VERTICAL® SECURITY

Stand: August 2016

Verfahren und zertifizierte Standards

- Plattform Operation nach ITIL V3
- DevOps Release und Patch Mgmt.
- Deutscher Rechtsraum & Datenschutz
- 24/7 Plattformbetrieb
- DIN EN ISO 9001
- DIN EN ISO 27001
- Trusted Cloud

Datenhoheit

vertical® ist von Grund auf darauf ausgelegt, Ihre Daten sicher und integer zu halten und zu verarbeiten. Die Plattform ist entsprechend redundant und mit Maßnahmen zur Datensicherung ausgestattet. Als alleiniger Eigentümer der Inhaltsdaten sind Sie stets in der Lage, eine Kopie anzufertigen und diese z.B. auf einem Offline-Medium aufzubewahren.

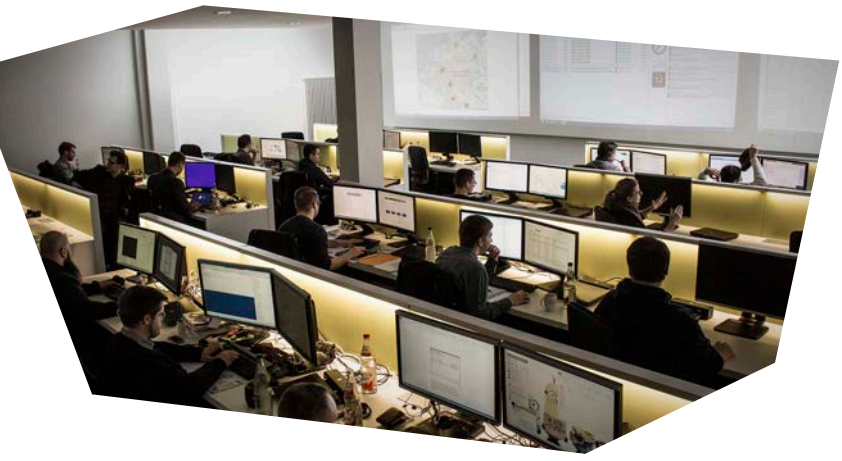
Sie entscheiden dabei eigenständig, welche Daten wie lange aufbewahrt werden (Data Retention) und welche Daten Sie unwiederbringlich löschen möchten.

Der Plattform- und Datenstandort ist Deutschland. Somit unterliegen die Daten und die Datenverarbeitung deutschem Recht und berücksichtigen das deutsche Datenschutzgesetz. Eine Speicherung der Daten außerhalb Deutschlands bedarf einer vorherigen expliziten Zustimmung durch den Kunden.

Service Management

Die gesamte Kommunikation zwischen Endbenutzer und dem Service Team wird transparent (via SystemCare) verarbeitet und protokolliert. Support-Anfragen werden als Incident erfasst und verarbeitet. Hierfür stehen den Benutzern diverse Schnittstellen (Userdesk, vertical® App, Hotline, Mail) zum ServiceDesk zur Verfügung.

Für betriebs- und IT-verantwortliche Personen in Ihrem Unternehmen steht zudem ein Management Cockpit (ControlCenter) zur Verfügung, in dem alle Service Anfragen, die Vorgänge im Detail sowie die SLA Einhaltung und Service Reports eingesehen werden können.



Platform Operations

Ein separates Expertenteam ist für den 24/7 Betrieb der Plattform verantwortlich. Die Betriebsprozesse sind nach ITIL V3 ausgerichtet und in Software abgebildet. In das Aufgabengebiet fallen Wartungen, das Patchmanagement, die Bearbeitung von Plattform-Incidents und die Durchführung von Changes nach Freigabe. Alle Zugriffe auf die Systeme werden zentral protokolliert und nur internem Personal gestattet. Für den Zugriff auf ein System mit erweiterten administrativen Rechten liegt immer ein Service Request zu Grunde.

