Leistungsbeschreibung
Cloud-Dienste und Cloud-Server im Rechenzentrum

Rechenzentrum:
Alle vom Rechenzentrum angemieteten Datenräume sind als separate IT Sicherheitsräume im Sinne des IT-Grundschutzkataloges, herausgegeben vom Bundesamt für Sicherheit in der Informationstechnik (BSI), gemäß Anforderung der Kategorie "Grundschutz" ausgerüstet. Es wurden spezielle Maßnahmen für Brandschutz, Klimatisierung sowie Überwachung (Zutrittssicherung, Videoüberwachung) getroffen. Die Umgebungsbedingungen wie Temperaturen und Luftfeuchtigkeit werden ständig überwacht, erfasst und aufgezeichnet. Beim Über- oder Unterschreiten von Grenzwerten werden entsprechende Maßnahmen eingeleitet. Die Netzversorgung sowie die Netzersatzanlage (NEA) sowie USV Anlage erfolgt für das Rechenzentrum mit gesondert bereitgestellter Trafostation des Energieversorgers. Das Rechenzentrum ist über mehrere (aktuell 9) 10GBit Leitungen an unterschiedliche Provider angebunden, um ausreichende Bandbreite und Redundanz sicherzustellen. Die tisoware-Lösung (Anwendung und Datenbank) steht Ihnen rund um die Uhr – ausgenommen vorher bekannt gemachter Wartungsfenster - zur Nutzung zur Verfügung. Das Rechenzentrum sichert eine hohe Verfügbarkeit von 99 % zu. Die Verfügbarkeit des Rechenzentrums liegt damit in den allermeisten Fällen über der Verfügbarkeit einer eigenen IT.

Cloud-Dienste / Cloud-Server:
Während Cloud-Server die Hardware, das Betriebssystem, die Netzanbindung und verschiedene Dienstleistungen wie Datensicherung und auch optional VPN Tunnel, Citrix Lizenzen usw. bereitstellen und das Vorhandensein der tisoware Applikationslizenzen voraussetzt, bietet der Cloud-Dienst ein Mietmodell sowohl für die Cloud-Server als auch für die Applikationssoftware tisoware.

Cloud-Server:
Bei den Cloud-Servern handelt es sich um Virtuelle Server auf der Basis von VMware vSphere in einer aktuellen Version, die auf VMware HA / DRS Clustern betrieben werden und sind somit durch die VMware Hochverfügbarkeitsfunktionen für den Ausfall einer Server Hardware geschützt. Durch ein vollautomatisches Load Balancing werden Cloud-Server entsprechend ihrer Leistungsanforderungen und dynamisch auf unterschiedlicher Hardware verteilt. Die Leistungswerte der Cloud-Server werden im Leistungsschein vereinbart. Bei den angebotenen Ressourcen handelt es sich um sogenannte virtuelle Ressourcen wie virtuelle CPUs, virtuelles RAM und virtuelle Disks. In der Pauschale für Cloud-Server sind auch die Lizenzen für Managed Cloud-Backup enthalten. Die Cloud-Server sind zum Betrieb der Applikationen von tisoware vorgesehen. Andere Anwendungen sind dafür nicht vorgesehen. Ein administrativer Zugriff auf die Server und deren Konfiguration ist kundenseitig nicht vorgesehen. Im Rahmen unseres Angebotes werden die tisoware-Dienste, hochverfügbar an den Schnittstellen (Citrix-Portal, WEB-Client, Datentransfer) bereitgestellt.

Datensicherung:
Zur Datensicherung der Cloud-Server wird ein Datensicherungsverfahren verwendet, bei dem der gesamte Server als Image gesichert wird. Es wird dazu keine Netzwerkverbindung zwischen Datensicherungssystem und Cloud-Server oder administrative Accounts in den zu sichernden Cloud-Servern benötigt. Dadurch kann eine hohe Sicherheit bei der Durchführung der Datensicherung gewährleistet werden. Die Datensicherungen werden 5x wöchentlich, in der Regel Montag bis Freitag, durchgeführt. Es können sowohl ganze Images als auch einzelne Files aus den Images wiederhergestellt werden. Die Wiederherstellung von Images und/oder Files wird nach Aufwand berechnet. Die Datensicherungen werden 14 Tage vorgehalten. Kopien von Datensicherungen werden georedundant, in ein zweites entferntes Rechenzentrum kopiert.

Es werden drei Service Levels zur Datensicherung von Cloud-Servern angeboten.

Basic: Die Datensicherungen werden 7 Tage vorgehalten.
Standard: Die Datensicherungen werden 14 Tage vorgehalten.
Premium: Die Datensicherungen werden 30 Tage vorgehalten.

