Vom Design her sichere Cloud-Lösung

Für Unternehmen, die sich für eine Cloud-Lösung entscheiden, ist Sicherheit eines der größten Anliegen. Interne Daten einem externen SaaS-Anbieter zu überlassen fordert rigorose Sicherheitsmaßnahmen.

Mehr als 125.000 Kunden vertrauen Zendesk ihre Daten an. Diese Verantwortung nehmen wir sehr ernst. Wir kombinieren Sicherheitsfunktionen der Enterprise-Klasse mit umfassenden Audits unserer Anwendungen, Systeme und Netzwerke, um zu gewährleisten, dass Kunden- und Unternehmensdaten rundum geschützt sind. Unsere Kunden können beruhigt sein, denn wir sorgen dafür, dass ihre Informationen, Interaktionen und Geschäftsabläufe immer sicher sind.

Darüber hinaus nutzen wir zum Schutz unserer Kundendaten absicherte Komponenten wie nach FIPS-140 zertifizierte Verschlüsselungslösungen. Teile unserer Lösung können entsprechend den PCI- und HIPAA/HITECH-Standards konfiguriert werden. Zendesk hat außerdem Tools entwickelt, die unseren Kunden die Einhaltung ihrer Verpflichtungen im Rahmen der DSGVO ermöglicht.

Die Customer-Experience-Produkte und -Lösungen von Zendesk erfüllen strikte Normen zu Sicherheit, Datenschutz und Compliance, darunter:

- ISO 27001:2013
- ISO 27018:2014
- SOC 2 Type II
- EU-US- und Schweiz-US-Datenschutzschild-Zertifizierung
- TrustArc-Datenschutzsiegel

Zendesk schafft von Anfang an Mehrwert für seine Kunden und ist dank seiner vom Design her sicheren nativen Cloud-Architektur, die auf Amazon Web Services (AWS) aufbaut, beliebig skalierbar. Sicherheit ist Teil unserer DNA und eng in alles integriert, was wir tun. Die folgenden Bereiche sind abgedeckt:

Physische Sicherheit

Wir nutzen branchenführende Best Practices, um die Vertraulichkeit, Verfügbarkeit und Integrität Ihrer Daten sicherzustellen. Zendesk nutzt Rechenzentren, die nach ISO 27001, PCI/DSS Service Provider Level 1 und/oder SOC II zertifiziert sind.

Netzwerksicherheit

Zendesk hat ein weltweites Sicherheitsteam, das rund um die Uhr in Bereitschaft ist, um bei Sicherheitsvorfällen sofort in Aktion zu treten. Durch Prüfung auf Netzwerkschwachstellen, Nutzung von Intrusion-Detection- und Intrusion-Prevention-Systemen (IDS/IPS) und Teilnahme an Threat-Intelligence-Programmen halten wir stets ein waches Auge auf die Daten unserer Kunden.

Anwendungssicherheit

Wir unternehmen Schritte, um Sicherheitsbedrohungen aktiv vorzubeugen, damit der Schutz von Kundendaten gewährleistet ist. Zendesk verfolgt einen Secure Development Lifecycle, bei dem die Schulung unserer Entwickler und die Durchführung von Design- und Code-Reviews eine zentrale Rolle spielen. Außerdem arbeitet Zendesk mit externen Sicherheitsexperten, um detaillierte Penetrationstests in unterschiedlichen Anwendungen unserer Produktfamilie durchzuführen.

Produktsicherheit

Wir machen es unseren Kunden leicht, Zugriffs- und Sharing-Richtlinien mit Authentifizierungs- und Single-Sign-On-Optionen zu managen. Außerdem bieten wir Zwei-Faktor-Authentifizierung und IP-Beschränkungen, damit Kunden genau festlegen können, wer Zugriff auf ihren Service hat. Die gesamte Kommunikation mit der Zendesk-UI oder den APIs wird durch den Industriestandard HTTPS über öffentliche Netzwerke verschlüsselt. Der Datenverkehr zwischen Ihnen und Zendesk ist also immer abgesichert.

