Anlage zur Sicherheit von Citrix Diensten

Version 2.0
Gültig ab 20. April 2020

Inhalt

Geltungsbereich 3

Sicherheitsprogramm und Richtlinien-Framework 3

Zugangskontrollen 4

Systementwicklung und -wartung 5

Asset-Management 6

Sicherheit für die Personalabteilung 7

Betriebsablaufsicherheit 8

Physische Sicherheit 9

Geschäftskontinuität und Notfallwiederherstellung 10

Reaktion auf Sicherheitsvorfälle 11

Lieferantenverwaltung 11

Compliance 12

Kundenaudits und -anfragen 13

Citrix Kontakte 14

Diese Anlage zur Sicherheit von Citrix Diensten (die „Anlage“) beschreibt die Sicherheitskontrollen, die in Verbindung mit der Ausführung von Citrix Cloud Services, technischen Support- oder Beratungsservices (die „Services“) implementiert werden, die Kunden im Rahmen der entsprechenden Citrix Lizenz- und/oder Serviceleistungsvereinbarung und der entsprechenden Bestellung der Services (zusammenfassend die „Vereinbarung“) zur Verfügung gestellt werden. Beta- oder Labor-/Technologievorschau-Services (einschließlich Citrix Cloud Labs) und interne Citrix IT-Systeme, die nicht an der Bereitstellung von Services beteiligt sind, fallen nicht in den Geltungsbereich dieser Anlage.

Großgeschriebene Begriffe haben die in der Vereinbarung angegebene oder hierin definierte Bedeutung. „Kundeninhalte“ sind alle Daten, die zur Speicherung auf das Kundenkonto hochgeladen werden, oder Daten in der Computerumgebung des Kunden, zu denen Citrix zur Erbringung von Services Zugang erhalten kann. „Protokolle“ sind Aufzeichnungen von Services, einschließlich, aber nicht beschränkt auf Daten und Informationen über Leistung, Stabilität, Nutzung, Sicherheit, Support und technische Informationen über Geräte, Systeme, zugehörige Software, Dienste oder Peripheriegeräte, die mit der Nutzung der Services durch den Kunden verbunden sind.

1. Geltungsbereich

Diese Anlage beschreibt die administrativen, physischen und technischen Sicherheitskontrollen, die Citrix anwendet, um die Vertraulichkeit, Integrität und Verfügbarkeit seiner Services zu gewährleisten. Diese Kontrollen gelten für die Betriebs- und Servicesysteme und -umgebungen von Citrix. Citrix verwendet ISO/IEC 27002 als Grundlage für sein Sicherheitsprogramm für Services.

Citrix ist bestrebt, seine Sicherheitspraktiken kontinuierlich zu stärken und zu verbessern, und behält sich daher das Recht vor, die hier beschriebenen Kontrollen zu ändern. Jegliche Änderungen werden das Sicherheitsniveau während der entsprechenden Servicedauer nicht vermindern.

2. Sicherheitsprogramm und Richtlinien-Framework

Citrix verfügt über ein Sicherheitsprogramm und einen Rahmen für Sicherheitsrichtlinien, die von Führungskräften von Citrix, die verschiedene Geschäftsbereiche des Unternehmens repräsentieren, festgelegt und genehmigt wurden.

2.1 Übersicht über Sicherheitsrisiken

Das Citrix Cyber Risk Oversight Committee (CROC) regelt die Aktivitäten des Sicherheitsrisikomanagements. Das CROC besteht aus funktionsübergreifendem Führungskräften. Das Team aus Führungskräften überprüft die Mitgliedschaft in den Ausschüssen jährlich, um eine angemessene Abdeckung der Geschäfts- und Betriebsbereiche zu bestätigen.

Das CROC tritt mindestens vierteljährlich zusammen und bietet Orientierungshilfen, Einblicke und Anweisungen zur Identifizierung, Bewertung und Behandlung von Sicherheitsrisiken sowohl in Unternehmen als auch in der Infrastruktur der Servicebereitstellung.

2.2 Sicherheitsrisikomanagement

Citrix setzt ein Programm zum Management von Sicherheitsrisiken (Security Risk Managment, SRM), das potenzielle Bedrohungen für Citrix Produkte und Services sowie für die Citrix Infrastruktur identifiziert, die Bedeutung der mit diesen Bedrohungen verbundenen Risiken bewertet, Strategien zur Risikominderung entwickelt und mit den Produkt- und Entwicklungsteams von Citrix zusammenarbeitet, um diese Strategien umzusetzen.

