Die Wahl zwischen Self-Hosting & Outsourcing

Eine Entscheidungshilfe für Unternehmen

MATESO
PASSWORD SAFE

Ist Cloud Computing die Zukunft?

Stellt man IT-Sicherheitsexperten diese Frage, gehen die Meinungen teilweise stark auseinander. Einerseits gibt es die Anhänger der "All-Cloud-Strategie": Die Hybrid Cloud ist für sie nur ein Übergangsmodell dazu, dass eigene Rechenzentren bald ausgedient haben. Andererseits werden von manchen auch komplett ausgelagerte Betriebsprozesse als eher kritisch angesehen. Nur Self-Hosted hat für sie als langfristige Kompromisslösung am Markt Bestand. Was wünschen sich aber Unternehmen? Sie hätten gerne beides – die Flexibilität einer Cloud-Lösung und dabei ein sicheres Gefühl, die Daten selbst unter Kontrolle zu haben. Aber ist das möglich?

> **Jedes Unternehmen ist ein Software-Unternehmen. Es geht nicht mehr nur darum, eine Lösung zu beschaffen und zu implementieren.**
>
> Watts S. Humphrey / Software-Pionier

Wie der sogenannte Vater der Software-Qualität, Watts Humphrey, schon vor über 20 Jahren richtig erkannte: "Jedes Unternehmen ist ein Software-Unternehmen. (...) Es geht nicht mehr nur darum, eine Lösung zu beschaffen und zu implementieren. Es geht nicht um eine einfache Softwarelösung. Es geht wirklich darum, dass Sie selbst über Ihre eigene Zukunft als digitales Unternehmen nachdenken."

Dieses Whitepaper dient deshalb dazu, wichtige Denkanstöße zu vermitteln, um sich über das Anforderungsprofil für Ihr Unternehmen klarer zu werden. So wird das Für und Wieder der Self-Hosted- , Cloud- und MSP-Modelle abgewogen und dabei ein Überblick geboten, welche Vorteile und potentielle Risiken diese im Vergleich zueinander und auch bezüglich dem Einsatz professioneller IT-Sicherheitslösungen wie Password Safe bieten.

Cloud Services

Mit Cloud-Services können Maschinen, Dienste und Applikationen online bereitgestellt und darauf zugegriffen werden. Bei der Nutzung von Public Cloud stellt der Anbieter mindestens eine Plattform bereit, die auch vom diesem verwaltet wird. Was hält IT-Entscheider davon ab, in die Cloud zu ziehen? Oftmals sind es Bedenken bezüglich Compliance und Datensicherheit. Denn Cloud bedeutet gegebenenfalls auch, dass private und schützenswerte Informationen an den Cloud-Anbieter ausgelagert werden. Dabei gibt es sensible unternehmerische Daten, die nicht unbedingt in die Hände von externen Anbietern gehören. Jeder Staat handhabt die Zugriffsrechte auf Daten auf Basis der dortigen Datenschutzgesetze und Vorschriften zudem unterschiedlich. Kunden müssen sich deshalb darüber im Klaren sein, dass die Daten des Kunden je nach Standort des Cloud-Anbieters und der Server der Rechtssprechung des dortigen Landes unterliegen.

Zudem kann jeder Anbieter seine eigenen Nutzungsbedingungen und Datenschutzbestimmungen aufstellen, wovor das Bundesamt für Sicherheit und Informationstechnik (BSI) warnt. Die Auswahl des Cloud-Anbieters – Stichwort “Trusted Clouds” – ist also entscheidend, wenn man sich letztendlich dazu entscheidet, je nach Lösung sogar die Datenhoheit an Externe abzugeben. Wenn aber Unternehmen schon in die eigene Infrastruktur investiert haben, lohnt sich auf jeden Fall zu prüfen, ob Cloud Services eine passende Ergänzung sein können.

