

Robots Not in Disguise

Emyr Thomas shines a light on the burgeoning use of Robotic Process Automation. While security challenges abound, he explains why the integrity of processes and continued availability are increasingly important.

I've just returned from paternity leave. Note to self – buy more coffee.

Although not my first, I'd forgotten what it's like to cradle a slumbering new born baby while you sit paralysed with fear that any small movement can shatter the (temporary) idyll.

The need for silence in these circumstances rendered normal television viewing impossible. It did, however, allow me to re-watch some movies from the silent era, including one of my favourites, Modern Times. It's the one set in the Great Depression where Charlie Chaplin plays a luckless factory worker – its most famous sequence is when he falls behind on a production line and ends up getting stuck within a machine.

Now, obviously this is a movie – one of the last before "talkies" took over Hollywood – but its themes still resonate. Particularly around the challenges of adapting to a modern, industrialised world.

In Robotic Process Automation, security challenges abound and the integrity of processes and continued availability are increasingly important.

The times they are (still) a-changin'

Today's organisations, like those of the past, continue to be built on structured processes, many of which are highly repetitive and labour intensive. That partly explains the allure of modern technology – it's a way of freeing up the intellectual capacity of employees previously locked in bureaucracy while also delivering huge efficiency and productivity gains.

Take Robotic Process Automation (RPA). This type of hyper-automation technology can help free-up employees, allowing them to deliver more valuable outcomes rather than constrain their time running through recurring administrative effort.

A combination of software tools that automate human tasks based on pre-programmed and rule-based activities, RPA can interact with in-house applications, websites and user portals to log in to applications, enter data, open emails and attachments, calculate and complete tasks and then log out – executing processes just like a human.

Organisations are increasingly adopting RPA but it's by no means straightforward. Not only do they have to reassure employees that this technology is not going to steal their jobs, but they also need to adapt to a new set of threats and risks that differ from those affecting traditional human users, and this requires security teams to think differently about their security posture and controls frameworks.

It's also important to remember that, as with any software development, the skills of the developers may not be located in country. Offshored supply chain threats will therefore exist and will need to be controlled appropriately, especially where sensitive data or critical processes are being automated.

This means that early development should be based upon representative test environments with masked data sets. Access to production environments should be tightly controlled, and limited to individuals with enhanced monitoring enabled. Development teams can scale and change quickly, so account management processing will need to be responsive to needs to ensure joiners, movers and leavers are continuously managed.

This is also true when it comes to support functions, where third party suppliers require second or third line investigation into an event or incident, the support engineer may require access to the running process to supervise the bot's actions. Having robust, auditable processes that can be tied to service tickets will mitigate against rogue engineers attempting to exfiltrate data.

But it's not just the security risks which are looming large. The integrity of processes and continued availability should not be neglected.

Organisations adopting RPA will want to think about the following controls:



Develop using representative test environments



Conduct supply chain assurance



Tightening application filtering controls



Rigorous data and process validation



Resilience planning

Re-thinking best practice

RPA is often deployed in areas where confidentiality risks have been most dominant and so controls to manage privacy and confidentiality requirements are generally mature. Organisations will need to review these controls tuned for human users. Robots have different characteristics and therefore, vulnerabilities to humans. For example, multi factor authentication becomes tricky when robots do not have an assigned personal device or token. Robots are generally far better at remembering long and complex strings, unlike humans, meaning compensation can be made through increased password complexity levels and frequency of password changes.

Refinement can also be made to controls such as application filtering, to limit the attack surface of a compromised bot. Robots do not (yet) have social needs, so collaboration tools like Instant Messaging can be restricted, and other business applications for HR and wellbeing could also be removed. Web access can be denied or further limited to only authorised sites that are necessary to execute the process, since they will not be taking lunch breaks and catching up on the latest sport results.

“Robotic Process Automation is often deployed in areas where confidentiality risks have been most dominant and so controls to manage privacy and confidentiality requirements are generally mature. Organisations will need to review these controls tuned for human users.”