Das SRM-Programm wendet branchenweit anerkannte Frameworks an, wie z. B. ISO/IEC 31000 und ISO/IEC 27005.

2.3 Informationssicherheit

Citrix hat einen Chief Information Security Officer (CISO) ernannt, der für die Sicherheitsaufsicht und die Strategie, Einhaltung und Durchsetzung von Richtlinien verantwortlich ist. Der Director of Security Monitoring and Response leitet den Reaktionprozess auf Sicherheitsvorfälle, einschließlich Untersuchung, Eindämmung und Behebung.

2.4 Physische und auf die Umgebung bezogene Sicherheit

Das Citrix Sicherheitsteam beaufsichtigt zusammen mit dem Facility Management den physischen Zugang zu den Citrix Einrichtungen.

3. Zugangskontrollen

Citrix erfordert den Einsatz von Zugangskontrollmaßnahmen, die sicherstellen sollen, dass für den Zugang auf Unternehmenssysteme, Vermögenswerte, Daten und Einrichtungen angemessene Privilegien zugewiesen und aufrecht erhalten werden, um vor potenziellen Schäden, Kompromittierungen oder Verlusten zu schützen. Citrix folgt dem Least-Privilege-Prinzip oder der rollenbasierten Sicherheit, die den Zugang der Benutzer auf das beschränkt, was für die Ausführung von Aufgaben oder Rollen notwendig ist.

Manager entwerfen Rollen, um eine angemessene Aufgabentrennung zu gewährleisten, indem sie Aufgaben und Privilegien auf mehrere Personen verteilen, um sich vor Betrug und Fehlern zu schützen.

3.1 Neue Konten-, Rollen- und Zugriffsanfragen

Citrix schreibt eine formellen Anfragen für den Zugriff auf Unternehmenssysteme oder -daten vor. Jede Zugriffsanfrage erfordert eine Mindestgenehmigung eines Vorgesetzten, um zu bestätigen, dass die Benutzerrolle Zugriff anfordert. Zugriffsadministratoren bestätigen, dass vor der Gewährung des Zugriffs auf Systeme oder Daten die erforderlichen Genehmigungen angefordert wurden.

3.2 Kontoüberprüfung

Citrix führt und aktualisiert eine Aufzeichnung der Sicherheitsprivilegien für Mitarbeiter und Auftragnehmer, die zum Zugriff auf Citrix Systeme mit Kundeninhalten berechtigt sind. Das Least-Privilege-Prinzip wird angewendet.

Citrix führt mindestens halbjährlich Überprüfungen von Benutzerkonten und zugewiesenen Berechtigungen für wichtige Systeme durch. Alle Änderungen, die als Ergebnis der Überprüfungen erforderlich sind, unterliegen einem formellen Zugriffsanfrageprozess, um den Benutzer zu bestätigen, und die Rolle des Benutzers erfordert Zugriff auf das/die entsprechenden System(e).

3.3 Entfernen von Konto-, Rollen- und Zugriffsberechtigungen

Citrix verlangt, dass der Benutzerzugriff unverzüglich nach der Benachrichtigung über die Änderung der Rolle eines Benutzers (falls zutreffend), die Kündigung, den Abschluss des Beschäftigungsverhältnisses eines Benutzers oder das Ausscheiden aus dem Unternehmen deaktiviert, widerrufen oder entfernt wird.

Anträge auf Entfernung des Zugriffs werden dokumentiert und verfolgt.

3.4 Anmeldeinformationen

Citrix verlangt eine mehrstufige Authentifizierung für den Remotezugriff von Mitarbeitern auf Citrix Systeme und setzt die folgenden Verfahren zur Handhabung und Verwaltung von Kennwörtern durch:

- Kennwörter müssen regelmäßig gemäß den von Citrix festgelegten Systemanforderungen erneuert werden.
- Kennwörter müssen die Anforderungen an Länge und Komplexität erfüllen, einschließlich einer Mindestlänge von 10 Zeichen und dürfen keine gewöhnlichen Wörter oder Wörter aus dem Wörterbuch enthalten.
- Deaktivierte oder abgelaufene Benutzer-IDs werden nicht an andere Personen vergeben.
- Citrix wendet Verfahren zur Deaktivierung von Kennwörtern an, die versehentlich weitergegeben wurden.
- Citrix überwacht wiederholte Versuche, sich mit einem ungültigen Kennwort Zugriff auf Services zu verschaffen, und führt automatisierte Aktionen durch, um wiederholte Versuche zu blockieren.