Vorteile auf einen Blick

- simpel und schnell realisierbar
- überschaubare Kosten
- keine Eigenverantwortung bei Updates und Sicherheit

Software as a Service

Wenn Anwendungen mit Cloud-Services kombiniert werden, kommt Software as a Service (SaaS) in`s Spiel: Software as a Service ist für Unternehmen gedacht, die Anwendungen ortsunabhängig über die Cloud via Browser oder API nutzen können. Der Anbieter übernimmt dabei die Wartung der Software. So bieten sie ein agiles und vor allem preiswertes Nutzungsmodell, bei dem der Kunde genau das kauft und bezahlt, was er auch benötigt.

Allerdings ist auch bei SaaS-Anbietern oftmals nicht klar ersichtlich, wie genau die Daten verarbeitet werden. Denn sie liegen auf dem Server des Anbieters, was in Bezug zur EU-DSGVO kritisch sein kann. Und je größer einer dieser Anbieter ist, umso größer ist auch die Gefahr eines Angriffs durch Dritte, um hier sensible Daten abzugreifen. Kommt es zudem zu einem technischen Problem beim SaaS-Anbieter, kann dies Einfluss auf das gesamte System des Kunden haben und auch den Zugriff auf die eigenen Daten erschweren oder verhindern. Und was, wenn der Anbieter seinen Dienst komplett einstellt? In diesem Falle wüsste niemand genau, was mit den dort gespeicherten Daten passiert. Dazu kommt, dass SaaS-Anwendungen oftmals unkontrolliert genutzt werden und das Risiko von Schatten-IT dadurch steigt.

Self-Hosted-Lösungen

Self-Hosting bedeutet, dass der Kunde die Software lokal oder in der Cloud installiert, betreibt und darauf zugreift. Zudem sind intern technische Kenntnisse und Personalressourcen notwendig, um die selbst gehosteten Anwendungen zu verwalten. Der große Vorteil ist dabei, dass sie die komplette Kontrolle über die Daten behalten und sie nicht in fremde Hände gegeben wird. Vor allem kritische Infrastrukturen wie Finanzdienstleister, Bundesbehörden und Telekommunikationsanbieter profitieren hiervon, da diese gesetzlich verpflichtet sein können, Daten in einer privaten, sicheren Umgebung zu speichern. Im Vergleich zu SaaS-Lösungen bietet Self-Hosted auch die Möglichkeit, Lösungen ihrem Einsatz gemäß bereitzustellen und somit die beste Performance zu gewährleisten.

Password Safe ist als Self-Hosted-Lösung verfügbar und kann entweder On-Premises, Hosted (dt. im Rechenzentrum) und in der Cloud betrieben werden. Password Safe bietet eine Desktop- als auch eine Web-Version. Durch die stateless Multi-Tier-Architektur werden die Daten nur auf der Datenbank gespeichert. Password Safe ist als Self-Hosted-Lösung weltweit einsetz- und verfügbar und kann je nach Bedarf skaliert werden.

Vorteile auf einen Blick

- volle Datenkontrolle und -sicherheit
- Support vom Hersteller
- bessere, flexible Skalierbarkeit
- Einhaltung gesetzlicher Vorschriften
- Kostenkontrolle und gesicherte Leistung
- an den Anwendungsfall angepasster Betrieb - z.B. erweiterte Ausfallsicherheit

Was bedeutet On-Premises?

Der Anbieter stellt dem Kunden seine Software zur Verfügung, die dann auf der eigenen Hardware des Kunden, hinter seiner eigenen Firewall, in seinem eigenen Rechenzentrum installiert und betrieben wird. Der Anbieter ist für die Bereitstellung der Software und Upgrades verantwortlich und kann auch den Support für die Softwareinstallation übernehmen, während der Kunde sich um den Betrieb der Software kümmert.

