Sicherheit auf Unternehmensniveau für robotergesteuerte Prozessautomatisierung

EINFÜHRUNG

Automation Anywhere begann vor 15 Jahren mit einer einfachen Frage: Warum wurden nach mehr als 20 Jahren Investitionen in Technologien zur Automatisierung von Geschäftsprozessen weniger als 20 % der Aufgaben automatisiert, die für eine Automatisierung Frage kommen würden? Das Hauptproblem wurde schnell erkannt – 85 % der Unternehmenssysteme fehlt es an gut definierten APIs, was zu einem ständig wachsenden IT-Rückstand bei Integrationsanfragen aus dem Geschäftsbereich führt.

Das Ziel von robotergesteuerter Prozessautomatisierung ist es, Geschäftsanwender in die Lage zu versetzen, Softwarebots zu erstellen, die mit Unternehmenssystemen wie Menschen interagieren können. Mit RPA kann jeder Geschäftsanwender mit Excel-Makro-Kenntnissen die Schritte aufzeichnen, die bei sich wiederholenden Aufgaben durchgeführt werden, und sie in ein leicht verständliches Skript für Bots umwandeln. RPA-Bots können sich mit Anmeldeinformationen bei Unternehmensanwendungen anmelden und Aufgaben automatisieren, die jede Unternehmensanwendung, auch ältere Anwendungen ohne APIs, umfassen. Bearbeitung von Ansprüchen, Darlehensabwicklung, Kontenabstimmung, Rechnungserstellung/-übermittlung und Berichterstellung sind nur einige Beispiele für mögliche Automatisierungen, die sich über verschiedene Geschäftsdisziplinen erstrecken.

Das Potenzial für erhebliche Zeit- und Kosteneinsparungen, eine verbesserte Kundenzufriedenheit, eine bessere Arbeitsmoral und die Möglichkeit, einen entscheidenden Vorteil gegenüber Mitbewerbern zu erzielen, ist leicht zu erkennen. Die vollständige Realisierung dieser Vorteile hängt jedoch von einer Lösung auf Unternehmensniveau ab.

Absolute Zuverlässigkeit, Skalierbarkeit und umfangreiche Funktionen zur Maximierung der Anwendbarkeit und Nutzerfreundlichkeit sind einige der wichtigsten Kriterien für die Automatisierung. Diese Elemente decken jedoch nicht die wichtigste Anforderung des Unternehmens ab: End-to-End-Sicherheit. Eine stabile Sicherheitsarchitektur mit Funktionen, die eine vollständige Unterstützung der Kernprinzipien wie minimale Berechtigungen und Aufgabentrennung ermöglichen, während End-to-End-Schutz fürwichtige Apps und vertrauliche Daten bereitgestellt wird, ist geschäftskritisch.

Dieses Dokument bietet einen Überblick über den branchenweit höchsten Sicherheitsstandard, wie von der auf dem Markt führenden Digital-Workforce-Plattform Automation Anywhere Enterprise gezeigt.

Das Potenzial für erhebliche Zeit- und Kosteneinsparungen, eine verbesserte Kundenzufriedenheit, eine bessere Arbeitsmoral und die Möglichkeit, einen entscheidenden Vorteil gegenüber Mitbewerbern zu erzielen, ist leicht zu erkennen. Die vollständige Realisierung dieser Vorteile hängt jedoch von einer Lösung auf Unternehmensniveau ab.

ARCHITEKTUR UND BETRIEB

Das Verständnis der Steuerelemente für die Sicherheit, die für eine RPA-Implementierung auf Unternehmensniveau erforderlich sind, hängt vom Verständnis der Komponenten der Lösung und ihrer Vorgänge ab.

Kernkomponenten

In Abbildung 1 sehen Sie die Kernkomponenten von Automation Anywhere Enterprise: Control Room, Bot Creator und Bot Runner.

Control Room

Der Control Room dient als Gehirn der Automatisierungsumgebung. Es handelt sich um ein Windows-Server-basiertes Verwaltungssystem mit einer integrierten Datenbank, das eine einheitliche Ansicht für die gesamte Systemverwaltung bietet. Der Control Room ist ebenfalls der Entstehungsort der Digital Workforce. Mit anderen Worten: hier wird der Einsatz der Bots geplant. Außerdem werden die Bots hier bereitgestellt, ausgeführt, überwacht und verwaltet. Darüber hinaus erleichtern integrierte Versionskontrollfunktionen (Apache Subversion Server) die Multi-User-Zusammenarbeit, setzen Best Practices für das Änderungsmanagement durch und schaffen ein zentrales Repository für produktionsbereite Bots.

Bot Creator

Bot Creator wird zum Erstellen von Bots verwendet. Es ist eine Windows-Desktop-App, die auf einer Arbeitsstation oder einem virtuellen Computer ausgeführt wird. Bot Creator wird von Geschäftsprozess-Experten zum Erstellen und Testen ihrer Automatisierung verwendet. Bots werden mithilfe des Aufgabeneditors erstellt, während Bot-Tests mit lokalen Nicht-Produktionstestdaten und App-Instanzen durch die Player-Funktion ermöglicht werden. Nach erfolgreichen Tests (z. B. hinsichtlich Leistung, Datenintegrität und Sicherheit) werden Bots in das Control Room-Repository eingecheckt und stehen für die Produktionsbereitstellung zur Verfügung.

Bot Runner

Mit Bot Runner werden Bots ausgeführt. Mit dem gleichen Anwendungscode wie für Bot Creator, aber mit einem anderen Lizenzschlüssel, nutzt der Bot Runner die Player-Funktion, um Bots in der Produktionsumgebung auszuführen, d. h. er verwendet Produktionsinstanzen der Zielanwendung und Produktionsdatenspeicher. Das Ausführen von Bots ist eigentlich alles, was Bot Runner tun können, da ihnen keine Erstellungs- und Bearbeitungsfunktionen zur Verfügung stehen. Für äußerst zuverlässige und umfangreiche Vorgänge wird auch das Pooling von Bot Runnern unterstützt.