Umzugs- und Rückführungs-Szenario

Es wurden bei der Entwicklung von vertical® anerkannte Standards eingesetzt- daher ist die Rückübertragung der Kundendaten (Business IT) jederzeit im entsprechenden Format möglich, ebenso lässt sich der Umzug der Infrastruktur zu einem anderen Provider mit minimaler Dienstunterbrechung realisieren. Sofern kundenindividuelle Dokumentationen vorliegen (beispielsweise über spezielle Prozesse, Applikationen, Design, Zugangsdaten; Betriebshandbuch), werden diese in gängigen Dateiformaten (Word, PDF, Excel, CSV, Text) ausgehändigt. Nach Freigabe durch den Kunden wird vertical die Kundeninstanzen und -Daten in den SaaS-Diensten sicher und unwiderruflich löschen.

Zertifizierungen

Neben den etablierten Prozessen und operativen Maßnahmen zur eigenen betriebsinternen Effizienz ist es uns ein Anliegen, diese durch anerkannten Standards und Normen nachzuweisen.

Die vertical® Plattform und die zugehörigen Betriebsprozesse werden den Anforderungen aus ISO Standards und der Trusted Cloud Initiative des Bundesministeriums für Wirtschaft und Energie gerecht.

Das DataCenter ist zudem ISO 27001 zertifiziert und erfüllt für die Schweiz die Outsourcing-Vorschriften der Eidgenössischen Finanzmarktaufsicht (FINMA).

Datenstandort & Absicherung

- Tier 3+ Rechenzentren
- Redundante Stromversorgung
- 72h autonomer Betrieb
- 24/7 Zugangssicherheit – und Kontrolle
- Zwei-Wegeführung der Datenleitungen
- TÜV SÜD: Prüfbescheinigung TIER III

vertical DataCenter

Das vertical DataCenter liegt in einem DataCenter Campus in Frankfurt am Main und ist mit einer Rechenzentrums-Fläche von 60.000 m2 Europas größter einzelner Rechenzentrumsstandort. Die auf einem knapp 54.000 m2 großen Grundstück freistehenden Gebäude sind nach den speziellen Anforderungen für die Nutzung als Rechenzentrum entwickelt, errichtet und ausgestattet worden. Um die hohen Sicherheits- und Verfügbarkeitsanforderungen zu erfüllen, wurde der Standort des Rechenzentrums aufgrund einer umfassenden Risikoanalyse (vor allem in Bezug auf Stromversorgung, Datennetzanbindungen und Schutz vor Elementarrisiken) ausgewählt.

Stromversorgung

Die gesamte Stromversorgung auf dem Campus wird als duale Strom- und Notstromversorgung mit einer unterbrechungsfreien A- und B-Versorgung bis in das Rack realisiert. Zusätzlich wird eine redundante Versorgung für alle kritischen technischen Gebäudeanlagen wie Klima-, Kälte-, Lüftungs- und Sicherheitsanlagen gewährleistet. Um eine höchstmögliche Ausfallsicherheit zu gewährleisten, erfolgt durch die Bereitstellung von A- und B-seitigen USV-Systemen in 2(n + 1) Konfiguration. Beide Seiten können somit unabhängig voneinander 100 Prozent der Last übernehmen. Alle versorgungskritischen, haustechnischen Anlagen sind ebenfalls USV-gestützt.

Darüber hinaus stehen zur Überbrückung längerfristiger Netzausfälle je Bauteil Netzersatzanlagen mit Dieselgeneratoren zur Verfügung, welche in n + 2 ausgelegt sind und die gesamte Versorgung des Rechenzentrums übernehmen.

Die Dieselbevorratung ist für einen autonomen Betrieb von 72 Stunden ausgelegt und wird priorisiert nachbevorratet.

Sicherheit und Betrieb

Die Sicherheit der Gebäude und Anlagen wird durch Betriebs- und Sicherheitspersonal gewährleistet. Rund um die Uhr überwachen Sicherheitskräfte und Techniker die Rechenzentren vor Ort. Jeden Tag, 24 Stunden, 7 Tage die Woche.