Hybrid Cloud als Verbindung zweier Welten

Auch wenn viele Unternehmen ihre Daten komplett in die Public Cloud umziehen, kann es für manche günstiger sein, nur einen Teil der Anwendungen in die Cloud zu migrieren – etwa aus Gründen der Compliance oder Datensouveränität. In diesem Fall bietet sich ein hybrides Cloud-Modell an, das die Möglichkeit einer öffentlichen Cloud mit der eigenen IT-Infrastruktur vor Ort vereint. Gerade für Unternehmen, die schon in die eigene Infrastrukturen sowie geschultes Personal und eigene Anwendungen investiert haben, ist die Hybrid Cloud gut geeignet. So können bereits existierende Ressourcen genutzt und mit externen Services ergänzt oder auch Prozesse ausgelagert werden. Und Investitionen in die klassische IT sind auch in Zukunft nicht mehr so hoch.

Durch das Hybrid Cloud Modell können Unternehmen selbst steuern, wo die Datenhoheit behalten werden soll. Auch mit einer prinzipiellen Self-Hosted-Lösung wie Password Safe ist dies möglich, wenn Unternehmen keine eigene geeignete IT-Infrastruktur zum Hosten besitzen.

Der entscheidende Vorteil bei diesem Modell: Im Gegensatz zu eigentlich allen SaaS-Anbietern kann der Kunde selbst gehostete Lösungen ohne jegliche Hardware nutzen oder die Hardware mit Cloud-Ressourcen für maximale Leistung kombinieren. Unternehmen können – bei Betrieb in der Cloud – entsprechende Hosting-Dienstleister auswählen, deren IT-Infrastrukur beispielsweise in Deutschland angesiedelt sind und der Schutz der eigenen Daten ist gewährleistet. So bietet die Public Cloud Lösung bei einem inländischen Standort einen DSGVO-konformen Datenschutz wie das eigene Rechenzentrum vor der Tür.

Tipps für die Umsetzung

Doch auch eine Hybrid-Lösung kann trickreich in der Umsetzung werden. Besondere Sorgfalt erfordert dabei das Datenbank-Hosting. Denn bei der hybriden Lösung können Unternehmen die Daten in der Cloud, im Rechenzentrum oder an beiden Orten hosten. Da eingehender Verkehr allgemein kostenlos ist, bietet es sich an, die Daten aus dem Rechenzentrum in die Cloud zu schicken. Die Datenbanken können in der Public Cloud und kleinere parallel in beiden Umgebungen betrieben werden. Gerade größere Systeme in der Cloud zu betreiben kann zu hohen Kosten führen, wenn die Daten wiederum On-Premises verarbeitet werden sollen.

Im Vergleich zu On-Premises-Umgebungen können in der Cloud alle Maschinen in sehr vielen Details angepasst werden, was kann im Hinblick auf die Erfüllung aller Anforderungen gefährlich sein. Deshalb ist es für Unternehmen unumgänglich, sich im Vorfeld darüber zu informieren, welche Anforderungen bestehen und welche potentiellen Herausforderungen es zu überwinden gilt. Im Falle von Password Safe gelten folgende Voraussetzungen:

- Maschinen mit Microsoft Server Betriebssystem für den SQL-Server mit den entsprechenden Systemvoraussetzungen
- Maschinen mit Microsoft Server Betriebssystem für den Anwendungsserver mit den entsprechenden Systemvoraussetzungen
- Für beide Maschinen wird jeweils eine Lizenz für das Betriebssystem benötigt. Der SQL-Server benötigt zudem noch eine MSSQL-Lizenz.

Vorteile auf einen Blick

- dank standardisierter und offener Lösungen lassen sich Anwendungen und Daten bei Bedarf auch auf andere Systeme umziehen
- nicht auf einen Anbieter angewiesen sein
- diverse Hosting-Optionen:
  - in der Cloud
  - inhouse
  - an beiden Orten

