WIE SICHER – SICHER „V“

Dynamic Services for Infrastructure with vCloud

SICHERHEIT IN DER CLOUD

Dynamic Services for Infrastructure with vCloud (DSI vCloud) von T-Systems ist eine hochsichere IaaS-Variante, mit der Unternehmen ihre Infrastruktur-Kapazitäten nach Bedarf erweitern können. Virtuelle Rechenzentren lassen sich auf Basis von VMware-Technologie bereits bestehenden internen Ressourcen hinzufügen. Der Vorteil für den Nutzer: VMware-Oberflächen und Tools sind in der Praxis des Rechenzentrumsbetriebs bekannt und weit verbreitet. DSI vCloud wird primär in deutschen Twin-Core-Rechenzentren produziert. Die Leistung kann aber auch aus anderen internationalen Standorten bezogen werden. DSI vCloud bietet eine Verfügbarkeit von bis zu 99,98 % p.a., wodurch das Produkt auch für den Betrieb von Produktivsystemen genutzt werden kann.

Der Leistungsumfang bezieht sich auch auf Backup-Funktionen, gemanagte Betriebssysteme, Secure Internet Access und die Fähigkeit zu Disaster Recovery. Damit adressiert es auch gehobene Anforderungen für Daten-Verfügbarkeit und Business Continuity. Die Zugriffswege sind verschlüsselt; ihre detaillierte Protokollierung unterstützt auch Sicherheits-Audits und komplexe Compliance-Anforderungen.

SICHERHEITSKOMPONENTEN IM ÜBERBLICK

TECHNISCH

- Infrastruktur in sicheren Twin-Core Rechenzentren von T-Systems
- Redundanz aller Komponenten in DSI vCloud
- Netzwerktrennung: Dedizierte Firewalls, gesicherte WAN-Verbindungen und eigene Kundennetze
- Kunden-Trennung auf den Ebenen Netzwerk, Compute, Speicher
- Absicherung aller externen Kommunikationsverbindungen
- Verschlüsseltes, authentifiziertes vCloud-Management-Front-End / API
- Internetzugriff auf Virtuelle Maschinen über Firewall-Instanzen
- Administration an DSI vCloud über interne Providerverbindungen
- Penetrationstests zur Verifizierung des hohen Sicherheitsniveaus
- Security und Compliance Logging sowie Monitoring
- Absicherung des vCloud Directors durch eine Web Application Firewall

ORGANISATORISCH

- Externe und interne Sicherheits- und Qualitätsprüfungen
- Datenverarbeitung: Deutsches (und europäisches) Datenschutzrecht
- Identity und Access Management
- Security-Management-Prozesse

T · · Systems ·

WARUM DIE vCLOUD SICHER IST

NETZWERK-INFRASTRUKTUR. Mit DSI vCloud werden Standardisierung und der Einsatz von Virtualisierung auch in Bezug auf das Netzwerk-Design angewandt. Dies bedeutet vor allem:

- Trennung der Netze (Service-, Internet-, Intranet-, Management-Zone)
- Einrichten von Demilitarized Zones (DMZ)
- Entkopplung durch Sicherheitsgateways (beispielsweise Web Application Firewall, Load Balancer, Reverse Proxy etc.)
- Mandanten auf Netzwerkebene werden auf Basis virtueller Netzwerke logisch getrennt

ANBINDUNG. Die Anbindung an das Cloud Management Portal erfolgt über zwei Möglichkeiten: Das hybrid Cloud Modell (DSI vCloud Hybrid) sieht die Anbindung über das Internet vor. Das virtual private Cloud Modell (DSI vCloud Private) ermöglicht die Anbindung ausschließlich über private Netzwerkverbindungen. MPLS, Ethernet Connect und IP-VPN müssen separat beauftragt werden. Über vordefinierte Rollen und Berechtigungen werden die Zugriffe auf DSI vCloud und die entsprechenden Ressourcen kontrolliert. Der Zugriff eines Kunden zu seinem Kundennetzwerk in DSI vCloud erfolgt immer über einen Firewall-Cluster mit dedizierter, virtueller Firewall. Der Netzwerkverkehr wird über Zonen getrennt. Dabei besteht eine Zone aus einem oder mehreren VLANs und ist an einen einzigen Kunden gebunden. Zur Veröffentlichung von Anwendungen oder virtuellen Maschinen, ist der Zugriff aus dem Internet auf die Ressourcen im Kunden-Netzwerk in DSI vCloud erlaubt. Dieser Zugriff wird über die DMZ und die Internet-Firewall realisiert. Kunden, die diese Option nutzen, bekommen ein zusätzliches Netzsegment über eine virtuelle Firewall-Instanz (vShield Edge) angelegt.

