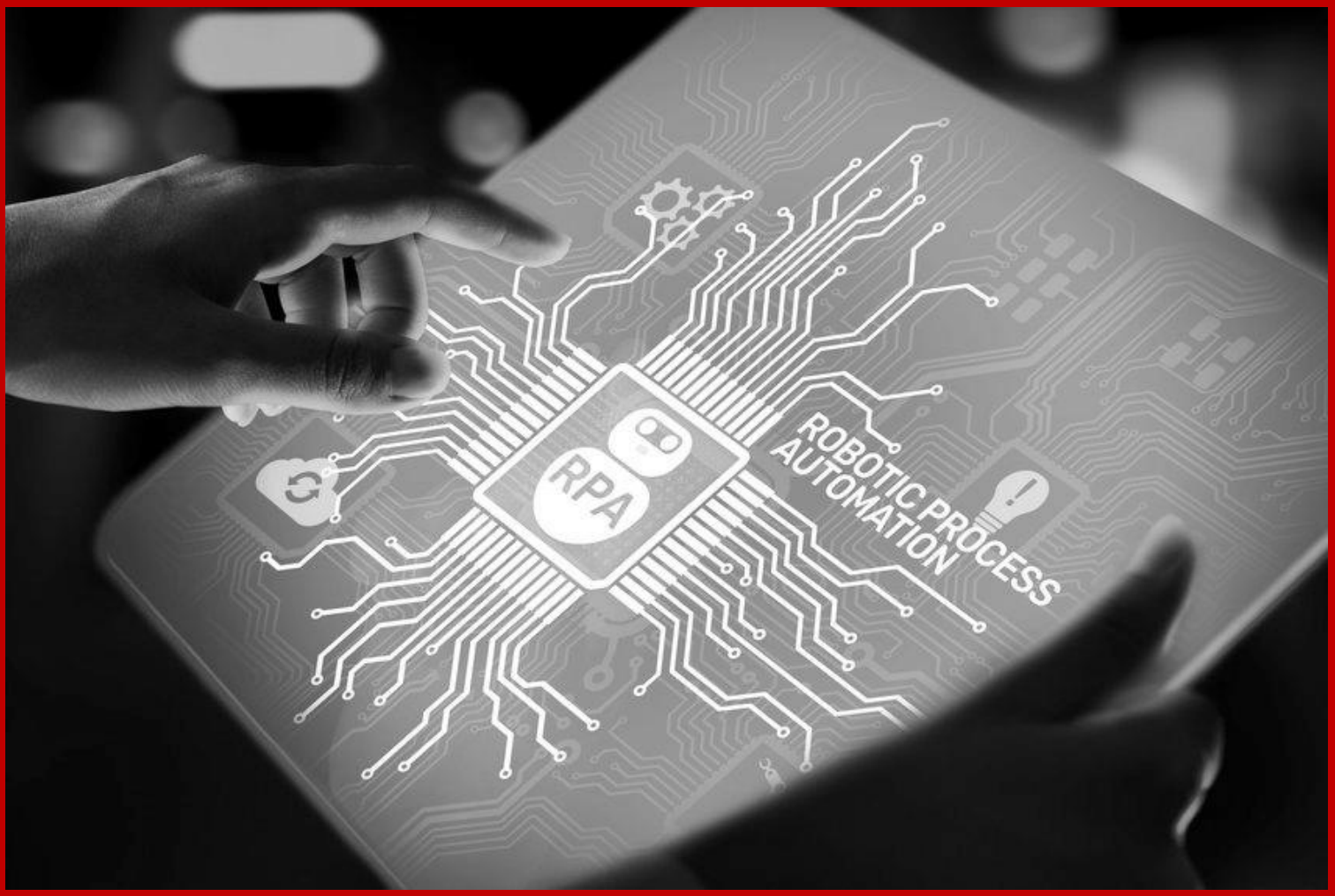
AMDO SOFT
ROBOTIC · PROCESS · AUTOMATION

BEFORE



Whitepaper zur Sicherheit der robotergesteuerten Prozessautomatisierung mit AmdoSoft/b4

EINFÜHRUNG

Warum AmdoSoft/b4 Robotic Process Automation (RPA) ins Unternehmen integrieren?

Die Automatisierung der Geschäftswelt nimmt seit Beginn des 21. Jahrhundert rapide zu. An der Vorfront dieser Welle steht die Robotic Process Automation (RPA). Sie erlaubt Anwendern den Fokus auf höherwertige Aufgaben setzen, indem Software Roboter präzise und kostengünstig alle standardisierten Routineaufgaben übernehmen. Robotic Process Automation ist daher für Wirtschaftsunternehmen eine attraktive Lösung, ihre Produktivität zu erhöhen, ihre Ausgaben zu senken und somit – sicher und nachhaltig – ihre Effizienz zu steigern.

Presseberichte von Marktforschern zeigen heute ein überwiegend großes Interesse an RPA-Lösungen für den deutschsprachigen Raum von mehr als 50% aller Unternehmen. Weltweit benutzen schon mehr als 20% aller Unternehmen einen Automation Service. Die berichteten Effizienzsteigerungen schwanken dabei zwischen 50% und 80% gegenüber Mitbewerbern.

Die Frage, welche Prozesse von Software-Robotern übernommen werden sollen, ist dabei von entscheidender Bedeutung, denn nur, wenn die richtigen Vorgänge automatisiert werden, kann ein optimales Ergebnis erzielt werden. Es hat sich gezeigt, dass der Einsatz von Robotern insbesondere in administrativen Bereichen wie Kundenservice, Buchhaltung, Personalwesen, Gesundheitswesen und Finanzdienstleistungen mit Dokumentenmanagementsystemen und Umsetzung von Compliance durch digitalisierte Prozesse mit reduzierten Ausgaben und erhöhten Bearbeitungsgeschwindigkeiten einhergehen. Im Allgemeinen können aber alle anderen Bereiche, die digitale, strukturierte, regelbasierte und zeitintensive Aufgaben enthalten, genauso von Robotic Process Automation profitieren. Monotone, wiederkehrende Aufgaben können abgegeben werden und es entsteht eine verbesserte Dokumentation, da alle Bearbeitungsschritte jederzeit exakt nachverfolgt und belegt werden können.

Ebenso werden teure menschliche Fehler ausgeschlossen, Prozesse didaktisch strikt vorgegeben und bei allen darauffolgenden Durchführungen eingehalten.

Das Ziel von AmdoSoft/b4 ist es, Geschäftsanwendern die Möglichkeit zu geben, selbständig Software-Roboter zu erstellen, die keine besonderen APIs benötigen, um mit allen Drittanbieter-Applikationen zu interagieren. Die Anpassung der Oberfläche an Laien des Programmierens ermöglicht auch Uninitiierten innerhalb weniger Wochen die Rolle eines Bot-Entwicklers einzunehmen und Automatisierungen für das Unternehmen zu entwerfen.

Das Schulen der b4 Bots geschieht anhand von Aufnahmen der Durchführung eines Arbeitsprozesses, das Feintuning wird über grafische Oberflächen geregelt. Die Automatisierungen selbst sind über Termine und Zeiten, von Nutzern oder als Antwort auf einen Trigger auslösbar.