Der Zugang zu den IT-Systemen ist erst nach persönlicher Authentifizierung beim Sicherheitsdienst möglich. Jeder Bewegung innerhalb des DataCenters wird eindeutig genehmigt und detailliert protokolliert. Jede physische Aktion an den Systemen wird per Kamera überwacht und aufgezeichnet.

So ist sichergestellt, dass kein Unbefugter Zutritt zu den technischen Anlagen hat und Fremde nicht an Ihre Daten kommen können.

Funktionen und Maßnahmen

- Redundante Plattform
- Backup der Daten
- Verschlüsselte Kommunikation
- Monitoring
- Getrennte Netzwerke
- Isolierte Business Applikationen
- Multi-Factor Authentication
- Automation

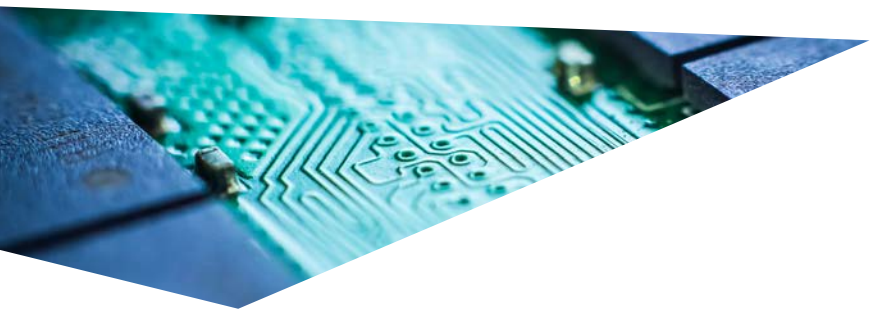
Plattform

Die vertical® Fabric ist eine „Private Hosted Cloud“ Umgebung, die auf die Bedürfnisse von deutschen Unternehmen ausgelegt ist. Standardisierung und Automatisierung der einzelnen angebotenen Dienste sorgen für eine schnelle und flexible Bereitstellung bei gleichbleibender Qualität. Um die Verfügbarkeit der Daten und Dienste gewährleisten zu können, wird die Plattform in mehreren redundanten Rechenzentren (Tier 3+) betrieben.

Unsere Software-as-a-Service-Dienste werden zudem im 24/7 Always On Modus betrieben, so dass einzelne Ausfälle und Wartungen keinen unmittelbaren Einfluss auf die globale Dienste- und Datenverfügbarkeit haben.

Alle Plattform-as-a-Service-Dienste werden kontinuierlich durch ein separates Backup-System gesichert. Diese Dienste werden hauptsächlich im Rahmen der Business IT verwendet und beinhalten somit alle darauf installierten (eigenen) Applikationen und Daten. Eine digitale Archivierung der Backups ist möglich - so können berechtigte Personen im Unternehmen diese herunterladen und auch offline archivieren.

Jeder Kunde auf der Plattform erhält eine volle Netzwerkisolierung, ein eigenes Netzsegment, eigene Router und nur dedizierten Datenverkehr zu und von den zentralen Diensten. Business-IT am Kundenstandort sowie weitere 3rd Party DataCenter-Services können jederzeit über vordefinierte VPN Endpunkte oder über eine exklusive Anbindung realisiert werden.



Monitoring

Die Plattform unterliegt einem umfangreichen technischen Monitoring. Hierdurch werden Abweichungen im Betrieb der Hardwarekomponenten rechtzeitig erkannt und gemeldet um Dienstbeeinträchtigungen vorzubeugen. Dies bezieht sich auch auf die darauf betriebenen Betriebssysteme und Applikationen.

Alle Systeme und die darauf durchgeführten Dateioperationen werden durch Anti-Virus-Scanner geprüft. Diese prüfen die Daten auf Netzwerk-, Plattform- und Betriebssystemebene. Zusätzlich prüfen Intrusion Detection Systeme (IDS), basierend auf Signaturen und Heuristiken, Anomalien im Datenfluss.

