stp·one

Security-Whitepaper

Managed Services

21.02.25

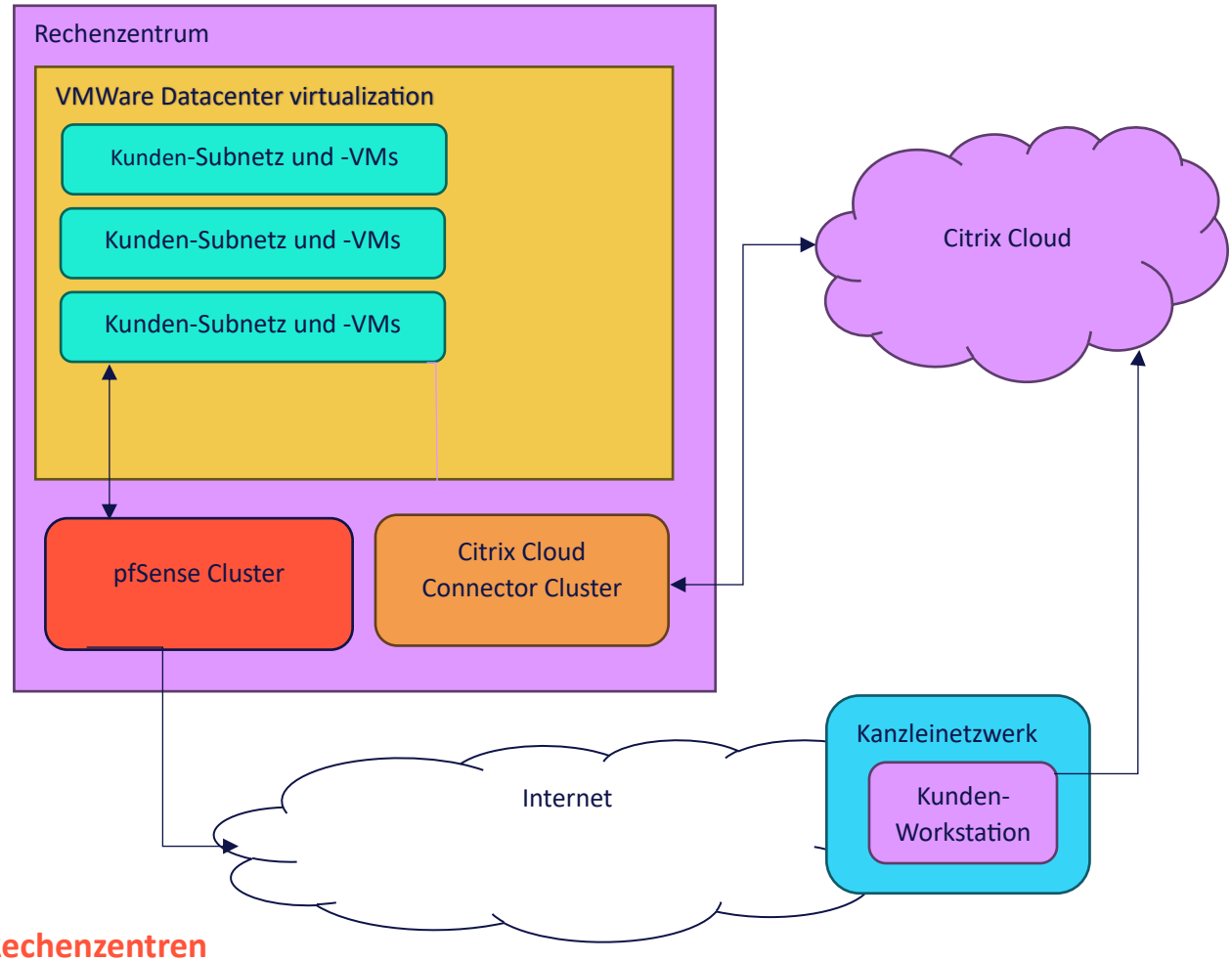
Einleitung

Dieses Whitepaper bietet einen Überblick über die Sicherheitsmaßnahmen und -praktiken, die in der Managed Services Architektur implementiert sind und angewendet werden.

