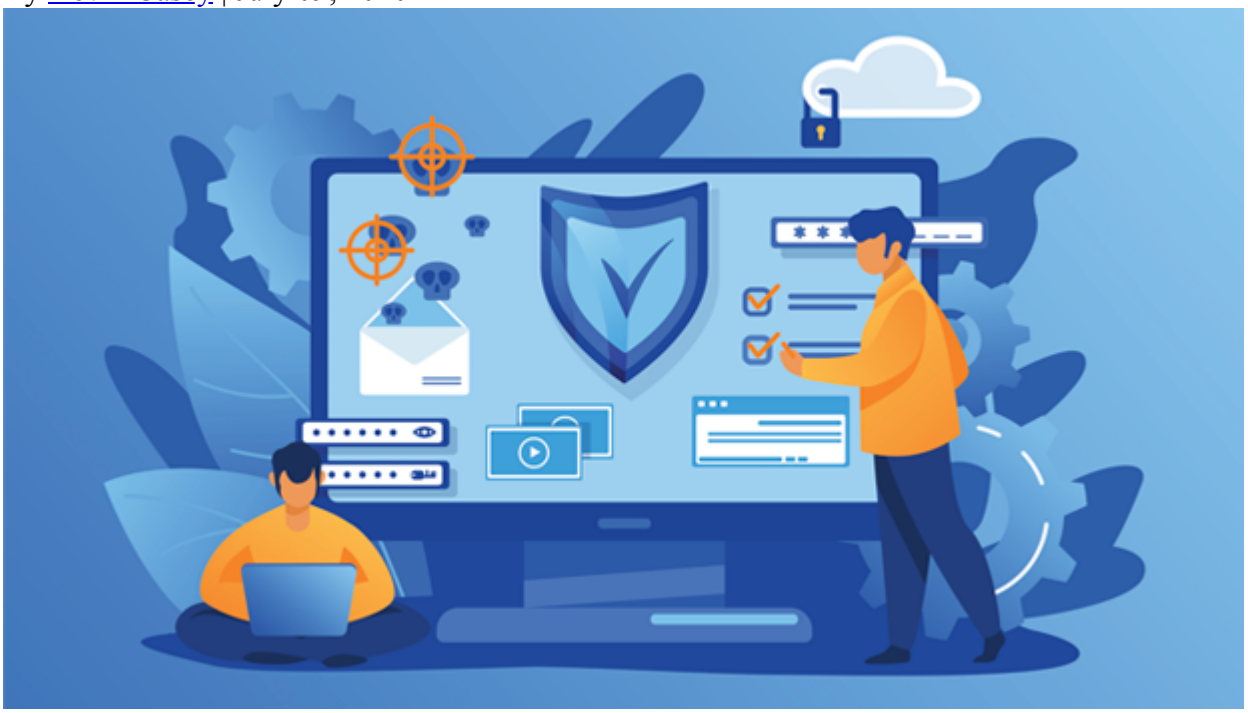
Robotic Process Automation (RPA): What you need to know about security

Robotic Process Automation (RPA): What you need to know about security

Just because you automate a process doesn’t mean you’ve secured it. If you're considering RPA, make sure you understand the security implications

12 readers like this

By Kevin Casey | July 09, 2020



There are myriad success factors to consider when implementing Robotic Process Automation (RPA). Conversely, there are some key lessons to learn early if you want to minimize problems with your RPA program over time.

One of these should ring familiar to any IT pro: You can't ignore security.

Just because you automate a process doesn't mean you've secured it. Moreover, RPA bots – the software that performs various computer-based tasks that would otherwise require human effort – come with some of the same risks as a person working with their laptop. Mistakes happen.

In fact, that's the fundamental reminder here: RPA is ultimately just another kind of software, so of course there's potential for security vulnerabilities if you're not alert.

"RPA bots, as with any software, can pose security risks as an attack surface if the proper procedures and setup are not incorporated," says Gautam Roy, head of product security at Automation Anywhere.

[Need straightforward definitions of RPA? Read: How to explain Robotic Process Automation (RPA) in plain English]

Where do RPA security risks start?

This speaks to one of the overarching things to understand about RPA security: Many of the risks arise from a lack of care or oversight. A completely ad hoc approach to introducing bots into an organizational process or system is more likely to cause issues than a strategic program. And an overall lack of security hygiene in an organization is not going to be saved by RPA.

An overall lack of security hygiene in an organization is not going to be saved by RPA

This is all good news for teams that already take security seriously, and another nudge for those that don't. Is password hygiene or access management already a mess in your company? That's still going to be a

problem when you automate certain tasks with RPA, for example.

"RPA bots, like humans, utilize privileged access to perform their tasks, including connecting into ERP, CRM, or other platforms – while moving data across systems from one process to the next," Roy says.