Alle Informationen laufen in einer zentralen Analyse-Software zusammen, welche es dem vertical Operations Team ermöglicht, umgehend und zielgerichtet bei Störungen, Angriffen und System-Fehlfunktionen zu reagieren.

Automation

Bei einer Bestellung von vertical® und der Veränderung von gebuchten Diensten werden zahlreiche verteilte Orchestrierungsvorgänge durchlaufen. Um dies schnell und für den Endkunden transparent durchführen zu können, werden diese Vorgänge mittels übergreifender Systemautomation (basierend auf SystemCare®) realisiert.

Zusätzlich ist die technische Betriebsautomation ein wichtiger Erfolgsfaktor in vertical®. Hierdurch können Systeme autonom auf Zustandsveränderungen reagieren und Maßnahmen zur Behebung einleiten wie dies ein Supportmitarbeiter oder Systemadministrator durchführen würde. Der entscheidende Vorteil für den Endkunden liegt in der Schnelligkeit und Akkuratheit dieser Durchführung – rund um die Uhr.

Sichere Kommunikation

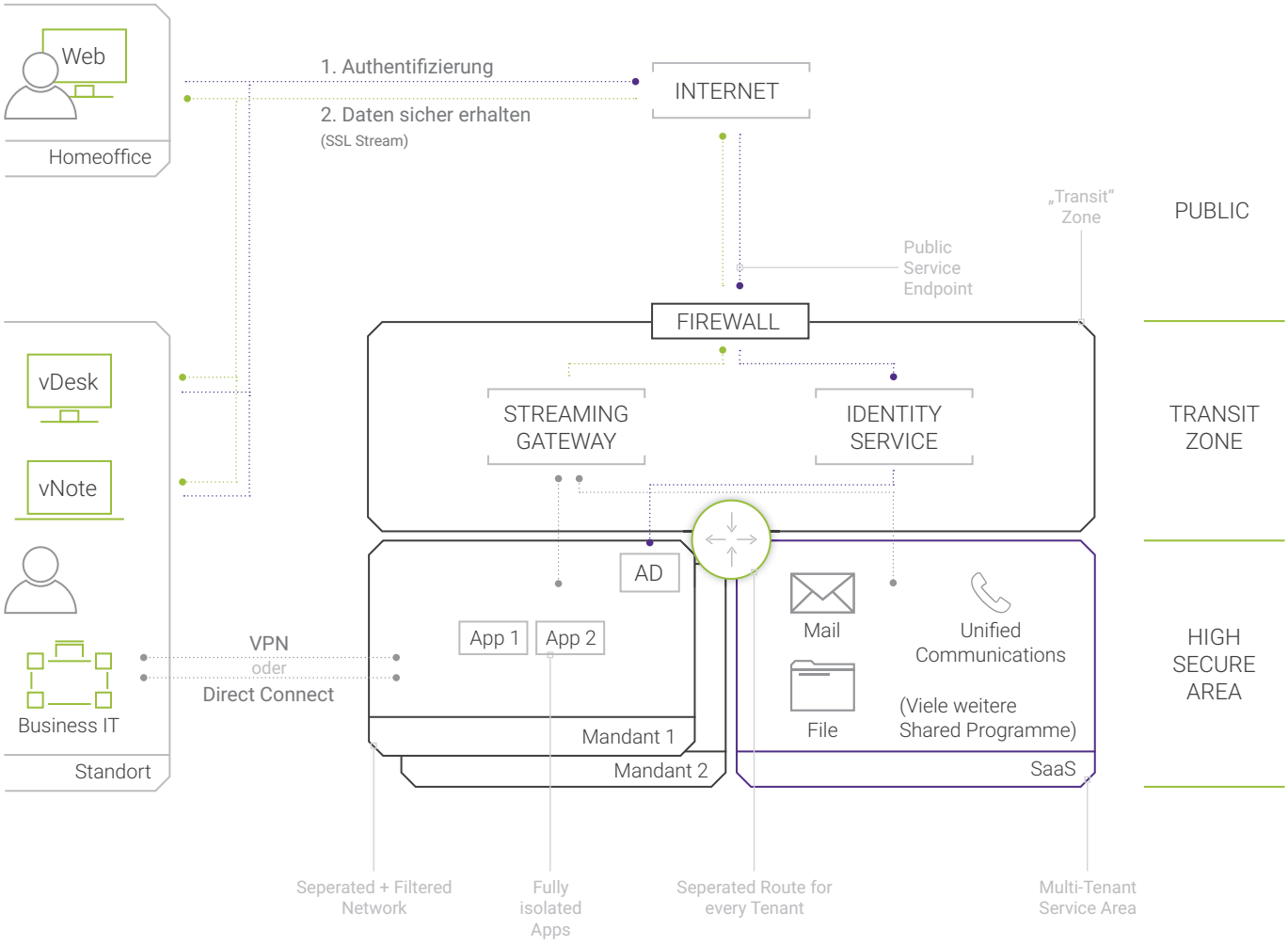
Der Einsatz von anerkannten Verschlüsselungs-standards und -protokollen wie AES, SSL, HTTPS oder IPsec verhindert den unbefugten Zugriff auf die über-tragenen Daten. Ein Multi-Zonen-Netzwerkkonzept sichert sämtliche Inhaltsdaten vor unbefugtem Zugriff. Die Applikationsserver einzelner Business-Applika-tionen werden zudem isoliert betrieben. Es werden nur dedizierte Kommunikationswege zugelassen, die ständig auf Schadsoftware und Anomalien geprüft werden.