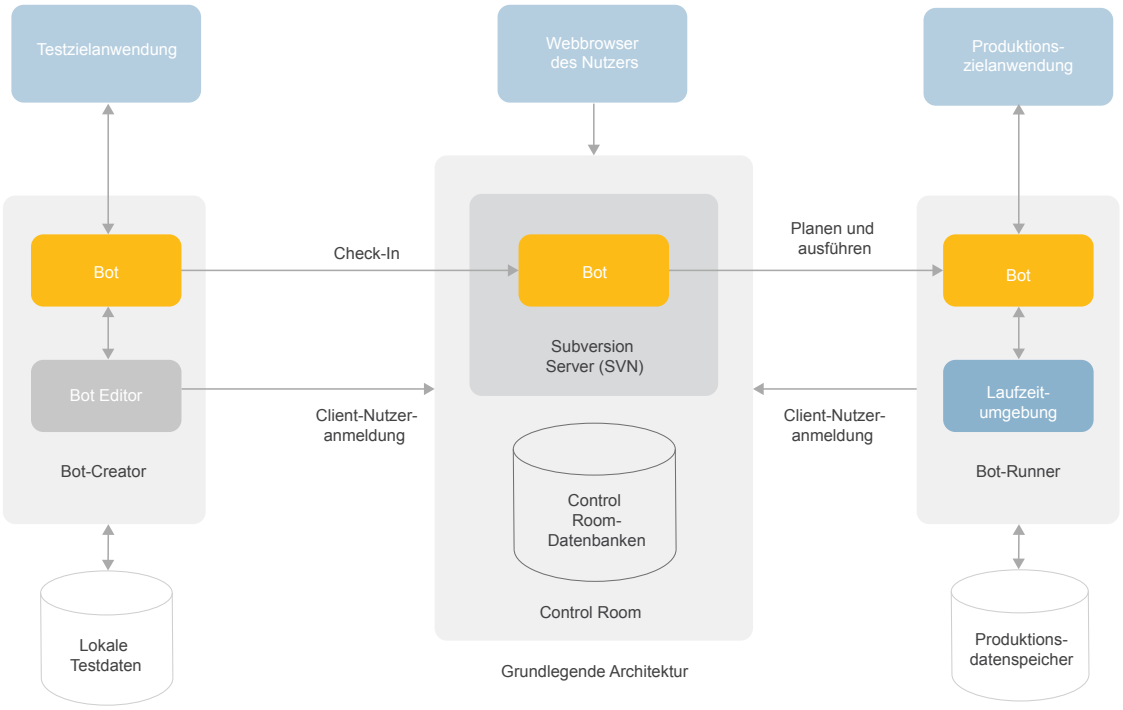


Abbildung 1: Grundlegende Architektur von Automation Anywhere Enterprise

Zusätzliche Komponenten für Unternehmen

Bei der Betrachtung umfangreicher Vorgänge kommen zwei weitere wichtige RPA-Lösungen zum Vorschein, die für Unternehmen relevant sind, die Bereitstellungen in großem Stil durchführen: On-Demand-Skalierung und Bot Insight.

On-Demand-Skalierung

Durch die Nutzung der öffentlichen Cloud von Amazon Web Services (AWS) bietet Automation Anywhere Enterprise RPA-as-a-Service mit allen zugehörigen Funktionen – einschließlich flexibler Produktionssteigerung/-reduzierung, nutzungsbasierter Messung, unbegrenzter horizontaler Skalierbarkeit und kontinuierlicher Überwachung und Audit-Protokollierung der Bot Runner-Infrastruktur. Das Ergebnis ist eine Hochverfügbarkeit mit mehreren Knoten, die die SLA-gesteuerte Leistung und Geschäftskontinuität unterstützt, selbst wenn die Automatisierungsauslastung dramatisch schwankt.

Bot Insight

Bot Insight ist ein vollständig integriertes Subsystem innerhalb des Control Rooms und führt nahezu in Echtzeit eine Analyse der Bot-Vorgänge und Geschäftsprozessdaten durch. Bot Insight generiert automatisch anpassbare Dashboards mit fortschrittlichen Algorithmen, die für jeden Bot einzigartig sind. Die Detailgenauigkeit, die Bot Insight auf der Grundlage fein abgestimmter Ereignisprotokolle für Bot-Vorgänge bereitstellt, ermöglicht nuancierte Warnmeldungen, Ad-hoc-Ermittlungen, interaktive Drilldowns, Zeitreihenanalyse und umfassende Einblicke in Betriebs-/Geschäftsprozesse. Darüber hinaus können alle Daten für SIEM-Protokolle (Security Information and Event Management) zur weiteren Analyse, Untersuchung und Berichterstellung exportiert werden.

Bots in Aktion: Zwei Arten von Automatisierungen

Vor dem Einstieg in die hochqualitativen Sicherheitsfunktionen von Automation Anywhere Enterprise müssen noch zwei grundlegende Automatisierungsarten erläutert werden: beaufsichtigt und unbeaufsichtigt.

Eine beaufsichtigte Automatisierung ist eine, bei der ein Nutzer an der Bot Runner-Maschine angemeldet ist, um die Bot-Ausführung zu beobachten und/oder aktiv zu unterstützen. Gründe dafür, dass ein Nutzer anwesend sein sollte, könnten sein, dass der Bot eine Funktion ausführt, die den Menschen unterstützt oder, dass der Bot Arbeit ausführt, die periodische Eingaben oder situative Anweisungen durch einen Nutzer erfordern. Beaufsichtigte Automatisierungen werden auch als Front-Office-Automatisierungen bezeichnet.

Unbeaufsichtigte Automatisierungen funktionieren, wie der Name schon sagt, ohne Geschäftsnutzer- oder Bedienerinteraktion. Unbeaufsichtigte Automatisierungen werden normalerweise von einem Bediener ausgeführt, der wenig über den Bot, die zu automatisierende Anwendung oder den Zweck der Automatisierung weiß. Der Bediener plant in Verbindung mit dem Geschäftsbereich die Ausführung von Bots auf Bot Runnern. Während der Ausführung überwacht der Bediener die betrieblichen Aspekte der laufenden Bots wie CPU, Speicher und Speichernutzung, um sicherzustellen, dass sie ohne Fehler oder Ausnahmen ausgeführt werden. Control Room-Dashboards zeigen während des Betriebs alle operativen Details der Bots an.

ENTERPRISE RPA-SICHERHEIT – MEHRSTUFIGE IDENTIFIKATION UND AUTHENTIFIZIERUNG

Ein Kernprinzip der Sicherheitsarchitektur von Automation Anywhere Enterprise besteht darin, dass ohne vorherige Authentifizierung der beteiligten Entität weder ein Zugriff noch eine Aktion zulässig ist. Dies gilt für Menschen und Bots gleichermaßen. Um die Autorisierung in RPA zu verstehen, muss man zunächst den Authentifizierungsprozess sowohl für reguläre als auch für unbeaufsichtigte Automatisierungen verstehen.

WER IST WER: TYPISCHE UNTERNEHMENSAUTHEN-TIFIZIERUNGEN

Anmeldeinformationen und Personas können mehrschichtig sein. Betrachten wir ein einfaches Szenario für die Unternehmensauthentifizierung (siehe Abbildung 2). Eine Enterprise-Nutzerin, Alice, authentifiziert sich bei ihrer Windows-Workstation. Alice meldet sich dann bei einer Anwendung an, die remote ausgeführt wird, und authentifiziert sich über eine Windows-basierte Active Directory-Anmeldung oder möglicherweise Kerberos-basiert auf ihrer Workstation mit einem gültigen Ticket. In diesem Szenario umfasst die Authentifizierungskette eine einzelne Person und deren Berechtigungsnachweise.

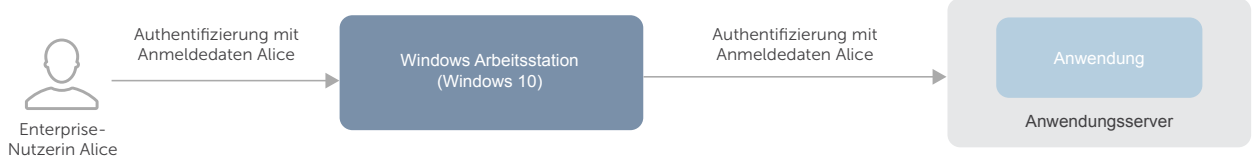


Abbildung 2: Typische Unternehmensauthentifizierung

Betrachten wir das Szenario einer beaufsichtigten Automatisierung aus Abbildung 3. In diesem Fall testet der Nutzer Bob entweder einen Bot oder führt eine beaufsichtigte Automatisierung im Rahmen eines normalen Arbeitstages durch. In Schritt 1 authentifiziert er sich bei der Bot Runner-Workstation mit seinen persönlichen Anmeldeinformationen (genau wie im obigen Alice-Szenario). In Schritt 2 startet er den Automation Anywhere Enterprise-Client und gibt seine Nutzer-ID und das Kennwort für den Control Room ein, wodurch die Client-Software für den Control Room authentifiziert wird. In Schritt 3 führt er den Bot aus, der wiederum auf eine Anwendung zugreift, die eine Authentifizierung erfordert. Die vom Bot in diesem Schritt verwendeten Anmeldedaten können entweder im Enterprise-Credential Vault gespeichert und während der Laufzeit vom Bot abgerufen werden, oder es kann eine Weiterleitung von Bobs persönlichen Anmeldedaten erfolgen (darauf basierend, dass Bob sich bei der Domain angemeldet hat und über ein Kerberos-Ticket verfügt, oder basierend auf einem beliebigen Single Sign-On). In jedem Fall ergeben sich insgesamt drei Ebenen der Identifikation und Authentifizierung.