While we tend to attribute a lot of security risks to the human element – it's the reason why phishing scams are so effective, for instance – it's important to realize that moving a task to a software bot doesn't magically prevent human error. Someone still has to implement and manage that bot.

What are the main RPA risks?

Most RPA security issues can be viewed through one of two overlapping lenses: Compliance risk and operational risk, according to Chris Huff, chief strategy officer at Kofax.

"Compliance risks typically involve poor RPA governance created by implementation methods bypassing established software development lifecycle best practices addressing network security, data privacy, and enterprise architecture," Huff says. "Operational risks include regulatory preparedness intended to establish guardrails and day-to-day controls supporting scalability and business continuity."

One of the broad appeals of RPA is that modern tools offer so-called low-code or no-code paths to implementation. While you can write your own RPA bots from scratch, there are plenty of commercial and open source tools that can help you get started with minimal development effort. Many of these tools have invested in drag-and-drop interfaces or turnkey options to appeal to non-technical users, such as finance or human resources pros. As a result, it's very possible for a team or department in your organization to launch a bot without help from IT – or without even letting IT know they're doing it.

[Related read: Robotic Process Automation (RPA): 6 open source tools]

That might sound like a good thing in companies where IT teams are already stretched to the max. But cut out the CIO at your own peril: Not partnering at all on your RPA project will probably cause long-term issues, including unnecessary or invisible security risks. You can have your cake and eat it, too, provided you take a collaborative approach.

Some RPA security risks persist because the person or team implementing RPA has no idea those risks existed in the first place.

"The root cause of compliance and operational risk is when organizations take a fragmented approach to launching automation programs," Huff says. "IT and business leaders must collaborate to effectively choose the right RPA solution and to further design and operate a Digital Management Office (aka Center of Excellence) that can support a model whereby IT addresses network, data, and regulatory concerns while the business focuses on identifying where to apply RPA, contributing to the design and development through citizen developer skills, and maintaining day-to-day operations sustaining deployed RPA bots."

Consider it another chapter in the shadow IT story: Some RPA security risks persist because the person or team implementing RPA has no idea those risks existed in the first place. Cross-functional partnership can mitigate that problem while still allowing, as Huff notes, teams to reap the benefits of low-code or no-code tools.

Prioritizing security in RPA tool selection

Speaking of tools, security needs to be part of the evaluation and selection criteria. This is one of the key ways in which IT can help while not tamping down the promise of that citizen developer approach Huff mentions above.

"When considering RPA solutions, it's critical to choose one that has a strong company commitment to making its solution safe and reliable," Roy says. "During this vetting process, it is important to consider looking for vendors with key safety features including multi-factor authentication, strong access control, encryption, and application security – while practicing good security hygiene related to sharing RPA login credentials and updating passwords consistently.

Remember, too, that RPA on its own is not particularly intelligent or adaptable. Some security and reliability issues get introduced because of changes made elsewhere.

"Most environments are complex and involve daily changes including application fixes, security updates, process changes, etc.," Huff says.

"RPA security" is as much about ensuring that your existing programs and processes properly account for RPA bots

Adjacent or complementary technologies such as process orchestration and process mining can help; this is also another reason why cross-functional partnership (epitomized by the Digital Management Office or Center of Excellence approach) matters.

Tom Thaler, director of product management for ARIS at Software AG, shares this scenario: Imagine an organization has deployed multiple RPA bots to perform repetitive tasks with its ERP system.

"Let's say the ERP system needs to be updated for security reasons or to ensure compliance with new regulations," Thaler says. "Often, the impact of the update, especially at the interface level, is unpredictable because IT doesn't know which robots are potentially affected – the robots stop working. A very stressful situation arises where fixing is required and critical processes can't be executed in the desired way."

Considered in this light, "RPA security" is as much about ensuring that your existing programs and processes properly account for RPA bots. *If we change X,* for example, *we also need to update Y.* Otherwise, you're going to break stuff, to put it plainly.

Make security core to your RPA strategy

This can be a downside of automation in general: It sounds like it will solve all your problems, well, automatically. While including security as part of your RPA vendor evaluation criteria is important, remember that – just as with other technologies – you're not completely offloading your risks by doing so.

Related content

- When automation meets security: Best practices
- 8 Robotic Process Automation (RPA) training and certification courses
- How to explain Robotic Process Automation (RPA) in plain English

Extending and applying other enterprise software security best practices to RPA is a great place to start, Roy says. Security is also as much a matter of organizational culture as it is a matter of technology – or at least it should be. Again, this is good news for security-centric teams when it comes to RPA adoption. If you care about security, you're more likely to take smart steps toward managing risks – and those will inherently help with RPA security. If you ignore security or treat it as an annoyance or afterthought, you're likely leaving yourself more vulnerable to incidents or attacks – and that will add unnecessary risk to your RPA program, too.

"As with other security best practices, those driving automation efforts must instill a culture of privacy protection and risk mitigation for their automation teams – from top to bottom," Roy says.