Hier kann man sich beispielhaft einfach eine automatisierte Antwort auf ein einkommendes Dokument vorstellen, welche ausgewählte Daten entnimmt, diese weiterverarbeitet und an relevante Mitarbeiter gefiltert weiterleitet.

Zwei Beispiele aus dem Alltag waren hier, für AmdoSoft in der Vergangenheit das Einrichten einer Automatisierung zur täglichen Aktualisierung von Energiepreisen im ERP-System für Energieversorgern und Verarbeitung von Corona-Testergebnissen für Gesundheitsämter. Diese Prozesse wurden von Partnern und Mitarbeitern der jeweiligen Institute erzeugt, getestet und in Betrieb genommen. Sie sind heute 24/7 im Einsatz.

Anhand der genannten Beispiele erkennt man schon den Bedarf an sicheren Anwendungen, um das Datengeheimnis zu wahren und Fremden keinen Zugriff auf die Daten zu gewähren. Diese Sicherheit bei der Automatisierung muss einhergehen mit Sicherheit im Umgang, Skalierbarkeit, Zuverlässigkeit und Benutzerfreundlichkeit der Plattform. Nur wenn beide Aspekte erfüllt sind gelingt die Einbindung von RPA auf Unternehmensniveau.

Die Arbeitsschritte der AmdoSoft/b4 RPA-Lösung, deren Trennung durch intelligente Architekturen und minimale Berechtigungen, der plattforminterne End-to-End-Sicherheitsstandard und weitere externe Sicherheitsmöglichkeiten werden in diesem Dokument verständlich geschildert.

ARCHITEKTUR UND BETRIEB

AmdoSoft/**b4** Komponenten

Um eine robotergesteuerte Automatisierung sicher und effizient auf Unternehmensniveau zu realisieren, braucht es eine starke und verlässliche Software. Das Verständnis der Komponenten ist dabei unerlässlich. In Abstimmung mit den aktuell praktizierten Sicherheitsstandards wird innerhalb der AmdoSoft/b4 Plattform die Verwaltungsebene b4 Controller von der exekutiven Ebene b4 Agents und b4 Bots getrennt. Der Zusammenhang der individuellen Komponenten ist in Abbildung 2 dargestellt. Der b4 Controller ist eine Windows-serverbasierte Software. Während b4 Bots auf allen gängigen Windows-Server und Windows-Workstation Betriebssystemen arbeiten, können b4 Agenten sowohl auf Windows als auch Linux Betriebssystemen aufgestellt werden.

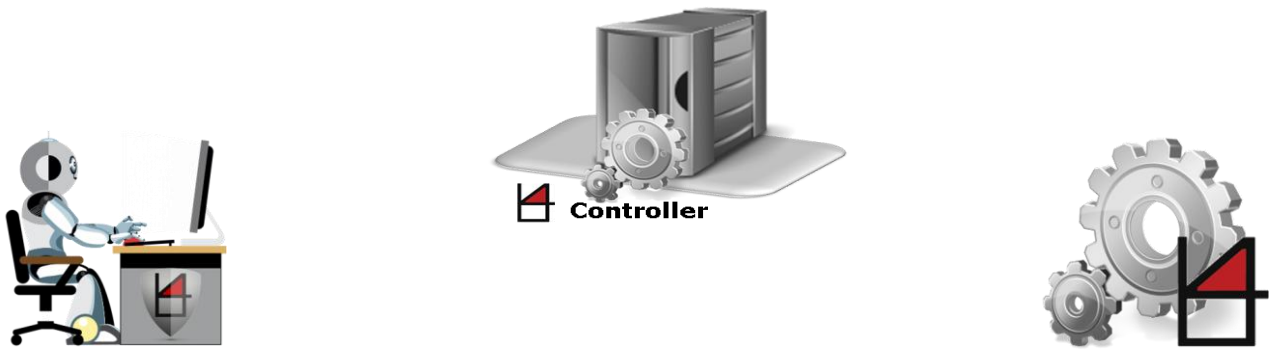


Abbildung 1: AmdoSoft/b4 Komponenten

b4 Controller

Der b4 Controller ist die Hauptverwaltungszentrale der Automatisierungsumgebung. Alle IT sowie unternehmens-relevante Prozesse können von hier aus angesteuert und mithilfe der integrierten Applikationen b4 Dashboard (Web-App) und b4 Console (Desktop-App) in Echtzeit überwacht werden.

Diese Engine ist mit einer verschlüsselten Datenbank ausgestattet und kann mit allen b4 Agenten verbunden werden, um die zentralisierte Kontrolle auf das gesamte System auszuweiten. Dabei werden systemübergreifend nur über unsere EBS Client API von Agenten ausgehend Verbindungsaufbaus initiiert und Informationen in Form von SSL-verschlüsselten Daten ausgetauscht. Dadurch bleiben kritische Daten vertraulich behandelt. Das gleichzeitige Arbeiten mehrerer Nutzer auf dieser Verwaltungsebene ist durch selbstständige Versionskontrollen und Autorisierung umgesetzt und ermöglicht so einen zentralisierten Hub, auf dem Strukturen, Leistungen und Wartungsarbeiten unternehmensweit koordiniert, aufgabenrelevant getrennt und durchgeführt werden.

b4 Agents

b4 Agenten sind auf den gewünschten Untersystemen installiert und erweitern so die Funktionalitäten des b4 Controllers auf das gesamte System. Dazu schickt der User Befehle vom b4 Controller an die b4 Agenten, welche lokal verarbeitet und detailliert beantwortet werden. Zudem gewährleisten die Agenten die Systemsicherheit, stellen eine breite Auswahl an Monitoring Möglichkeiten sowie die IT-Automatisierung über APIs bereit.

Das Monitoring wird durch Sammeln von benutzerdefinierten Systeminformationen ausgeführt. Die Agenten erstellen von selbst live Alarme und Berichte und senden diese verschlüsselt zurück an den Controller.

Getrennt vom Controller bearbeiten b4 Agenten alle Vorgänge und Ereignisse der softwaregesteuerten b4 Bots lokal als zwischengeschaltete Instanz. Dadurch wird die Sicherheit der Untersysteme gewährleistet und bietet einen zusätzlichen Schutz vor Datenlecks durch den Einsatz externer Firewalls.

Die Unterschiede zwischen Agenten und Bots sind in den bearbeitenden Aufgaben und Scopes zu erkennen. Agenten entsprechen in ihren Aufgabenbewältigungen IT-Administratoren. Sie sind in der Lage lokal native Scripts, in zum Beispiel Bash oder Powershell, auszuführen. Dazu gibt es innerhalb der Automation Manager Perspektive der Console eine vorgefertigte Script-Bibiliothek und die Möglichkeit eigene Scripts zu schreiben. Die Scripts können anschließend parallel als Advanced Executive Service (AES) auf die Agenten und dadurch auf das gesamte Netzwerksystem übertragen werden. Mit der eigens dafür entwickelten internen Schnittstelle ist das Entwickeln und Verteilen von Scripts somit ein b4 interner Prozess und die damit verbundene Sicherheit in der IT-Automation ein klarer Marktvorteil von AmdoSoft Systems.

b4 Bots

Die softwaregesteuerten b4 Bots sind die unterste, exekutive Ebene der RPA-Lösung. Sie emulieren alle möglichen Eingaben und Prozesse, die eine Person in beliebigen Umgebungen (Apps, Web-Apps) auf den Systemen durchführen würde, direkt auf dem Desktop. Dazu zählen sich häufig wiederholende Prozesse wie das Bearbeiten von E-Mails, Arbeiten in Web oder ERP Umgebungen und Filtern/Zusammenstellen von Informationen.

