Kundendaten: „Privacy First“ in der Automation Anywhere Cloud

Bei dem Automation Anywhere® Cloud-Portfolio handelt es sich um eine gehostete Service-Plattform. Das Cloud-Portfolio umfasst einen integrierten Control Room und in der Cloud gehostete Funktionen zur Bot-Erstellung. Darüber hinaus besteht die Möglichkeit, die mit der Cloud verbundenen Bot Runner-Verbindungen innerhalb der Infrastruktur des Kunden auszuführen. Auch weitere Produkte, wie IQ Bot™, können in der Cloud gehostet werden.

Das Cloud-Angebot dient der Gewährleistung des Datenschutzes und wird gemäß DSGVO und anderen Datenschutzgrundsätzen und -richtlinien bereitgestellt.

DATENSICHERHEIT

Innerhalb der Bereitstellungsarchitektur kommt eine sichere Methode zum Einsatz, bei der der Schutz der Infrastruktur und Daten von Kunden an erster Stelle stehen.

Die Datenverbindung zwischen dem Bot Runner im Kundennetzwerk und dem Control Room, der sich in der Cloud befindet, ist verschlüsselt. Sichere Verschlüsselungsprotokolle wie HTTPS und TLS 1.2 werden zum Verschlüsseln von Daten während der Übertragung verwendet. Für in der Cloud gespeicherte Daten wird eine entsprechende Verschlüsselung für ruhende Daten verwendet (z. B. AES 256-Bit-Verschlüsselung).

Der vollständige Sicherheitsstatus für Cloud-Vorgänge, anhand dessen das Cloud-Angebot bereitgestellt wird, die Verschlüsselungstechnologien und die Netzwerksicherheit der Umgebung, werden im Cloud Security Operations-Leitfaden beschrieben, den Sie hier finden: <insert URL>

DATENERFASSUNG

Das Bereitstellungsmodell umfasst Kunden, die ihre Bots erstellen und die Bot-Bereitstellungen über den Control Room in der Cloud verwalten. Sobald die Bots erstellt wurden, werden sie getestet und für die Ausführung auf der Rechnerinfrastruktur der Nutzer bereitgestellt.

In der folgenden Tabelle finden Sie die Daten, die für das Automation Anywhere Cloud-Portfolio erfasst werden. Die Tabelle bietet Ihnen einen Überblick, welche Daten möglicherweise zur Identifizierung einer natürlichen Person verwendet werden könnten.

Datenelement	Daten-kategorie	Beschreibung
Nutzername	Personenbezogene Daten	E-Mail, Vor- und Nachname, bevorzugter Name, Zeitzone, letzte Anmeldung, Passwort, Fragensatz, AD-Domain
Nutzerpasswort	Personenbezogene Daten	
Passwortsicherheits-schlüssel	Personenbezogene Daten	Sicherheitsschlüssel für Credential Vault-Passwort
Bot Runner-Gerätezugriff	Personenbezogene Daten	Gerätenutzername und Zugriffsdaten
Definitionen von Rollen	Personenbezogene Daten	Admin, Autor usw.
Rollen, die Nutzern, dem Gerät, der Ressource zugeordnet sind	Personenbezogene Daten	Nutzerrollen
Bot-Gerät IP/FQDN	Personenbezogene Daten	Geräte-IP-Adresse oder FQDN kann zu einem Nutzer nachverfolgt werden
Bot-Definition (Repository)	Metadaten	Daten, die als Teil der Bot-Definition gespeichert werden
Anmeldedaten für die Bot-Anwendung	Personenbezogene Daten	Anwendungsnutzer, URL, öffentlicher Schlüssel, Routingname
Bot-Zeitpläne im Control Room	Metadaten	Bot-Management; wann und wo Bots ausgeführt werden sollen
WLM-Workflowdefinition	Metadaten	Wann und wo Bots in welcher Sequenz ausgeführt werden sollen
Auditprotokolle	Personenbezogene Daten	Kann Identifikationsmerkmale enthalten: Gerätenachrichtenprotokoll, Bereitstellungsnachrichtenprotokoll, E-Mail-Nachrichtenprotokoll, Auftragsausführungsprotokoll: (Start-/Endzeit, Nutzer-ID, Zeitplan, Automatisierungsname, Bereitstellungs-ID. Gerätename, Bot-Name, Nutzername), Bearbeitungsprotokoll für die Nutzerverwaltung, Credential Vault-Nachrichtenprotokoll, Server- und Datenbankänderungsprotokolle
Fehlerprotokolle	Personenbezogene Daten	Kann Identifikationsmerkmale enthalten
Betriebsanalysen	Metadaten	Dienststatus
Nutzungsdaten	Metadaten	Nutzungsdaten von Funktionen, aktivierte Lizenzen, aggregiert ohne personenbezogene oder Nutzerdaten-IDs. Für IQ Bot: Lerninstanzen von Nutzern, Domänen, Betriebsstatistiken, Validierungsänderungen, hochgeladene Dokumente und Extraktionsergebnisse.
Nutzungsdaten	Personenbezogene oder Metadaten	Lerninstanzen von Nutzern, Domänen, Betriebsstatistiken, Validierungsänderungen, hochgeladene Dokumente von Nutzern und Extraktionsergebnisse.