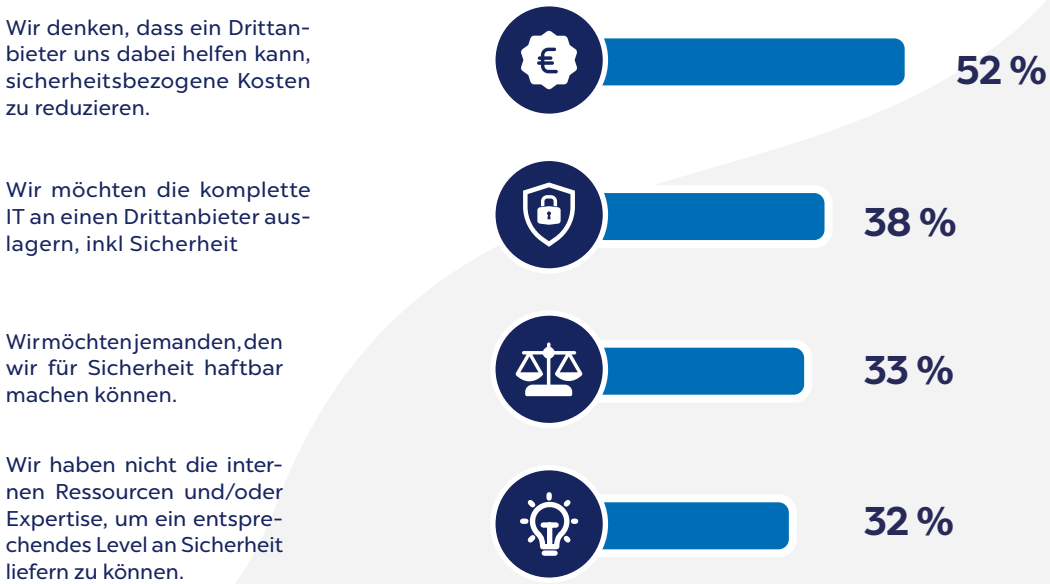
Managed Services

Mittlerweile sind vor allem Managed Services auf dem Vormarsch, um auch kleineren und mittelständischen Unternehmen Anwendungen anbieten zu können, die zuvor nur Großunternehmen und Konzernen vorbehalten waren. Denn in Betrachtung der herkömmlichen IT – der klassischen Bereitstellung dedizierter oder virtueller Server in der eigenen Infrastruktur – bedeutet Self-Hosted meist auch höhere Investitionen für das eigene Unternehmen, die kleinere Unternehmen schwer umsetzen können. Dabei wird vom Netzwerk über die Server-Architektur, Speicherung und Sicherheit von Lösungen enorme Expertise und Erfahrung in der Betreuung von IT-Lösungen vorausgesetzt. Dazu kommen Faktoren wie Zeit und Personal, um Services inhouse zu managen.

Warum sich Unternehmen für Managed Services entscheiden

Laut einer Studie von Kaspersky möchte jedes zweite Unternehmen mit einem MSP vor allem die sicherheitsbezogenen Kosten reduzieren. Sogar rund 32 % können aufgrund des Mangels von Expertise und Ressourcen in dem Bereich nur durch einen MSP ihre Geschäftstätigkeit fortsetzen. Besonders auffällig war, dass 74 % angaben, dass die Cybersicherheit bei der Wahl ihres MSP´s ein Schlüsselmerkmal darstellte.

Gründe für das Planen einer Auslagerung des IT-Securitys-Managements an einen MSP



Quelle: Kaspersky MSP Report 2019

Entscheidet sich ein Unternehmen hingegen für das Outsourcing von Services an einen Managed Service Provider, bedeutet dies, auch auf das gesamte Know-how des MSP zurückgreifen zu können. Gerade, wenn ein Server nicht zu 100 % ausgelastet wäre und dennoch komplett bezahlt werden müsste, tendieren Unternehmen anstelle des produkt- zum servicebezogenen Ansatz, um ihre Kosten so gering wie möglich zu halten. Die Managed Service Lösung ist sofort einsatzbereit und der Kunde zahlt nur, was auch benötigt und tatsächlich genutzt wird. Wird ein Service nicht mehr benötigt, kann er vom Managed Service Provider umgehend deaktiviert werden. Dies macht gerade kleine Unternehmen wettbewerbsfähiger, da sie schneller auf neue Situationen reagieren und ihren Bedarf angleichen können. So ist eine Entscheidung zum Auslagern der Prozesse auch eine Entscheidung für das Unternehmen, wenn es erkannt hat, den Aufwand nicht (mehr) alleine stemmen zu können.