Diese Vorgänge können ganz einfach über Aufnahmen der jeweiligen Prozesse, während ihrer Durchführung durch einen Nutzer, aufgezeichnet werden. Der Aufnahmeprozess wird per Knopfdruck in der b4 Console gestartet und läuft im Hintergrund (sichtbar nur durch eine Markierung auf dem Desktop). Über Shortcuts können Screenshots für Bildrekonstruktions-Algorithmen innerhalb der Aufnahmen gespeichert werden, die dann direkt als Referenzen für Teilschritte der Automatisierung dienen. Alle Eingaben vom erstellenden Nutzer werden erkannt, in Aktionen gelistet, archiviert und innerhalb der b4 Automation Manager Perspektive als sogenannte "Recordings" bereitgestellt. Nach dem Testen und Feintuning stehen diese dann als ausführbare, automatisierte und skalierbare Prozesse zur Verfügung, die der Bot dann funktions- und auch systemübergreifend umsetzen kann. Hierbei können, je nach Aufgabenstellung des Nutzers, zusätzliche Anforderungen an Leistung, Datenintegrität und Sicherheit gewährleistet werden. So zum Beispiel können Tastatureingaben zusätzlich zur Datenbank-Verschlüsselung als extra verschlüsselte Variablen getarnt werden. Die Bots dienen sowohl im personengesteuerten Assistentenmodus als auch im unabhängigen Arbeitermodus.

Im Gegensatz zu Agenten entsprechen Bots in ihrem Einsatz eher Sachbearbeitern. Bots führen die fertigen, abgestimmten Prozesse, auch Checkpoints (CP) genannt, als Arbeitsschritte innerhalb der Anwendungen der zugewiesenen Systemumgebung aus. Sie haben dieselben Rechte wie ein lokaler Nutzer. Die Agenten sind als Administratoren zu verstehen. Diese führen ausschließlich die entwickelten Scripts und interne Kommunikation mit der Verwaltungsebene aus. Ein klarer Vorteil der Eingliederung der Objekte, Scripts und Checkpoints in denselben Rule-Workflow der Graphical Rule Editor Perspektive ist, dass systemadministrative Arbeitsschritte (AES) in logische Verknüpfungen mit aufgaben-fokussierten Arbeitsschritten (CP) eingepflegt werden können. Ein Beispiel für diese Hybridisierung wäre ein vollautomatisiertes Systemupdate mit anschließender Neuinstallation oder Aktualisierung einer Nutzeranwendung ganz ohne wiederholten Personalaufwand.

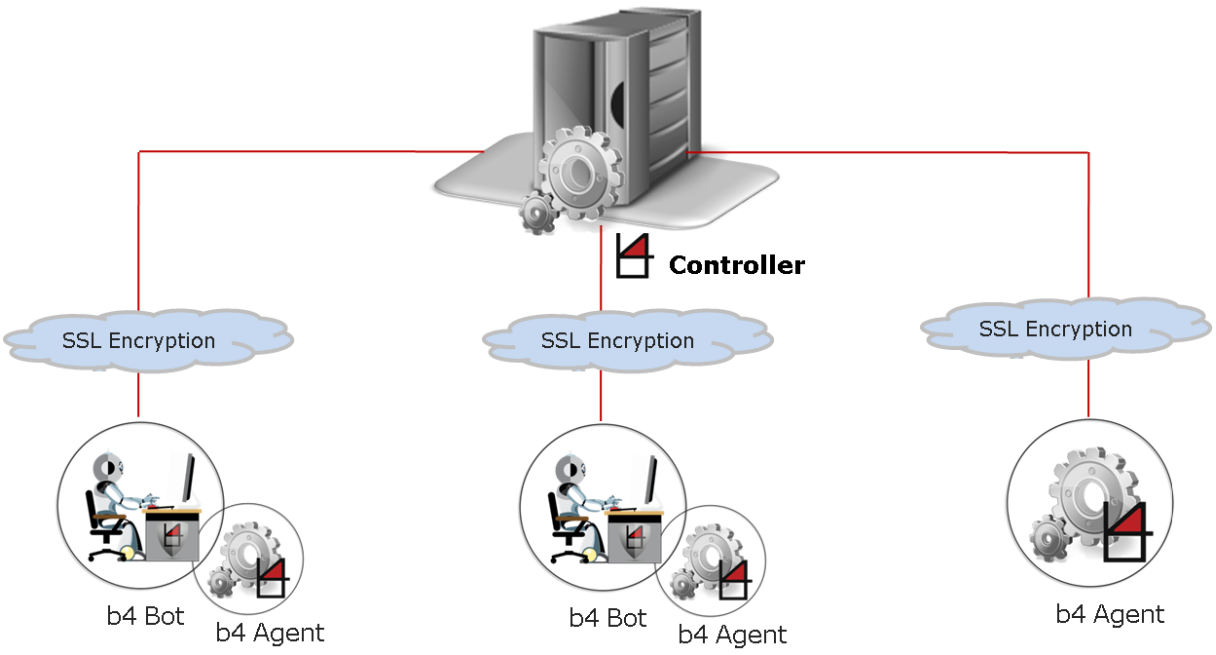
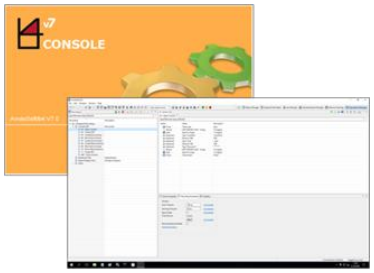


Abbildung 2: Architektur der RPA Lösung durch AmdoSoft/b4

AmdoSoft/b4 User Interfaces

Die oben genannten Komponenten sind für den Nutzer größtenteils unsichtbar und arbeiten zuverlässig und unnachgiebig im Hintergrund der GUI Anwendungen. Die drei User Interfaces sind:



b4 Console

b4 Dashboard

b4 Report Designer

Abbildung 3: AmdoSoft/b4 User Interfaces

b4 Console

Die Hauptkomponente von AmdoSoft/b4 ist eine Applikation mit mehreren Perspektiven, welche die komplette Systemadministration, Systemüberwachung und RPA Lösungen abdecken. Dem Nutzer werden auf Grundlage von detailreichen Ereignisprotokollen durch anpassbare Live-Statusmeldungen, Zeitreihenanalysen und kunden-spezifischen Berichten alle Informationen zu Bot- und Systemvorgängen präsentiert.