Es werden drei Ebenen der Authentifizierung für das in Abbildung 4 dargestellte unbeaufsichtigte Szenario verwendet, obgleich mit ein paar kleinen Änderungen. In diesem Fall beginnt der Nutzer Charles mit der Authentifizierung beim Control Room, sodass er einen Bot auswählen kann, der sofort oder zu einem geplanten Zeitpunkt ausgeführt werden soll.

Wenn in Schritt 2 die Zeit für die Bot-Ausführung beginnt, initiiert der Control Room eine automatische Anmeldung an der Bot Runner-Workstation unter Verwendung der Berechtigung „BotRunnerUser“. Nachdem der Bot in die lokale Player-Funktion heruntergeladen (Schritt 3) und gestartet wurde, authentifiziert er sich bei der Zielanwendung mit den Anmeldedaten BotApplicationUser (Schritt 4). Genau wie bei dem beaufsichtigten Automatisierungsszenario kann es sich bei den BotApplicationUser-Anmeldedaten um Anmeldedaten handeln, die vom Credential Vault abgerufen wurden, oder es kann sich um Pass-Through-Anmeldedaten für BotRunnerUser handeln.

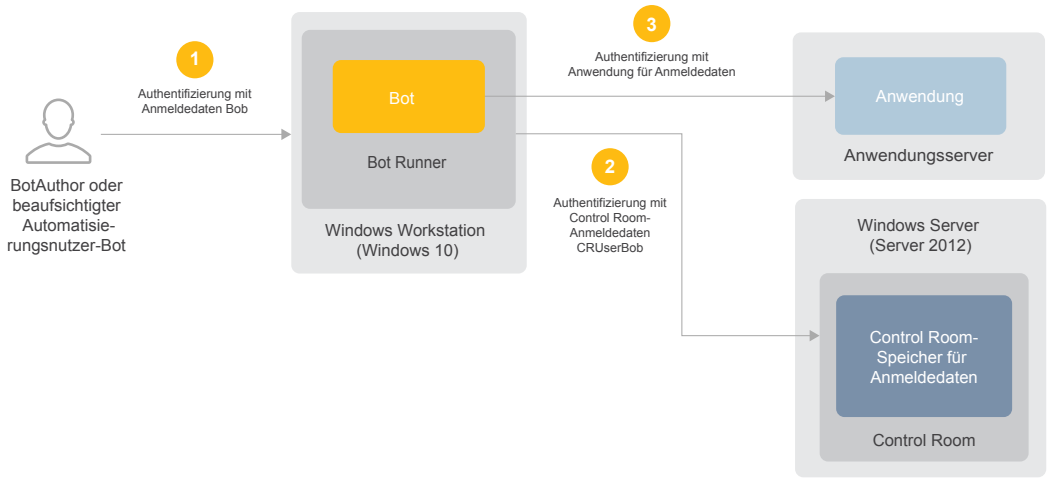


Abbildung 3: Authentifizierungsprozess für das beaufsichtigte Automatisierungsszenario

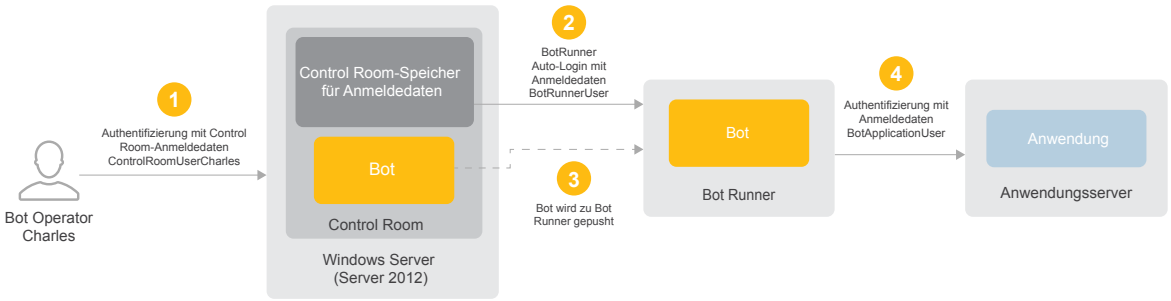


Abbildung 4: Authentifizierungsprozess für das unbeaufsichtigte Automatisierungsszenario

Authentifizierungsoptionen und IAM-Integrationen

Zu den unterstützten Optionen für die Control Room-Authentifizierung gehören Active Directory mit LDAP, Active Directory mit Kerberos und lokale Authentifizierung mit dem eingebetteten Credential Vault (wird in einem späteren Abschnitt beschrieben).

Andere Identitäts- und Zugriffsverwaltungsoptionen, die für Unternehmensbereitstellungen verfügbar sind, umfassen:

+ Unterstützung für SAML 2.0-basiertes Single Sign-On
+ Integration in Zugangs-/Anmeldeverwaltungslösungen von Drittanbietern (z. B. CyberArk)

UMFASSENDE ROLLENBASIERTE ZUGRIFFSSTEUERUNG

Eine erfolgreiche Authentifizierung ist nur die erste Stufe der obligatorischen Durchsetzung der Zugriffskontrolle, die die Sicherheitsarchitektur von Automation Anywhere Enterprise bietet. Ebenso wichtig ist die Autorisierung, insbesondere wenn es um die Einhaltung der Grundprinzipien der minimalen Berechtigungen und der Aufgabentrennung geht. Die Autorisierung in Automation Anywhere ist mit einer detaillierten rollenbasierten Zugriffssteuerung (RBAC) konfiguriert.

Zur Veranschaulichung von RBAC definieren wir einige verschiedene Rollen. Die Rollen, die Sie in Ihrer Bereitstellung verwenden, können abweichen. Zusätzlich verwenden Sie möglicherweise weitere Rollen. Es gibt fünf verschiedene Rollen (siehe Tabelle 1) in der Grundarchitektur und in den Hauptfunktionen der RPA-Plattform. BotAuthor verwenden den Bot Creator, um Geschäftslogik zu erfassen und entsprechende Automatisierungen zu erstellen. BotAuthor arbeiten mit Testanwendungen und Datensätzen, sodass Produktionssysteme während der Entwicklungsphase nicht beeinträchtigt werden. Ein einzelner Bot durchläuft in der Regel viele verschiedene Iterationen und Versionen, nicht nur während der ersten Entwicklung, sondern auch dann, wenn die zugehörigen Geschäftsprozesse und/oder Zielanwendungen aktualisiert werden. BotTester arbeiten auch mit Bot Creator zusammen, um Bots auf Leistung, Datenintegrität und Sicherheit zu testen und sicherzustellen, dass jeder Bot das tut, was er tun soll. BotTester dienen als zweite Stufe der Autorisierung für den Bot, bevor er mit Produktionsdaten und Anwendungen ausgeführt werden kann.

