How to Build Stronger IT Security through Automation

Code playbooks automate security configuration and update processes for consistency, efficiency and timeliness.

IT security is a race to protect systems and data before they are affected by the latest cyber threats. Software patches and configuration checks provide vital protections, but it can be difficult for IT teams to keep up. One reason: The growing use of Internet of Things (IoT) devices and digital government processes mean there are more devices to monitor, more software to update and more connections to protect.

"The number of things we have to modify to keep them secure is forever increasing and that's becoming more of a challenge for government," says Otto Doll, senior fellow for the Center for Digital Government (CDG) and former CIO for Minneapolis, Minn.

This paper examines how government agencies can leverage automation to enable a more effective and proactive security strategy.

CRITICAL SECURITY DETAILS

Maintaining IT system security requires attention to a complex and interconnected set of features and configuration settings. Getting one detail wrong on one application or device can have significant ramifications.

This level of security management is critical for on-premises systems, but what about applications, servers and storage systems in the cloud? Although the cloud provider has primary responsibility for security, the agency IT team still needs to verify the provider's controls are adequate and consistent with security measures for on-premises systems.

Routine security management involves many repetitive tasks which often must be completed within a short time frame. To automate these tasks (at least partially), IT teams have traditionally used homegrown scripts. But scripts have multiple drawbacks. A script is typically written for a specific system and not in a standardized form that allows it to be adapted for other needs; there is often not a single place to store, find and share scripts, which can lead to duplicate or conflicting efforts; and the script developer is often the only person who fully understands what it does and how to maintain it.

Proprietary vendor tools are another solution to automate security management tasks, although they also have limitations. They focus only on a specific system or infrastructure, so the agency must rely on the vendor for updates and the tools may not easily extend to the cloud.

Additionally, scripts and proprietary vendor tools cannot fully capture and leverage employee knowledge, especially about older systems. This knowledge gap is an ongoing concern as employees retire or take other job opportunities. Government IT teams need an easy, consistent and effective way to document and share internal expertise.

A NEW APPROACH: THE SECURITY AUTOMATION PLAYBOOK

The automation playbook has emerged as a new approach to security management tasks.

A playbook contains standardized software code that performs a specific configuration or update task in a way that is automated, repeatable and verifiable. Playbooks typically contain simple, clear code, so they are easier to apply, control and maintain than scripts. This simplicity also makes playbooks easier to adopt by other developers or IT operations staff, which reduces duplication of effort and supports IT task consistency.

"The goal should be to reduce the potential for human error and deliver a consistent level of IT service while getting the most out of the infrastructure you have so you can maximize your ROI," says Chris Reynolds, senior cloud architect at Red Hat.

Unlike scripts, an agency doesn't necessarily need to write its own playbooks. Standard playbooks for common tasks are available through the open Ansible community (see sidebar to the left) or in commercial versions. State and local governments

ABOUT RED HAT ANSIBLE AUTOMATION

Red Hat® Ansible® Automation is a simple-to-use IT automation engine that transforms the repetitive, inefficient tasks of software release cycles into predictable, scalable and simple processes. Red Hat® Ansible® Automation automates cloud provisioning, application deployment, configuration management and service orchestration to let developers spend more time on their work and help operations more easily support deployment pipelines. Together, these capabilities create a quick, comprehensive and coordinated approach to delivering business value.

With the average cost of a breach now hovering around **$4 MILLION,** government agencies must do more to protect their networks, endpoints and critical infrastructure.

can benefit from the expertise embedded in standard playbooks, such as compliance requirements.

MAKING THE TRANSITION TO PLAYBOOK AUTOMATION

Automation is now an expectation for all IT activity, especially among employees who have experienced the fast, automated provisioning of cloud resources. Yet to be successful, automation is best adopted gradually.

Start by looking for security management scripts that are easy to convert to playbooks. A good candidate might be a script that installs and runs software updates on a particular device. This strategy provides a way to verify the playbook code performs as expected and provides the reassurance of using the script if a fallback is needed.

Replacing security management scripts with automation playbooks involves a culture change. This change will become easier when employees gain experience developing and using playbooks and see improvements and time savings.

“Culture change happens when people realize how much time it can free up for higher-value projects,” says Reynolds.

As organizational confidence builds, IT can extend playbook automation to more processes and systems. The goal is to automate as many routine security monitoring and management tasks as possible to improve security measures and free IT employees to focus on higher-level work.

BUILDING ON STRENGTHS

Eighty percent of all cyberattacks are due to poor proactive security measures. With the average cost of a breach now hovering around $4 million, government agencies must do more to protect their networks, endpoints and critical infrastructure.

“It’s important to have flexible security processes,” says Morgan Wright, senior fellow for CDG and former senior advisor in the U.S. State Department Antiterrorism Assistance Program. “You have to be adaptable because skills are changing all the time and the threats are changing as well.”

Playbook automation can enable agencies to use staff resources more effectively, save time, standardize efforts, maintain consistency and take advantage of the collective wisdom in a broad security community.

STAYING AHEAD IN THE SECURITY RACE

Many common security management tasks can benefit from automation, including:

- Configuring a large set of new network switches with a consistent security baseline
- Installing a monthly software update within an overnight maintenance time frame
- Performing routine configuration compliance checks or system penetration testing to identify potential security gaps
- Monitoring server and application logs and automating responses to detected events
- Collecting system evidence related to security incidents
- Applying updated security policies across multiple devices
- Identifying which systems are running the OS version targeted by a threat, then automatically installing the security patch

Government agencies demand performance, transparency, and value — exactly what Red Hat offers. As the standard for Linux in governments worldwide, our cloud, virtualization, storage and platform solutions bring freedom and collaboration to the public sector. Bring the power of open source to your agency.

Learn more at **www.redhat.com/government**