Ein klarer Vorteil der AmdoSoft/b4 Software ist hier ihr Ursprung aus dem Bereich IT-Automation. So sind für Systemadministratoren bekannte Aufgabenbereiche und deren Bearbeitung in einem simplen Workflow bereitgestellt. Es werden IT-Automationen von der Object Manager Perspektive aus über Skripte und APIs über ein paar Mausklicks skalierbar auf massive Systeme realisiert und Wartungsarbeiten auf Teile des Systems können geplant, konfiguriert, mitgeteilt und durchgeführt werden.

b4 Dashboard

Das b4 Dashboard ist die Web-Applikation des AmdoSoft/b4 Tools. In Form von Dashlets, kleinen Widget-ähnlichen Fenstern, stehen eine Vielzahl von Funktionalitäten zur Verfügung. Durch einen gesicherten Log-in erhalten Sie Zugriff auf einstellbare Dashlets, welche benutzerdefinierte Systemressourcen und prozessspezifische Botvorgänge detailliert auf gewünschte Arten anzeigen. Somit können wichtige Informationen auf Anfrage auch gesichert, standortunabhängig eingesehen und rapide auf unvorhergesehene Ereignisse, wie Systemausfälle oder unerwünschte Zugriffe auf Applikationen oder Maschinen, entgegengewirkt werden.

b4 Report Designer

In der b4 Report Designer Engine (RDE), eine vom b4 Dashboard und der b4 Console getrennte Anwendung, werden Berichte für das Unternehmen oder Kunden gestaltet. Es besteht die Möglichkeit User-Profile für die RDE anzulegen, ohne dass der Nutzer Zugriff auf die b4 Console haben muss.

Objekte und Statusmeldungen lassen sich im RDE durch Platzhalter in Berichte einpflegen, ohne deren Informationen an die bearbeitenden Nutzer preiszugeben. Nur die Objektnamen sind in dieser Perspektive sichtbar, nicht aber die Meldungen/Informationen selbst. Durch Drag-and-drop können Berichtformate erstellt werden, die Zeiträume der zu füllenden Informationen eingestellt und abschließend von der b4 Console aus genehmigt und mit gesammelten Informationen ausgefüllt werden. Durch diese Eingliederung wird gewährleistet, dass mindestens ein Entwickler/Administrator (b4 Console) und ein Geschäftsanwender (RDE) bei der Generierung eines vollständigen Berichts involviert sind. Eine Strukturierung, die Datensicherheit und Best Practice reflektiert.

Logos, Bilder, Grafiken und Formatierung lassen sich einfach einbinden, dimensionieren und über eine Gitterstruktur anpassen. Die Eingliederung der Objekte geschieht dann ganz automatisch beim Zeitpunkt der geplanten Auslieferung. Über die Schedule Report Manager Perspektive der b4 Console sind dann automatisierte Berichte, deren Termine, Datum und Versandart (z.B. E-Mail) konfigurierbar.

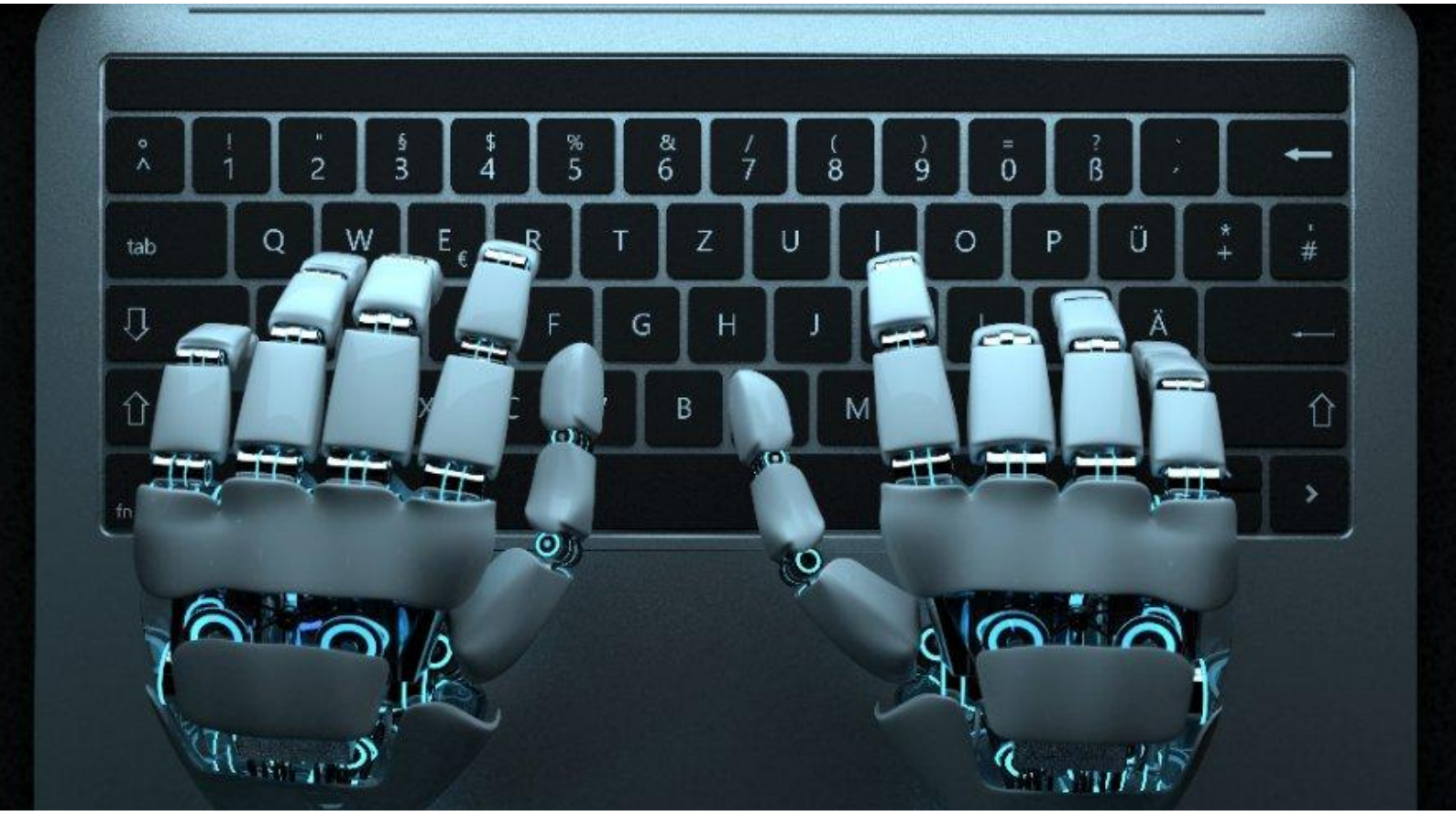
RPA EINSATZ, AUTORISIERUNG UND VERARBEITUNGSDOMÄNEN

Einsatz-Mode

Für das Verständnis der Sicherheit beim Einsatz von Softwarerobotern in der Automatisierung genügt es nicht nur die Werkzeuge zu kennen. Die Arbeitsweise sollte natürlich auch transparent sein. Robotic Process Automation Software erledigt effizient und kostengünstig alle standardisierten Routineaufgaben. Dabei wird im Allgemeinen beim Einsatz von Softwarerobotern zwischen zwei Formen unterschieden: Dem assistierten und eigenständigen Arbeiten.