Citrix wendet Praktiken an, die darauf ausgelegt sind, die Vertraulichkeit und Integrität von Kennwörtern bei deren Vergabe, Verteilung und Speicherung zu wahren, wie z.B:

- Citrix verlangt, dass Kennwörter während ihres gesamten Lebenszyklus mit Hash angewendet werden
- Citrix verbietet die gemeinsame Nutzung von Kennwörtern

4. Systementwicklung und -wartung

Citrix wendet einen „Secure by Design“-Prozess an, der Standards und Änderungskontrollverfahren umfasst, die auf die Sicherheitsanforderungen der Informationssysteme, die Überprüfung und das Testen des Codes und die Sicherheit bei der Verwendung von Testdaten ausgerichtet sind. Dieser Prozess wird von einem spezialisierten Sicherheitsteam geleitet und überwacht, das auch für die Überprüfung des Designs, die Bedrohungsmodellierung, die manuelle Codeüberprüfung und Stichproben sowie Penetrationstests zuständig ist.

4.1 Prinzipien für sicheres Design

Citrix hat eine formale Methodik für den Lebenszyklus der Systementwicklung (Systems Development Life Cycle, SDLC) eingeführt, die die Entwicklung, den Erwerb, die Implementierung und die Wartung von computergestützten Informationssystemen und die damit verbundenen technologischen Anforderungen regelt.

Citrix verwendet ein softwarebasiertes System für die Verwaltung von Open Source-Prüfungen und -Genehmigungen, wozu auch regelmäßige Scans und Audits seiner Softwareprodukte gehören. Citrix verfügt über dokumentierte Richtlinien, die allen Mitarbeitern zur Verfügung stehen, bezüglich der Nutzung von Open Source sowie Schulungen für Entwickler und deren Management zu bewährten Open Source-Methoden.

4.2 Änderungsmanagement

Der Citrix Änderungsmanagementprozess für Infrastruktur und Software richtet sich an Sicherheitsanforderungen und setzt voraus, dass Software- und Infrastrukturänderungen vor der Migration in die Produktionsumgebung autorisiert, formal dokumentiert, getestet (falls zutreffend), überprüft und genehmigt werden. Infrastruktur- und Softwareänderungen werden mit Hilfe von Arbeitsverwaltungssystemen verwaltet und verfolgt.

Der Änderungsmanagementprozess ist angemessen getrennt, und der Zugang zur Migration von Änderungen in die Produktion ist auf autorisierte Mitarbeiter beschränkt.

5. Asset-Management

5.1 Physisches und virtuelle Asset-Management

Citrix unterhält ein dynamisches Inventar der von Citrix verwalteten physischen und virtuellen Systeme, die zur Erbringung der Services verwendet werden („Service-Assets“). Systemeigentümer sind für die Wartung und Aktualisierung ihrer Service-Assets in Übereinstimmung mit den Citrix Sicherheitsstandards verantwortlich.

Es gibt formelle Löschverfahren, die das sichere Löschen von Citrix- und Kundendaten regeln. Citrix löscht Daten, wenn sie nicht mehr benötigt werden, auf der Grundlage einer Klassifizierung und unter Verwendung von Löschprozessen, die verhindern sollen, dass Daten rekonstruiert oder gelesen werden können.

Die technologischen Citrix Assets werden bereinigt und gelöscht, wenn sie in dem ihnen zugewiesenen oder zugewiesenen Bereich nicht mehr benötigt werden. Zu den technologischen Asstes gehören unter anderem einzelne Computergeräte, Multifunktions-Computergeräte, Bildgebungsgeräte und Netzwerkgeräte. Die Entsorgung wird durch Services für globale Sicherheitsrisiken und Informationssicherheit koordiniert.

5.2 Anwendungs- und Systemverwaltung

Anwendungs- und Systemeigentümer sind verantwortlich für die Überprüfung und Klassifizierung der Daten, die sie speichern, auf die sie zugreifen, über die sie verfügen oder die sie übertragen. Neben anderen Kontrollen sind Mitarbeiter und Auftragnehmer zu Folgendem verpflichtet:

- Kundeninhalten als eine der beiden höchsten Kategorien vertraulicher Citrix Informationen klassifizieren und entsprechende Zugriffsbeschränkungen anwenden.
- Drucken von Kundeninhalten beschränken und gedruckte Materialien in sicheren Behältern entsorgen
- Unternehmens- oder vertrauliche Informationen nicht auf Geräten speichern, die nicht den Anforderungen der Sicherheitsrichtlinien und -standards von Citrix entsprechen
- Unbeaufsichtigte Computer und Daten sichern