DATENNUTZUNG

Betrieb und Support

Cloud Operations überwacht Bereitstellungssysteme und die operative Leistung, um den Dienst gemäß dem Service-SLA <link here> zu betreiben, zu skalieren und zu unterstützen. Automation Anywhere hat in der Regel keinen Einblick in die oben aufgeführten Kundendaten.

Sollten Supportdienste Zugriff benötigen, um Probleme zu beheben, dann findet dies nur mit der entsprechenden Genehmigung des Kunden statt.

Automation Anywhere geht folgendermaßen vor, um das Produkt zu verbessern:

- Nutzungsdaten von Funktionen werden analysiert. Dies kann z. B. durch das Hinzufügen von Telemetriedaten geschehen, die operative Transparenz für die Nutzung von Funktionen ermöglichen. So kann Automation Anywhere Prioritäten und das Produkt optimieren. Hier ein paar Beispiele:
  - Wir überprüfen, wie häufig Excel-Befehle verwendet werden, damit wir Befehle für zukünftige Versionen priorisieren können
  - Wir stellen Ihnen Empfehlungen für Best Practices bereit
  - Wir stellen Ihnen Supportdienste für die Aktualisierung, die Sicherung und das Beheben von Problemen bereit
  - Wir personalisieren Produkte für Sie und geben Ihnen Empfehlungen
  - Für IQ Bot verwenden wir Kundendaten, um die Qualität der KI-Lernfähigkeiten zu verbessern

Weitere Informationen zu den Datenschutzrichtlinien von Automation Anywhere finden Sie unter: https://www.automationanywhere.com/in/privacy

Datenspeicherung nach Kündigung des Abonnements

Automation Anywhere speichert Kundendaten, Konfigurationen (Bots), IQ Bot-Daten und die meisten Protokolle 30 Tage lang nach Ende des Abonnements des Kunden. Einige Protokolle können bis zu 180 Tage nach Ende des Abonnements des Kunden gespeichert werden.

Ausführliche Informationen zur Datenverarbeitung und zur Datenspeicherung finden Sie hier: https://www.automationanywhere.com/support/DPA.pdf

DATENSCHUTZ

Automation Anywhere bietet eine umfassende Reihe von Sicherheitsfunktionen, die Datenschutz entweder automatisch bereitstellen oder so konfiguriert werden können, dass Datenschutz sichergestellt wird. Wie bei jeder Unternehmensanwendung hängt die einheitliche und ordnungsgemäße Verwendung von Sicherheitskontrollen von der Organisation ab, die die Anwendung einsetzt. Die Autorisierung der Nutzer hängt von den IT-Administratoren ab, die Kontrollen implementieren sollten, damit nur autorisierte Mitarbeiter Zugriff haben.

Der Dateneigentümer sollte sicherstellen, dass nur autorisierte Mitarbeiter, für die eine geschäftliche Notwendigkeit besteht, auf den Dienst zugreifen können. Firmenanwendern mit Zugriff können in Form von Rollen innerhalb der rollenbasierten Zugriffssteuerung (RBAC) des Produkts fein abgestufte Berechtigungen erteilt werden. Die RBAC-Modelle gewährleisten doppelte Kontrolle und Aufgabentrennung innerhalb der Abläufe. Berechtigungen können für alle Aspekte von Produktvorgängen implementiert werden, einschließlich Anmeldedaten, Bots, Bot Runner, Bot Creator, Bot-Zeitpläne, IQ Bot-Lerninstanzen, Zugriff auf Auditprotokolle, Warteschlangen für das Workflow-Management und Pools.

Automation Anywhere bietet vollständige Überprüfungsfunktionen, bei denen alle Nutzeraktionen innerhalb der Plattform überwacht und Aufzeichnungen über alle vom Betriebspersonal ausgeführten Zugriffe und Aktionen bereitgestellt werden. Die Überprüfung ist für alle privilegierten und nicht privilegierten Rollen automatisiert, um den Best Practices zu entsprechen, wie in NIST AC-6 definiert.