Auch Password Safe ist als Managed Service verfügbar, um allen Unternehmen die für sie richtige Password Security Lösung anbieten zu können. Die Managed Service Provider sind vom Hersteller MATESO selbst umfangreich geschulte und zertifizierte Dienstleister, die eine hohe Expertise im IT-Security-Bereich aufweisen. Die Server werden sicher im DACH-Raum gehostet.

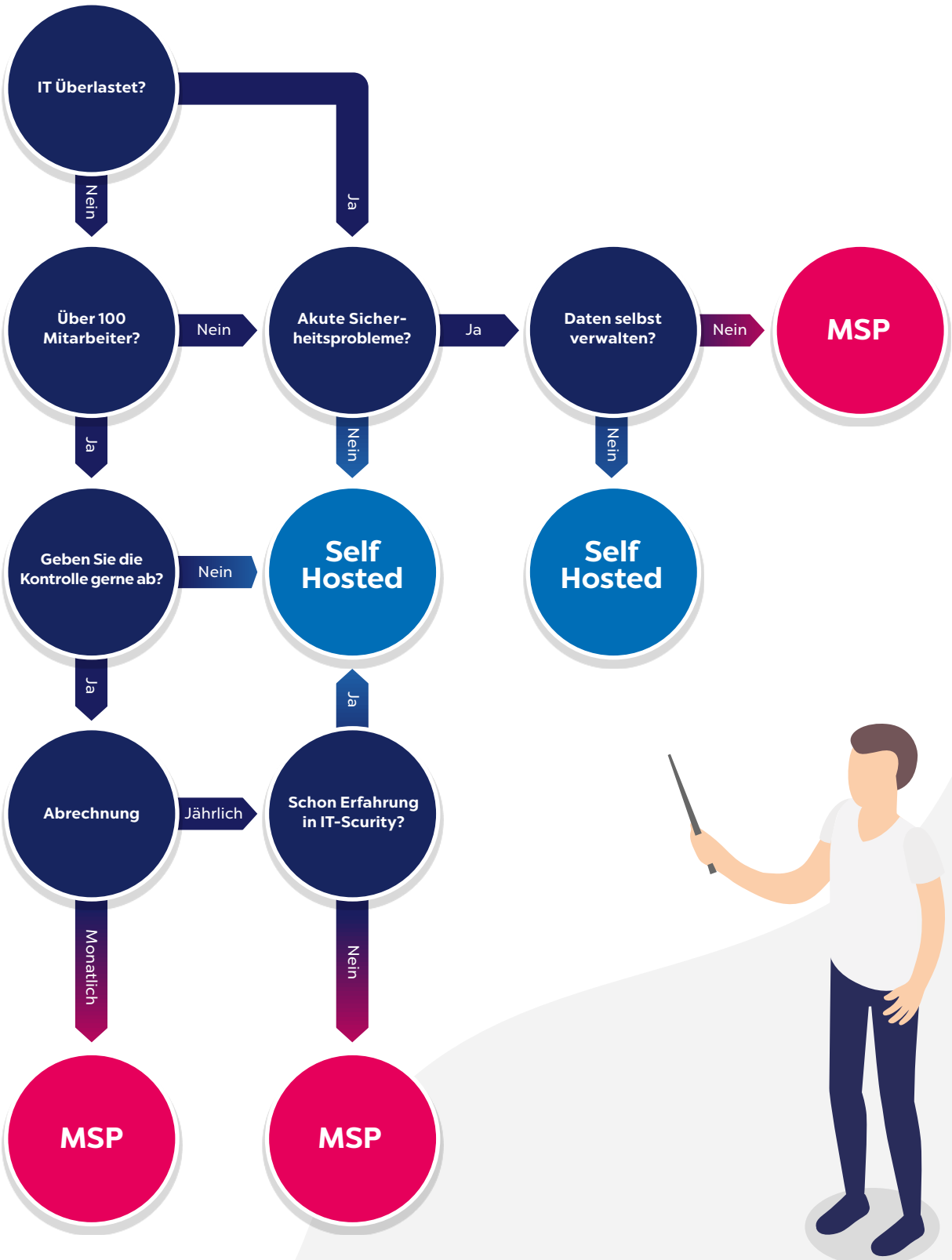
Mehr Informationen zu Password Safe MSP

Vorteile auf einen Blick

- Datenhoheit bei zertifizierten Partnern in der DACH-Region
- große Expertise und Erfahrung durch persönlichen Ansprechpartner und Berater
- standardisierte und auch individuelle Lösungen möglich
- Investitionen und Kapazitäten durch auf Kosten abgestimmte Nutzung sparen
- überall verfügbar
- kein eigener Server-Aufwand und Verantwortung mehr
- neue Funktionen einfach beim Partner anfragen, ohne selbst Updates ausführen zu müssen
- nicht mehr um Backups kümmern müssen

Entscheidungshilfe MSP / Self-Hosted

Sie wissen nicht, ob Sie selbst hosten oder einen MSP in Anspruch nehmen sollten? Nutzen Sie unsere Entscheidungshilfe für eine erste Einschätzung.



Fazit

Um flexibler auf die neuen Marktanforderungen und Kundenwünsche reagieren zu können, nutzen viele Unternehmen bereits heute schon Public Cloud Lösungen für ihre Workloads. Die Akzeptanz in Cloud-Infrastrukturen dahingehend steigt kontinuierlich. Es kann für ein Unternehmen jedoch kostengünstiger sein, Anwendungen mit speziellen Abhängigkeiten On-Premises zu behalten und nur einen Teil der Services in die Cloud zu migrieren. Daher muss fallweise geprüft werden, ob bestimmte Workloads aus Gründen der Compliance und Datensouveränität intern verwaltet werden müssen. Liegt dieser Fall vor, ist ein hybrides Cloud-Modell zu empfehlen.