Bei der assistierten Automatisierung überwacht der Nutzer Teilschritte des Prozesses. So kann der Roboter unterstützende Aufgaben durchführen und auf eine abschließende Bewertung oder Bestätigung des Nutzers warten. Gründe für den Einsatz sind unter anderem Prozesse, in denen Zwischenschritte interpretiert werden müssen und/oder Ergebnisse, die Anweisungen eines Nutzers benötigen. Die Zusammenarbeit kann sich auch auf Prozesse beziehen, in denen der Roboter eine rein unterstützende Aufgabe erledigt.

Unbeaufsichtigte Automatisierungen umfassen alle vollautomatischen Prozesse und benötigen keine Eingaben vom Nutzer. Dabei wird nicht unterschieden, ob ein Nutzer den Prozess startet oder dieser über einen Scheduler geplant und durch einen Timer gestartet wird. Diese Art der Automatisierung ist sehr praktisch, da dieser Nutzer kein Verständnis vom eigentlichen Prozess oder der Automatisierung eines Roboters haben muss. Ein Bot-Entwickler kann so für eine immense Mehrzahl an Geschäftsnutzern durch minimalen Input (Ziele, verwendete Applikationen, Formate) komplette und meist repetitive Aufgaben verkürzen oder gar ganz abnehmen. Ein klares Zeitersparnis fürs Unternehmen. Während der Bot-Exekution kann der Nutzer dann in Echtzeit die Arbeiten des Bots verfolgen und sicherstellen, dass keine Ausnahmen oder Fehler erfolgen. Die Prozesse lassen sich ganz einfach in b4 Console und b4 Dashboard durch live Statusmeldungen und Berichte überschauen. Dazu muss der Nutzer nicht extra auf der arbeitenden Maschine eingeloggt sein.



Mehrstufige Authentifizierung von AmdoSoft/b4 RPA

Ein wesentlicher Bestandteil des Sicherheitskonzepts von AmdoSoft/b4 ist die Authentifizierung jeder Entität vor Zugriffen oder Aktionen. Kann die Entität nicht authentifiziert werden oder besitzt diese nicht die nötigen Berechtigungen vom Administrator, dann wird der Zugriff verweigert, Objekte unzugänglich gemacht und Aktionen geblockt. Alle damit verbundenen Daten sind somit gesperrt und abgeschirmt. Es wird bei dieser Behandlung nicht zwischen Roboter und Menschen unterschieden. Im folgenden Abschnitt bieten wir für einen anschaulichen Vergleich der Authentifizierung in Standardprozessen zwischen Nutzer und Roboter an.

Vergleich: Nutzer vs. Roboter – Authentifizierung

Erstes Szenario ist eine typische Unternehmens-authentifizierung für einen Nutzer. Zu Arbeitsbeginn meldet sich dieser auf eine Windows-Session an. Diese erste Authentifizierungsebene ist durch den Windows-Log-in gewährleistet. Um einen Geschäftsprozess zu starten, wird eine Remote-Applikation gestartet, welche mögliche kritische Unternehmens-/Kundendaten handhabt. Dazu benötigt der Nutzer noch eine zweite Authentifizierung.

Das Szenario umfasst also einen einzelnen Nutzer und seine Log-ins.

Beim zweiten Szenario wird eine unbeaufsichtigte Automatisierung verwendet. In diesem Fall wurde ein b4 Bot von einem Bot-Entwickler in dem Prozess trainiert und die Zugriffsrechte zur Durchführung an den Nutzer übergeben (an sich ist das Erstellen eines Bots und dessen Zugriffssteuerung mit einer weiteren Authentifizierung durch den Bot-Entwickler gebunden). Der Nutzer meldet sich wie im Vorherigen auf seine Windows Station mit seinen Windows Kenndaten an. Nach der ersten Authentifizierung benutzt er seine b4 Console-ID und Passwort, welche in dieser zweiten Authentifizierung gegen die verschlüsselte Datenbank-Instanz abgeglichen werden. Der Nutzer manövriert in die Object Manager Perspektive, die im Einklang mit Best Practices nur die für ihn relevanten Objekte beinhaltet. Er startet den Bot, der nun alle manuellen Aufgaben übernimmt. Dazu stellt die b4 Console eine verschlüsselte Verbindung zum b4 Controller her, die über ein TLS Handshake-Protokoll genehmigt werden muss. Findet diese gesicherte Verbindung statt, wird an den Remote-Bot-Client auf dem gezielten System mit der erwünschten Remote-Applikation ein Befehl für die Exekution der Automatisierung geschickt. Der Prozess wird vom Bot-Client gestartet. Dieser muss sich zusätzlich noch auf der Remote-Maschine einloggen. Dies stellt die dritte Authentifizierungsebene dar, welche sich für die Bots auch ganz unabhängig von bisherigen Nutzer-Log-ins einstellen lässt. Ab jetzt werden Statusinformationen des Vorgangs für den Nutzer innerhalb der b4 Console sichtlich gemacht.

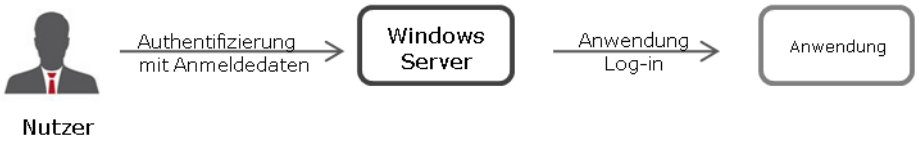


Abbildung 4: Unternehmensauthentifizierung für einen Nutzer

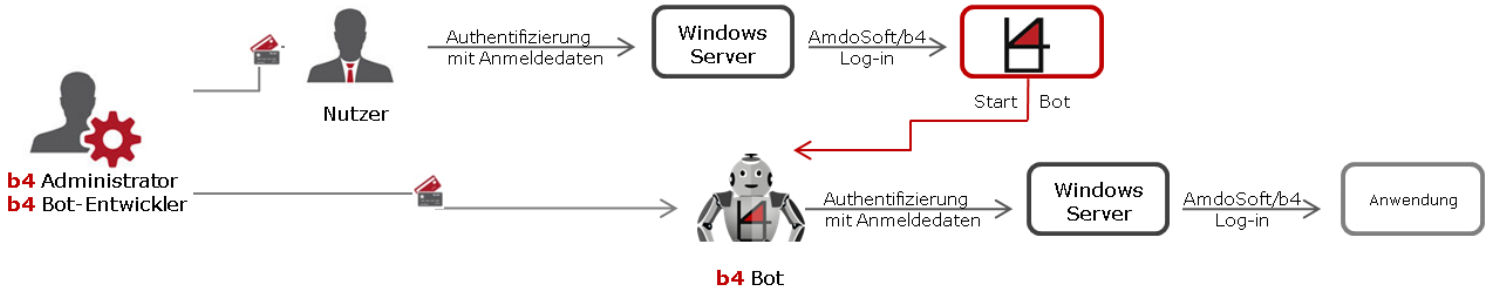


Abbildung 5: Unbeaufsichtigte Automatisierung

Durch Einbindung eines „Timer-Objekts" in den Workflow, kann der Prozessablauf automatisch zu bestimmten Zeiten durchgeführt werden. Mit definiertem „Trigger-Objekt" wird auf bestimmte Veränderungen oder Ereignisse auf dem Untersystem oder Anwendungen reagiert und der Vorgang gestartet. Dazu müssen bei der Objekterstellung allerdings wieder alle drei Authentifizierungen durchlaufen werden.