Da Bots Softwareprogramme sind, die von Experten des Kunden entwickelt wurden, müssen modernste Secure Software Development Life Cycle-(SDLC)-Prozesse vom Kunden entsprechend implementiert werden.
Zu diesem Zweck unterstützt Automation Anywhere die Trennung von Entwicklungs-, Test- und Produktionsumgebungen durch eine Kombination aus separaten Bereitstellungen und RBAC, wie oben beschrieben.

Pseudonymisierung

Die DSGVO nennt insbesondere die Pseudonymisierung als geeignetes technisches Mittel zum Schutz von Daten. Durch Pseudonymisierung werden Daten in künstliche Kennungen umgewandelt. Auf diese Weise können Verantwortliche und Auftragsbearbeiter die Daten so verarbeiten dass sie ohne zusätzliche Daten, die separat gespeichert werden, nicht mehr zur Identifizierung einer natürlichen Person verwendet werden können. Die Tokenisierung ist ein weiterer Ansatz, bei dem Daten so umgewandelt werden, dass sie später referenziert werden können. Die tokenisierten Daten können jedoch nicht zur Identifizierung einer natürlichen Person verwendet werden.

Automation Anywhere empfiehlt die Verwendung von Pseudonymisierung von Daten für Entwicklungs- und Testumgebungen. Für IQ Bot werden Dokumente und Bilder in der Produktionsumgebung mit aktuellen Nutzerinformationen verarbeitet. Technisch gibt es keine Möglichkeit, diese Dokumente automatisch zu pseudonymisieren und IQ Bot zu verwenden.

Datenremanenz in Control Room

Es gibt Fälle, im denen Daten in den Datenbanken gespeichert werden, die den Control Room unterstützen. Insbesondere bei der Verwendung von Workflow-Management, IQ Bot und Bot Insight™ (zukünftige Version). In allen Fällen bezüglich der Datenremanenz im Control Room reduzieren Pseudonymisierung und Tokenisierung den Aufwand für Verantwortliche und Auftragsbearbeiter bei der Einhaltung der DSGVO. Außerdem werden, wenn Protokolle zur Fehlerbehebung aktiviert werden, Informationen wie der Nutzername (Nutzer der Plattform) in den Protokollen gespeichert.

Workflow-Management und Warteschlangen

Wenn Sie Workflow-Management (zukünftige Version) verwenden, um mehrere Bots für dieselbe Automatisierung bereitzustellen, werden die in den Warteschlangen platzierten Aufgabenelemente in der Control Room-Datenbank gespeichert. Über die Benutzeroberfläche vom Control Room kann jedes Aufgabenelement abgefragt, überprüft und gelöscht werden. Bei der Verarbeitung personenbezogener Daten in Aufgabenelementen können Warteschlangen regelmäßig gelöscht werden.

Anmeldedaten können von jedem Administrator mit den entsprechenden Berechtigungen, die durch die entsprechende Rolle vorgegeben werden, hinzugefügt und gelöscht werden. Der Control Room unterstützt das Abfragen, Überprüfen und Löschen von Anmeldedaten zu jeder Zeit.

Der Control Room bietet die Möglichkeit, Nutzerkonten mit entsprechenden RBAC-Steuerelementen einzurichten und zu entfernen. Der Administrator des Unternehmens ist für den entsprechenden Zugriff auf Nutzer und Ressourcen verantwortlich. Der Administrator sollte eine Richtlinie mit dem erforderlichen Zugriffsgrad gemäß den Datenschutzrichtlinien für Unternehmen und Nutzer erstellen. Wenn ein einzelner Nutzer Zugriff oder Einschränkungen beim Zugriff auf seine persönlichen Daten anfordert, kann er sich an den Administrator des Kunden wenden. Die Administratoren des Kunden können die Konten des Nutzers im Control Room löschen.

Weitere Informationen über Anfragen in Bezug auf den Datenschutz gemäß DSGVO sowie Kopien personenbezogener Daten finden Sie im Anfrageformular für Zugangsrechte zu Daten betroffener Personen von Automation Anywhere.

ZUSAMMENFASSUNG

Kunden verlassen sich darauf, dass die heutigen cloudbasierten, geschäftskritischen Angebote Lösungen bereitstellen, deren zentrale Bestandteile Zugriffssicherheit und Datenschutz sind.

Das Automation Anywhere Cloud-Portfolio wurde entwickelt, um anspruchsvolle betriebliche Richtlinien zu erfüllen und zu übertreffen, und das aus gutem Grund: Datenschutz und Sicherheit ist uns bei der Bereitstellung von Automatisierung für Kunden sehr wichtig.

Weitere Informationen zu den bahnbrechenden Cloud-Lösungen von Automation Anywhere finden Sie auf der Seite „Cloud“.