Bei allen vorgestellten Vor- und Nachteilen sollten sich Unternehmen nicht zuletzt eine entscheidende Frage stellen: "Hosten Sie gerne selbst oder empfinden Sie es eher als lästig?" Denn mit allem Für- und Abwägen von preislichen, zeitlichen und sicherheitstechnischen Faktoren bleibt die Entscheidung unter dem Strich eine des "Wollens", die nur individuell getroffen werden kann und sich durch obige Frage vielleicht schon erübrigt hat. Sicher ist – professionelle Systeme sollten sich eben diesen individuellen Entscheidungen für ein "Pro, mit oder gegen die Cloud" anpassen und für jede Eventualität die richtige Lösung bieten können.

Autor:
Kristina Kaya
Product Marketing Managerin

MATESO

Die MATESO GmbH ist ein führendes deutsches IT-Unternehmen, das sich seit der Firmengründung in 2006 erfolgreich im DACH-Raum etabliert hat. Die entwickelte Passwort-Sicherheitslösung Password Safe wird durch ihr weltweites Partnernetzwerk international vertrieben. Namhafte Referenzen bezeugen den Technologie- und Know-how-Vorsprung der IT-Software.

Heute verzeichnet das stetig wachsende Unternehmen branchenübergreifend über 10.000 Firmenkunden mit mehreren Millionen Anwendern weltweit – darunter 21 Firmen der Dax 30.

PASSWORD SAFE

Pioneer im Enterprise Password Management

Password Safe dient Unternehmen als zentraler digitaler Tresor zur Sicherung, Verwaltung und Überwachung von sensiblen Daten wie Passwörtern, Dokumenten und Geheimnissen.

MATESO GmbH
Daimlerstraße 15, D-86356 Neusäß
Web: www.passwordsafe.de
E-mail: sales@passwordsafe.de
Tel: +49 821 74 77 87-0

MATESO
PASSWORD SAFE