Das Fazit ist, dass in puncto Authentifizierungen durch die Verwendung von b4 Bots keine Sicherheitsblockade wegfällt, die den Anwender genauso betrifft. Zusätzlich entsteht eine weitere Ebene durch die Verwendung der AmdoSoft/b4 Plattform.

Rollenbasierte Autorisierung

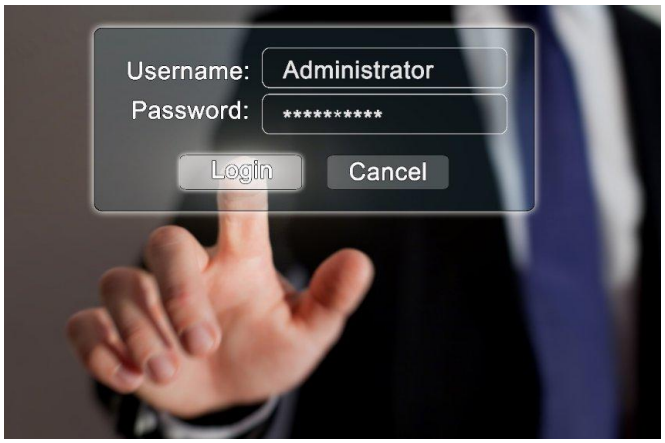
Für die Durchsetzung der Zugriffskontrolle ist eine erfolgreiche Authentifizierung nur die erste Stufe in der Sicherheitsstruktur von AmdoSoft/b4. Um die Grundprinzipien der Aufgabentrennung und minimalen Berechtigungen einzuhalten, ist die Autorisierung ebenso wichtig. Die Autorisierung in AmdoSoft/b4 ist mit einer konfigurierbaren, rollenbasierten Zugriffssteuerung (RBAC - Role Based Access Control) umgesetzt. So können Administratoren als übergestellte Instanz anderen Nutzern Zugriffsrechte auf spezifische Teile der Plattform erteilen. Dies kann entweder individuell für einzelne Nutzer erfolgen oder durch die Einteilung von mehreren Nutzern in Gruppen mit definierbaren Rechten.

Es gibt drei voreingestellte Gruppen in der Grundarchitektur der b4 Plattform:

- SuperUser
- ObjectManager
- ReportsOnly

Teilnehmer der Gruppe SuperUser haben uneingeschränkten Zugang zu den vielfältigen Funktionen innerhalb der Benutzeroberflächen und sind Administratoren gleichgestellt. Gruppenmitglieder im ObjectManager haben Rechte Objekte innerhalb der b4 Console wie Roboter, aufgenommene Prozesse, Arbeitsschritte, Monitore oder Timer (um hier nur einige zu nennen) einzusehen und zu bearbeiten. Diese Gruppe eignet sich hervorragend für Mitarbeiter, die mit dem Erstellen der Automatisierung eines b4 Bots beauftragt sind.

Selbsterstellte Gruppen können die Einteilung dieser Gruppen erweitern und detaillierter vorgehen. So können Zugriffe auf einzelne Perspektiven innerhalb der b4 Console eingestellt werden, um Aufgabenbereiche auch weiter durch Zugriffsrechte zu sichern. Eine Erweiterung stellt die Abstimmung für Zugriffe auf Objekte und Untersysteme mit spezifischen Gruppen dar. Die makroskopische Unterteilung der Belegschaft auf die drei Benutzeroberflächen und zugehörige Berechtigungen sind so frei anzupassen.



Unabhängige Kontrollumgebungen

Neben den umfangreichen RBAC-Funktionen bietet AmdoSoft/b4 eine logische Aufgabentrennung. Die Architektur der Plattform ist dafür extra in mehrere Perspektiven unterteilt, um Arbeitsschritte in der Erstellung der Automatisierung (und Berichterstellung) klar voneinander zu trennen.

Die Automation Manager Perspektive auf der b4 Console ermöglicht Recordings von Geschäftsarbeitsschritten aufzunehmen. Diese sind eine Simulation der Arbeitsschritte eines Nutzers und werden während der Ausführung eines Prozesses aufgenommen. Dabei werden alle Aktionen des Nutzers (Mausklicks, Tastatureingaben ...) in einer detaillierten Liste zusammengestellt und können nach dem Beenden einer Aufnahme direkt bearbeitet werden. Das Abspielen der Aufnahmen ist sofort auf Abruf ausführbar und kann in einer Testumgebung verifiziert werden. Sobald Sicherheitsprüfungen in der Funktionsweise erfolgreich abgeschlossen sind und sicher ist, dass der Prozess allen Ansprüchen gerecht wird, lassen sich die Recordings auf einen b4 Bot übertragen und stehen somit für das ganze System in Form eines finalisierten Checkpoints zur Ausführung bereit. Ob der Prozess spezifisch nur für eine Maschine festgelegt wird oder unabhängig auf mehreren Maschinen ablaufen soll, spielt dabei keine Rolle. Anschließend lassen sich innerhalb des Graphical Rule Editors logische Zusammenhänge und Abfolgen der Arbeitsschritte eines Geschäftsvorgangs anhand von Diagrammen und als Icons dargestellte Objekte auch ganz ohne Programmierkenntnisse zu vollkommenen Prozessen zusammensetzen. Funktionalitäten wie Checks der Arbeitsvorgänge und Benachrichtigungen per E-Mail können hier leicht per Drag-and-drop eingebunden werden. Die Darstellung in diesen Flowchart-typischen Diagrammen, auch "Rules" genannt, in Kombination mit den live Statusnachrichten und erstellten Berichten ermöglicht die Übersicht über tausende, parallele Prozesse und relevante Anpassungen an veränderliche Marktsituationen.

Von der Object Manager Perspektive aus werden alle erstellten Objekte zentral gesteuert. Hier werden auch Prozesse gestartet, Systemressourcen und Bots überwacht, oder Netzwerkstrukturen verwaltet. Anhand personalisierbarer Statusnachrichten und Beschreibungen sind die Ergebnisse schnell einsehbar.

Diese Abgrenzung von Entwicklungsumgebungen und Produktionssystemen dient der zusätzlichen Sicherheit. Die bereits erarbeiteten Lösungen bleiben so unbeeinträchtigt von neuen Ansätzen. Die Automatisierung wird von zwei Ebenen kontrolliert, dem Entwicklerteam und den Geschäftsanwendern.