Nachdem ein Bot getestet und einer Sicherheitsüberprüfung unterzogen wurde, arbeitet der BotPromoter mit dem BotAuthor/BotTester zusammen, um die Version des Bots festzulegen, der in der Produktion verwendet werden soll. Dies ist die einzige Version des Bots, die für den BotOperator sichtbar ist, der sich mit den Geschäftsbereich(en) koordiniert, um den Bot zu planen und auszuführen. Der BotOperator ist auch für die Überwachung der Bot-Leistung im Control Room verantwortlich, einschließlich der Fehlerbehebung bei auftretenden Laufzeitproblemen. Die Verantwortung für die allgemeine Verwaltung der Plattform einschließlich der Konfiguration von Komponenten, Schnittstellen und aller Rollen/Berechtigungen liegt schließlich beim RPA-Administrator.

Erweiterte Aufgabentrennung

Diese grundlegende Rollendefinition stellt einen grundlegenden Ausgangspunkt für RBAC dar, innerhalb der Automation Anywhere Enterprise-Plattform ist jedoch eine noch umfangreichere Aufgabentrennung möglich. Mit dem Assistenten für die Rollenerstellung können Administratoren auf einfache Weise nutzerdefinierte Rollen festlegen und Berechtigungen erstellen, die die gesamte Suite von Control Room-Objekten und -Funktionen berücksichtigen, einschließlich Nutzerverwaltung, Lizenzierung, Credential Vault, Bot Runner-Sätze, Bot-Zeitpläne, Bot-Vorgänge/Dashboards und Auditprotokolle. Wenn jedes Privileg ausgewählt ist, fügt der Assistent dynamisch Schritte für kontingente/abgeleitete Privilegien hinzu.

Wenn zum Beispiel die Berechtigungen für „BOTS > Meine Bots anzeigen > Meine Bots ausführen“ ausgewählt sind (siehe Abbildung 5), fügt der Workflow einen Schritt hinzu, um die spezifischen Bot-Ordner (d. h. Botsätze) anzugeben, für die Zugriff gewährt wird. Das Endergebnis ist die Möglichkeit, High-Fidelity-Rollen zu erstellen, die über austarierte Zugriffskontrollen verfügen, um die Anforderungen der strengsten, sichersten und durch Compliance regulierten Umgebungen zu erfüllen.

Rolle	Beschreibung
RPA Admin	Verwaltet das System (Konfiguration von Komponenten, Rollen, Schnittstellen)
BotBuilder	Ein Geschäftsprozess-Experte, der mit dem Task-Editor Bots erstellt und grundlegende Funktionstests durchführt
BotTester	Ein Qualitätssicherungstester, der die Bots auf Funktionsgenauigkeit, Leistung und Sicherheit überprüft
BotPromoter	Ein Administrator, der Bots zwischen Entwicklungs-, Test- und Produktionsphasen genehmigt und verschiebt
RPAOperator	Ein Operator, der Bots plant, ausführt und deren Leistung überwacht

Tabelle 1: Primäre RPA-Rollen in Automation Anywhere Enterprise

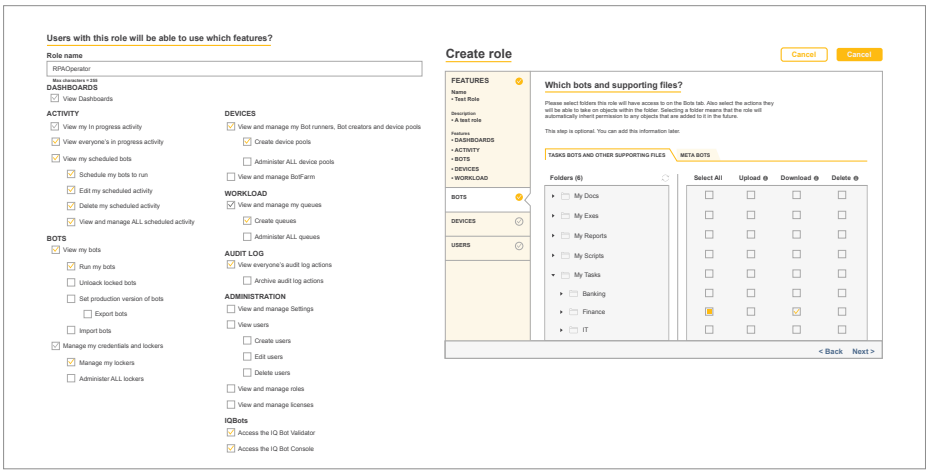


Abbildung 5: Rollenerstellung mit fein abgestimmter Autorisierung

Unabhängige Kontrollebenen

Neben den umfassenden RBAC-Funktionen bietet Automation Anywhere Enterprise eine logische Aufgabentrennung, indem es eine Architektur verwendet, die die Aufgaben der Bot-Entwicklung und der Bot-Ausführung vollständig voneinander trennt.

Bot Creator können nur Bots zum und vom Versionskontrollsystem im Control Room hochladen und herunterladen. Gleichzeitig sind Bot Runner auf die Ausführung von Bots beschränkt. Sie haben keinen Zugriff auf die Bot-Erstellung und Testfunktionen. Diese architektonisch erzwungene Aufgabentrennung stellt eine doppelte Autorisierung dar, die mit den Best Practices des National Institute of Standards und Technologies (NIST) in Einklang steht, da es (mindestens) sowohl einen Entwickler als auch einen Geschäftsanwender erfordert, um eine Geschäftsprozessautomatisierung durchzuführen.

Unabhängige Verarbeitungsdomänen

Ein leistungsfähiger Anwendungsfall für die RBAC-Funktionen der Plattform, vor allem für große Unternehmen, ist die Einrichtung von unabhängigen Verarbeitungsdomänen (siehe Abbildung 6). In diesem Zusammenhang ist die „Verarbeitungsdomäne“ eine Sammlung von Automatisierungen (Bots), Bot Runnern und Nutzern. Dies kann durch strikte Organisation/Speicherung der Bots für jede gewünschte Domäne in einem entsprechenden Ordner im Control Room erfolgen.

Fallbeispiel: Mit Finanzanwendungen verknüpfte Bots werden in einem Finanzordner abgelegt, während die mit HR verknüpften Bots in einem HR-Ordner abgelegt werden. Bot-Betreibern für die Finanzabteilung würden dann Privilegien nur für Finanzen-Bots und für Finanzen-Bot-Runner zugewiesen. Bot-Betreiber für HR würden Privilegien nur für HR-Bots und Bot Runner bekommen und so weiter für andere Verarbeitungs-/Automatisierungsdomänen (siehe **Abbildung 6**).

Das Endergebnis ist eine weitere Aufgabentrennung und Isolation der zugehörigen Apps und Daten – diesmal auf Ebene der Organisationseinheiten/Domänen – da einzelne Betreiber keine Bots außerhalb ihrer jeweiligen Domäne anzeigen oder betreiben können.