5.3 Datenaufbewahrung

Kundeninhalte, die als Teil der Citrix Cloud-Services gespeichert sind, sind für einen begrenzten Zeitraum nach der Beendigung der Services für den Kunden zugänglich und werden dann (mit Ausnahme von Sicherungskopien) gelöscht, nachdem der Kunde eine Bestätigung über die Löschung erhalten hat. Weitere Einzelheiten sind in der Dokumentation zu den einzelnen Services aufgeführt. Kundeninhalte können auch nach Erbringung der Services beibehalten werden, wenn dies aus rechtlichen Gründen erforderlich ist. Citrix wird die Anforderungen dieser Anlage erfüllen, bis diese Kundeninhalte endgültig gelöscht wurden.

6. Sicherheit für die Personalabteilung

Die Aufrechterhaltung der Sicherheit von Kundeninhalten ist eine der Kernanforderungen für alle Mitarbeiter und Auftragnehmer von Citrix. Der Code of Business Conduct von Citrix verlangt von allen Mitarbeitern und Auftragnehmern die Einhaltung der Sicherheitsrichtlinien und -standards von Citrix und zielt insbesondere auf den Schutz vertraulicher Informationen sowie persönlicher Daten von Citrix Kunden, Partnern, Lieferanten und Mitarbeitern ab.

Alle Mitarbeiter und Auftragnehmer von Citrix unterliegen Vertraulichkeitsvereinbarungen, die sich auf Kundeninformationen beziehen. Das für die Sicherheit zuständige Citrix Gremium kommuniziert auch regelmäßig mit den Mitarbeitern über Themen der Informations- und physischen Sicherheit, um das Sicherheitsbewusstsein zu bestimmten Themen aufrechtzuerhalten.

6.1 Background-Checks

Citrix bedient sich derzeit bei allen Neueinstellungen weltweit der Anbieter von Background-Checks und verlangt das Gleiche für das Personal von Drittanbietern, es sei denn, dies ist durch örtliche Gesetze oder arbeitsrechtliche Bestimmungen eingeschränkt.

6.2 Schulungen

Alle Mitarbeiter sind verpflichtet, Schulungen zum Datenschutz und zu den Unternehmensrichtlinien zum Schutz der Sicherheit vertraulicher Informationen von Citrix zu absolvieren, wozu auch die vertraulichen Informationen unserer Kunden, Partner, Lieferanten und Mitarbeiter gehören. Die Schulungen befassen sich mit den Datenschutzpraktiken und den Prinzipien, die für den Umgang von Mitarbeitern mit persönlichen Daten gelten, einschließlich der Notwendigkeit, Einschränkungen für die Nutzung, den Zugriff, die Weitergabe und die Aufbewahrung persönlicher Daten festzulegen. Mitglieder der Abteilung Engineering durchlaufen eine spezifische Schulung mit den Themen Entwicklung, Architektur und Codierung.

6.3 Durchsetzung

Alle Mitarbeiter sind verpflichtet, die Sicherheits- und Datenschutzrichtlinien und -standards von Citrix einzuhalten. Bei Nichteinhaltung drohen Disziplinarmaßnahmen bis hin zur Kündigung des Arbeitsverhältnisses.

7. Betriebsablaufsicherheit

7.1 Netzwerk- und Systemsicherheit

Citrix verfügt über dokumentierte Standards zur Netzwerk- und Systemhärtung, die sicherstellen sollen, dass Netzwerke und Systeme sicher konfiguriert werden. Zu den nach diesen Standards erforderlichen Verfahren gehören unter anderem:

- Ändern oder Deaktivieren von Standardeinstellungen und/oder Konten
- Anwenden von Anmeldebannern
- Kontrollierte Nutzung des administrativen Zugriffs
- Einschränken von Servicekonten nur für den Zweck, für den sie erstellt wurden
- Konfigurieren geeigneter Protokollierungs- und Alarmeinstellungen für Audits

Citrix erfordert die Implementierung von Anti-Malware-Software auf Servern und Arbeitsstationen und scannt das Netzwerk nach bösartiger Software.