Architektur

Folgende aufeinander aufbauenden Ebenen sind Bestandteile der Architektur

1. Rechenzentren auf deutschem Staatsgebiet. Rechen-, Speicher- und Netzwerkressourcen vom Anbieter überwacht und gesichert. Im Englischen: MIaaS (Managed Infrastructure as a Service)
2. VMWare Datacenter mit Windows Domain-Controller und Terminal-Servern für jeden Kunden
3. pfSense Firewall Cluster
4. Citrix Cloud Connector Cluster
5. Workstation des Kunden



Rechenzentren

Die Rechenzentren unseres Partners befinden sich auf deutschem Staatsgebiet (aktuell an den Standorten Aachen, Düsseldorf und Berlin) und verfügen über diese Eigenschaften:

- Redundante Branderkennung inkl. Brandfrüherkennungssystemen

- Gasgestütztes Brandbekämpfungssystem
- N+1 Redundante Klimatisierung inkl. Temperaturüberwachung
- A/B Stromversorgung in allen Racks
- USV-Absicherung der A/B Versorgung
- Notstromversorgung durch Generatoren
- Mehrere Datenanbindungen über verschiedene Leitungswege
- Mehrstufiges physikalisches Sicherheitskonzept
    - Außenhautüberwachung mittels Sensoren und Kameras (CCTV)
    - Innenraumüberwachung mittels Alarmsensoren
    - Schlüsselkartensystem zur Zugangssicherung aller kritischen Bereiche
    - Besucherprotokollierung
- Aufschaltung auf 24h/7d Wachdienst
- 24h/7d Überwachung aller kritischen Systeme und Parameter
- Backups werden in getrennten Brandschutzabschnitten vorgehalten.

Dies Maßnahmen stellen den optimalen sicheren und zuverlässigen Betrieb der ghosteten Systeme sicher.

Alle genutzten Rechenzentren sind nach ISO 27001, ISO 9001 sowie ISO 14001 zertifiziert.

VMWare Data Center Virtualization

Hohe Verfügbarkeit und Sicherheit sind Schlüsselmerkmale des Betriebs von virtuellen Maschinen in einem mit VMware virtualisierten Rechenzentrum.

VMWare bietet mit vMotion eine Methode zum unterbrechungsfreien Umzug einer VM auf einen anderen Rechner. Alle Daten werden während einer vMotion-Migration verschlüsselt übertragen. Dies schützt die Daten, während sie zwischen Hosts und über Netzwerke bewegt werden.

Die Kundennetzwerke werden durch hybride VLANs voneinander gekapselt, so dass ein gegenseitiger Zugriff ausgeschlossen ist. Hybrid meint hier das Zusammenspiel von virtuellen VMWare-Netzwerkadaptern mit gemanagten physischen Layer 2 Switches.

pfSense Firewall Cluster

Das hochverfügbare Firewall Cluster stellt die Verbindung der virtuellen Maschinen im Rechenzentrum mit dem Internet her und stellt einen sicheren VPN-Tunnel in das lokale Netzwerk von Kanzleien her (nur für Betrieb ohne Citrix).

pfSense legt einen starken Fokus auf Sicherheit und läuft auf dem FreeBSD-OS mit angepasstem Kernel. FreeBSD ist bekannt für seine im Vergleich zu anderen Unix-artigen Betriebssystemen überlegenen Sicherheitskonzepte.

Im Rahmen der Managed Services wird pfSense eingesetzt für sicheres Routing, NAT, Stateful Packet Inspection (dynamisches Filtern), Anti spoofing, Angriffsverhütung (z.B. IDS/IPS, snort) sowie als IPSec und OpenVPN Service.

Citrix Cloud Connector Cluster

Citrix ermöglicht das Ausführen von entfernten Anwendungen über den Browser oder über die Citrix Workspace App. Dabei ist es möglich, die Anwendungen auf einem virtuellen Desktop auszuführen oder als nahtlos eingeblendete Anwendung.

Mit der Verwendung von virtuellen Apps und Desktops werden die Angriffsflächen von lokalen Endpunkten erheblich reduziert. Durch die zentrale Speicherung der Daten im Rechenzentrum ist es viel schwieriger für den Angreifer, sie zu stehlen. Die virtuelle Sitzung läuft nicht auf dem lokalen Computer und Benutzer haben keine Berechtigung, Apps innerhalb der virtuellen Sitzung zu installieren. Die Daten innerhalb der Sitzung sind sicher im Rechenzentrum.