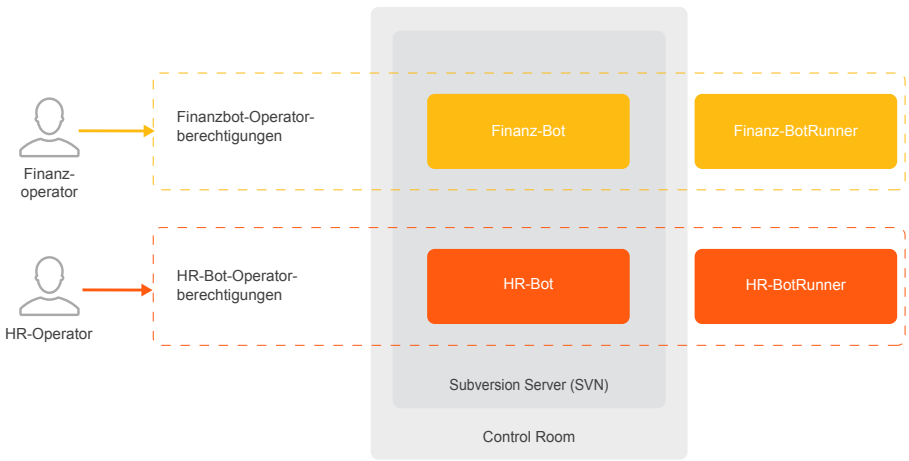


Abbildung 6: Unterstützung für unabhängige Verarbeitungsdomänen

END-TO-END-DATENSCHUTZ

Die Authentifizierung auf mehreren Ebenen und eine fein abgestimmte Zugriffssteuerung sind für eine streng kontrollierte Umgebung unerlässlich. Dies gilt auch für den durchgängigen Datenschutz, der auch erforderlich ist, um die Vertraulichkeit und Integrität geschäftskritischer Prozesse, sensibler Daten und sonstiger Informationen (z. B. Anmeldedaten) zu gewährleisten.

Die Automation Anywhere Enterprise-Plattform deckt diesen Bedarf mit einem eingebetteten Credential Vault ab und bietet eine umfassende Reihe von Sicherheitsvorkehrungen, die nicht nur Daten in Ruhe und während der Übertragung schützen, sondern auch, während sie auf einzelnen Systemen verwendet werden.

Verschlüsselungsschlüssel und der Credential Vault

Abbildung 7 zeigt die von der Plattform verwendeten primären Verschlüsselungsschlüssel sowie ihre Beziehung zum Credential Vault. Die gesamte Verschlüsselung wird mit FIPS 140-2, Level 1-validierten kryptographischen Modulen durchgeführt.

Während der Installation (linker Teil von **Abbildung 7**) generiert das System ein RSA-2048-Bit-Public/Private-Schlüsselpaar und einen AES-256-Bit-Schlüssel. Der private Schlüssel des RSA 2048-Paares wird als Hauptschlüssel bezeichnet, während der AES 256-Schlüssel als Datenschlüssel bezeichnet wird. Der Hauptschlüssel wird dem Installationsadministrator zur Aufbewahrung an einem physisch sicheren Ort außerhalb des Systems übergeben. Der öffentliche Schlüssel wird zum Verschlüsseln des Datenschlüssels verwendet. Sowohl der öffentliche Schlüssel als auch der verschlüsselte Datenschlüssel werden dann in der Datenbank gespeichert.

Während des Starts oder Neustarts des Control Room (rechter Teil von **Abbildung 7**) wird der Administrator aufgefordert, den Hauptschlüssel anzugeben. Der verschlüsselte Datenschlüssel wird aus der Datenbank abgerufen und mit dem Hauptschlüssel entschlüsselt. Der Datenschlüssel ist jetzt einsatzbereit. Während das System Daten aus dem Credential Vault speichert und abruft, wird der Datenschlüssel zum Verschlüsseln und Entschlüsseln dieser Daten verwendet.

Der Credential Vault wird zum Speichern aller vom System verwalteten Anmeldeinformationen und kritischen Systemkonfigurationsdaten verwendet. Er kann auch verwendet werden, um andere vertrauliche Daten (z. B. Name-Wert-Paare) zu speichern, die in der Automatisierung einer Organisation verwendet werden. Infolgedessen können BotAuthor die unsichere Praxis der Hardcodierung von Anmeldedaten und anderer sensibler Daten/Argumente direkt in ihren Automatisierungen vermeiden. Innerhalb des Credential Vault werden die Daten von Lockern organisiert. Locker ermöglichen die Zuweisung verschlüsselter Anmeldedaten pro Nutzer, geschützt durch Berechtigungen und Rollen als Teil der RBAC-Funktionen von Automation Anywhere. Jeder Locker kann einem einzelnen Nutzer oder einer Rolle zugewiesen werden, um den Locker-Zugriff auf bestimmte RPA-Nutzer zu beschränken.

SCHUTZ von ruhenden Daten

Neben dem Verschlüsseln lokaler Anmeldedaten und der Auswahl der von Bots verwendeten Laufzeitdaten bietet der Credential Vault einen sicheren Speicher für vertrauliche Konfigurationsparameter und Details zu den integrierten Versionskontroll- und E-Mail-Diensten.

Schutz von Daten während der Übertragung

Alle Netzwerkdienste auf den Clients und im Control Room verwenden Transport Layer Security (TLS) 1.2, um die Datensicherheit und -integrität während der Übertragung zwischen Komponenten sicherzustellen.

Die für die Bot Creator/Runner-Authentifizierung beim Control Room verwendeten Anmeldedaten werden verschlüsselt, bevor sie über eine TLS-gesicherte Verbindung übermittelt werden. Diese zusätzliche Verschlüsselungsebene schützt nicht nur vor Problemen mit dem Netzwerkstack (z. B. Heartbleed), sondern verhindert auch die Offenlegung der Anmeldedaten für Implementierungen, bei denen die TLS-Verbindung der äußeren Schicht an einem Front-End-Lastausgleich beendet wird.

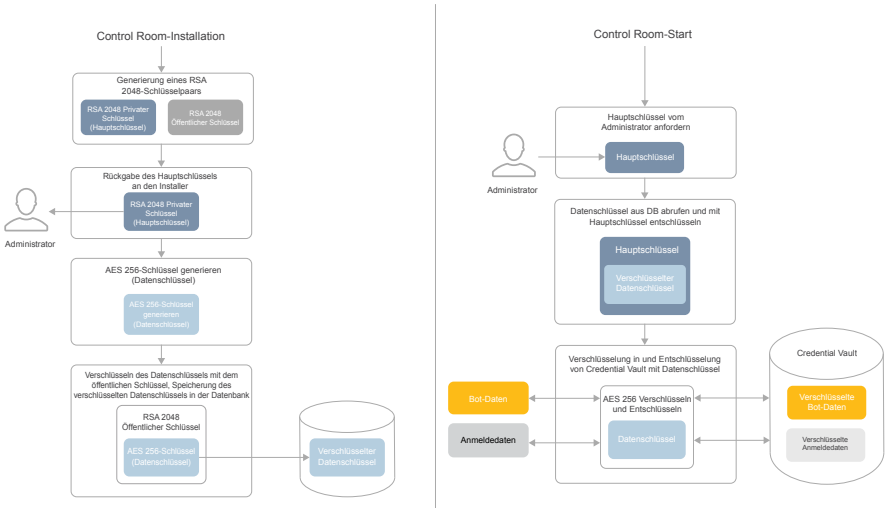


Abbildung 7: Die Automation Anywhere Enterprise-Verschlüsselungsarchitektur

Schutz der verwendeten Daten

Die Laufzeitsicherheit beginnt mit dem Schutz verteilter Anmeldedaten. Insbesondere gibt es keinen lokalen Speicher für Anmeldedaten für Bot Runner. Anmeldedaten und andere Daten, die dynamisch aus dem Credential Vault für die Verwendung in Automatisierungen abgerufen werden, werden ausschließlich in verschlüsselter Form im flüchtigen Speicher aufbewahrt – und werden gelöscht, sobald die Ausführung des zugeordneten Bots abgeschlossen ist.