Prioritising integrity and availability

As the business shifts responsibility from humans to machines and becomes increasingly dependent upon technology for its business processes, it will need to consider maturing the controls that manage integrity and availability in equal measure.

Robots diligently follow pre-programmed rules without any deviation. Unlike humans, they are not susceptible to enticement or luring to click on links that they were not expecting. Any unexpected event is likely to be ignored or handled by an exception. Attackers are likely to adapt their attack style away from phishing and to other process manipulation technique.

We may see an attacker look to spoof email addresses, IP addresses, and input malformed data to deceive the bot to process data incorrectly. Attacks such as SQL injections, Cross-Site Request Forgery (CSRF), watering-hole attacks and Distributed Denial of Service (DDoS) are likely to be the most common techniques adopted by attackers.

Data and process validation is critical to achieve integrity, especially as use cases become more complex and interlinked. The impact of any hardcoded process errors will increase with pace of processing and less observation from humans.

This is especially the case when untrusted data sets are used, such as those received from outside sources like email – which is a key method used by attackers to subvert automated processes. Organisations therefore need to deploy input validation techniques, as well as tightening up filtering to RPA machines which will prevent re-direction to malicious websites.

As the business and its customers becomes increasingly dependent upon automated processes, service availability will also become a fast-rising priority. With backup and restore controls in order to recover from failures and incidents vital, organisations need to double check that restoration procedures are documented, up to date and are available during emergencies.

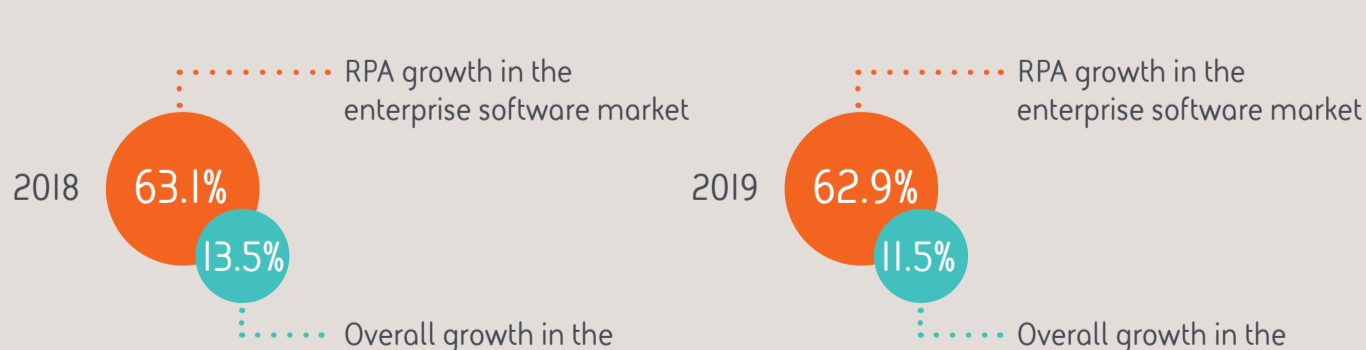
And finally, organisations need to be aware that increasing business and consumer demand will strain technology resources. In order to maintain service availability, resource demand will need to be estimated, continually monitored and technical controls implemented to allow successful scalability of services.

Buckle up

RPA is one of the fastest-growing segments in the enterprise software market – it grew 63.1% in 2018 and 62.9% in 2019, compared with the 13.5% and 11.5% growth, respectively, of the overall enterprise software market.


Such numbers are a testament to its accelerating popularity, and clearly this technology is only going to take even further root. But equally organisations also need to take the time to ensure the necessary safeguards are in place to maximise its full potential.

Baby steps, in other words. How apt.



About the author

Emyr Thomas is a Lead Consultant for Operational Technology Security at BAE Systems Applied Intelligence

 emyr.thomas@baesystems.com