Virtuelle Maschinen

Der sichere Betrieb des Betriebssystems der virtuellen Maschinen wird durch sorgfältig konfigurierte Gruppenrichtlinien gewährleistet. Zusätzlich wird eine zentral verwaltete Virenschutz-Software der Firma eset (www.eset.com/de/) auf jedem System eingesetzt.

Der Zustand der virtuellen Hardware und des Netzwerkes jedes Systems wird ständig überwacht. Sollten Probleme festgestellt werden, arbeiten wir proaktiv an der Lösung.

Workstation des Kunden

Optional auf Kundenwunsch: Ein kompromittierter lokaler Computer kann Tastenanschläge und Informationen, die auf dem Endpunkt angezeigt werden, erfassen. Citrix bietet Administratoren die Möglichkeit, diese Angriffsvektoren mit einer Zusatzfunktion namens App-Schutz zu verhindern. Mit dieser Funktion können CVAD-Administratoren Richtlinien speziell für eine oder mehrere Liefergruppen durchsetzen. Wenn Benutzer sich von diesen Liefergruppen aus mit Sitzungen verbinden, hat der Endpunkt des Benutzers entweder einen Anti-Bildschirmaufnahme- oder einen Anti-Keylogging-Schutz oder beides auf den Endpunkten durchgesetzt.

Datenschutz

Betrieb

Das Onboarding und der Betrieb der Managed Services wird von speziell geschulten Mitarbeitern der STP sichergestellt. Die Mitarbeiter greifen im Rahmen der betrieblichen Notwendigkeit kontrolliert auf die virtuellen Maschinen der Kunden zu, um z.B. Konfigurationen, Fehlerbehebungen oder Wartungen durchführen zu können.

Mitarbeiter des Partners haben keinerlei Zugriff auf die VMs des Kunden und damit auch nicht auf dessen kanzleiinterne Daten.

Vereinbarung mit dem Partner / Unterauftragsverarbeitern

STP und dessen Partner bzw. Unterauftragsverarbeiter haben neue Datenschutzvereinbarungen (AWS-GDPR-DPA) vereinbart, die auch die neuen von der Europäischen Kommission veröffentlichten SCC (Standardvertragsklauseln) enthalten und damit DSGVO-konforme Verarbeitung der Daten umfasst.

STP garantiert die Einhaltung des anwaltlichen Berufsgeheimnisses im Rahmen des Betriebs der Managed Services.

Speicherung der Daten

Kanzleiinterne Daten werden ausschließlich in auf deutschem Staatsgebiet befindlichen Rechenzentren gespeichert (aktuell an den Standorten Aachen, Düsseldorf und Berlin). Eine Übertragung ins Ausland findet nicht statt. Backups der Kunden-VMs werden am Standort der VMs (on site) gespeichert, jedoch in einem anderen Brandschutzabschnitt.

Bei einer Vertragskündigung werden sowohl die VMs des Kunden als auch die Backups gelöscht. Ausschließlich Kundendaten, für welche eine gesetzliche Vorhaltepflicht besteht, werden bei STP gespeichert.

Falls sie weitere Cloud-Produkte von STP nutzen, konsultieren Sie bitte die entsprechenden Security-Paper und FAQs zu Speicherort und Verarbeitungsort.

Fazit

Die beschriebene Architektur bietet eine robuste und sichere Umgebung für unsere Kunden. Durch die Implementierung von Best Practices und fortschrittlichen Sicherheits- und Virtualisierungsfunktionen trägt sie dazu bei, die Sicherheit der Kundendaten und -anwendungen zu gewährleisten.

Bitte beachten Sie, dass dieses Whitepaper einen allgemeinen Überblick über die Sicherheitsmaßnahmen in der beschriebenen Architektur zum aktuellen Zeitpunkt (siehe Datum auf der Titelseite) bietet. Wir optimieren die Sicherheit kontinuierlich, dabei kann es zu Abweichungen kommen, wobei STP stets sicherstellt gleichwertige oder bessere Technologien einzusetzen.

Für spezifische Fragen oder Bedenken bezüglich der Sicherheit wenden Sie sich bitte an uns.