Unabhängige Objektgenehmigungen

Die Unterteilung der Umgebungen ist eine makroskopische Hilfestellung, um das sichere Arbeiten im Bereich RPA und System-Monitoring zu gewährleisten. Dabei sind die unterschiedlichen Objekte einer Art, zum Beispiel Recordings oder Rules, in Grundzustand gleichgestellt. Über objektspezifische Genehmigungen ergeben sich zusätzliche mikroskopische Möglichkeiten. Im Zusammenspiel mit der Zuweisung von Nutzern in Gruppen, können Objekte und deren Funktionen auf Mitarbeiter maßgeschneidert werden.

Gehen wir dazu kurz eine Situation für eine Verarbeitungsdomäne durch. Die Entwickler erstellen für den b4 Bot einen Checkpoint, in dem automatisch zu Beginn des Arbeitstages Informationen aus eingegangenen E-Mails gefiltert und dann in einer separaten Mail gesammelt werden. Diese soll anschließend als Rundmail an einen Teilbereich des Vertriebs geschickt werden. Es stehen jetzt die Optionen frei, ob man den Start des Prozesses durch einen Geschäftsanwender ausführen lassen will oder ob der Prozess vollautomatisch geschehen soll. Im zweiten Fall wird keine Autorisierung seitens des Personals benötigt und der Teilbereich sieht nur das Ergebnis in Form einer E-Mail. Im ersten Fall besteht zusätzlich die Möglichkeit Rules und Checkpoints, die diesem Vorgang zugeordnet sind, von allen anderen Prozessen abzugrenzen. Dazu genehmigt man in den Objekteinstellungen nur Mitgliedern einer bestimmten Gruppe die Exekution und die Sichtbarkeit, nicht aber das Abändern oder Löschen. Der Prozess wird so zusätzlich vor menschlichen Fehlern abgesichert.

Das Ergebnis ist eine weitere Isolation der zugehörigen Daten und Apps auf Ebene der Organisation, da einzelne Nutzer keine Objekte außerhalb ihrer jeweiligen Domäne sehen oder steuern können.

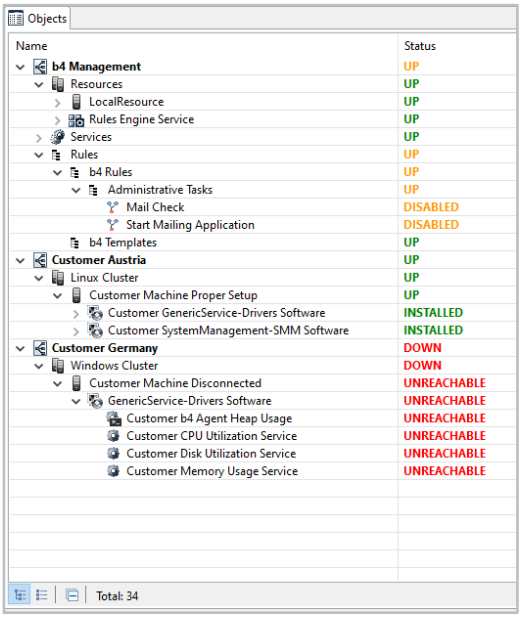


Abbildung 6: Objektansicht Entwickler

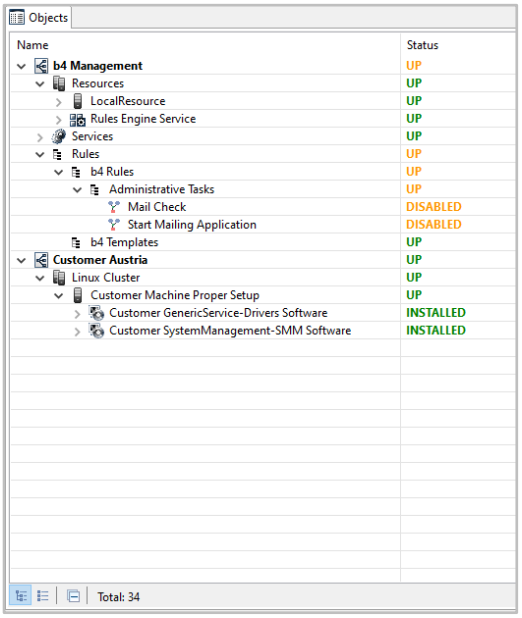


Abbildung 7: Objektansicht Nutzer

END-TO-END DATENSCHUTZ

Die Authentifizierung in mehreren Instanzen in Kombination mit der hochpräzisen Zugriffssteuerung sind für eine kontrollierte Arbeitsdomäne unentbehrlich. Um Datenschutz auf allen Ebenen zu gewährleisten, müssen geschäftsspezifische Daten, Prozesse und die damit verbundenen Informationen auch während der Funktionen der bereitgestellten Software geschützt werden.

Die AmdoSoft/b4 Plattform verteidigt Anwenderdaten durch mehrere Sicherheitsvorkehrungen. Dabei stellt die verschlüsselte Datenbank nur den ersten Schritt in der Abdeckung dar. Zusätzliche Schritte, um ruhende, auf einem System verwendete oder zwischen Systemen ausgetauschte Daten abzuschirmen, werden in den folgenden Abschnitten zusammengefasst dargelegt.

Verschlüsselte Datenbanken und Sicherheit ruhender Daten

Die b4 Controller, b4 Agent und b4 Bot Objekt-Datenbanken (SQL DB) sind durch einen standardisierten Cypher-Algorithmus verschlüsselt. Es werden alle Informationen und Daten, unter anderem auch die für IT-Automation und RPA gebrauchten Daten, gesichert. Für empfindliche System- oder Nutzerdaten (z.B. hinterlegte Passwörter) sind weitere Key-Generator Algorithmen im Einsatz. Als Teil der AmdoSoft-Qualitätskontrollen werden Schnittstellen zu diesen Datenbanken täglich während des Entwicklungsprozesses gescannt und mögliche Schwachstellen beseitigt, bevor diese jemals in produktiven Umgebungen zum Einsatz kommen.

Zu den auf der Controller-Datenbank gesicherten Informationen gehören die hinterlegten Anmeldedaten der Nutzer und ihre Zugriffsrechte, alle für die Bot-Runtime benötigten Daten, d.h. alle Anmeldedaten für Drittanbieter-Applikationen oder systemkritische Log-ins für (virtuelle) Maschinen. Die Runtime Parameter umfassen auch Konfiguration sowie bereitgestellte Versionskontrolle und Mailing Dienste. Die Sicherung ist dementsprechend höchstes Gebot. Dafür laufen während des Entwicklungsprozesses weitere tägliche Datenbank-Scans, um herauszufinden, ob für den Benutzer kritische Daten extrahiert werden können. Ist das möglich, so wird die neue Implementation verworfen und diese Sicherheitslücke mit höchster Priorität behoben.

Die b4 Agent/b4 Bot-Datenbanken beinhalten nur die nötigsten Daten für die Exekution von Remote-Prozessen. Diese sind für alle anderen Informationen absichtlich "taubstumm" designt und haben keine Rechte, diese anzufordern. Eine erstellbare dritte Verschlüsselung von Prozess-Input-Parametern als encrypted variables innerhalb der Automation Manager Perspektive verleiht eine weitere Schutzschicht.