Netzwerkkontrollen regeln den Zugriff auf Kundeninhalte. Dazu gehören gegebenenfalls: die Konfiguration einer nicht vertrauenswürdigen Zwischenzone zwischen dem Internet und dem internen Netzwerk, die einen Sicherheitsmechanismus zur Beschränkung des Zugriffs und des nicht autorisierten Datenverkehrs enthält; die Segmentierung des Netzwerks, um den nicht autorisierten Zugriff auf Kundeninhalte zu verhindern; und die Trennung von Web- und Anwendungsservern von den entsprechenden Datenbankservern in einer abgestuften Struktur, die den Verkehr zwischen den Schichten einschränkt.

7.2 Protokollierung

Citrix sammelt Protokolle, um das korrekte Funktionieren seiner Services zu bestätigen, bei der Fehlerbehebung von Systemproblemen zu helfen und seine Netzwerke und Kundeninhalte zu schützen und zu sichern. Protokolle können Zugriffs-ID, Zeit, gewährte oder verweigerte Autorisierung, Diagnosedaten wie Ablaufverfolgungs- und Absturzdateien sowie andere relevante Informationen und Aktivitäten enthalten.

Protokolle können in identifizierbarer Form verwendet werden (i) für die Bereitstellung, Sicherung, Verwaltung, Messung und Verbesserung der Services und der damit verbundenen Analysen, (ii) wie vom Kunden oder seinen Endbenutzern angefordert und/oder (iii) für die Einhaltung der Citrix Richtlinien, des anwendbaren Rechts, der Vorschriften oder auf Anfrage der Regierung. Dazu kann die Überwachung der Leistung, Stabilität, Nutzung und Sicherheit der Services und der damit verbundenen Komponenten gehören. Kunden dürfen diese Überwachung nicht blockieren oder stören.

Weitere Informationen zu Kundeninhalten und der Handhabung von Protokollen finden Sie im Citrix Trust Center im Abschnitt „Datenschutz und Compliance“, der mehrere Whitepapers zur Citrix Protokollierung enthält.

7.3 Schutz bei der Datenübertragung

Citrix hat sichere Übertragungsprotokolle für die Übertragung von Daten über öffentliche Netzwerke eingesetzt, die Teil der Services sind. Die Services sind durch Verschlüsselung geschützt, und der Zugriff über das Internet ist durch TLS-Verbindungen geschützt.

8. Physische Sicherheit

8.1 Citrix Einrichtungen

Citrix hat die folgenden Kontrollen implementiert, die den unbefugten Zugang zu allen Einrichtungen verhindern sollen:

- Der Zugang zu den Einrichtungen ist auf autorisierte Personen beschränkt.
- Besucher müssen sich in eine digitale Besucherliste eintragen und müssen jederzeit begleitet oder beobachtet werden.
- Ausweiskarten sind für Mitarbeiter, Auftragnehmer und Gäste erforderlich und müssen jederzeit sichtbar sein, wenn sie sich in der Einrichtung befinden.
- Der Sicherheitsdienst verwaltet und kontrolliert den Zugang zu Einrichtungen nach Geschäftsschluss.
- Wachleute, Einbruchserkennung und/oder CCTV-Kameras überwachen Gebäudeeingangspunkte, Lade- und Versanddocks und öffentliche Zugangsbereiche (die Mechanismen zur Überwachung des Zugangs können je nach Einrichtung und Standort unterschiedlich sein).

Zudem bieten Citrix Einrichtungen Folgendes:

- Feuerunterdrückungs- und Feuererkennungssysteme oder -vorrichtungen
- Klimaregelungssysteme oder -geräte (Temperatur, Feuchtigkeit usw.)
- Zugängliche Wasserhauptabsperr- oder Teilabsperrventile
- Alternative Stromquellen (Generator, UPS-System usw.)
- Notausgänge und Evakuierungswege

Datenschränke, die sich in Büros befinden, sind durch Zugang per Ausweis und Überwachung geschützt.

8.2 Datencenter

Zusätzlich zu den oben beschriebenen Citrix Einrichtungskontrollen für Citrix-eigene und von Citrix verwaltete Einrichtungen führt Citrix zusätzliche Kontrollen in den Datencentern ein, die es zur Bereitstellung von Services nutzt.

Citrix verwendet Systeme zum Schutz vor Datenverlusten aufgrund von Stromversorgungsausfällen oder Leitungsstörungen, einschließlich einer globalen und redundanten Service-Infrastruktur, die mit Standorten für die Notfallwiederherstellung eingerichtet ist. Datencenter und Internetdienstanbieter (Internet Service Providers, ISPs) werden evaluiert, um die Leistung in Bezug auf Bandbreite, Latenz und Isolierung der Notfallwiederherstellung zu optimieren.