Monitoring:
Die Cloud-Server werden durch VMware vCenter und VMware Monitoring Systeme 24x7x365 überwacht. Überwacht werden dabei die Ressourcen (CPU, RAM, Netzwerk, Disk) sowie die für den Betrieb der Server notwendige Infrastruktur. Zusätzlich werden von tisoware bestimmte Überwachungsfunktionen für bestimmte Dienste wie TomCat, Datentransfer von und zu den Buchungsterminals, Datentransfer zu Exchange sowie dem Email Versand kontinuierlich ausgeführt. Falls erforderlich werden diese Dienste neu gestartet.

Support:
Der Support umfasst telefonische Unterstützung während der Servicezeit (üblicherweise
Mo - Fr, 08:00 Uhr – 17:00 Uhr). Gesetzliche Feiertage in Bayern und Baden-Württemberg, der 24.12. und der 31.12. sowie vorher bekannt gemachte Wartungsfenster sind von der Servicezeit ausgenommen. Weitere Festlegungen sind im Software-Wartungsvertrag getroffen.

Wartungsfenster:
Wartungsfenster finden außerhalb der regulären Servicezeiten statt. Darüber hinaus gehende Wartungsfenster können mit dem Kunden vereinbart werden. Bei wichtigen Gründen wird der Kunde seine Zustimmung nicht unbillig verweigern. tisoware ist in diesen Wartungsfenstern berechtigt, Anwendungen zu pflegen und / oder Server zu warten, Datensicherungen oder sonstige Arbeiten vorzunehmen. Der Kunde erteilt bereits jetzt seine Zustimmung dazu, dass während der gesamten Vertragslaufzeit eine geplante Nichtverfügbarkeit in diesen Wartungsfenstern besteht. Wenn und soweit der Kunde in Zeiten der geplanten Nichtverfügbarkeit die Dienste nutzen kann, so besteht hierauf kein Rechtsanspruch. Kommt es bei der Nutzung eines Dienstes während eines Wartungsfensters zu einer Leistungsreduzierung oder Leistungseinstellung, besteht für den Kunden kein Anspruch auf Mangelhaftung oder Schadenersatz.

Firewall:
Die ein- und ausgehenden Verbindungen werden mittels modernster Firewalls überprüft, überwacht und ggf. abgelehnt und protokolliert. Es werden nur die notwendigen Ports, Protokolle und Dienste freigeschaltet. Mittels VPN-Verbindung (Site-to-Site) erfolgt eine Authentifizierung an der Core-Firewall und die Verbindung zum Zielserver / Zielnetzwerk. Die Verfügbarkeit von VPN Verbindungen ist grundsätzlich abhängig von der gewählten tisoware Edition –vgl. auch Feature Matrix. Web-Zugriffe über HTTP(S)- Verbindungen werden durch die WAF (Web-Application-Firewall) entgegengenommen. Hiernach erfolgt eine Prüfung gegen Security-Profile und das Routing zu den Ziel-Ressourcen.

Voraussetzungen, die durch den Kunden sichergestellt werden müssen:

Leitungsanbindung des Kunden: Bereitstellung einer stabilen und ausreichend dimensionierten Internetverbindung vom Kunden in das Internet durch den Kunden. Leitungsprobleme durch den lokalen Internet Service Provider (ISP) fallen nicht in die Verantwortung von tisoware. Die Entstörung liegt in der Verantwortung des Kunden. tisoware kann auf Wunsch Unterstützung leisten oder vermitteln. Diese Leistungen können gegen zusätzliche, gesonderte Vergütung nach Aufwand vereinbart werden. Geeignet für die Leitungsanbindung sind ausschließlich Business Internet Verbindungen mit einer festen IP-Adresse.

Firewall (nur Enterprise-Edition): Zur Betreuung der vor Ort beim Kunden befindlichen Firewall Geräte müssen entsprechende Zugänge zur Verfügung gestellt werden, die auch schreibenden Zugriff auf die Geräte erlauben, sofern die Konfiguration nicht kundenseitig umgesetzt wird.

LTE-Modem (nur Enterprise-Edition): Als Option zu einer Managed Firewall können mit einem LTE-Modem Failover-Verbindungen über ein beliebiges LTE-Netz eingerichtet werden, um die Verfügbarkeit bei Leitungsproblemen zu erhöhen. LTE-Karten oder Mobilfunkverträge sind nicht im Leistungsumfang enthalten und sind vom Kunden zu stellen.

Betrieb verschiedener Geräte: Zum Betrieb der Lösung setzen wir die Nutzung eines aktuellen und von uns freigegebenen Browsers voraus. Hierzu verweisen wir auf die Umgebungsrichtlinien der jeweils einzusetzenden tisoware-Version.