An Enhanced Security Framework for Robotic Process Automation

K. Murugappan and T. Sree Kala

Abstract Robotic process automation (RPA) is an emerging field in any industry that takes care of automation of the monotonous jobs. This can help to optimize the resources utilization for the organization, save the cost, time and improve the accuracy and quality of the jobs performed. However, lack of security in the implementation and the management of these RPAs shall affect the business in an adverse way. In the current scenario, privacy has also taken important role, and allowing bots (RPA) to have an access to these privacy applications can lead to regulatory compliance issues and invite heavy penalty to the company, and at certain times, it may result in business shutdown. Hence, in this paper, we explored various security risks associated with the bots automation and provided a proposal to build a holistic security framework for the RPA environment.

Keywords Robotic process automation · Bots · Noncompliance · Regulatory · Policy compliance

1 Introduction

Robotic process automation (RPA) is a software program that imitates human actions when interacting with a computer systems application and accomplishing automation of repetitive, conditional-based processes. This shall be called as a software robot or a bot. These bots also can leverage artificial intelligence and machine learning technologies to improve the experience of organization workforce and customers. While doing so, the bots may have an access to the organization's critical applications and that can be misused by the unauthorized users. Also, mis-configuration and lack of management controls can result in security breaches, data leakage and financial impacts. To counter these potential risks, there is no single end-to-end comprehensive framework available in the IT industry. Since this RPA solution is being embraced by organizations around the world to carry out

K. Murugappan (✉) · T. Sree Kala
VISTAS, Chennai, India

K. Khanna et al. (eds.), *Cyber Security and Digital Forensics*,
Lecture Notes on Data Engineering and Communications Technologies 73,
https://doi.org/10.1007/978-981-16-3961-6_20

crucial processes across multiple business functions, this paper would help in providing an insight to those security risks and provide a framework to safeguard the organization and its customer assets.

2 Problem Identification

When RPA is interacting with multiple applications (in-house or off-the-shelf), it increases the attack surface. Other problems are manual override of the bot set-up, unauthorized changes, software licence misuses where generic ID is used, weak credentials storage, security incident response is not aligned or designed to cope up with the bot's speed and volume of transaction, no accountability established for the bots used in the network, regulatory noncompliance, a corrupt bot can access sensitive data and move laterally in the network or destroy high value information, security breach can result to disclosure of sensitive information to external parties, a rogue robot can create security vulnerabilities for data at rest or in motion, and Service denials.

3 Proposed Solution

As per a 2018 report by Ernst and Young for RPA implementations, organizations should consider the technical, process and people elements of the entire robotics ecosystem. A secure implementation should be in accordance with the entire product lifecycle starting from requirements, architecture to the ongoing operations. This is well captured in the below sections.

3.1 Security Framework—Key Pillars

In Fig. 1, key pillars for building a security framework are provided. This shall be tailored as per the organization's requirement.

Governance: The organization should ensure a governance framework which will build strategy and security requirements from an RPA perspective. This shall explain the management support and its commitment to ensure the data security [1].

Risk Management: Any risks that shall obstruct the RPA objective of the business have to be mitigated based on the priority.

Product and Software Security: Organizations should perform a product architecture risk assessment both internally and externally.

Access Management: Role-based access control is one of the most crucial features to keep in mind while opting for an RPA solution [2]. A credential

Fig. 1 Security framework

management process must be put in place for the bots to store credentials in a vault and access it as and when needed as per assigned privilege.

Change and Release Management: Any changes to the RPA systems and applications are authorized and implemented accordingly to avoid unauthorized or unnecessary downtime or security breaches.

Configuration Management: All deployed configurations are backed up and version controlled to ensure the timely recovery in case of any operational failure or application or hardware issues [3].

Incident and Problem Management: Focus on any operational and security incident to be addressed and avoid any repeated issues.

Business Continuity Planning (BCP) and Resilience: This will support the business resumption in case of a disaster.

Key Risk Indicators (KRI): This will support the RPA business to take a quick proactive action and avoid any significant impact to the business.

Audit and Compliance: The organization must conduct regular audits to ensure that the bots are compliant to all industry regulations in order to avoid hefty fines and a tarnished brand image.