Sicherheit bei der Übertragung

Der Austausch zwischen Controller und Clients (Bots/Agenten) wird durch die TCP/IP-Protokolle und das Verschlüsselungsprotokoll Transport Layer Security (TLS) 1.2 geschützt. Das TLS Handshake-Protokoll sorgt dafür, dass die Identität der beiden Instanzen überprüft und erst nach der Generierung und dem Austausch der passenden Keys eine Verbindung aufgebaut wird. Der Verbindungaufbau findet immer nur von der Client-Seite aus statt und ermöglicht einen additiven Schutz durch eine Firewall. Durch diese einseitige Verbindungsaufbau-Strukturierung ist es möglich den Kontakt auf einen einzigen, vom Admin selbst festgelegten, und konfigurierbaren TCP-Port zu setzen, über den der Informationsaustausch limitiert und gesichert abläuft. Hier zahlt sich unser in über 20 Jahren IT-Automation gewonnenes Wissen aus, da unsere eigens entwickelte EBS-Client API durch eine hervoragende und täglich getestete Cibersuite gesichert ist. Durch die Verschlüsselung der übermittelten Daten wird auch eine aufwendige Einrichtung von VPNs für jeden Client optional. In kleinen bis mittelgroßen Projekten ist dieser Aufwand noch vernachlässigbar. Beim Aufsetzten von hunderten oder tausenden TCP-Ports für Agenten/Bots verschlingt dieser Vorgang dann doch Resourcen, die an anderer Stelle besser investiert wären.

Sicherheit bei der Verarbeitung

Für die Verwendung während der Automatisierung durch Bots muss der Schutz auch auf die Runtime ausgeweitet werden. Dafür wird nur das Minimum an Daten, welches für den Prozess benötigten wird, verarbeitet. Durch b4 Console-Funktionen werden weitere Schutzmechanismen während der Runtime bereitgestellt. Der unbefugte Zugriff in Form von Datenlecks oder durch Eingriff auf Bots kann durch folgende akkurate Aktionen unterbunden werden.

Über die zentrale Steuerung ist es möglich alle Log-ins, Aktionen und Prozesse auf der b4 Controller- oder ferngesteuerten b4 Botseite zu überwachen, und falls nötig zu pausieren, stoppen, zurückzusetzen und mit anderen Einstellungen neu zu starten. Dazu zählen auch alle der Automatisierung zugehörigen Funktionalitäten bis hin zu Agenten und Bots.

b4 Bot Runtimes lassen sich auf definierte Zeiträume festlegen. Im Detail können Termine und Laufzeiten einzelner Arbeitsschritte, Teilprozesse und auch die Dauer des gesamten Prozesses unabhängig voneinander eingestellt werden. Die Automatisierung wird beendet, falls die eingestellte Zeit überschritten wird. Dadurch ist der Eingriff durch Dritte über zeitliche Faktoren limitiert.

Überprüfung der Schnittstellen

Um Schnittstellen der Server-Client Verbindung zu sichern, baut AmdoSoft neben eigener Qualitätskontrollen auf eine zusätzliche, externe Absicherung durch das Vulnerability Management Scanning von Qualys, Inc. Dabei wird diese aus derselben Perspektive wie potenzielle Angreifer betrachtet. Ein Vor-Scan tastet alle gängigen TCP-Ports ab und versucht Informationen über die dort stattfindenden Prozesse und das Betriebssystem zu sammeln. Die einzigartige schlussbasierte Scan Engine überprüft danach, ob es Schwachstellen auf dem Betriebssystem, Diensten und Applikationen der gefundenen Hosts gibt. Die stets aktualisierte Gefahrenliste ermöglicht spontan auf neu auftretende Gefahren zu reagieren und diese schnell abzusichern und so notfalls auf ältere Versionen der Software zu hotfixen.

EXTERNE RPA SICHERUNG

Die AmdoSoft/b4 Architektur umfasst Windows-Desktop-, Web- sowie Serverklassen-Strukturen für den zentralen Controller, die Remote-Clients und User Interfaces. Um die Plattform fließend in eine Geschäftsumgebung einzubetten, sind auch externe Sicherheitsmaßnahmen empfehlenswert.

Schutz vor Viren durch Anti-Malware

Sowohl Server als auch Client Instanzen wie die remote b4 Console und b4 Bots werden auf der Unternehmens-Desktop-Infrastruktur ausgeführt. Um diese vor Angriffe durch Viren und Malware zu schützen, empfiehlt sich der Einsatz von vertrauenswürdigem Antivirus/Anti-Malware-Programmen. Dazu müssen nur die Einstellungen für die b4 Plattform-Dienste angepasst werden.

Schutz durch Firewalls

Der Einsatz von lokalen, server- und netzwerkbasierten Firewalls wird durch die getrennte Architektur unterstützt.

Standardmäßig sind die Einstellungen so zu treffen, dass nur die Controller-/Agent-Protokolle unternehmensweit zugelassen werden. Die netzwerkbasierten Firewalls sollten eingesetzt werden, um die verschiedenen Entwicklungs-, Test- und Produktionsumgebungen der RPA voneinander und dem restlichen Unternehmensnetzwerk zu trennen. Dabei sollten langfristige unbeaufsichtigte Automatisierungen mit zusätzlicher Sorgfalt in stärker isolierten Umgebungen betrieben werden. Im Zuge der minimalen Berechtigungen versteht sich von selbst, dass nur die für den Prozess benötigten Ressourcen bereitgestellt werden.

Schutz durch IPS

Um direkte externe Angriffe auf die b4 Plattform zu verhindern, bietet es sich an, hinter der Firewall ein zusätzliches externes IPS (Intrusion-Prevention-System) zu installieren. Das IPS agiert im Netzwerkverkehrsfluss zwischen Server und Client, reagiert auf Bedrohungen anhand von vorab erkannten, anomalie-basierten oder festgelegten Signaturen und unternimmt automatische Schritte, um die empfangenen Pakete abzulehnen und den Datenverkehr von der Quelladresse zu stoppen.

FAZIT

Die AmdoSoft/b4 Robotic Process Automation Lösung ist eine abgesicherte Plattform, welche durch clevere Unternehmensstrukturen und gezielten Einsatz einen klaren Mehrgewinn für die Produktivität und Effizienz zukunftsorientierter Unternehmen darstellt. Monotone, wiederkehrende Prozesse zu automatisieren und somit Mitarbeitern mehr Zeit verschaffen sich auf wichtigere, kreativere Aufgaben zu fokussieren. Wir möchten auch Ihnen dabei helfen, mit Sicherheit in der Automatisierung, als auch der Sicherheit durch Zuverlässigkeit, Skalierbarkeit und Benutzer-freundlichkeit im Umgang mit der b4-Plattform.

Für weitere Informationen zu AmdoSoft Systems GmbH und unseren Services gehen Sie bitte auf www.amdosoft.com.

Our Business
is
to Automate
your
Business Processes