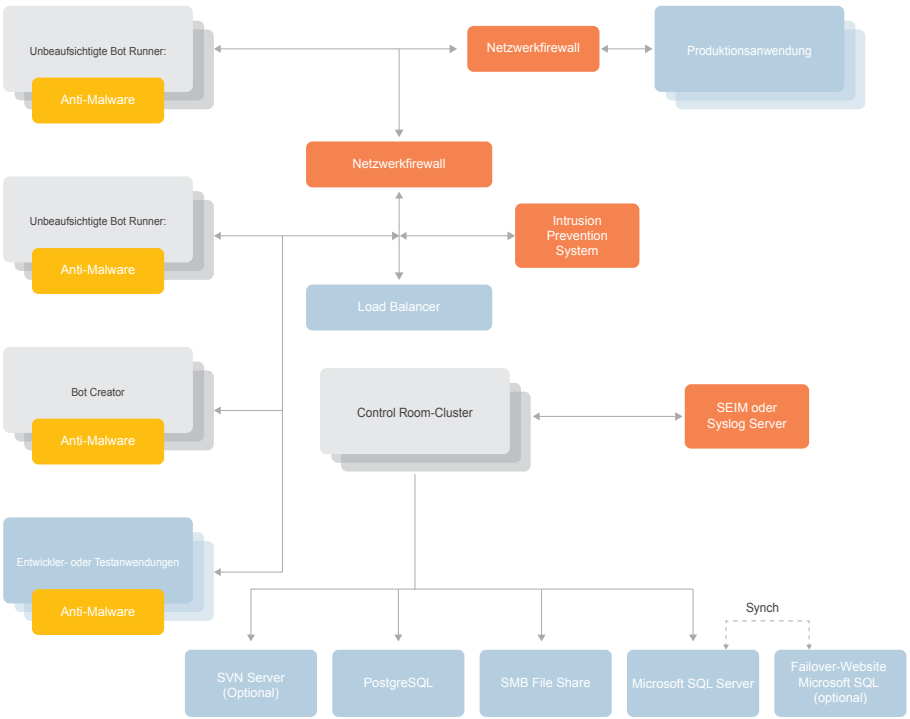
Weitere Funktionen und Konfigurationsoptionen, die verwendet werden können, um unbefugten Zugriff auf vertrauliche Informationen (z. B. Datenlecks) oder Manipulationen an Bots während der Laufzeit zu verhindern, sind:

+ Geschützter Modus: Wenn auf dem lokalen Bildschirm keine Programmfenster angezeigt werden und angemeldete Nutzer die Option haben, die Bilderfassung auf Bot Creatorn und Bot Runnern zu deaktivieren, um zu verhindern, dass vertrauliche Informationen auf dem Bildschirm von Bots gespeichert werden
+ Eingabesperre: Die Fähigkeit, die Maus und die Tastatur für die Maschine zu deaktivieren, auf der eine Automatisierung läuft
+ Zeitlimit: die Möglichkeit, ein Zeitlimit festzulegen, nach dessen Ablauf eine Automatisierung beendet wird, wenn die Ausführung nicht abgeschlossen ist
+ Zentrale Steuerung: Die Fähigkeit, ferngesteuerte Automatisierungen innerhalb des Control Rooms zentral zu steuern (d. h. anzuhalten, wieder aufzunehmen und zu stoppen)

SICHERN DER RPA-BEREITSTELLUNG

Die AAE-Architektur besteht aus einer Standard-Desktop- und Serverklassen-Infrastruktur für die Clients bzw. den Control Room. In diesem Abschnitt werden die Best Practices zum Schutz der RPA-Plattform mit externen Sicherheitskontrollen beschrieben, die in jedem Unternehmen vorhanden sind. Netzwerkbasierte Firewalls, Intrusion-Detection-Systeme, Anti-Malware und externe Protokollserver sind Standardsicherheitskontrollen, die für die RPA-Bereitstellung genauso relevant wie für die weitere Infrastruktur in Ihrer Umgebung sind. Das Diagramm unten zeigt, wo diese Komponenten in der RPA-Bereitstellung eingesetzt werden.

Jede externe Sicherheitskontrolle wird im Folgenden ausführlich in Bezug auf Platzierung und Konfiguration erläutert. Der Zugriff auf unterstützende Netzwerkdienste wie Active Directory, SVN Server, PostgreSQL, SMB File Share, Microsoft SQL und Produktionsanwendungen kann über Netzwerkfirewalls oder abhängig von ihrer Platzierung hinsichtlich der RPA-Komponenten direkt erfolgen.



Netzwerkbasierte Zugriffssteuerung – Schutz von RPA durch Firewalls

Netzwerkbasierte Firewalls und lokale serverbasierte Firewalls werden verwendet, um den Control Room oder alle Knoten in einem Control Room-Cluster bei einer Clusterbereitstellung zu schützen. Standardmäßig sollten im Unternehmensnetzwerk nur Protokolle zugelassen werden, die im Control Room erforderlich sind. Darüber hinaus sollten alle Clusteringprotokolle nur zwischen Knoten im Control Room-Cluster zulässig sein. Netzwerkbasierte Firewalls werden verwendet, um Entwicklungs-, Test- und Produktions-RPA-Umgebungen vom Unternehmensnetzwerk und voneinander zu isolieren (siehe folgender Abschnitt „Secure Software Development Lifecycle“).

Bei unbeaufsichtigten Automatisierungsumgebungen werden die Bot Runner in einem eigenständigen isolierten Netzwerk platziert und durch eine netzwerkbasierte Firewall geschützt. Beaufsichtigte Automatisierungen werden von Arbeitsstationen des Unternehmens ausgeführt, auf denen der Bot Runner-Client installiert ist, und über die Perimeterfirewalls des Unternehmens oder interne Firewalls geschützt, die die Desktop-Infrastruktur des Unternehmens schützen.

In der nachstehenden Tabelle finden Sie die Protokolle, die vom Control Room und vom Client verwendet werden.

3.10 List of Port Numbers

Below table lists the configurable ports used by our platform

3.10.1 Client

Port	Description	Deployment	Used for
110 995	POP3	Client	“Email Automation” command to retrieve emails from mail server.
143 993	IMAP	Client	
21	FTP/SFTP	Client	“FTP/SFTP” command
25 465 587	SMTP	Client	“Send email, Error handling” command “Email notification” feature
161	UDP	Client	“SNMP” command
22 23	Terminal Emulator	Client	“Terminal Emulator” command
4530	TCP	Client (AAProxyServer.exe)	Used by the client to communicate with plugins via TCP socket for AAE Client, Editor or Player

80	HTTP	Control Room	Web UI access (No TLS, not recommended)
443	HTTPS	Control Room	Web UI access (Recommended)
25 465 587	SMTP	Control Room	Send email when important events occur (user created, password set/reset, role changed etc.)
1433	TCP	Microsoft SQL Server	Default port used by Microsoft SQL Server
5672	TCP	Control Room	Cluster Messaging
47500-47600	TCP	Control Room	Cluster Messaging and Caching
47100-47200	TCP	Control Room	Cluster Messaging and Caching

Anti-Malware – Schutz von RPA vor Viren und Malware

Der AA-Client wird auf der Desktop-Klasseninfrastruktur ausgeführt und sollte in jeder Hinsicht als Unternehmens-Desktop betrachtet werden. Anti-Malware/Antivirus-Software wird verwendet, um die Client-Umgebung vor bösartiger Software in Form von Viren und Malware zu schützen.