3.2 Process Flow

Figure 2 provides the process flow of the bot establishment in a network that starts from *initiate* step [4]. In this step, the requestor, usually from the business, raises a request, and it is validated by the respective business subject matter expert (SME) for the business value added. Based on the positive outcome of this qualifying activity, the resource planning will kick start. Once the planning is done, the required resources (people, process, technology, location, schedule, cost and quality) will be determined and allocated to the project, and build phase will begin.

During this phase, the actual bot package will be developed, and then, it moves into testing phase. In this phase, test strategy and test cases are tested. If the test results are satisfied, final package would be deployed into the production. After deployment, this is managed for maintenance purposes and minor bug fix or enhancements. Finally, the bot can be terminated after the end of life or once the business objective is achieved.

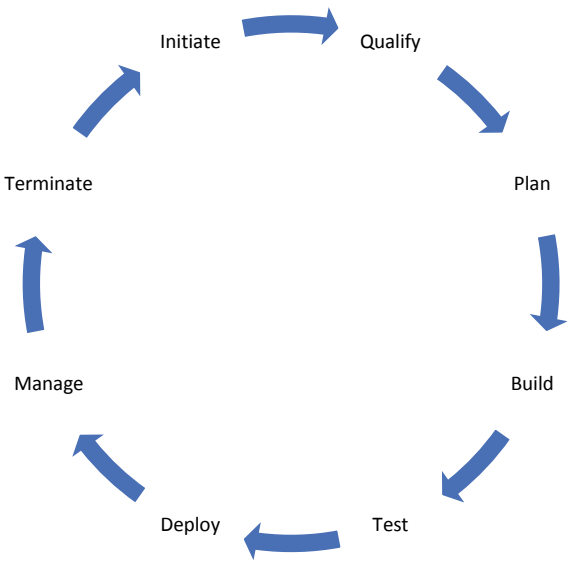

Fig. 2 Process flow of the proposed work

4 Control Requirements in Each Phase

The control requirements in each phase are listed below. The audit and compliance are applicable for every phase.

Phase	Includes	Control requirement
Initiate	Request creation is restricted to authorized users/limited users only	• Limit the request creation based on job role
Qualify	Requirement is captured or understood clearly from the business	• Risk management • RPA vendor or platform selection • Business and security requirement sign-off
Plan	Proper planning for development estimate, detailed process breakdown, value stream map and estimated savings	• Policy adherence • Return on investment is calculated and accounted for every resource • Project/change request is created
Build	• Code/script development • Bot ID creation request • FTE redeployment • Communication and escalation • Package creation • Version control • Bot reuse • Best practices establishment	• Secure coding or vendor recommended security practices are followed
Test	• Unit test • System integration test (SIT) • Quality assessment test (QAT) • User acceptance test (UAT) • Business sign-off	• Every test case is tested • All significant and high rated errors are fixed • Positive and negative tests conducted • Functional and non-functional tests are performed
Deploy	• Infra requirements (virtual machine/ physical system) • Bot installation and configuration • Code deployment to production • License request and management • ID creation in authentication servers, applications and e-mail systems • Bot console management • Scheduling • SMOKE test • Saving confirmation • Handover to operation • Project closure	• Dedicated deployment team • Deployment team not to have an access to development and testing environment • Release ticket is created • Version control/configuration management
Manage	• User access management • Communication plan • Upgrades (operating system, applications and databases) • Change request (functional /technical)	• Unique account for every bot (attended and unattended) • Log monitoring • Bot task monitoring and traceability • Segregation of duties (SOD)

(continued)

(continued)

Phase	Includes	Control requirement
	• Hot fix • Patch management (OS, applications) • Issue management • Monitoring • Logs management • Backup and archival • Bot inventory and its mapped applications	• Privileged account management • No direct write access to the database • Strong passwords • Least privilege and need to know basis access management • Periodic vulnerability assessment • Penetration test performed at least once in a year or whenever significant change in the environment • Software and bot license management • Regulatory compliance • KRI is established and monitored • Periodic backup • Periodic restoration test • BCP/DR • Security incident and problem management
Terminate	Bot decommissioning	• Periodic bot reconciliation and review process established • Unnecessary or unwanted bots de-commissioned

5 Technical Security Requirements

Data Flow: End-to-end data flow is identified for the bot, and blueprint is created with upstream and downstream applications or interfaces [5].