Datensicherheit

Data-in-Transit-Verschlüsselung: Die Kommunikation zwischen Kunden und den Zendesk-Servern wird durch HTTPS und Transport Layer Security (TLS) über öffentliche Netzwerke verschlüsselt. TLS wird auch zur Verschlüsselung von E-Mails unterstützt.

Data-at-Rest-Verschlüsselung: Für primäre und sekundäre DR-Datenspeicher und die Speicherung von Anhängen kommt Data-at-Rest-Verschlüsselung zum Einsatz.

Verfügbarkeit und Geschäftskontinuität

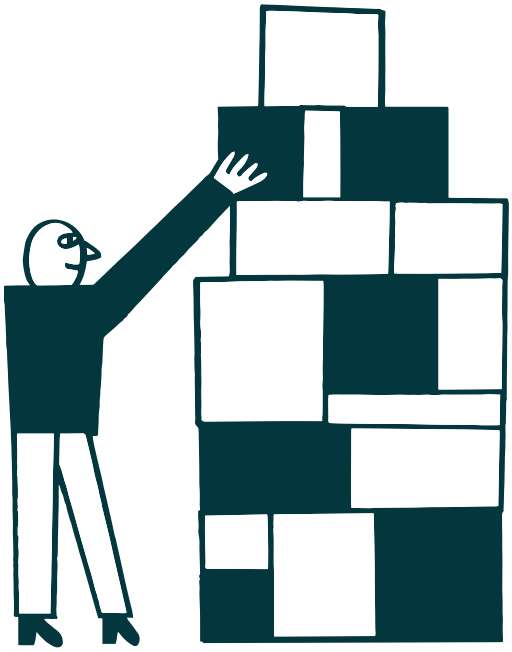
Durch das Disaster-Recovery-Programm von Zendesk ist sichergestellt, dass unsere Services im Katastrophenfall verfügbar bleiben oder leicht wiederherstellbar sind. Wir verwenden Service-Clustering und Netzwerkredundanzen zum Eliminieren eines Single Point of Failure (SPOF). Über eine öffentliche Systemstatusseite mit Informationen zu geplanter Wartung und relevanten Sicherheitsereignissen halten wir unsere Kunden immer auf dem Laufenden.

Compliance-Zertifizierungen und Mitgliedschaften

Wir implementieren neben den von AWS gebotenen Funktionen weitere sicherheitstechnische Best Practices, um nicht nur branchenübliche Vorgaben einzuhalten, sondern selbst die striktesten Anforderungen zu erfüllen.

Datenzugriff durch Zendesk

Um die Diagnose und Behebung von Fehlern in einem Zendesk-Konto zu erleichtern, können Administratoren Zendesk Support die Genehmigung erteilen, für eine bestimmte Zeit die Rolle eines Agenten zu übernehmen. Die Option zur Kontoannahme ist in den Sicherheits-einstellungen zu finden. Diese Option ist standardmäßig deaktiviert und kann nur von einem Kontoadministrator aktiviert werden. Der Kontozugriff kann für einen bestimmten Zeitraum oder auf unbegrenzte Zeit gewährt werden; die Einstellung lässt sich jederzeit wieder deaktivieren.



Weitere Infos

„Wenn wir Software für eine US-Bundesbehörde evaluieren, verlangen wir von allen Anbietern, dass sie die höchsten Sicherheitsstandards einhalten. Über SOC 2 Type II Reporting, ISO-Zertifizierung und Cloud Security Alliance Self Assessment wies Zendesk die Einhaltung dieser Standards nach. Da Zendesk außerdem das ideale Produkt hat, das alle Anforderungen der FCC erfüllt, konnten wir von einer On-Premise- zu einer SaaS-Lösung wechseln."

Dustin Laun

Contractor, Sr. Advisor of Innovation/Technology

Falls Sie Fragen zu unseren Sicherheits- und Compliance-Methoden haben oder Zugriff auf unseren SOC 2-Bericht brauchen, senden Sie eine E-Mail an security@zendesk.com.