Der Datenzugriff über die vertical® Endpunkte ist Ende-zu-Ende verschlüsselt, so dass sogar im klassischen Unternehmens-LAN ausschließlich verschlüsselte Daten übertragen werden.

Multi-Factor Authentication

Auf Wunsch steht Ihnen zur Absicherung Ihrer Zugänge eine Mehr-Faktor-Authentifizierung zur Verfügung, bei der Sie zur erfolgreichen Anmeldung neben den bekannten Benutzerdaten auch noch über ein weiteres Medium den Zugriff freischalten müssen. Besonders interessant kann dies für User mit Zugang zu besonders sensitiven Unternehmensdaten sein. In Kombination mit vertical® Web bedeutet dies, dass ein unbefugtes Einloggen nicht möglich ist und der User über den Versuch sogar in Kenntnis gesetzt wird.

Sicherheits-Architektur



Hinter dem einfachen „Next Generation Workplace“ Modell verbirgt sich eine komplexe Systemlandschaft, um alle angebotenen Funktionen, die Sicherheit und die Flexibilität von vertical sicherstellen zu können.
Hierbei sind alle Zugänge durch eine dedizierte Authentifizierung gesichert. Nach erfolgreicher Authentifizierung werden die Daten ausschließlich verschlüsselt über produkt-/protokollspezifische Gateways übertragen.
Somit ist eine gleichbleibende Funktionalität und Sicherheit, unabhängig vom Verwendungsort sichergestellt.

Alle Systeme mit Kundendaten befinden sich in separaten Netzwerk-Zonen und genießen den höchsten Datenschutz. Alle Applikationen werden isoliert voneinander betrieben, so dass keine direkte Kommunikation zwischen Systemen in derselben Zone möglich ist. Jegliche Kommunikation wird auf Schad-Code geprüft und auf Anomalien untersucht.
Neben dem sicheren „Konsumieren“ aller Dienste über das öffentliche Internet, können jederzeit über sichere oder dedizierte Verbindungen lokale Systeme oder anderweitig betrieben Business-IT in den Digitalen Arbeitsplatz eingebunden werden.

vertical GmbH
Otto-Volger-Straße 3 - 5 a/b
65843 Sulzbach
Hotline +49 6196 8017 0
Fax +49 6196 8017 299
www.vertical.de
info@vertical.de