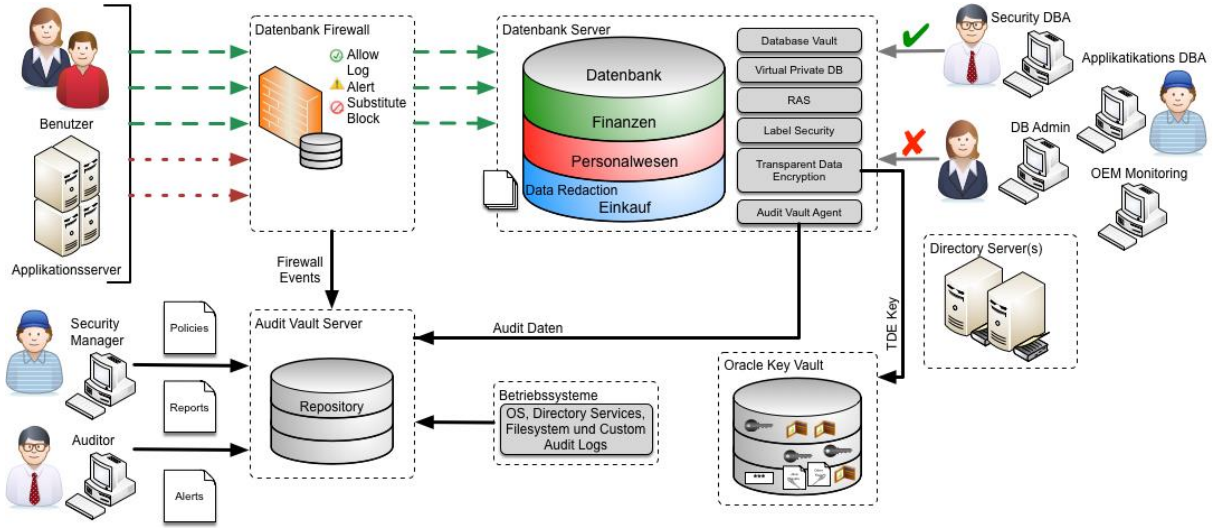

Abbildung 2 Maximum Data Security Architektur

Vom Prinzip her entspricht diese Architektur einer Zwiebel. Im Zentrum stehen die sensitiven Daten. Diese lassen sich dann Schicht für Schicht mit aktiven oder passiven Massnahmen schützen. Dazu gehören folgende Massnahmen:

- **Härtung der Datenbanken**
  Umsetzten von Security Best Practice, Einschränkung kritischer init.ora Parameter, Betriebssystem Zugriff etc.
- **Authentifizierung und Autorisierung**
  Umfassendes Benutzer- und Rollenkonzept nach dem Least Privilege Prinzip
- **Row Level Security**
  Einschränkung der Daten durch *Virtual Private Database* (VPD) und / oder *Real Applikation Security* (RAS). D.h. ein Benutzer sieht nur die für ihn relevanten Informationen.
- **Segregation of Duties und Database Vault**
  Zusätzlicher Schutz von kritischen Daten durch den Einsatz von *Oracle Database Vault* und *Oracle Label*

Security. Mit der Definiton von Realms, Rules und Command Rules lässt sich der Zugriff feingranular gestalten. Zudem wird mit Database Vault eine Trennung der Verantwortlichkeiten explizit forciert. Kritische System Privilegien werden eingeschränkt z.B. alle ANY-Privilegien oder ALTER USER gehen nur noch für den eignen Account.

- **Starke Authentifizierung und Enterprise User Security**
  Verwendung von starker Authentifizierung mit Kerberos oder SSL sowie dem Einsatz von Enterprise User Security zur externen Benutzer- und Rollenverwaltung. Benutzer und Rollen werden nicht mehr dezentral in jeder Datenbank verwaltet, sondern zentral in einem Oracle Verzeichnis, z.B. *Oracle Unified Directory*.
- **Transportverschlüsselung**
  Zur Verschlüsslung des Netzwerkverkehrs von / zu der Datenbank mit der nativen Netzwerkverschlüsslung oder SSL/TLS
- **Verschlüsselung der Daten**
  Verschlüsselung der Daten at Rest mit *Oracle Advanced Security* und *Transparent Data Encryption* (TDE) wobei hier die Master Key's bzw. Oracle Wallets ausserhalb der Datenbank respektive ausserhalb der Cloud- Umgebung in einem zentralen Hardware Security Module oder *Oracle Key Vault* verwaltet werden.
- **Auditing**
  Überwachung der Zugriffe mit Audit Policies, Fine Grained Audit, etc in Kombination mit dem Betriebssystem Auditing
- **Datenbank Firewall**
  Überwachung der einzelnen Zugriffe mit einer Database Firewall. Kritische Abfragen können direkt blockiert werden und / oder Events erzeugen.
- **Zentrale Auswertung**
  Zentrale Sammlung und Auswertung der Audit Daten und Firewall Events mit *Oracle Audit Vault and Database Firewall*
- **Test Daten Management**
  Maskierung und Anonymisierung von Test Daten durch *Oracle DataMasking*.