Datencenter befinden sich in Einrichtungen, die ISP-Träger-neutral sind und physische Sicherheit, redundante Stromversorgung, Infrastruktur-Redundanz und Betriebszeitvereinbarungen von wichtigen Lieferanten bieten.

Wenn Citrix für die Bereitstellung der Services Datencenter Dritter oder Cloud-Services nutzt, beauftragt Citrix Anbieter, die die physischen und umgebungsbedingten Sicherheitsanforderungen der Citrix Einrichtungen erfüllen oder übertreffen.

9. Geschäftskontinuität und Notfallwiederherstellung

9.1 Geschäftskontinuität

Citrix plant strategisch für die Fortführung des Geschäftsbetriebs in ungünstigen oder störenden Situationen und entwirft Systeme, damit die Services während des Auftretens solcher Ereignisse funktionsfähig bleiben.

Citrix führt mindestens alle zwei Jahre eine Business Impact Analysis (BIA) auf Abteilungsebene durch, mit einer jährlichen Überprüfung jedes Jahr. Die BIA wird zur Erstellung eines abteilungsbezogenen Geschäftskontinuitätsplans (Business Continuity Plan, BCP) verwendet, der für jede Abteilung deren Ressourcenbedarf, Wiederherstellungsparameter und -methoden, Umzugsanforderungen und die während des gesamten Prozesses erforderlichen Sicherheitsmaßnahmen zur Vermeidung von Ausfällen oder Lücken identifiziert und dokumentiert. Der Leiter jeder Abteilung überprüft und genehmigt den BCP jährlich oder bei wichtigen organisatorischen Änderungen.

Citrix verfügt über Notfall- und Notfallpläne für alle Citrix Einrichtungen. Für den Fall, dass die Einrichtungen nicht verfügbar sind, haben die Mitarbeiter die Möglichkeit, entweder in anderen Citrix Einrichtungen oder an einem Ort ihrer Wahl von einem Remotestandort aus zu arbeiten. Zusätzliche Wiederherstellungsstrategien werden gegebenenfalls in den BCPs dokumentiert.

9.2 Notfallwiederherstellung

Citrix ist bestrebt, die Auswirkungen von Service- oder Betriebsunterbrechungen zu minimieren, indem Prozesse und Kontrollen implementiert werden, die eine stabile und ordnungsgemäße Wiederherstellung sowie eine Wiederherstellung der Geschäftssysteme und -daten von Citrix gewährleisten. Citrix implementiert Redundanz für alle unternehmenskritischen Systeme, Daten und Infrastruktur. Der Notfallwiederherstellungsplan (Disaster Recovery Plan, DRP) nutzt die in der oben erwähnten BIA durchgeführte Bewertung, um Parameter, Methoden, Prioritäten und Sicherheitsvorkehrungen für die Wiederherstellungszeit zu identifizieren und zu dokumentieren, die während des gesamten Prozesses erforderlich sind, um Ausfälle oder Lücken zu vermeiden.

Der Plan skizziert die Gesamtstruktur und den Ansatz zur Wiederherstellung kritischer Systeme und Daten, einschließlich, aber nicht beschränkt auf die Wiederherstellung:

- Rollen und Verantwortlichkeiten von Einzelpersonen oder Teams
- Kontaktinformationen für wichtiges Personal oder Drittparteien
- Schulungsanforderungen und -pläne für wichtiges Personal
- Wiederherstellungsziele, Wiederherstellungsprioritäten und Erfolgsmetriken
- Schema der vollständigen Wiederherstellung

Der Leiter überprüft und genehmigt den DRP jährlich oder bei wichtigen organisatorischen Änderungen.

10. Reaktion auf Sicherheitsvorfälle

Citrix verwendet einen Cyber Security Incident Response Plan (Reaktionsplan für Cyber-Sicherheitsvorfälle), der die Prozesse zur Erkennung, Meldung, Identifizierung, Analyse und Reaktion auf Sicherheitsvorfälle mit Auswirkungen auf von Citrix verwaltete Netzwerke und/oder Systeme oder Kundeninhalte detailliert beschreibt. Schulungen zur Reaktion auf Sicherheitsvorfälle und Tests finden mindestens jährlich statt.