STORAGE. Bei DSI vCloud wird der Storage zwischen mehreren Kunden geteilt, die sicher voneinander getrennt sind. Der Storage wird virtualisiert über den Hypervisor bereitgestellt. Ein direkter Zugriff auf das Storage System ist dadurch ausgeschlossen. Zusätzlich werden die physikalischen Festplatten seitens T-Systems verschlüsselt.

SICHERHEITS-MONITORING. Die Infrastruktursysteme von DSI vCloud, sowie die optional von T-Systems betriebenen Betriebssysteme (Managed OS), werden über Sicherheits-Monitoring und Alerting-Tools überwacht, z. B.:

- **Tivoli Module ONSEC:** für Authentifizierung und Autorisierung
- **SIUX System Scanner und WinAudit:** vergleichen Betriebssystem-Konfigurationen (Linux, Windows) mit Sicherheitsvorgaben
- **Anti-Virus:** Warnung, Alarm und aktiver Schutz durch die Antiviren-Software für Windows Betriebssysteme
- Das öffentlich über das Internet erreichbare DSI vCloud Self-Service Portal wird regelmäßig auf Schwachstellen überprüft

ÜBERPRÜFUNG. DSI vCloud wurde von Anfang an internen und externen Penetrationstests, Lasttests und Funktionstest unterzogen. Mit den positiven Testergebnissen wurde die Mehrmandantenfähigkeit der Plattform DSI vCloud nachgewiesen. Die Beurteilung ergab keine Schwachstellen, die den unbefugten Zugriff auf die Daten anderer Kunden ermöglichen.

PROTOKOLLIERUNG. Zur Nachvollziehbarkeit der Systemänderungen ist in DSI vCloud eine automatisierte Protokollierung ausgewählter Komponenten implementiert.

VERANTWORTUNGSABGRENZUNG. Der Kunde hat die volle Kontrolle für seine aufgesetzten Virtuellen Maschinen (VM) und es liegt in seinem Verantwortungsbereich, diese nach seinen spezifischen Schutzbedürfnissen zu sichern. Dazu gehören z. B. Backups der VM, Datenverschlüsselung innerhalb der VM, die Integration in sein Identitätsmanagement oder Patch-Management. Disaster Recovery im Self-Service für DSI vCloud ist eine optionale Leistung.

EMPFEHLUNGEN. Zur Erhöhung der Sicherheit der Kunden sind folgende Sicherheits-Features empfohlen, die von DSI vCloud zur Verfügung gestellt werden:

- Account- und Berechtigungsmanagement im vCloud Director
- Verwendung von sicheren Netzwerkprotokollen
- Definition der Firewall-Regeln basierend auf Whitelists
- Trennung der vCloud-internen Applikationen in verschiedenen Tiers durch Logische Netze
- Backup der virtuellen Maschinen über die enthaltene und optional nutzbare Backup as a Service Lösung (BaaS)
- Absicherung aller Systeme die in Richtung Internet kommunizieren oder zur Administration genutzt werden durch eine starke Authentifizierung

STANDARDS BEI T-SYSTEMS. Mit der Enterprise Security Architecture for Reliable ICT Services (ESARIS) betreibt T-Systems eine Enterprise-Architektur für Informationssicherheit. Sie definiert standardisierte Vorgehensweisen, Prozesse und Anforderungen hinsichtlich Risk Management and Certification, Evidence and Customer Relation, Service Management, Customer and Users, Networks, Data Center. Die Standards basieren auf ISO 27001, ITIL und weiteren Normen. Die internen Standards von T-Systems sind Bestandteil des zertifizierten Informations-Sicherheit-Management-Systems.

T-SYSTEMS BESITZT CORPORATE-ZERTIFIKATE FÜR FOLGENDE STANDARDS:

- Qualitätsmanagement nach DIN EN ISO 9001
- IT-Service-Management-System (ITILv3) nach ISO/IEC 20000
- Managementsystem für Informationssicherheit nach ISO/IEC 27001
- Umweltmanagementsystem nach ISO14001
- Managementsystem für Arbeits-/ Gesundheitsschutz OHSAS 18001
- Assurance Engagements für Service Organisationen ISAE3402

WEITERE INFORMATIONEN
Internet: https://cloud.telekom.de/infrastruktur/vcloud

KONTAKT
Heiko Röhr
Director Sales VMware
Telefon: +49 40 306005173
E-Mail: DSI@t-systems.com

HERAUSGEBER
T-Systems International GmbH
Hahnstr. 43d
60528 Frankfurt am Main
Deutschland