Data Flow Security: In each stage of the bot, data flow security is ensured. This shall include and not be limited to access control and encryption for achieving confidentiality, hashing for achieving data integrity and backup and recovery control for achieving availability [6].

Encryption: Minimum encryption shall be AES 256 and can be used in data at rest, data in transit and processing stages. The hashing algorithm shall be MD5 or SSH latest version.

Audit Trail: Every activity of the bot is logged and tracked with timestamps [7].

Passwords: Strong passwords for the bots and secured with password/credential vault.

Single Sign-On: Centralized authentication is enabled, and no local authentication is recommended.

Alert Management: In case of security breach, an alert is trigged to the concerned stakeholders/security administrator.

Vulnerability Management: Periodic vulnerability scanning and Threat modelling exercises are established to identify technical vulnerabilities and process gaps.

Security Testing: Identify bot security vulnerabilities by performing static and dynamic testing.

Penetration Testing: If any of the bots is exposed to Internet, then penetration testing is mandatory.

Remote Control: All remote console accesses are to be safeguarded with two-factor authentication.

Security by Design: It is better to ensure the security in each stage of the bot development instead of trying to fix gaps at the later stages.

Accountability: Every bot needs to have unique ID and mapped to a business owner so that accountability is established.

Sensitive Data: Sensitive data are to be wiped out before reassigning the bot to any other business.

Regulatory and Policy Compliance: Every Bot needs to be in compliance with the organization policy, standards and regulatory requirements. For example, Sarbanes–Oxley Act (SOX) and Health Insurance Portability and Accountability Act (HIPAA).

PKI Solution: Public key infrastructure shall be used to secure the bot communication process.

6 Comparative Analysis

In the current industry, there are many commercial RPA platforms available, every player has their own way of developing, implementing and managing the RPA, and this might lead to a platform dependent security and inconsistency in following the security measures when the organization wants to implement the RPA with multiple vendors. This paper provides the comprehensive and holistic approach in implementing the RPA security framework, and consistency shall be maintained across the organization even if multivendor environment exists.

7 Conclusion

The need for RPA is increasing and proliferating in every industry; however, implementing the RPA should not impact the existing systems and services in the adverse way. To strikeout the balance, we need to really consider security versus stability. In this paper, the key pillars, process flow and control requirements are discussed for each phase of the bot lifecycle, and these can help to establish the strong security framework for the organization when implementing the RPA solution.

References

1. Deborah, G.: Robotic Process Automation (RPA) Within Federal Identity Management (2019). https://www2.deloitte.com/content/dam/Deloitte/us/Documents/public-sector/us-gps-robotic-process-automation.pdf. Accessed, 1 March 2021
2. Gautam, R.: 4 Security Must-Haves for a Safe RPA Solution (2020). https://www.automationanywhere.com/company/blog/product-insights/four-security-must-haves-for-a-safe-rpa-solution. Accessed, 1 March 2021
3. CemDilmegani.: Technical Buyer's 11 Point RPA Checklist: In-Depth Guide (2021). https://research.aimultiple.com/rpa-technology. Accessed, 1 March 2021
4. UIPATH Best Practices for IT Compliant RPA Implementation (2021). https://www.uipath.com/resources/automation-whitepapers/information-technology-compliant-rpa-implementation . Accessed, 1 March 2021
5. Enríquez, J.G., Jiménez-Ramírez, A., Domínguez-Mayo, F.J., García-García, J.A.: Robotic process automation: a scientific and industrial systematic mapping study. IEEE Access **8**, 39113–39129 (2020). https://doi.org/10.1109/ACCESS.2020.2974934
6. Lewin, A.R.W., Edwards, P.P.: Open-Source Robotics and Process Control Cookbook, USA, pp. 222–225 (2005)
7. Sumit, S.: RPA Implementation: Key Considerations (2018). https://www.pwc.in/assets/pdfs/publications/2018/rpa-implementation-key-considerations.pdf. Accessed, 1 March 2021