Intrusion-Detection-Systeme – Schutz von RPA vor direkten Angriffen

Intrusion-Detection- und Intrusion-Prevention-Systeme (IPS) schützen das Unternehmensnetzwerk, indem netzwerkbasierte Angriffe durch Netzwerkdatenverkehrsanalyse erkannt werden. Wie jeder andere kritische Bereich des Rechenzentrums wird auch die RPA-Plattform am Ausgangspunkt hinter der netzwerkbasierten Firewall durch ein IPS-System geschützt. Die Platzierung von IPS in Ihrem Netzwerk sollte auf der Grundlage von Unternehmenskonventionen betrachtet werden und gleichermaßen für die RPA-Plattform gelten.

Security Event Incident Management (SEIM) – Schutz von RPA durch externes Auditing

Control Room-Protokolle können zur externen Speicherung, Verarbeitung und Warnung an ein SEIM-System (Security Event Incident Management) weitergeleitet werden. Die Integration mit SIEM oder einem syslog-basierten Auditkonsolidierungs- und -reduktionssystem verbessert Sicherheitsstatus, Governance und Compliance erheblich. Konfigurieren Sie den Control Room so, dass Audit-Protokolle an den entsprechenden Syslog-Sammelserver in der Umgebung weitergeleitet werden.

EXTERNE VALIDIERUNG VON SICHERHEITS-KONTROLLEN

Für Bundesbehörden, die AAE bereitstellen, ist eine der Anforderungen, dass die Sicherheitskontrollanforderungen des Federal Information Security Management Act (FISMA) erfüllt werden, wenn sie in einem lokalen IT-System eingesetzt werden.

AAE unterstützt Sicherheitsfunktionen, die AAE in eine bereits vorhandene FISMA-kompatible Umgebung integrieren und Steuerelemente wie zentrale Authentifizierung (z. B. Active Directory (AD), zentrale Protokollverwaltung, Analyse und Berichterstellung unterstützen. Funktionen über ein SIEM (Security Information and Event Management) sowie Netzwerkpartitionierung und Netzwerkzugriffskontrolle über virtuelle lokale Netzwerke (VLANs) und Firewalls) sind vorhanden und können gegebenenfalls in AAE integriert werden.

AAE unterstützt die Implementierung anwendbarer Sicherheitskontrollen und ermöglicht es IT-Experten, den SSP eines IT-Systems zu aktualisieren, um die sichere Bereitstellung und Verwendung von AAE zu gewährleisten. Weitere Informationen zu den FISMA-Steuerelementen finden Sie unter AAE-Funktionen, die mit ausgewählten FISMA Moderate-Steuerelementen aus NIST SP 800-53 Rev. 4 verglichen und bezüglich Einschränkungen oder Unterstützung von Steuerungsanforderungen analysiert wurden. Das NIST-Framework kann anderen Frameworks wie HIPAA und PCI zugeordnet werden. Weitere Informationen zu den FISMA-Steuerelementen, die in Automation Anywhere Enterprise implementiert sind, finden Sie im Whitepaper Automation Anywhere Enterprise – Through The Lense of FISMA.

SECURE SOFTWARE DEVELOPMENT LIFECYCLE (SDLC) SUPPORT

Um die Steuerelemente und Sicherheitsmaßnahmen für die Automatisierungsumgebung zu maximieren, kann das zuvor beschriebene grundlegende Bereitstellungsszenario „erweitert“ werden, um weitere Best Practices für den Secure Software Development Lifecycle (SDLC) bereitzustellen, z. B. von FISMA, FedRamp und PCI DSS benötigte Verfahren. Das resultierende erweiterte Bereitstellungsmodell bietet drei verschiedene RPA-Zonen – jeweils eine für Entwicklung, Nutzerakzeptanztests (UAT) und Produktion (siehe Abbildung 8). Jede Zone ist logisch getrennt (isoliert), wobei verschiedene Nutzergruppen unterschiedliche Rollen und Berechtigungen erhalten. Die gestrichelten vertikalen Linien stellen Netzwerksegmentierung und Firewalls dar.

Wie im Basisbereitstellungsmodell beginnt der Bot-Lebenszyklus in der Entwicklung. Sobald die BotAuthor mit dem Bot zufrieden sind, übertragen UAT-BotPromoter den Bot vom Entwicklungsversionierungs-Repository (SVN) in das UAT-Repository. Der ausschließliche Zweck der UAT-Zone besteht darin, Bots auf Genauigkeit, Leistung und Sicherheit zu testen. Sobald ein Bot die Abnahmeprüfung bestanden hat, wird er von einem Produktions-BotPromoter in die Produktionszone weitergeleitet. An diesem Punkt erreicht er den Produktionsstatus und steht RPAOperatorn für den Einsatz in Produktionsanwendungen zur Verfügung. In jedem Schritt des Prozesses werden Prüfungen und Zertifizierungen von verschiedenen Administratoren mit unterschiedlichen Rollen und Berechtigungen durchgeführt. Eine strikte Aufgabentrennung und mehrschichtige Steuerelemente sind standardmäßig integriert, um sicherzustellen, dass die Digital Workforce zuverlässig, skalierbar, effizient, sicher und konform ist.

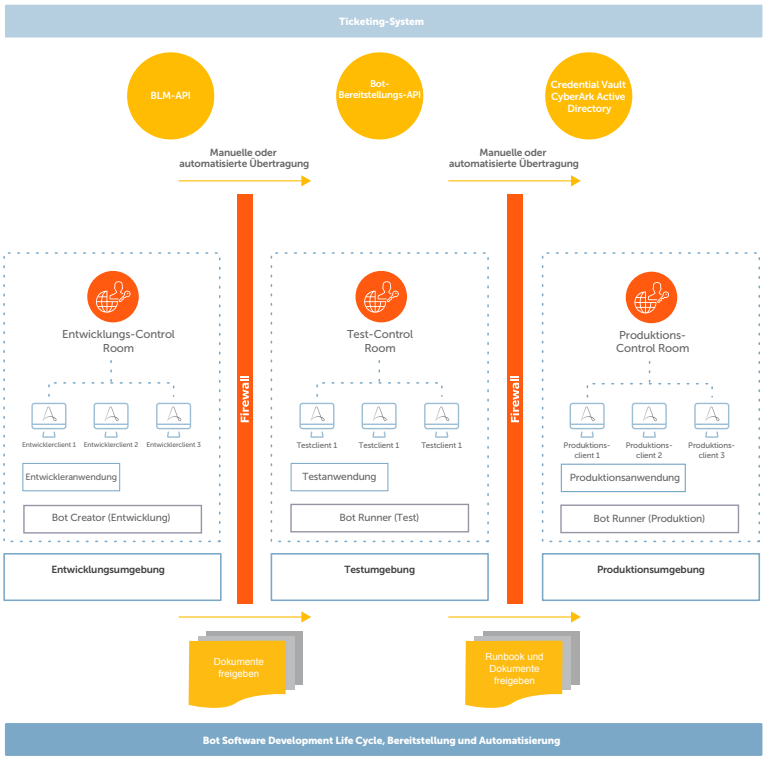


Abbildung 8: Erweitertes Bereitstellungsmodell für vollständige SDLC-Unterstützung

PROTOKOLLIERUNG UND ÜBERWACHUNG

Umfassende Auditprotokollierungs-, Überwachungs- und Berichtsfunktionen sind wesentliche Komponenten der Sicherheitsarchitektur für jede hochkarätige IT-Lösung. Automation Anywhere Enterprise ist keine Ausnahme.