Je nach gewählter Sicherheitsklasse werden die Daten durch mehr oder weniger Zwiebelschalen geschützt. Somit kann der betriebliche Aufwand wie auch die Kosten moderat gehalten werden. Benötigte Features und Optionen werden nur dort eingesetzt, wo sie auch zwingend nötig sind.

Alternativen

Bis anhin wurden primär Oracle Features und Optionen angesprochen. Selbstverständlich lassen sich viele der angesprochenen Massnahmen teilweise oder ganz durch Produkte von Drittanbietern umsetzten. Speziell bei Cloud basierten Systemen bieten sich Alternativen an, welche bei einem spezifischen Anwendungsfall einfacher umzusetzen sind als eine rein Oracle basierte Lösung. Als typisches Beispiel gilt hier die Verschlüsselung. Damit Oracle Datenbanken sicher in einer Cloud verschlüsselt sind, braucht es neben *Oracle Advanced Security* und einem On-Premises basierten Key Management zwingend immer auch *Oracle Database Vault*. Mit TDE aber ohne Database Vault, kann ein Administrator die verschlüsselten Daten in den Datafiles nicht lesen, er kann dafür über die Benutzer root oracle (SYSDBA) Zugriff via SQLPlus erlangen und Daten dann direkt abfragen. Werden die Daten dagegen bereits vor dem Speichern in der Datenbank verschlüsselt, sind diese Daten auf für hochprivilegierte Benutzer nicht lesbar. Der Einsatz eines solchen Produktes hat üblicherweise aber Einfluss auf das Datenmodell und die Applikation.

Neben den verschiedenen Produkten zur Verschlüsselung auf Betriebssystem-, Datenbank- oder Applikationsebene bieten sich im weiteren Produkte zur aktiven und passiven Überwachung der Datenbank Zugriffe. Unternehmen wie Imperva, IBM und McAfee aber auch Oracle mit Oracle Audit Vault and Database Firewall bieten in diesem Kontext verschiedene Produkte an.

Diese Lösungen überwachen den Netzwerkzugriff auf die Datenbank und entscheiden, bevor die Abfrage überhaupt bei der Datenbank ankommt, anhand von Firewall Regeln, ob ein Zugriff ausgeführt werden darf oder nicht. In Kombination mit lokal installierten Agenten kann eine Datenbank effektiv geschützt werden, ohne an der Datenbank oder dem Datenmodel direkt etwas ändern zu müssen. Auf diese Weise lassen sich recht einfach Compliance Auflagen umsetzten. Nichtsdestotrotz braucht es für den Einsatz dieser Produkte genauso ein Sicherheitskonzept, Know-how sowie entsprechende Investitionen bei der Beschaffung, Konfiguration und Betrieb der Lösung.

Fazit

Oracle sowie Dritthersteller bieten verschieden Produkte, um das Risiko eines Datenverlustes zu reduzieren und Datenbanken in der Cloud sowie On-Premises sicher zu betreiben. Doch je nach eigesetzter Technologie und Architektur sind der Aufwand und die Kosten sicher massgebliche Punkte, welche explizit zu betrachten sind. Trotzdem bieten moderne Cloud basierte Umgebungen interessante Alternativen, welche heutzutage in jedem IT Projekt zu berücksichtigen sind. Ein Unternehmen muss dazu aber "seine Daten" und deren Wert kennen. Mit entsprechenden Risikoanalysen, genauen Definitionen der Ist- und der Sollwerte sowie Prüfung der Bedürfnisse können rechtliche Fallstricke gezielt umgangen werden. Gepaart mit den technischen Vorkehrungen kann ein Unternehmen beruhigt seinen sicheren Weg in die Cloud antreten. Das Vertrauen zum gewählten Cloud Dienstleister spielt dabei, wie mehrmals angemerkt, sicher eine wesentliche Rolle. Schliesslich geht es um die Daten ihres Unternehmens.

Viel Erfolg beim Einsatz von Trivadis-Know-how wünscht Ihnen

Stefan, Oehrli
Solution Manager / Partner

Trivadis AG

Sägereistrasse 29
CH- 8152 Glattbrugg
Telefon: + +41 58 459 55 55
E-Mail: stefan.oehrli@trivadis.com
www.trivadis.com

Weiterführende Informationen, Links…

Trivadis Unternehmenswebseite www.trivadis.com

Trivadis Security Expert Team www.trivadis.com/de/security

Blog Stefan Oehrli www.oradba.ch/category/oud