„Sicherheitsvorfall“ bedeutet unbefugten Zugriff auf Kundeninhalte, der zum Verlust der Vertraulichkeit, Integrität oder Verfügbarkeit führt. Wenn Citrix feststellt, dass Kundeninhalte, die sich in seiner Kontrolle befinden, Gegenstand eines Sicherheitsvorfalls waren, wird der Kunde innerhalb der gesetzlich vorgeschriebenen Frist benachrichtigt. Die Mitteilung von Citrix beschreibt, soweit bekannt, die Art des Vorfalls, den Zeitraum und die potenziellen Auswirkungen auf den Kunden.

Citrix führt über jeden Sicherheitsvorfall eine Aufzeichnung.

11. Lieferantenverwaltung

Citrix kann Subunternehmer und Vertreter beauftragen, Services bereitzustellen. Alle Subunternehmer und Vertreter sind nur dann zum Zugriff auf Kundeninhalte berechtigt, wenn dies zur Erbringung der Services erforderlich ist, und sind an schriftliche Vereinbarungen gebunden, die sie dazu verpflichten, mindestens das Datenschutzniveau zu gewährleisten, das von Citrix durch diese Ausstellung gefordert wird. Citrix bleibt zu jeder Zeit für die Einhaltung der Bestimmungen der Vereinbarung durch seine Subunternehmer und Vertreter verantwortlich. Eine Liste der Citrix-Subunternehmer, die Zugriff auf Kundeninhalte haben können, finden Sie im Citrix Trust Center.

11.1 Onboarding

Das Third Party Risk Management-Programm (Risikomanagement-Programm für Dritte) von Citrix bietet einen systematischen Ansatz für das Management von Sicherheitsrisiken, die durch den Einsatz von Drittanbietern entstehen. Citrix arbeitet daran, Sicherheitsrisiken zu identifizieren, zu analysieren und zu mindern, bevor es zu einer Beteiligung von Dritten kommt.

Citrix schließt Vereinbarungen mit Lieferanten ab, um relevante Sicherheitsmaßnahmen und -verpflichtungen zu dokumentieren, die mit den in diesem Anhang aufgeführten übereinstimmen.

11.2 Fortlaufende Bewertung

Citrix führt in regelmäßigen Abständen Sicherheitsrisikobewertungen durch, um sicherzustellen, dass die Sicherheitsmaßnahmen während der gesamten Lieferantenbeziehung angewendet werden. Änderungen der erbrachten Services oder Änderungen bestehender Verträge erfordern eine Bewertung des Sicherheitsrisikos, um zu bestätigen, dass die Änderungen kein zusätzliches oder unangemessenes Risiko darstellen.

11.3 Offboarding

Citrix benachrichtigt die Beschaffungsabteilung des Unternehmens 90 Tage vor dem Plan zur Beendigung einer Lieferantenbeziehung oder vor dem Auslaufen eines Vertrags mit einem Lieferanten. Die Beschaffungsabteilung des Unternehmens koordiniert die Beendigung der bestehenden Beziehungen, um zu bestätigen, dass die Unternehmensdaten und Assets von Citrix gesichert und ordnungsgemäß behandelt werden.

12. Compliance

12.1 Umgang mit personenbezogenen Daten

Personenbezogene Daten sind Informationen, die sich auf eine identifizierte oder identifizierbare Person beziehen. Der Kunde legt die personenbezogenen Daten fest, die in die Kundeninhalte aufgenommen werden sollen. Bei der Bereitstellung der Services fungiert Citrix als Datenverarbeiter, und der Kunde bleibt der Datenverantwortliche für alle in den Kundeninhalten enthaltenen personenbezogenen Daten. Citrix wird auf Anweisung des Kunden bezüglich der Verarbeitung solcher personenbezogener Daten handeln, wie in der Vereinbarung festgelegt.

Weitere Informationen zur Verarbeitung personenbezogener Daten, die der Datenschutz-Grundverordnung unterliegen, einschließlich der Mechanismen, die für den internationalen Transfer solcher Daten verwendet werden, finden Sie im Datenverarbeitungsabkommen von Citrix.

12.2 Standort der Services

Citrix Cloud Services-Kunden behalten die Kontrolle über die Wahl des geographischen Standorts ihrer Cloud Services-Umgebung (*siehe auch Citrix Cloud Geographical Considerations*). Zu keinem Zeitpunkt während des geltenden Cloud Services-Abonnements wird Citrix ohne Zustimmung des Kunden den geografischen Standort der vom Kunden gewählten Umgebung ändern. Beachten Sie, dass als Teil der allgemeinen Service-Bereitstellung Kundeninhalte in die Vereinigten Staaten oder in andere Länder übertragen werden können, in denen Citrix und/oder seine Serviceanbieter tätig sind, soweit dies zur Bereitstellung der Services erforderlich ist.