Über die Plattform hinweg werden Ereignisdetails (wer, was, wann, wo und Ergebnis) automatisch für über 60 Arten von Nutzer-/Entitätsaktionen erfasst – einschließlich Erstellung, Änderung, Aktivierung, Deaktivierung und Entfernung von Nutzern, Bots, Bot Creatorn und Bot Runnern. Die Zulassung wird durch eine Kombination aus automatischer Erfassung, Bindung jeder Aktivität an eine bestimmte Identität und einer schreibgeschützten Standardrichtlinie erreicht. RBAC kann auch eingesetzt werden, um genau zu steuern, welche Rollen überhaupt für Auditprotokolle sichtbar sind.

Aus Überwachungssicht sind automatisierte Dashboards und Berichte innerhalb des Control Rooms zugänglich und können angepasst werden, um anormale Aktivitäten (oder andere Details, die das Automatisierungs- oder Sicherheitsteam für interessant hält) zu erkennen und zu alarmieren. Darüber hinaus unterstützt der Export von Protokollen die Verwendung anderer Infrastrukturen für Analyse, Berichterstellung und Vorfallsermittlung/-reaktion, die bereits von der Organisation verwendet werden, z. B. SIEM, UEBA und erweiterte Analysetools.

ZUSÄTZLICHE SICHERHEITS- UND AUSFALLSICHERHEITSFUNKTIONEN FÜR UNTERNEHMEN

Automation Anywhere Enterprise unterstützt darüber hinaus die Sicherheits- und Ausfallsicherheitsziele von Unternehmen mit:

+ Einer verteilten (und flexiblen) Komponentenarchitektur, die sich nahtlos in die vorhandene Hochverfügbarkeits-/Notfallwiederherstellungsinfrastruktur (HA/DR) eines Unternehmens einfügt
+ Einem integrierten Versionskontrollsystem (Apache Subversion), das in Verbindung mit den umfassenden RBAC-Funktionen der Plattform äußerst strikte Änderungsverwaltungsrichtlinien und -prozesse implementieren und durchsetzen kann
+ Tools wie die Hibernate- und ReactJS-Frameworks während der Entwicklung von Plattformcode, um die Anfälligkeit für häufige Angriffe zu vermeiden (wie SQL Injection und Cross Site Scripting)
+ Einem Sicherheitsplan/-protokoll für die Code-Entwicklung, für den/das laufendes Scannen mit mehreren Tools und Schichten erforderlich ist, um Softwareschwachstellen zu erkennen und zu beseitigen

Weitere Informationen zu diesen und vielen anderen Steuerelementen, Sicherheitsmaßnahmen und Sicherheitsfunktionen, die Bestandteil von Automation Anywhere Enterprise sind, finden Sie hier: https://www.automationanywhere.com/images/Enterprise-Architecture.pdf

API-AUTOMATISIERUNG

Da die Bereitstellung von Bots exponentiell wächst, ergeben sich neue Herausforderungen rund um die sichere Authentifizierung und das betriebliche Bot-Lebenszyklusmanagement. Es ist notwendig, die Zeit für die Bereitstellung zu reduzieren und von Menschen verursachte Fehler zu beseitigen. Automation Anywhere bietet APIs für die Integration in die Automatisierung von Drittanbietern für die sichere Authentifizierung und Bereitstellung des Bot-Lebenszyklusmanagements. In diesem Abschnitt werden APIs beschrieben, die die oben genannten Funktionen bereitstellen.

Credential Vault – API

Der Automation Anywhere Credential Vault wird für die verschlüsselte Speicherung von Anmeldedaten verwendet, die von einer Automatisierung (Bot) für die sichere Authentifizierung verwendet wird. Die Credential Vault-APIs können für die Synchronisierung von Anmeldedaten mit externen Identity Access Management Systems (IAM) über ein Bereitstellungsprogramm verwendet werden, für Notfallszenarien, in denen einem Bot unter bestimmten Umständen ein Passwort zugewiesen wird, das sich fortlaufend ändert, bei externer Verwaltung von Anmeldedaten über ein externes Bereitstellungsprogramm.

Bot-Bereitstellungs-API

Die Bot-Bereitstellungs-API ermöglicht es externen Anwendungen, einen Automatisierungs-Workflow auf einem Bot Runner zu starten. In Fällen, in denen ein Bot über die API gestartet werden kann, können Bots, die sicherheitsrelevante Funktionen ausführen, von einer externen Anwendung bereitgestellt werden. Beispielsweise kann eine SIEM-Lösung eine Warnung auslösen, die einen Bot startet, um die Datenerfassung aus dem in der Warnung angegebenen System durchzuführen. Bei dieser Datensammlung kann es sich um alles Mögliche handeln, z. B. das Aussetzen ausgeführter Prozesstabellen, Snapshots von Dateiprüfsummen, die Ressourcenauslastung und die aktuell angemeldeten Nutzer.

Bot-Lebenszyklusmanagement (API)

Mithilfe der Bot-Lebenszyklusmanagement (BLM)-API kann eine externe Bereitstellungsanwendung den Prozess des Verschiebens von Bots von einem Control Room in einen anderen automatisieren. Dies ist wichtig in Unternehmen, die Secure Development Lifecycle (SDLC) verwenden. Weitere Informationen finden Sie im Abschnitt über SDLC. Der SDLC-Prozess kann automatisiert werden, indem Ticketing-Systeme wie Jira oder Zendesk integriert werden, um die Entwicklung, Tests, Sicherheitsüberprüfung und Förderung der Produktion von Bots auszulösen. Ein automatisierter SDLC-Prozess liefert ein Runbook für die Erstellung von Bots und sorgt in einem überprüfbaren Prozess, der alle Governance-Kontrollen bereitstellt, die Ihr Unternehmen benötigt, dafür, dass jeder Bot in der Produktion das tut, wofür er entwickelt wurde.

SCHLUSSFOLGERUNG

Robotergesteuerte Prozessautomatisierung ist extrem nützlich für moderne Unternehmen, die die Betriebskosten senken, die Kundenzufriedenheit erhöhen und sich einen Wettbewerbsvorteil verschaffen möchten. Als führende Digital-Workforce-Plattform trägt Automation Anywhere Enterprise dazu bei, diese und andere Vorteile optimal zu nutzen, indem neben Zuverlässigkeit, Skalierbarkeit und Benutzerfreundlichkeit auch die Sicherheit zur Erhaltung der Vertraulichkeit, Integrität und Verfügbarkeit der gesamten Automatisierungsumgebung geboten wird.

Weitere Informationen zu Automation Anywhere Enterprise finden Sie unter: https://www.automationanywhere.com/products/enterprise.