The RPA Security Checklist and Best Practices

No comments

RPA (Robot Process Automation) is a software technology that makes it easy to build, deploy, and manage software robots that mimic human actions when interacting with digital systems and software. A secure RPA infrastructure is critical for businesses and IT departments. Considering RPA functions as people do, every enterprise application, including CRM and ERP, and the confidential customer and personal information inside those applications is at risk. RPA is secure. Security incidents can cost a lot. A special identity should be assigned to each RPA bot and process. Furthermore, you should implement password and username authentication along with two-factor authentication.

Introduction to RPA Security

Among the industries that use robotic process automation are small-to-medium-sized healthcare companies and global financial services corporations. It necessarily deals with a lot of confidential business data. Software robots automate daily business tasks such as transferring files, processing orders, and conducting payroll by processing information

from numerous company databases and logging into different accounts using provided credentials. By using this approach, an automation platform has access to the information of employees, customers, and vendors (inventory lists, passwords, etc.).

Credentials for robotic process automation are often exchanged so that they may be reused. Since these accounts and credentials are left unmodified and unsecured, cyber attackers can use them to escalate privileges and gain access to critical data, applications, and systems. As a result of many businesses using it having many bots in production at any given time, administrators can extract credentials from vulnerable sites. The risk, therefore, is very high.

RPA Security Checklist

1- It is recommended to store all sensitive data in a secure database and encrypt it.

It includes passwords, employee names, financial information, etc. Sensitive data should be protected both at rest and in transit. All RPA systems should undergo malware scanning on a regular basis. The scanning should be performed by a reputable third-party service. Also, ensure to detect and remove any malicious code quickly. User management rules should control all accesses to the RPA system to ensure that only authorized users interact with the system. Authenticate all users with administrative privileges by two-factor authentication (2FA). 2FA is an additional verification level for users trying to access the system. 2FA can include smart cards, text messages with security codes, or biometrics.

2- Review service accounts' access periodically.

Remove any unnecessary service accounts from the system. Service accounts are a security risk if they access the RPA system. It is essential to review and adjust user permissions regularly. You can do so through a change management process. Do not store sensitive data in the RPA system unless it is necessary. Storing sensitive data in an RPA system increases the risk of a security incident. If someone gains access to this information, it can potentially cause a lot of damage to your organization's reputation and revenue. For example, if someone steals a credit card number, it could result in millions of dollars in fraudulent charges.

3- Conduct compliance assessments while segregating the network.

This will also ensure that the RPA system is not a part of the enterprise network. Conduct a penetration test to identify any potential security vulnerabilities. Also, you can conduct penetration tests by a third party or internal security teams. Also, ensure the RPA team has access to this information and knows what to do during a security incident.

4- Manage bot credentials with a centralized, encrypted vault.

To secure the RPA environment, make sure to use an RPA security checklist to ensure that credentials, such as

usernames and passwords, do not reside in the RPA system storage. In this way, you will reduce your risk of a security breach.

Best Practices for Security Automation

RPA The RPA Security Checklist and Best Practices

In addition to this checklist, here are some additional best practices for ensuring the security of your RPA system:

1. Use a secure authentication protocol for bots.

2. Create a password vault for all your organization's bot credentials, and ensure they are encrypted.

3. Be careful not to use the same credentials across two bots.

4. Remove sensitive credentials from a bot after removing them from production.

5. Use 2FA for administrative accounts to add an extra layer of security to your RPA infrastructure.

6. Make sure only those users needing access to sensitive information have it and adjust permissions periodically to ensure they still have it.

RPA Security Risks

The following are the security risks associated with RPA:

Disclosure of Confidential information

An organization's business and operations are confidential if they are not publicly available and have commercial value. Unauthorised disclosure of a company's financials, marketing plans, planned initiatives, or other private materials could be detrimental.

System limitations

Due to security issues in an information system, cyber-attacks could perform incorrect operations and gain unauthorised access. Several vulnerabilities can appear when a staff member visits a hazardous website. One is that the webpage in this scenario is a threat resource that causes vulnerabilities. Here are a few examples:

An authorisation is missing

There is no encryption of data

Security issues with passwords

SQL injection

Uploading infected software

Any organization's internal systems and databases are referred to as internal systems and databases, often associated with privileged accounts or accounts with more access to data. Examples are IT team members' accounts (e.g., local administrator roles) or employees who work with sensitive data, such as finance managers' accounts. Security risks associated with its bots abusing privileged access are essentially the same as those related to human abuse of privileged access. Consider the following example:

An attacker could exploit privileged access granted to Robotic process automation bot accounts to steal or misuse your critical business information.

Attackers can program a bot to disrupt critical corporate activities such as client and order processing.

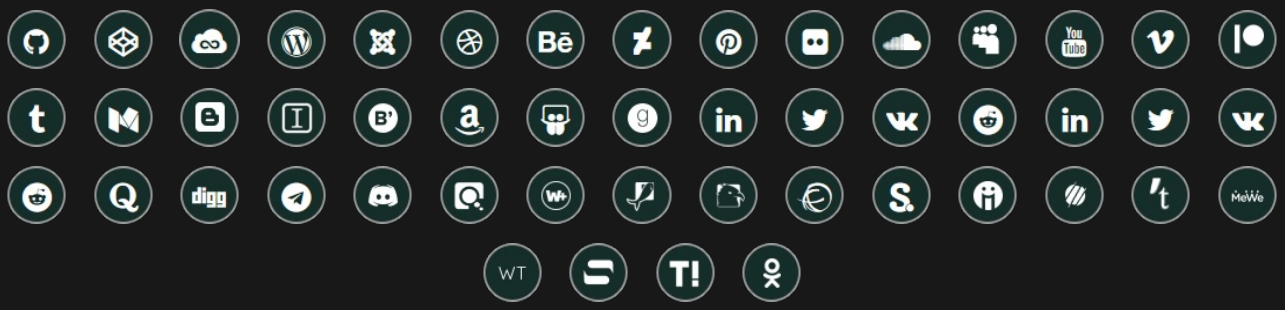
Conclusion

Implementing RPA correctly and carefully will prevent security concerns and data misuse. If its bots aren't monitored regularly, they may fail to produce correct results and errors. Security measures should be implemented because the bot may be accessing sensitive data. For security purposes, logs need to be added, password vaults need to be set up, and proper frameworks need to be set up. These methods allow IT bots to be enhanced, their performance can be improved, and business risk can be reduced.

Join Arashtad Community

Follow Arashtad on Social Media

We provide variety of content, products, services, tools, tutorials, etc. Each social profile according to its features and purpose can cover only one or few parts of our updates. We can not upload our videos on SoundCloud or provide our eBooks on Youtube. So, for not missing any high quality original content that we provide on various social networks, make sure you follow us on as many social networks as you're active in. You can find out Arashtad's profiles on different social media services.



Get Even Closer!

Did you know that only one universal Arashtad account makes you able to log into all Arashtad network at once? Creating an Arashtad account is free. Why not to try it? Also, we have regular updates on our newsletter and feed entries. Use all these benefitial free features to get more involved with the community and enjoy the many products, services, tools, tutorials, etc. that we provide frequently.

SIGN UP | NEWSLETTER | RSS FEED