12.3 Offenlegung von Kundeninhalten

Citrix darf Kundeninhalte in dem gesetzlich vorgeschriebenen Umfang offenlegen, einschließlich als Reaktion auf eine Vorladung, gerichtliche oder behördliche Anordnung oder ein anderes bindendes Instrument (jeweils eine „Forderung“). Außer in Fällen, in denen dies gesetzlich verboten ist, wird Citrix den Kunden unverzüglich über jede Anforderung informieren und dem Kunden die Unterstützung zukommen lassen, die vernünftigerweise erforderlich ist, damit der Kunde rechtzeitig auf die Anforderung reagieren kann.

12.4 Kundensicherheit und regulatorische Anforderungen

Die Services sind so konzipiert, dass sie in einer größeren IT-Umgebung des Kunden bereitgestellt werden können, so dass der Kunde die volle Verantwortung für alle Sicherheitsaspekte behält, die nicht ausdrücklich von Citrix verwaltet werden, einschließlich, aber nicht beschränkt auf Zugangskontrollen, Firewalls, Anwendungen und Netzwerke, die der Kunde in Verbindung mit den Services nutzen kann.

Die Kunden bleiben dafür verantwortlich, zu bestimmen, ob ihre Nutzung der Services, einschließlich der Bereitstellung von Citrix Zugang zu Kundeninhalten als Teil der Services, über die in der Vereinbarung, einschließlich dieser Anlage, festgelegten Anforderungen hinausgehenden gesetzlichen Bestimmungen oder Sicherheitsanforderungen unterliegt. Kunden müssen daher sicherstellen, dass sie keine Kundeninhalte einsenden oder speichern, die Gesetzen unterliegen, die spezifische Kontrollen vorschreiben, die nicht in dieser Ausstellung enthalten sind, wie z. B. die US International Traffic in Arms Regulations (ITAR) oder ähnliche Bestimmungen eines Landes, das den Import oder Export von Verteidigungsartikeln oder Verteidigungsdienstleistungen einschränkt, geschützte Gesundheitsinformationen („PHI“), Zahlungskarteninformationen

(„PCI“) oder Daten für den kontrollierten Vertrieb gemäß Regierungsvorschriften, es sei denn, dies ist in der Vereinbarung und der anwendbaren Servicebeschreibung angegeben und die Parteien haben im Voraus zusätzliche Vereinbarungen (wie z. B. ein HIPAA Business Associate Agreement) getroffen, die für die Verarbeitung solcher Daten durch Citrix erforderlich sind.

13. Kundenaudits und -anfragen

Bis zu einmal jährlich wird Citrix auf Audit-Anfragen in Form von Antworten auf Risikobewertungen der Kunden antworten. Kunden können auch jederzeit auf das Citrix Due Diligence Package zugreifen, um ein aktualisiertes Sicherheitspaket und einen aktualisierten Fragebogen zu erhalten. Das Citrix Security Due Diligence Package wurde für Sicherheitsanfragen von Kunden erstellt und bietet leicht zugängliche Sicherheitsinformationen. Das Citrix Due Diligence Package enthält drei Dokumente für jedes Produkt: einen ausgefüllten Fragebogen „Standardized Information Gathering (SIG) Lite“ von Shared Assessments mit mehr als 300 Fragen, einen Überblick über die Sicherheitslage und die Kontrollen von Citrix sowie ein Nachweispaket ausgewählter Richtlinien und Kontrollen. Der SIG-Fragebogen ist der von unseren Kunden am häufigsten verwendete Fragebogen und wird in allen Branchen eingesetzt. Das Due Diligence Package kann im Citrix Trust Center heruntergeladen werden.

14. Citrix Kontakte

Funktion	Kontakt
Kundensupport	https://www.citrix.com/contact/technical-support.html
Melden eines Sicherheitsvorfalls	secure@citrix.com
Vermutete Schwachstellen in Citrix Produkten	https://www.citrix.com/about/trust-center/security.html#lightbox-38764 (Klicken Sie auf die Schaltfläche „Sicherheitsproblem melden“.

Vertrieb für Unternehmen
Nordamerika | 800-424-8749
Weltweit | +1 408-790-8000

Standorte
Firmensitz | 851 Cypress Creek Road Fort Lauderdale, FL 33309, United States Silicon Valley | 4988 Great America Parkway Santa Clara, CA 95054, USA